**SECRETARIA DISTRITAL DE SALUD DE BOGOTA**

# PLAN DE CONTINGENCIA DE LA PLATAFORMA DE TIC

**Documento Técnico**
**Versión 5.0**

**Enero 31 del 2015**

## CONTROL DE ACTUALIZACIONES

| FECHA | VER. | HOJAS MOD. | MODIFICACIÓN | ELABORÓ / REVISÓ | APROBO |
|---|---|---|---|---|---|
| 2009.10.30 | 1.0 | | Elaboración de Documento | **Elaboró:** Ing. Marco a: Robayo<br>**Revisó:** Ing. | **SDS:** Ing. Jairo Bahamon |
| 2010.01.30 | 1.1 | Actualización Graficas | | **Elaboró:** Ing. Marco a: Robayo<br>**Revisó:** Ing. Jairo Bahamon | **SDS:** Comité de Seguridad de la Información SDS |
| | | 215-232 | Creación de grafica por cada modulo de recuperación | | |
| | | 234-236 | Adición del resultado y conclusiones la prueba 01 del plan en Noviembre de 2009 | | |
| | | 236-238 | Adición del resultado y conclusiones la prueba 02 del plan en Diciembre de 2009 | | |
| 2010.03.18 | 1.2 | Actualización por evento del aire acondicionado del centro de computo | | **Elaboró:** Ing. Marco a: Robayo<br>**Revisó:** Ing. Jairo Bahamon | **SDS:** Comité de Seguridad de la Información SDS |
| | | 228 | Actualización al procedimiento de recuperación del modulo de Infraestructura física. | | |
| | | 229-231 | Creación de la priorización y semaforización por criticidad de los servidores de la SDS. | | |
| 2010.12.10 | 1.3 | Actualización por evento del aire acondicionado del centro de computo | | **Elaboró:** Ing. Marco a: Robayo<br>**Revisó:** Ing. Jairo Bahamon | **SDS:** Comité de Seguridad de la Información SDS |
| | | 10-16 | Actualización de los datos de las instancias y bases de datos de SQL Server | | |
| | | 83 | Creación de link para acceder a los activos de información de la SDS en matriz de la Comisión Distrital de Sistemas. | | |
| 2011.07.28 | 2.0 | 246-248 | Actualización de la priorización y semaforización por criticidad de | **Elaboró:** Ing. Marco a: Robayo | **SDS:** Comité de Seguridad de la |

| | | | | | |
|---|---|---|---|---|---|
| | | | los servidores de la SDS, aportando más datos de descripción. | **Revisó:** Ing. Jairo Bahamon | Información SDS |
| 2012.11.28 | 3.0 | 11 – 18<br>27<br>32 – 35<br>57 – 63 | Actualización del documento del Plan de Contingencia versión 3.0 de acuerdo a los servicios TIC de la SDS. | **Elaboró:** Ing. John Triana<br><br>**Revisó:** Ing. Jairo Bahamon | **SDS:** Ing. Jairo Bahamon |
| 2014.01.15 | 4.0 | 1, 11-17,19-25, 26 – 29,31-37,39-43,58-63,228-230,232,233,235,236,238,240,241,243,244,248 | Actualización del documento del Plan de Contingencia versión 4.0 de acuerdo a los servicios TIC de la SDS. | **Elaboró:** Ing. Hermes Pérez<br><br>**Revisó:** Ing. John Triana | **SDS:** Ing. John Triana |
| 2015.01.31 | 5.0 | 1, 11-17,19-25, 26 – 29,31-37,39-43,58-63,228-230,232,233,235,236,238,240,241,243,244,248 | Actualización del documento del Plan de Contingencia versión 5.0 de acuerdo a los servicios TIC de la SDS. | **Elaboró:** Ing. Heliodoro Huertas / Jazmín Pintor<br><br>**Revisó:** Ing. John Triana | **SDS:** Ing. Hector Alirio Rojas Borbón |

## TABLA DE CONTENIDO

# INTRODUCCION

La definición de procedimientos de contingencia y recuperación de servicios informáticos, es una herramienta que integrada con una solución adecuada de infraestructura tecnológica, permite a la organización restablecer las operaciones de misión crítica apalancadas en la tecnología y recuperar la capacidad de procesamiento y producción en un marco de tiempo aceptable después que un incidente o desastre que ocasione interrupción al Centro de Cómputo Principal de la organización.

Estos procedimientos deben integrarse con los planes de emergencia previamente documentados por el Comité de Emergencias para ayudar a proteger integralmente a los funcionarios, y a los negocios de la Secretaria de Salud, debido a incidentes y/o eventos catastróficos. Estos procedimientos son complementarios al desarrollo de un plan de Continuidad y Recuperación de Desastres (DRP-BCP).

Estos procedimientos de contingencia y recuperación, establecen las decisiones y acciones gerenciales necesarias para recuperarse de un incidente ocurrido en las plataformas incluidas en el alcance del proyecto.

Este documento aplica específicamente para las instalaciones administrativas de la Secretaria Distrital de Salud en Bogotá D.C., Colombia; tercer piso del edificio administrativo, donde actualmente se encuentra ubicado el Centro de Cómputo Principal. Los procedimientos aplican principalmente a los equipos de recuperación que soportan la infraestructura de tecnología (hardware, software, aplicaciones, comunicaciones, etc.) donde funcionan.

La Dirección de Planeación y Sistemas con el objetivo de soportar la plataforma tecnológica de TIC de la Secretaría Distrital de Salud, ha desarrollado el siguiente enfoque para cumplir con los objetivos del Plan de Contingencia:

- Ejecución de análisis de riesgos y análisis del impacto en la entidad.
- Definición de estrategias y preparación de recursos para minimizar el impacto en el desarrollo de las actividades propias de la razón de ser de la Secretaría Distrital de Salud.
- Prevención por medio de controles y capacitación a sus funcionarios.
- Asignación de responsabilidades y tareas para responder durante y después de la contingencia en una manera controlada.

La Dirección de Tecnologías de la Información y las Comunicaciones-TIC de la Secretaría Distrital de Salud, tiene claro que la protección de los recursos genera continuidad de la organización y respaldo en las operaciones para los empleados, clientes y directivos. Estos recursos incluyen productos, servicios, personal, propiedad física y recursos informáticos. La protección de estos recursos es esencial para el éxito de la prestación del servicio por parte de la Secretaría Distrital de Salud.

La Dirección de Tecnologías de la Información y las Comunicaciones-TIC de la Secretaría Distrital de Salud, ha desarrollado una serie de estrategias para la recuperación de los procesos y servicios críticos de la entidad. Estas estrategias están basadas en varios elementos que incluyen el hardware y software actualmente utilizado por la Secretaría Distrital de Salud, las actividades de prevención y preparación ejecutadas hasta el momento, el análisis de riesgos y el análisis de impacto en la entidad.

- Análisis de Riesgos – Identifica para la Secretaría Distrital de Salud los riesgos potenciales dentro de su ambiente informático

- Análisis del Impacto en la entidad –Identifica los procesos críticos de la entidad y los sistemas de información asociados que provee la Secretaría Distrital de Salud. Este análisis también ayuda establecer los tiempos máximos que puede estar un servicio o proceso sin funcionar antes de que ocurra una perdida (operativa, financiera, imagen, etc.) significativa a la Secretaría Distrital de Salud.

# OBJETIVOS

- Asegurar la continuidad de los procesos que soporta el la plataforma tecnológica de TIC.

- Ofrecer una metodología que describa claramente las acciones a seguir que permitan continuar de manera eficiente y oportuna las operaciones críticas institucionales, minimizando el impacto negativo en la entidad, proveedores y Clientes.

- Prevenir que la Secretaría Distrital de Salud tenga un impacto operacional o financiero de una magnitud que pueda dejar a la entidad en alto Riesgo de funcionamiento.

- Satisfacer las obligaciones con empleados, clientes/usuarios, proveedores y otros socios durante la presentación y recuperación de una contingencia.

- Identificar alternativas de funcionamiento, cubriendo aspectos relacionados con posibles confusiones, omisiones y duplicación de esfuerzos.

- Establecer controles preventivos necesarios para asegurar la permanente disponibilidad de la información.

- Cubrir todos y cada uno de los procesos vitales en la operación de la plataforma tecnológica de TIC y considerar todos los componentes que la soportan.

## 1. ALCANCE

- El proyecto cubrirá las funciones y operaciones de la plataforma tecnológica de TIC dentro de la Secretaría Distrital de Salud, teniendo en cuenta la operatividad del hardware y software crítico.

- El plan de contingencia se orientara principalmente en el centro de cómputo, lugar en donde se concentran los equipos de procesamiento central (servidores, Switches, SAN, VTL, centros de cableado, etc.), que soportan la plataforma de TIC de la SDS.

- El plan se basará en las operaciones críticas detectadas de acuerdo al análisis de riesgos potenciales en la utilización de los sistemas de la entidad.

- La metodología de trabajo utilizada para el desarrollo de este Plan de Contingencias está compuesta por las siguientes etapas:

  - Etapa 1 - Organización del proyecto.
  - Etapa 2 - Análisis del Riesgo.
  - Etapa 3 - Análisis de Impacto.
  - Etapa 4 - Desarrollo de las Estrategias.
  - Etapa 5 - Pruebas del Plan.
  - Etapa 6 - Desarrollo de normas y políticas del plan.
  - Etapa 7 - Mantenimiento.

- El desarrollo del plan no incluirá la generación de estrategias propias de las dependencias de la organización diferentes a la plataforma tecnológica de TIC.

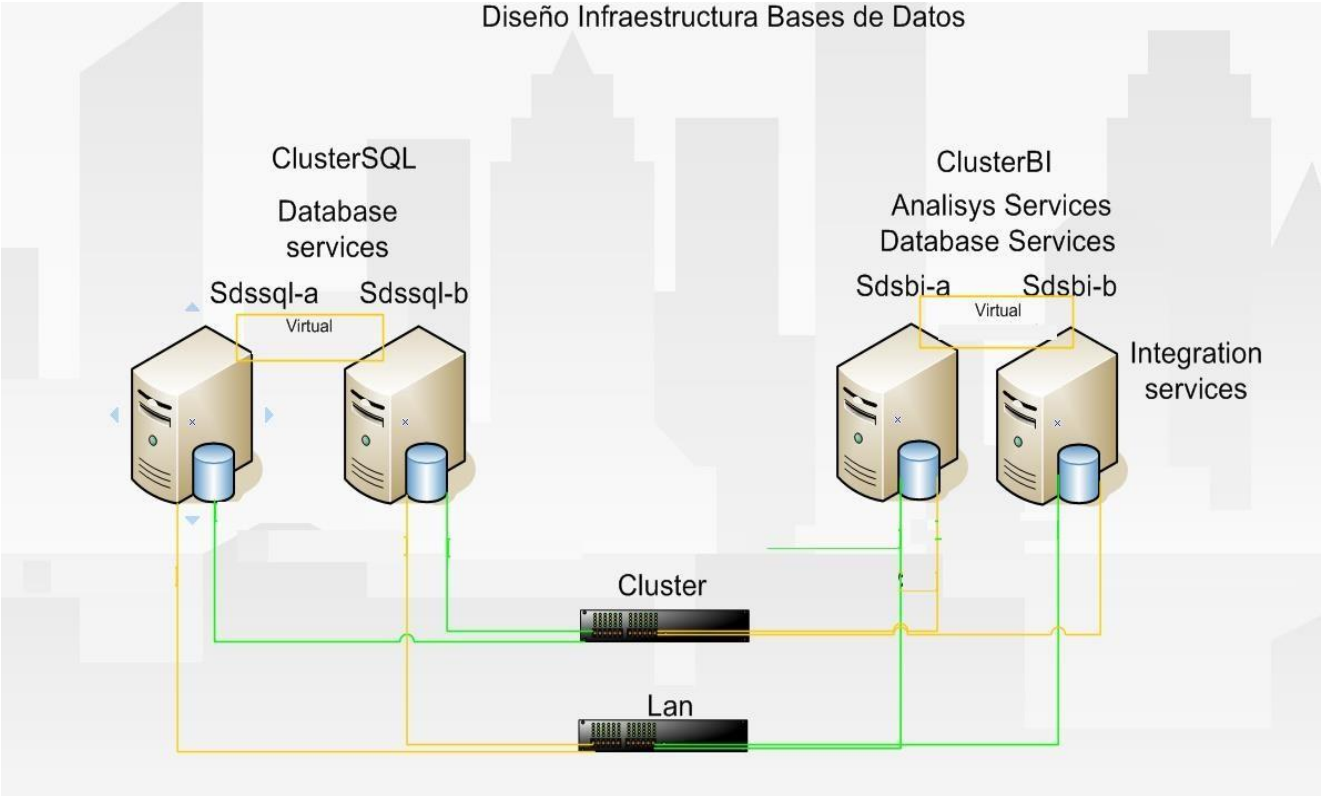
- El plan ha sido desarrollado para facilitar la toma de decisiones oportunas ante anomalías o fallas que se presenten en la plataforma tecnológica y de TIC de la entidad.

- El presente plan de contingencia atacara la recuperación de la operación de la entidad basado en los siguientes frentes o núcleos de operación:

  - ✓ Bases de datos (SQL, Oracle).
  - ✓ Aplicaciones (Web y livianas).
  - ✓ Mensajería (Exchange)
  - ✓ Infraestructura (Servidores, Storage).
  - ✓ Redes y comunicaciones (Switches, routers, canales).
  - ✓ Infraestructura Física (Ups, Electricidad, Aire acondicionado).
  - ✓ Seguridad Informática (Lógica y física).

**11. Bases de Datos:** La Secretaria Distrital de Salud para la operación de sus aplicaciones y para sus nuevos desarrollos usa y tiene implementado el motor de bases de datos de Microsoft SQL Server 2008, este se define como el motor estándar de la entidad. En la actualidad existen unas aplicaciones que interactúan con bases de datos Oracle 8i. La siguiente es la arquitectura de base de datos SQL Server de la SDS:

### Grafico 1.2.1.1. Arquitectura de Bases de Datos




En la SDS se cuenta con un esquema de alta disponibilidad para las BD de SQL Server que consiste en un Clúster configurado activo-activo en donde están las bases de datos de producción (activos de información):

**Tabla 1 Listado de bases de datos configuradas en los servidores SQL de la SDS Actualizado**

| name | crdate | cmptlevel |
|---|---|---|
| master | 2003-04-08 09:13:36.390 | 100 |
| tempdb | 2015-01-06 16:19:43.853 | 100 |
| model | 2003-04-08 09:13:36.390 | 100 |
| msdb | 2008-07-09 16:46:27.767 | 100 |
| PICSI | 2012-06-19 17:28:50.940 | 100 |
| pabsds | 2009-04-30 10:40:39.993 | 100 |
| BancodeDatos | 2009-05-20 12:34:25.847 | 80 |
| Barreras | 2009-07-31 19:28:53.757 | 80 |
| Bd_procesamiento_Rips | 2009-09-07 16:19:24.977 | 100 |
| ReportServerSDS | 2011-12-03 16:03:29.280 | 100 |
| ReportServerTempDB | 2011-12-03 16:03:42.607 | 100 |

| | | |
|---|---|---|
| IntegraInventarios | 2013-06-21 16:09:34.920 | 100 |
| sdsredsangre | 2009-09-28 10:29:37.473 | 100 |
| Mapariesgosbd | 2009-09-28 15:35:43.847 | 100 |
| distribution | 2010-04-21 10:46:19.333 | 90 |
| APS_Caracterizacion | 2014-11-16 19:22:04.650 | 100 |
| CapacidadInstalada | 2014-09-30 11:13:55.607 | 100 |
| OperationsManager | 2010-02-03 14:47:45.740 | 100 |
| APS_esecurity | 2014-11-16 19:22:27.573 | 100 |
| APS_FormBuilder | 2014-11-16 19:23:01.507 | 100 |
| APS_Seguimiento | 2014-11-16 19:23:27.820 | 100 |
| SeguridadAPS | 2014-11-16 19:23:56.273 | 100 |
| ARANDASDS_HST_71 | 2010-02-01 16:54:53.640 | 80 |
| OperationsManagerDW | 2010-02-03 15:44:08.053 | 100 |

| | | |
|---|---|---|
| Sira | 2011-12-23 13:09:04.630 | 100 |
| SeguridadAPSLogs | 2014-11-16 19:24:18.557 | 100 |
| SIVIGILA | 2014-05-30 20:08:08.517 | 90 |
| DBAXXXXXX | 2014-12-19 16:58:42.647 | 100 |
| PaiServicioWeb | 2014-01-20 16:10:44.477 | 100 |
| Siias | 2013-04-07 16:53:43.557 | 100 |
| PortalSecretariaSS | 2010-12-14 11:12:15.803 | 90 |
| SecretariaSS | 2010-12-14 11:13:38.983 | 90 |
| Sidba | 2013-01-31 17:23:45.420 | 100 |
| Pai | 2011-10-03 05:42:15.480 | 100 |
| SilaspPreproduccion | 2014-09-15 23:34:26.750 | 100 |
| Vi | 2014-12-24 09:00:35.800 | 90 |
| ArandaDB | 2011-03-16 10:58:17.060 | 90 |

| | | |
|---|---|---|
| BarrerasEnSalud | 2014-03-05 19:43:35.363 | 100 |
| Resolucion4505 | 2014-03-28 10:13:28.703 | 100 |
| BSC_SDS | 2011-06-30 12:14:06.030 | 90 |
| CostoUnitario | 2014-04-01 15:19:02.423 | 100 |
| Tempsdsredsangre2014 | 2014-06-26 11:41:37.127 | 100 |
| GOB_BOY | 2014-05-05 09:55:44.557 | 100 |
| master | 2003-04-08 09:13:36.390 | 100 |
| tempdb | 2015-01-06 16:24:40.687 | 100 |
| model | 2003-04-08 09:13:36.390 | 100 |
| msdb | 2008-07-09 16:46:27.767 | 100 |
| XXXXXXXXXXXX | 2012-03-25 20:10:12.780 | 100 |
| XXXXXXXXXXXXXXX | 2010-01-25 09:34:47.410 | 100 |

| | | |
|---|---|---|
| XXXXXXXXXXXXXXX | 2010-01-25 09:35:08.883 | 100 |
| XXXXXXXXXXXXXXXXXXXXX | 2010-01-25 09:35:12.563 | 100 |
| DBASDSSQLB | 2014-11-06 10:08:57.043 | 100 |
| XXXXXXXXXXXXXX | 2010-03-02 08:31:48.653 | 100 |
| XXXXXXXXXXXXXX | 2010-03-02 08:42:47.163 | 100 |
| XXXXXXXXXXXXXXXXX | 2010-03-10 10:12:32.670 | 100 |
| XXXXXXXXXXXXXXX | 2010-03-10 15:51:10.950 | 100 |
| XXXXXXXXXXXXX | 2010-03-11 07:59:34.297 | 90 |
| XXXXXXXXXXXXX | 2010-03-02 10:10:18.360 | 90 |
| XXXXXXXXXXXXXX | 2010-04-20 10:35:59.907 | 100 |
| master | 2003-04-08 09:13:36.390 | 100 |
| tempdb | 2014-12-10 10:41:16.693 | 100 |

| | | |
|---|---|---|
| model | 2003-04-08 09:13:36.390 | 100 |
| msdb | 2008-07-09 16:46:27.767 | 100 |
| DatamartAPS_VFS | 2009-01-28 13:54:45.973 | 100 |
| DatamartComunes | 2009-01-28 14:14:51.910 | 90 |
| BDCentralizadaDWH | 2009-03-06 09:21:09.943 | 100 |
| DatamartAPS | 2009-06-09 10:34:55.977 | 90 |
| StageAPS | 2009-06-09 10:37:15.770 | 90 |
| ReportServer | 2009-11-03 14:03:33.377 | 100 |
| ReportServerTempDB | 2009-11-03 14:03:33.910 | 100 |
| paiDWH | 2011-11-08 12:21:43.413 | 100 |
| BSC_SDS | 2012-07-09 14:56:55.030 | 90 |
| SSODB | 2011-07-28 20:24:12.470 | 100 |
| BizTalkMgmtDb | 2011-07-28 20:24:20.810 | 100 |

| | | |
|---|---|---|
| BizTalkDTADb | 2011-07-28 20:24:28.260 | 100 |
| BizTalkMsgBoxDb | 2011-07-28 20:24:34.457 | 100 |
| BizTalkRuleEngineDb | 2011-07-28 20:26:28.150 | 100 |
| BAMPrimaryImport | 2011-07-28 20:26:34.270 | 100 |
| BAMStarSchema | 2011-07-28 20:26:35.693 | 100 |
| BAMArchive | 2011-07-28 20:26:36.400 | 100 |
| CalidadSoftware | 2012-04-26 14:09:10.623 | 90 |
| CalidadSoftwareSeguridad | 2012-04-26 14:10:15.810 | 90 |
| DBA | 2011-06-20 10:51:43.427 | 100 |
| mpsssoOld | 2013-07-08 10:41:27.517 | 90 |
| PlCSl | 2012-07-25 11:32:12.480 | 100 |
| APS_Caracterizacion | 2012-08-02 11:50:31.397 | 100 |
| APS_esecurity | 2012-08-02 11:54:01.440 | 100 |

| | | |
|---|---|---|
| APS_FormBuilder | 2012-08-02 11:55:07.140 | 100 |
| costosHospitalesDWH | 2012-07-30 18:34:59.043 | 100 |
| APS_Seguimiento | 2012-08-02 12:01:30.807 | 100 |
| SDSRedSangreUDistrital | 2012-03-20 16:03:01.410 | 100 |
| BarrerasUDistrital | 2012-03-20 16:13:17.597 | 80 |
| SeguridadAPS | 2012-08-02 12:11:29.903 | 100 |
| SeguridadAPSLogs | 2012-08-02 12:12:20.590 | 100 |
| SISGE | 2012-11-22 15:54:33.120 | 100 |
| Sorteo_Plazas | 2012-12-26 15:27:51.687 | 80 |
| AMDB | 2013-04-02 15:55:25.070 | 100 |
| GestionDocumental | 2014-09-05 09:32:11.380 | 100 |
| AdventureWorksDW | 2013-09-06 09:44:27.600 | 100 |
| paiDWH_v2 | 2014-10-27 14:28:12.683 | 100 |

| | | |
|---|---|---|
| RIPSSubsidiado | 2014-12-19 10:18:17.810 | 100 |
| sirabd | 2013-05-15 11:25:28.560 | 100 |
| TablasHistoricosRegimenSubsidiado | 2013-03-06 10:04:24.463 | 100 |
| Sirep31122010 | 2014-02-12 15:54:33.317 | 90 |
| Sirep31122013 | 2013-12-11 12:13:22.410 | 90 |
| SilaspVaHistorico | 2013-04-15 16:52:43.260 | 90 |
| SilaspVeHistorico | 2013-04-17 17:40:51.760 | 90 |
| mpssso | 2013-07-08 10:43:11.133 | 80 |
| consolidacionCostosHospitalesDWH | 2013-09-27 11:09:43.560 | 100 |
| Sirep30062013 | 2013-11-26 10:33:06.470 | 90 |
| Sirep31122012 | 2013-11-26 15:51:36.767 | 90 |
| TempSircPruebas | 2014-02-28 15:28:48.327 | 100 |

| | | |
|---|---|---|
| TblControlRafa | 2014-06-18 10:56:17.880 | 90 |
| InvApp_BD | 2014-05-02 14:43:26.877 | 100 |
| master | 2003-04-08 09:13:36.390 | 100 |
| tempdb | 2014-12-10 10:40:54.693 | 100 |
| model | 2003-04-08 09:13:36.390 | 100 |
| msdb | 2008-07-09 16:46:27.767 | 100 |
| XXXXXXXXXXXXXXXX | 2014-01-15 17:11:54.940 | 100 |
| XXXXXXXXXXX | 2014-01-15 17:13:27.163 | 100 |
| XXXXXXXXXXXXX | 2014-01-15 17:13:51.070 | 100 |
| XXXXXXXXXXXXX | 2014-01-15 17:18:48.047 | 100 |
| XXXXXXXXXXXXXXX | 2014-01-15 17:23:19.323 | 100 |
| XXXXXXXXXXXXXX | 2014-01-15 17:24:23.750 | 100 |

| | | |
|---|---|---|
| XXXXXXXXXXXXXXX | 2014-01-15 17:26:25.933 | 100 |
| XXXXXXXXXXXXXXX | 2014-01-15 17:26:44.613 | 100 |
| XXXXXXXXXXXXXXX | 2014-01-15 17:26:56.980 | 100 |
| XXXXXXXXXXXXXXXX | 2014-01-15 17:27:10.320 | 100 |
| XXXXXXXXXXXXXXX | 2014-01-15 17:27:31.243 | 100 |
| XXXXXXXXXXXXXXXX | 2014-01-15 17:27:46.793 | 100 |
| XXXXXXXXXXXXXXX | 2014-01-15 17:29:37.027 | 100 |
| XXXXXXXXXXXXXXXX | 2014-01-29 12:13:05.513 | 100 |
| XXXXXXXXXXXXXXXXX | 2014-05-27 09:34:50.497 | 100 |
| XXXXXXXXXXXXX | 2014-05-27 09:42:47.107 | 100 |
| XXXXXXXXXXXXXXXXXXX | 2014-05-27 09:48:18.870 | 100 |
| XXXXXXXXXXXXXXX | 2014-05-29 15:49:58.590 | 100 |
| XXXXXXXXXXXXXX | 2014-05-29 15:51:49.597 | 100 |

| | | |
|---|---|---|
| XXXXXXXXXXXX | 2014-05-30 11:26:06.460 | 100 |
| XXXXXXXXXXX | 2014-05-30 11:30:44.103 | 100 |
| XXXXXXXXXXXX | 2014-05-30 12:18:24.270 | 100 |
| XXXXXXXXXXXXXX | 2014-05-30 13:37:45.410 | 100 |
| SP2010_SubscriptionService | 2014-05-30 14:33:58.090 | 100 |
| SP2010_SecureService | 2014-05-30 15:01:32.110 | 100 |
| SP2010_ProfileService | 2014-05-30 15:13:56.663 | 100 |
| SP2010_ProfileSync | 2014-05-30 15:20:22.893 | 100 |
| SP2010_ProfileSocial | 2014-05-30 15:26:13.483 | 100 |
| XXXXXXXXXXXXXXX | 2014-05-30 15:54:33.130 | 100 |
| XXXXXXXXXXXXXXXXXXXXXXXXXXX | 2014-05-30 16:02:07.337 | 100 |

| | | |
|---|---|---|
| XXXXXXXXXXXXX | 2014-05-30 16:09:16.207 | 100 |
| SP2010_TEMPORAL | 2014-05-30 16:21:28.667 | 100 |
| name | create_date | compatibility_level |
| master | 2003-04-08 09:13:36.390 | 100 |
| tempdb | 2015-01-06 16:19:12.140 | 100 |
| model | 2003-04-08 09:13:36.390 | 100 |
| msdb | 2008-07-09 16:46:27.767 | 100 |
| ReportServer | 2009-09-28 11:24:43.857 | 100 |
| ReportServerTempDB | 2009-09-28 11:24:44.433 | 100 |
| DBASDSBIB | 2014-08-27 15:17:20.090 | 100 |
| DBRIPS | 2014-10-10 05:25:08.920 | 100 |
| BDRIPS | 2010-01-27 13:23:39.970 | 90 |
| name | create_date | compatibility_level |

| | | |
|---|---|---|
| master | 2003-04-08 09:13:36.390 | 110 |
| tempdb | 2014-12-05 23:48:20.980 | 110 |
| model | 2003-04-08 09:13:36.390 | 110 |
| msdb | 2012-02-10 21:02:17.770 | 110 |
| ReportServer$CAPITALSALUD | 2014-05-20 11:03:17.763 | 110 |
| ReportServer$CAPITALSALUDTempDB | 2014-05-20 11:03:18.647 | 110 |
| Sirc | 2014-12-05 19:52:03.620 | 100 |
| procesosAseguramiento | 2014-12-05 20:07:40.430 | 100 |
| Sirep | 2014-12-05 20:51:36.073 | 90 |
| swsirc | 2014-12-06 00:20:13.107 | 100 |
| silasp | 2014-12-06 09:44:47.620 | 100 |

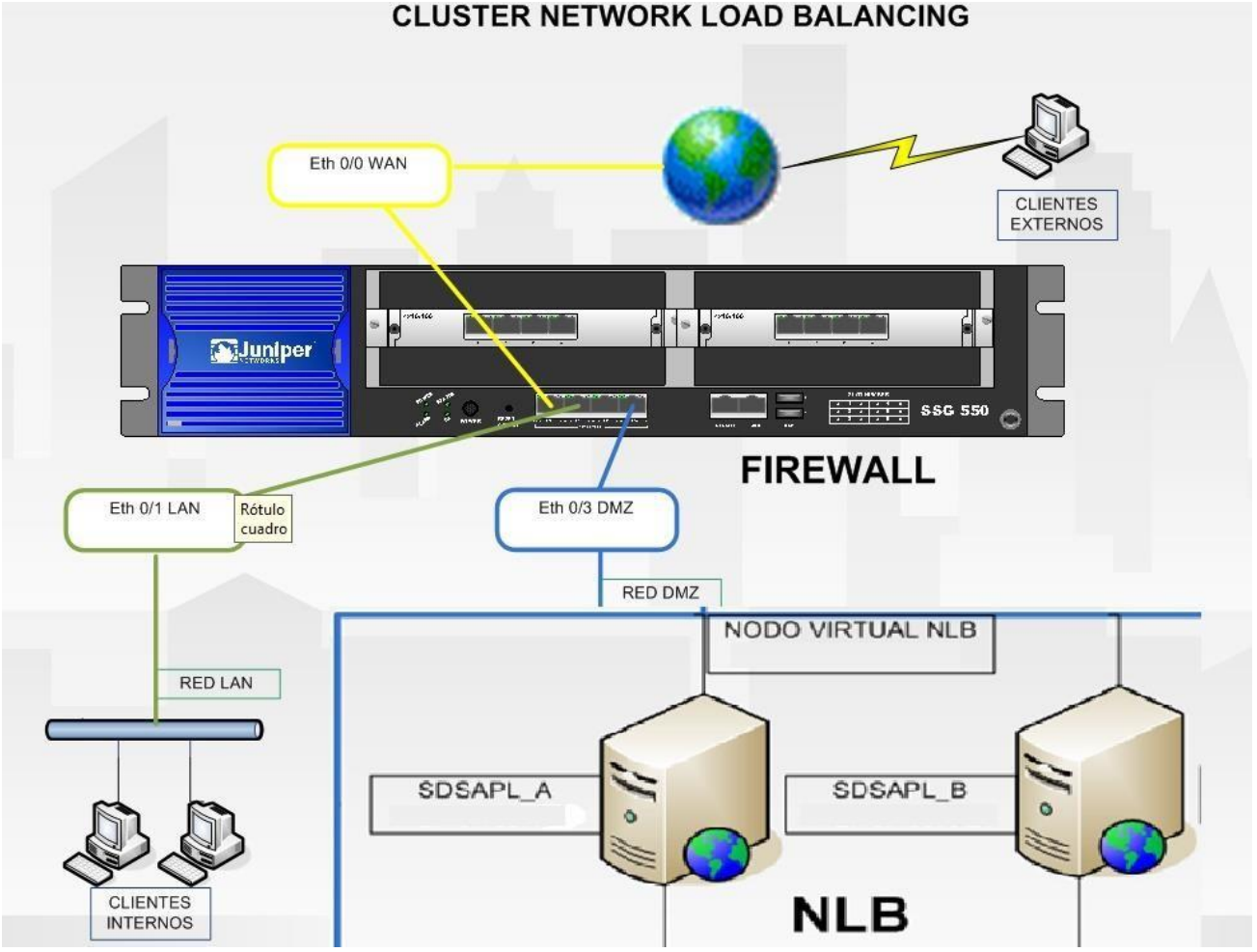
| | | |
|---|---|---|
| SIAsegura | 2014-12-06 15:00:06.147 | 90 |
| ResiduosSDS | 2014-12-06 15:21:12.543 | 90 |
| procesosLE | 2014-12-06 15:39:07.467 | 100 |
| ISOlucion | 2014-12-06 20:10:35.670 | 100 |
| Digiturno45 | 2014-12-06 20:15:53.313 | 90 |
| cobroCoactivo | 2014-12-06 20:19:35.460 | 100 |
| BDCentralizadaStage | 2014-12-06 20:25:55.040 | 100 |
| BDCentralizadaSDS | 2014-12-06 20:27:01.653 | 90 |
| BDCentralizadaDWH | 2014-12-06 20:29:56.993 | 100 |
| APS_Caracterizacion | 2014-12-07 00:26:25.180 | 100 |
| Espora | 2014-10-15 09:18:00.143 | 110 |
| APS_esecurity | 2014-12-07 00:28:45.877 | 100 |
| APS_FormBuilder | 2014-12-07 00:30:25.830 | 100 |

| | | |
|---|---|---|
| APS_Rips | 2014-12-07 00:32:02.687 | 100 |
| APS_Seguimiento | 2014-12-07 00:33:31.683 | 100 |
| BIDocumenter | 2014-12-07 00:37:30.653 | 100 |
| Pruebas_Mortalidad | 2014-10-24 09:24:54.693 | 100 |
| POB869 | 2014-11-10 13:49:03.983 | 100 |
| SEPTIEMBRE | 2014-11-10 13:54:20.113 | 100 |
| Territorios | 2014-11-10 13:56:49.140 | 100 |
| CIE10 | 2014-12-07 00:41:47.717 | 90 |
| XXXXXXXXXXXXXXX | 2014-12-07 00:47:10.910 | 100 |
| XXXXXXXXXXXXXXX | 2014-12-07 00:48:59.907 | 100 |
| XXXXXXXXXXXXXXXXX | 2014-12-07 00:51:06.613 | 100 |
| XXXXXXXXXXXXXX | 2014-12-07 00:53:08.370 | 100 |

| | | |
|---|---|---|
| XXXXXXXXXXXXXX | 2014-12-07 00:54:55.653 | 90 |
| XXXXXXXXXXXXXXX | 2014-12-07 00:56:59.310 | 100 |
| XXXXXXXXXXXXXX | 2014-12-07 00:59:37.570 | 100 |
| XXXXXXXXXXXXXXX | 2014-12-07 01:01:44.430 | 90 |
| XXXXXXXXXXXXXXX | 2014-12-07 01:12:20.513 | 100 |
| XXXXXXXXXXXXXXXXX | 2014-12-07 01:15:11.273 | 100 |
| XXXXXXXXXXXXXXXX | 2014-12-07 01:16:59.427 | 100 |
| SeguridadAPS | 2014-12-07 01:20:20.827 | 100 |
| SeguridadAPSLogs | 2014-12-07 01:21:46.927 | 100 |
| DBASDSCS | 2014-12-15 09:30:34.483 | 100 |
| sqlnexus | 2014-12-17 16:27:29.133 | 110 |
| zCopyAPS_Caracterizacion | 2015-01-01 19:59:10.293 | 100 |

| | | |
|---|---|---|
| XXXXXXXXXXXXXXXXXXXXX | 2015-01-01 20:19:05.210 | 100 |
| zCopyAPS_Seguimiento | 2015-01-01 20:22:47.430 | 100 |
| zCopySeguridadAPS | 2015-01-01 20:27:08.663 | 100 |

**12. Aplicaciones:** La Secretaria Distrital de Salud tiene una serie de aplicaciones para uso interno y externo sobre las cuales se soporta la operación de la misma, estas aplicaciones garantizan el normal desempeño de las funciones de la entidad. En cuanto a las aplicaciones que la SDS publica hacia internet se tiene una infraestructura de servidores para garantizar una óptima prestación del servicio, esto con el uso de un esquema de alta disponibilidad y balanceo de carga NLB (Network Load Balancing de Microsoft), con la siguiente arquitectura:




Este esquema de NLB garantiza que las aplicaciones publicadas estén disponibles y con un adecuado performance en su desempeño, ya que cada uno de sus nodos es una máquina robusta y que con el balanceo de cargas se optimiza la ejecución de las diferentes aplicaciones. A continuación se presenta una relación de las aplicaciones que la entidad pública hacia internet y que además son de uso interno.

Aplicativos (activos de software):

**Tabla 1 Listado de aplicativos en producción en el servidor de aplicaciones de la SDS. Actualizado**

| Numero servicio | Pool de aplicaciones | Identity | Managed Pipeline Mode | Framework |
|---|---|---|---|---|
| 1 | PIGI | ApplicationPoolIdentity | Classic | v2,0 |
| 2 | PIGI | ApplicationPoolIdentity | Classic | v2,0 |
| 3 | APS | NetworkService | Integrated | v2,0 |
| 4 | DefaultAppPool | NetworkService | Integrated | v2,0 |
| 5 | Barreras | NetworkService | Integrated | v4,0 |
| 6 | Silasp | NetworkService | Integrated | v2,0 |
| 7 | Carnetizacion | NetworkService | Classic | v2,0 |
| 8 | Carnetizacion | NetworkService | Classic | v2,0 |
| 9 | CExigibilidad | ApplicationPoolIdentity | Integrated | v4,0 |
| 10 | CIE10 | ApplicationPoolIdentity | Integrated | v2,0 |
| 11 | Cip | ApplicationPoolIdentity | Integrated | v4,0 |
| 12 | cobroCoactivo | ApplicationPoolIdentity | Integrated | v4,0 |

| | | | | |
|---|---|---|---|---|
| 13 | Comprobadordederechos | NetworkService | Classic | v2,0 |
| 14 | correo | ApplicationPoolIdentity | Integrated | v4,0 |
| 15 | CostosUnitarios | NetworkService | Integrated | v4,0 |
| 16 | DefaultAppPool | NetworkService | Integrated | v2,0 |
| 17 | DefaultAppPool | NetworkService | Integrated | v2,0 |
| 18 | Silasp | NetworkService | Integrated | v2,0 |
| 19 | InfoEra | ApplicationPoolIdentity | Integrated | v2,0 |
| **Numero servicio** | **Pool de aplicaciones** | **Identity** | **Managed Pipeline Mode** | **Framework** |
| 20 | integraInventarios | ApplicationPoolIdentity | Integrated | v4,0 |
| 21 | Silasp | NetworkService | Integrated | v2,0 |
| 22 | LibreElec | NetworkService | Classic | v2,0 |
| 23 | Linea195 | ApplicationPoolIdentity | Integrated | v4,0 |
| 24 | LstBarrerasSaludExcel | ApplicationPoolIdentity | Integrated | v4,0 |
| 25 | LstSidbaExcel | ApplicationPoolIdentity | Integrated | v4,0 |

| | | | | |
|---|---|---|---|---|
| 26 | Mia | ApplicationPoolIdentity | Integrated | v2,0 |
| 27 | Microfichas | ApplicationPoolIdentity | Integrated | v4,0 |
| 28 | observatorio | ApplicationPoolIdentity | Classic | v2,0 |
| 29 | OLAP | reportCubo | Classic | v2,0 |
| 30 | pabsds | NetworkService | Classic | v2,0 |
| 31 | pai | ApplicationPoolIdentity | Integrated | v4,0 |
| 32 | pai_reportes | ApplicationPoolIdentity | Integrated | v2,0 |
| 33 | CExigibilidad | ApplicationPoolIdentity | Integrated | v4,0 |
| 34 | PIGI | ApplicationPoolIdentity | Classic | v2,0 |
| 35 | PIGI | ApplicationPoolIdentity | Classic | v2,0 |
| 36 | DefaultAppPool | NetworkService | Integrated | v2,0 |
| 37 | Redsangre | ApplicationPoolIdentity | Integrated | v2,0 |
| 38 | ReportServer | NetworkService | Classic | v2,0 |
| 39 | ReportServer | NetworkService | Classic | v2,0 |

| | | | | |
|---|---|---|---|---|
| 40 | Residuos | ApplicationPoolIdentity | Classic | v2,0 |
| **Numero servicio** | **Pool de aplicaciones** | **Identity** | **Managed Pipeline Mode** | **Framework** |
| 41 | REvistaDigital | ApplicationPoolIdentity | Integrated | v2,0 |
| 42 | siasegura | ApplicationPoolIdentity | Integrated | v4,0 |
| 43 | sidba | ApplicationPoolIdentity | Integrated | v4,0 |
| 44 | Siias | ApplicationPoolIdentity | Integrated | v4,0 |
| 45 | Sirc | ApplicationPoolIdentity | Integrated | v4,0 |
| 46 | Sirep | ApplicationPoolIdentity | Integrated | v2,0 |
| 47 | SirepSaevad | ApplicationPoolIdentity | Integrated | v4,0 |
| 48 | siTerritorio | ApplicationPoolIdentity | Integrated | v2,0 |
| 49 | SivigilaDC | ApplicationPoolIdentity | Classic | v2,0 |
| 50 | ASP.NET 1.1 | NetworkService | Classic | v1,1 |
| 51 | ASP.NET 1.1 | NetworkService | Classic | v1,1 |

| | | | | |
|---|---|---|---|---|
| 52 | Comprobadordeder echos | NetworkService | Classic | v2,0 |
| 53 | APS | NetworkService | Integrated | v2,0 |
| 54 | APS | NetworkService | Integrated | v2,0 |
| 55 | Comprobadordeder echos | NetworkService | Classic | v2,0 |
| 56 | Comprobadordeder echos | NetworkService | Classic | v2,0 |
| 57 | DefaultAppPool | NetworkService | Integrated | v2,0 |
| 58 | Comprobadordeder echos | NetworkService | Classic | v2,0 |
| 55 | PortalProtect | ApplicationPoolIdentity | Classic | V2.0 |
| 56 | XXXXXXXXXXX | seds\spfs | Classic | V2.0 |
| 57 | XXXXXXXXXXX | sdews\spser | Classic | V2.0 |
| 58 | XXXXXXXXXXXX | sds\upett | Classic | V2.0 |
| 59 | XXXXXXXXXX | sds\dgfrs | Classic | V2.0 |
| 60 | XXXXXXXXXX | SDSI | Classic | V2.0 |

| | | | | |
|---|---|---|---|---|
| 61 | XXXXXXXXXX | SDenert\fdf | Classic | V2.0 |
| 62 | Office Server | Sdsented\fdf0 | Classic | V2.0 |
| 63 | XXXXXXXXXX | SDSInter\fdf | Classic | V2.0 |
| 64 | xxxxxxxxxxxxx | Fedr\fdfd | Classic | V2.0 |
| 65 | xxxxxxxxxxx | Dsf\fdfdf | Classic | V2.0 |
| Numero servicio | Pool de aplicaciones | Identity | Managed Pipeline Mode | Framework |
| 66 | crue | Local System | N/A | PHP v5.4.4 |
| 67 | moodle | Local System | N/A | PHP v5.4.4 |
| 68 | sisa | Local System | N/A | PHP v5.4.4 |
| 69 | catalogo | Local System | N/A | PHP v5.4.4 |
| 70 | certirips | Local System | N/A | PHP v5.3.8 |
| 71 | encuestas | Local System | N/A | PHP v5.3.8 |
| 72 | proinvcoop | Local System | N/A | PHP v5.3.8 |
| 73 | sispic | Local System | N/A | PHP v5.3.8 |

| | | | | |
|---|---|---|---|---|
| 74 | biblioteca | Local System | N/A | PHP v5.3.8 |
| 75 | osab | Local System | N/A | PHP v5.5.4 |
| 76 | ojs | Local System | N/A | PHP v5.5.4 |
| 77 | sakai | Local System | N/A | Java v1.7,0.25 |

| Numero servicio | Pool de aplicaciones | Identity | Managed Pipeline Mode | Framework |
|---|---|---|---|---|
| 1 | PIGI | ApplicationPoolIdentity | Classic | v2,0 |
| 2 | PIGI | ApplicationPoolIdentity | Classic | v2,0 |
| 3 | APS | NetworkService | Integrated | v2,0 |
| 4 | DefaultAppPool | NetworkService | Integrated | v2,0 |
| 5 | Barreras | NetworkService | Integrated | v4,0 |
| 6 | Silasp | NetworkService | Integrated | v2,0 |
| 7 | Carnetizacion | NetworkService | Classic | v2,0 |
| 8 | Carnetizacion | NetworkService | Classic | v2,0 |
| 9 | CExigibilidad | ApplicationPoolIdentity | Integrated | v4,0 |
| 10 | CIE10 | ApplicationPoolIdentity | Integrated | v2,0 |

| | | | | |
|---|---|---|---|---|
| 11 | Cip | ApplicationPoolIdentity | Integrated | v4,0 |
| 12 | cobroCoactivo | ApplicationPoolIdentity | Integrated | v4,0 |
| 13 | Comprobadordederechos | NetworkService | Classic | v2,0 |
| 14 | correo | ApplicationPoolIdentity | Integrated | v4,0 |
| 15 | DefaultAppPool | NetworkService | Integrated | v2,0 |
| 16 | DefaultAppPool | NetworkService | Integrated | v2,0 |
| 17 | Silasp | NetworkService | Integrated | v2,0 |
| 18 | InfoEra | ApplicationPoolIdentity | Integrated | v2,0 |
| **Numero servicio** | **Pool de aplicaciones** | **Identity** | **Managed Pipeline Mode** | **Framework** |
| 19 | integraInventarios | ApplicationPoolIdentity | Integrated | v4,0 |
| 20 | Silasp | NetworkService | Integrated | v2,0 |
| 21 | LibreElec | NetworkService | Classic | v2,0 |
| 22 | LstSidbaExcel | ApplicationPoolIdentity | Integrated | v4,0 |
| 23 | Mia | ApplicationPoolIdentity | Integrated | v2,0 |

| | | | | |
|---|---|---|---|---|
| 24 | observatorio | ApplicationPoolIdentity | Classic | v2,0 |
| 25 | OLAP | reportCubo | Classic | v2,0 |
| 26 | pabsds | NetworkService | Classic | v2,0 |
| 27 | pai | ApplicationPoolIdentity | Integrated | v4,0 |
| 28 | pai_reportes | ApplicationPoolIdentity | Integrated | v2,0 |
| 29 | CExigibilidad | ApplicationPoolIdentity | Integrated | v4,0 |
| 30 | PIGI | ApplicationPoolIdentity | Classic | v2,0 |
| 31 | PIGI | ApplicationPoolIdentity | Classic | v2,0 |
| 32 | DefaultAppPool | NetworkService | Integrated | v2,0 |
| 33 | Redsangre | ApplicationPoolIdentity | Integrated | v2,0 |
| 34 | ReportServer | NetworkService | Classic | v2,0 |
| 35 | ReportServer | NetworkService | Classic | v2,0 |
| 36 | Residuos | ApplicationPoolIdentity | Classic | v2,0 |

| Numero servicio | Pool de aplicaciones | Identity | Managed Pipeline Mode | Framework |
|---|---|---|---|---|
| 37 | REvistaDigital | ApplicationPoolIdentity | Integrated | v2,0 |
| 38 | siasegura | ApplicationPoolIdentity | Integrated | v4,0 |
| 39 | sidba | ApplicationPoolIdentity | Integrated | v4,0 |
| 40 | Sirc | ApplicationPoolIdentity | Integrated | v4,0 |
| 41 | Sirep | ApplicationPoolIdentity | Integrated | v2,0 |
| 42 | siTerritorio | ApplicationPoolIdentity | Integrated | v2,0 |
| 43 | SivigilaDC | ApplicationPoolIdentity | Classic | v2,0 |
| 44 | ASP.NET 1.1 | NetworkService | Classic | v1,1 |
| 45 | ASP.NET 1.1 | NetworkService | Classic | v1,1 |
| 46 | Comprobadordederechos | NetworkService | Classic | v2,0 |
| 47 | Silasp | NetworkService | Integrated | v2,0 |
| 48 | Silasp | NetworkService | Integrated | v2,0 |

| | | | | |
|---|---|---|---|---|
| 49 | APS | NetworkService | Integrated | v2,0 |
| 50 | APS | NetworkService | Integrated | v2,0 |
| 51 | Comprobadordeder echos | NetworkService | Classic | v2,0 |
| 52 | Comprobadordeder echos | NetworkService | Classic | v2,0 |
| 53 | DefaultAppPool | NetworkService | Integrated | v2,0 |
| 54 | Comprobadordeder echos | NetworkService | Classic | v2,0 |
| 55 | PortalProtect | ApplicationPoolIdentity | Classic | V2.0 |
| 56 | Sheerersd | Fddf\retrekju | Classic | V2.0 |
| 57 | xxxxxxxxx | Fdwd\dfgpotr | Classic | V2.0 |
| 58 | xxxxxxxxxx | Vfr\fddgewe | Classic | V2.0 |
| 59 | xxxxxxxxxxxx | sds\pluhert | Classic | V2.0 |
| 60 | xxxxxxxxxxxxxxx | SDKIYE\dfderuq | Classic | V2.0 |
| 61 | xxxxxxxxxxxxxx | Fds\dfswelier | Classic | V2.0 |

| | | | | |
|---|---|---|---|---|
| 62 | Office Server | Fdsd\ghtrwqew | Classic | V2.0 |
| 63 | xxxxxxxxxxxxxx | FDS\NBVWETR | Classic | V2.0 |
| 64 | xxxxxxxxxxxxx | Fdsd\dftrpee | Classic | V2.0 |
| 65 | xxxxxxxxxxxxx | Ffdss\djenezr | Classic | V2.0 |
| Numero servicio | Pool de aplicaciones | Identity | Managed Pipeline Mode | Framework |
| 66 | crue | Local System | N/A | PHP v5.4.4 |
| 67 | moodle | Local System | N/A | PHP v5.4.4 |
| 68 | sisa | Local System | N/A | PHP v5.4.4 |
| 69 | catalogo | Local System | N/A | PHP v5.4.4 |
| 70 | certirips | Local System | N/A | PHP v5.3.8 |
| 71 | encuestas | Local System | N/A | PHP v5.3.8 |
| 72 | proinvcoop | Local System | N/A | PHP v5.3.8 |
| 73 | sispic | Local System | N/A | PHP v5.3.8 |

| | | | | |
|---|---|---|---|---|
| 74 | biblioteca | Local System | N/A | PHP v5.3.8 |
| 75 | osab | Local System | N/A | PHP v5.5.4 |
| 76 | Ojs | Local System | N/A | PHP v5.5.4 |
| 77 | sakai | Local System | N/A | Java v1.7,0.25 |

**13. Correo Google Apps):** La SDS tiene implementado como sistema de mensajería (correo electrónico Google Apss) La información es considerada el principal activo de las empresas. Por esta razón, contar con un respaldo o backup de la información es una inversión segura si se considera que la pérdida de datos clave puede repercutir en la estabilidad y continuidad de la empresa.

El plan de Recuperación de Desastres consiste en contar con respaldos de información crítica del negocio ante situaciones como: ataques informáticos, robo, incendio, inundación u otro desastre. La eficacia de un plan de recuperación de desastres se suele medir de dos maneras: Recovery Time Objective (RTO) y Recovery Point Objective (RPO). La primera opción RTO es el tiempo en que se tarda en recuperar los datos en caso de pérdida y la segunda opción RPO es el punto de recuperación de los datos, es decir, en qué momento temporal anterior a la pérdida se recuperan los datos.

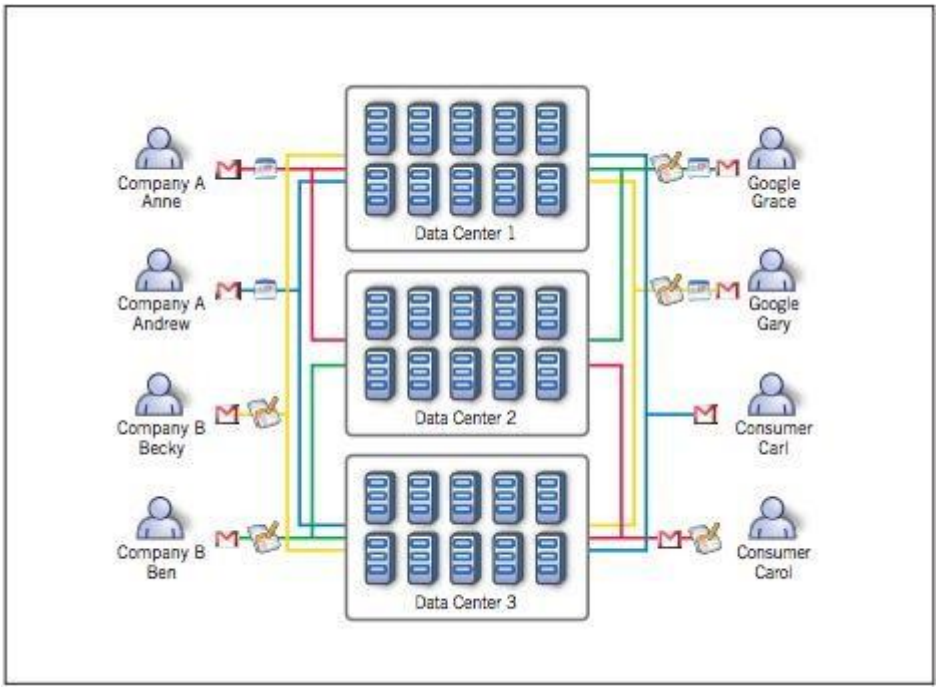
Teniendo en cuenta lo anterior Google posee una de las mayores redes de procesamiento de datos en el mundo, los datos de los clientes y la protección de la propiedad intelectual tiene la prioridad más alta. Los centros de datos de Google están protegidos en todo momento. Google dispone de un equipo de seguridad que se concentra exclusivamente en la seguridad en los sitios de la empresa. Los controles implementados por Google se ajustan a los requisitos establecidos por la auditoría SAS 70 Tipo II.

En este contexto Google ofrece servicios en la nube fiable, los cuales se caracterizan por entornos informáticos redundantes y la asignación dinámica de recursos , permiten a los clientes acceder a sus datos prácticamente en cualquier momento y en cualquier lugar en dispositivos con capacidad para Internet.

Los controles de seguridad aplicados por Google, que aíslan los datos durante el procesamiento en la nube, se desarrollaron al lado de la tecnología de la base desde el principio. La seguridad es por lo tanto un componente clave de cada uno de los elementos de computación en la nube.
Para reducir al mínimo la interrupción del servicio debido a un fallo de hardware, desastres naturales u otras catástrofes, Google implementa un programa de

recuperación de desastres en todos sus centros de datos. Este programa incluye múltiples componentes para reducir al mínimo el riesgo de cualquier punto de fallo, incluyendo las siguientes medidas:

- La replicación de datos y copia de seguridad: Para ayudar a asegurar la disponibilidad en caso de un desastre, los datos de Google Apps son replicados en varios sistemas dentro de un centro de datos, y también replicado en un centro de datos secundario.




Google dispone de un conjunto de centros de datos geográficamente distribuidos que están diseñados para mantener la continuidad del servicio en el caso de un desastre u otro incidente en una región. Conexiones de alta velocidad entre los centros de datos ayudará a asegurar la conmutación por error rápidamente. La gestión de los centros de datos y la administración del sistema también se distribuye para proporcionar una cobertura independiente de la ubicación en un esquema siguiendo el sol.

Además de la redundancia de los datos y centros de datos regionales dispares, Google también tiene un plan de continuidad empresarial para su sede en

Mountain View, CA. El cual involucra personas y servicios no disponibles hasta por 30 días. Este plan está diseñado para permitir la continuación de las operaciones de los servicios para los clientes. Google realiza pruebas regulares del plan de recuperación de desastres.

La aplicación y la arquitectura de la red de Google ha sido diseñada para una máxima fiabilidad y tiempo de funcionamiento. La plataforma de computación de Google supone un posible fallo de hardware, y un robusto software de conmutación por error puede resistir esta interrupción. Todos los sistemas de Google son intrínsecamente redundantes por su diseño, y cada subsistema no depende de ningún servidor en particular físico o lógico para su operación.

Google Apps ofrece una manera con sólidas capacidades de recuperación de desastres, para Google la meta de diseño RPO (Objetivo de Punto de Recuperación) es igual a cero pérdidas de datos y la meta de diseño RTO (Recovery Time Objetive) es conmutación por error al instante. Google lo hace a través de la replicación sincrónica o en directo de los datos: cada acción que sus usuarios realicen en su correo electrónico es a la vez replicado en dos centros de datos a la vez, de modo que si un centro de datos falla, casi al instante se transfieren sus datos al otro.

Los datos se replican varias veces a través de los servidores de Google, por lo que, en el caso de un fallo de la máquina, los datos serán accesibles a través de otro sistema, la información también se replican a los centros de datos secundarios para garantizar la seguridad en caso de fallas en uno de los centros de datos principales.

El objetivo de Google es no perder los datos cuando se están transferido de un centro de datos a otro, por tanto tiene conexiones de alta velocidad entre ellos, para poder transferir los datos muy rápidamente de un conjunto de servidores a otro. Esto le permite a Google replicar grandes cantidades de datos al mismo tiempo y se transfieren los datos con tanta rapidez que ni siquiera los usuarios perciben cuando un centro de datos está experimentando una interrupción.

Google Apps tiene el mismo nivel de replicación de datos para todas las

aplicaciones importantes en la suite de Google Apps: Gmail, Google Calendar, Google Docs y Google Sites.

Todo lo anterior confirma que si hay un desastre o una interrupción que afecta a uno de sus centros de datos, Google es capaz de trasladar a los usuarios a un centro de datos alternativo, por lo que se puede seguir trabajando sin interrupciones. Su correo electrónico y los documentos serán accesibles para que su organización pueda continuar a pesar del desastre. Esta es una de las principales razones por las que los negocios confían sus datos a Google Apps.

**14. Infraestructura (Servidores, Storage):** La Secretaria Distrital de Salud (SDS) cuenta con una red de datos de 1400 puntos de red, esta plataforma de red se soporta sobre plataforma Microsoft Windows Server 2008 R2 para 34 servidores físicos y 28 servidores virtuales y con 1400 puntos dobles certificados y 144 puntos de red sin certificar, los cuales operan con sistemas operativos Windows 2000, Windows XP, Windows Vista, Windows 7 y Windows 8. Todas las aplicaciones y procesos de operación crítica se ejecutan sobre esta plataforma y sobre estos servidores, existen otros componentes hardware que son complemento de esta plataforma como son las unidades de Storage SAN “red de área de almacenamiento, en inglés SAN (Storage Área Network)” y la EVA, sistemas para el respaldo de la información “Librería SDLT y la VTL virtual tape library” o librería de cintas virtuales. Todos estos componentes están bajo una estructura y un diseño para soportar la operación de la entidad, a continuación se describe esta arquitectura:

## Grafica 1.2.3.1 Red de Servidores

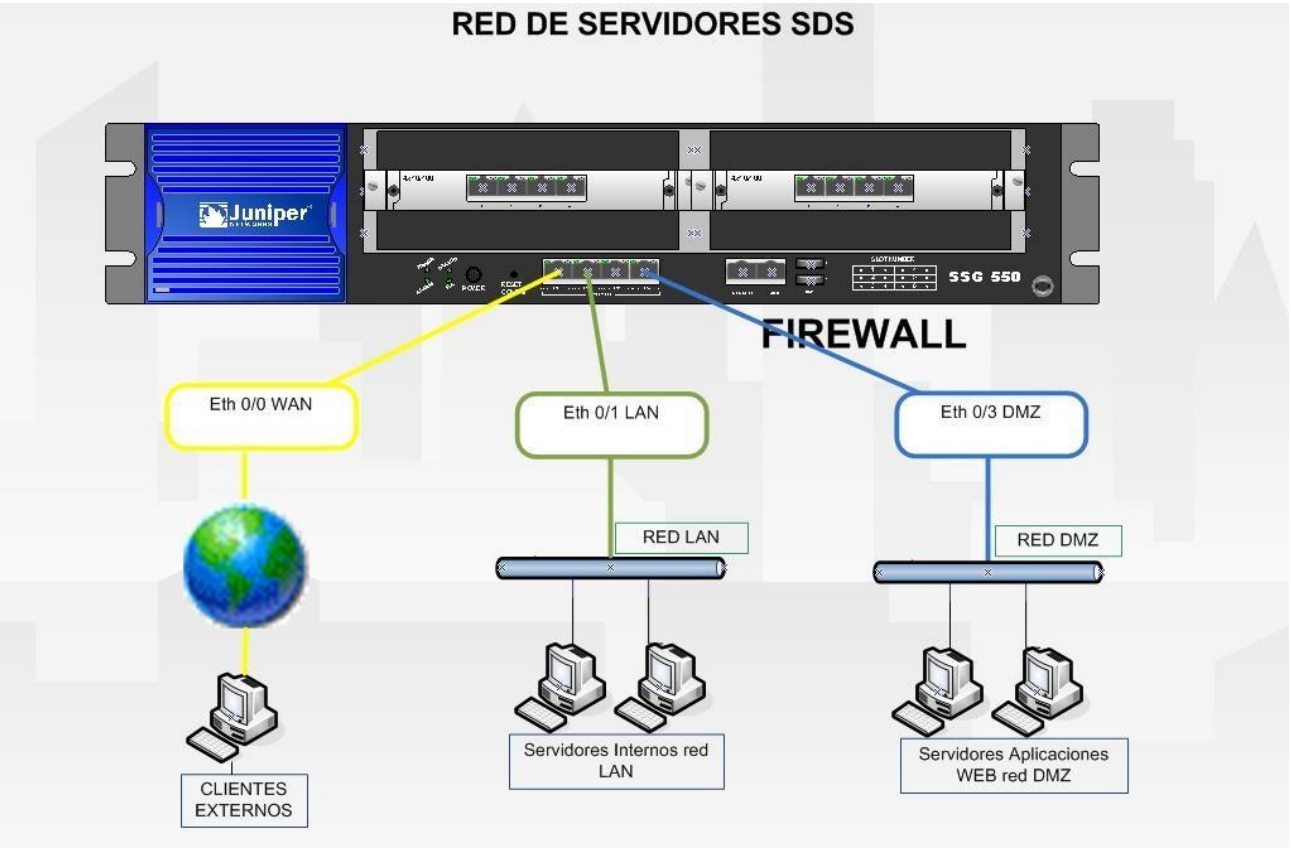


**Tabla 1.2.3.2 Servidores de la SDS EN FUNCIONAMIENTO.**

# SERVIDORES RACK

| ITEM | MARCA | PROCESADOR | SISTEMA OPERATIVO | MEMORIA | DISCOS |
|---|---|---|---|---|---|
| 01 | IBM System X3650 | 2 X Intel Xeon 2.5GHz | Windows 2008 R2 Enterprise | 08 GB | 5 HDD 146 GB |
| 02 | Dell PowerEdge 4600 | 2 X Intel Xeon 2.2GHz | Windows 2008 Enterprise | 04 GB | 6 HDD 33.9 GB c/u |
| 03 | Dell PowerEdge 2600 | 2 X Intel Xeon, 3.06 GHz | Windows 2003 Standard | 04 GB | 3 HDD 136 GB /cu |
| 04 | HP DL360 Generacion IV | 2 X Intel Xeon 3Ghz | Windows 2003 Standard | 02 GB | 2 DD 72 GB c/u |
| 05 | Compaq Proliant DL380 | 2 X Intel Xeon 3Ghz | Windows 2008 R2 Enterprise | 10 GB | 2 HDD 72.8GB c/u<br>2 HDD 146.8 GB c/u |
| 06 | Compaq Proliant DL580 | 2 X PIII Xeon, 900 MHz | Windows 2000 Adv Serv | 04 GB | 3 HDD 36.4 GB c/u |
| 07 | HP DL385 G2 | 1 X AMD OPTERON 2.81 GHz | Windows 2003 R2 Enterprise | 08 GB | 2 DD 146 GB c/u |
| 08 | Dell Power Edge 2950 | 2 X Intel Xeon, 1.6 GHz | Windows 2008 Enterprise | 04 GB | 4 HDD 300 GB c/u |
| 09 | Dell Power Edge 2950 | 2 X Intel Xeon, 1.6 GHz | Windows 2008 Enterprise | 04 GB | 4 HDD 300 GB c/u |
| 10 | IBM System X3650 | Intel Xeon 2.5 GHz | Windows 2008 R2 Enterprise | 08 GB | 5 HDD 146 GB |

# SERVIDORES BLADE ENCLOSURE 1 C7000

| ITEM | RACK | MARCA | PROCESADOR | SISTEMA OPERATIVO | MEMORIA | DISCOS |
|---|---|---|---|---|---|---|
| 01 | 01 | Blade 01 - HP Proliant BL460c | 2 X Intel Xeon Quad Core, 3 GHz | Windows 2008 Enterprise | 20 GB | 2 HDD 146 GB c/u |
| 02 | 01 | Blade 02 - HP Proliant BL460c | 2 X Intel Xeon Quad Core, 3 GHz | Windows 2008 Enterprise | 20 GB | 2 HDD 146 GB c/u |
| 03 | 01 | Blade 03 - HP Proliant BL460c | 2 X Intel Xeon Quad Core X5150 @ 3 GHz | Windows 2008 Enterprise | 16 GB | 2 HDD 146 GB c/u |
| 04 | 01 | Blade 04 - HP Proliant BL460c | 2 X Intel Xeon Quad Core X5150 @ 3 GHz | Windows 2008 Enterprise | 14 GB | 2 HDD 146 GB c/u |
| 05 | 01 | Blade 05 - HP Proliant BL460c | 2 X Intel Xeon Quad Core X5150 @ 3 GHz | Windows 2008 Server Enterprise | 16 GB | 2 HDD 146 GB c/u |
| 06 | 01 | Blade 06 - HP Proliant BL460c | 1 X Intel Xeon Quad Core X5150 @ 2.66 GHz | Windows 2003 R2 Enterprise | 14 GB | 2 DD 146 GB c/u |
| 07 | 01 | Blade 07 - HP Proliant BL460c | 1 X Intel Xeon Quad Core 2.66 GHz | Windows 2008 Enterprise | 14 GB | 2 HDD 146 GB c/u |
| 08 | 01 | Blade 08 - HP Proliant BL460c | 2 X Intel Xeon Quad Core, 3 0 GHz | Windows 2008 Enterprise | 16 GB | 2 HDD 146 GB c/u |
| 09 | 01 | Blade 09 - HP Proliant BL460c | 1 X Xeon Quad Core 2.66 GHz | Windows 2003 R2 Enterprise | 18 GB | 2 DD 146 GB c/u |
| 10 | 01 | Blade 10 - HP Proliant BL460c | 1 X Intel Xeon Quad Core, 2.66 GHz | Windows 2008 Enterprise | 16 GB | 2 DD 146 GB c/u |
| 11 | 01 | Blade 11 - HP Proliant BL460c | 2 X Intel Xeon Quad Core X5150 @ 3 GHz | Windows 2008 Enterprise | 16 GB | 2 HDD 146 GB c/u |
| 12 | 01 | Blade 12 - HP Proliant BL460c | 2 X Intel Xeon Quad Core X5150 @ 3 GHz | Windows 2008 Enterprise | 16 GB | 2 DD 146 GB c/u |
| 13 | 01 | Blade 13 - HP Proliant BL460c | 1 X Intel Xeon Quad Core, 2.66 GHz | Windows 2008 Enterprise | 10 GB | 2 DD 146 GB c/u |
| 14 | 01 | Blade 14 - HP Proliant | 2 X Intel Xeon Quad Core, 3 GHz | Windows 2008 Enterprise | 20 GB | 2 DD 146 GB c/u |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | BL460c | | | | |
| 15 | XXXXXXX | 01 | Blade 15 - HP Proliant BL460c G6 | 2 X Intel Xeon Quad Core, 3 GHz | Windows 2008 Enterprise | 16 GB | 1 HDD 97 GB c/u<br>1 HDD 137 GB c/u<br>1 HDD 340 GB c/u<br>1 HDD 322 GB c/u |
| 16 | XXXXXXX | 01 | ProLiant BL460c G7 | 2 X Quad-Core Intel Xeon, 2400 MHz | Windows 2008 R2 Enterprise | 32 GB | 2 DD 146 GB c/u |

# SERVIDORES BLADE ENCLOSURE 2 C7000

| ITEM | RACK | MARCA | PROCESADOR | SISTEMA OPERATIVO | MEMORIA | DISCOS |
|---|---|---|---|---|---|---|
| 01 | 03 | Blade 01 - HP Proliant BL460c G8 | Intel(R) Xeon(R) CPU E5-2609 0 @ 2.40GHz (4 Cores) | Windows 2008 Enterprise R2 | 32 GB | 2 HDD 350 GB c/u |
| 02 | 03 | Blade 02 - HP Proliant BL460c G8 | • Intel(R) Xeon(R) CPU E5-2670 0 @ 2.60GHz (8 Cores)<br>• Intel(R) Xeon(R) CPU E5-2670 0 @ 2.60GHz (8 Cores) | Windows 2012 Datacenter | 163 GB | 2 HDD 350 GB c/u |
| 03 | 03 | Blade 03 - HP Proliant BL460c G8 | Intel(R) Xeon(R) CPU E5-2609 0 @ 2.40GHz (4 Cores) | Windows 2008 Enterprise R2 | 32 GB | 2 HDD 350 GB c/u |
| 04 | 03 | Blade 04 - HP Proliant BL460c G8 | Intel(R) Xeon(R) CPU E5-2609 0 @ 2.40GHz (4 Cores) | Windows 2008 Enterprise R2 | 32 GB | 2 HDD 350 GB c/u |
| 05 | 03 | Blade 05 - HP Proliant BL460c G8 | Intel(R) Xeon(R) CPU E5-2609 0 @ 2.40GHz (4 Cores) | CONTINGENCIA | 32 GB | 2 HDD 350GB c/u |
| 06 | 03 | Blade 06 - HP Proliant BL460c G8 | • Intel(R) Xeon(R) CPU E5-2670 0 @ 2.60GHz (8 Cores)<br>• Intel(R) Xeon(R) CPU E5-2670 0 @ 2.60GHz (8 Cores) | Windows 2012 Datacenter | 163 GB | 2 DD 350 GB c/u |
| 07 | 03 | Blade 06 - HP Proliant BL460c G8 | • Intel(R) Xeon(R) CPU E5-2670 0 @ 2.60GHz (8 Cores)<br>• Intel(R) Xeon(R) CPU E5-2670 0 | Windows 2012 Datacenter | 163 GB | 2 DD 350 GB c/u |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | @ 2.60GHz (8 Cores) | | | |
| 08 | XXXXXXXX | 03 | Blade 06 - HP Proliant BL460c G8 | • Intel(R) Xeon(R) CPU E5-2670 0 @ 2.60GHz (8 Cores)<br>• Intel(R) Xeon(R) CPU E5-2670 0 @ 2.60GHz (8 Cores) | Windows 2012 Datacenter | 163 GB | 2 DD 350 GB c/u |

**Tabla 1.2.3.4 Servidores Virtuales de la SDS.**

# SERVIDORES VIRTUALES

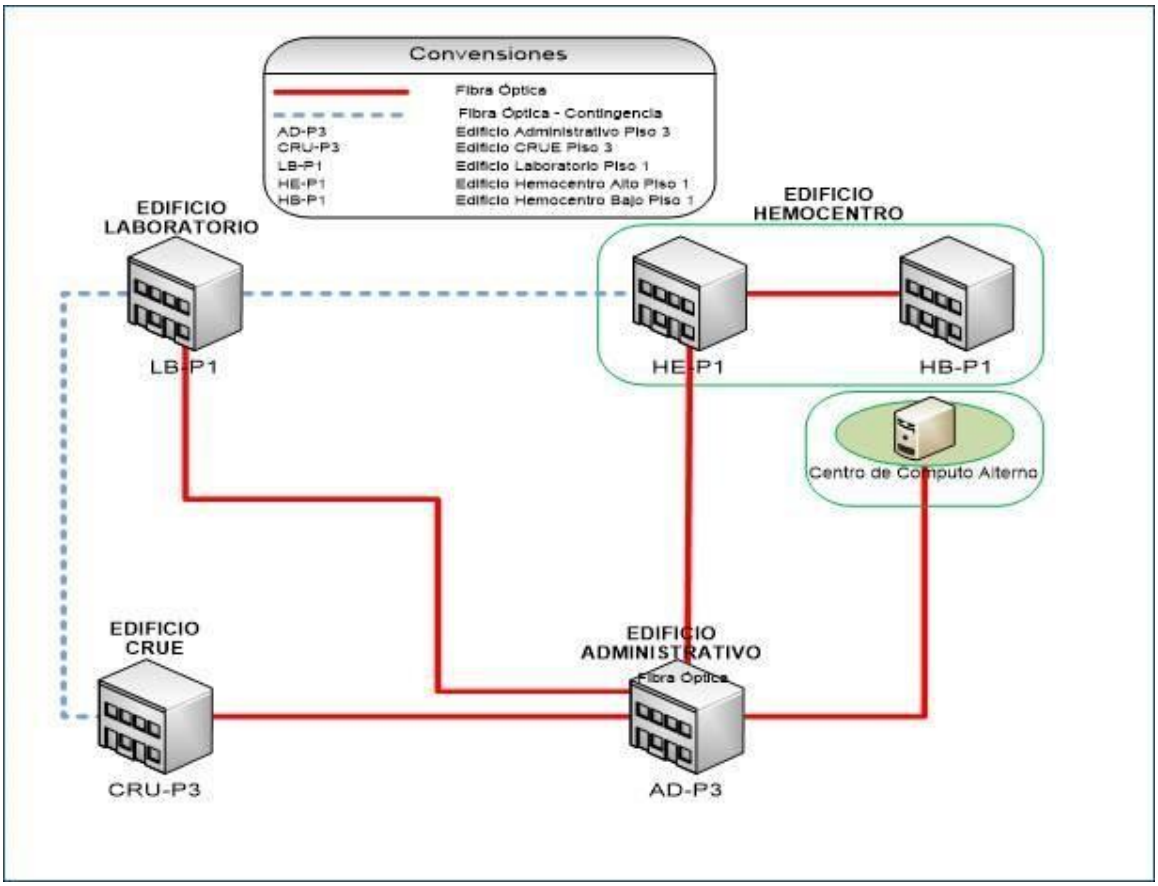
| ITEM | RACK | MARCA | PROCESADOR | SISTEMA OPERATIVO | MEMORIA | DISCOS |
|---|---|---|---|---|---|---|
| 01 | 03 | HYPER-V | 1 X Procesadores Virtuales | DEBIAN | 06 GB | 1 HDD 80 GB c/u |
| 02 | 03 | HYPER-V | 2 X Procesadores Virtuales | Windows 2008 Enterprise | 08 GB | 1 HDD 100 GB c/u<br>1 HDD 500 GB c/u |
| 03 | 01 | HYPER-V | 4 X Procesadores Virtuales | Windows 2008 Enterprise | 04 GB | 1 HDD 50 GB c/u |
| 04 | 01 | HYPER-V | 2 X Procesadores Virtuales | Windows 2003 R2 Enterprise | 02 GB | 1 HDD 50 GB c/u<br>1 HDD 20 GB c/u |
| 05 | 01 | HYPER-V | 4 X Procesadores Virtuales | Windows 2008 Enterprise R2 | 03 GB | 1 HDD 50GB c/u |
| 06 | 01 | HYPER-V | 2 Procesadores Virtuales | Windows 2003 Enterprise | 01 GB | 1 HDD 50GB c/u |
| 07 | 03 | HYPER-V | 1 X Procesadores Virtuales | Windows 2003 R2 Enterprise | 06 GB | 1 HDD 50GB c/u |
| 08 | 01 | HYPER-V | 4 X Procesadores Virtuales | Windows 2008 R2 Enterprise | 01 GB | 1 HDD 50GB c/u |
| 09 | 01 | HYPER-V | 2 X procesadores Virtuales | Windows 2008 Enterprise | 03 GB | 1 HDD 50GB c/u |
| 10 | 01 | HYPER-V | 2 X procesadores Virtuales | Windows 2008 Standart R2 | 04 GB | 1 HDD 50 GB c/u<br>1 HDD 20 GB c/u |
| 11 | 01 | HYPER-V | 2 X procesadores Virtuales | Windows 2008 Enterprise | 06 GB | 1 HDD 50GB |

| | | | | | | |
|---|---|---|---|---|---|---|
| 12 | 01 | HYPER-V | 4 x Procesadores Virtuales | Windows 2008 Enterprise | 08 GB | 1 HDD 50 GB |
| 13 | 03 | HYPER-V | 2 X procesadores Virtuales | Windows 2008 Enterprise R2 | 02 GB | 1 HDD 100 GB |
| 14 | 01 | HYPER-V | 1 X procesadores Virtuales | Windows 2008 Enterprise | 02 GB | 1 HDD 80 GB |
| 15 | 03 | HYPER-V | 1 X procesadores Virtuales | Windows 2008 Standart R2 | 04 GB | 1 HDD 100 GB |
| 16 | 03 | HYPER-V | 1 X procesadores Virtuales | Windows 2008 Enterprise R2 | 06 GB | 1 HDD 80 GB |
| 17 | 03 | HYPER-V | 1 X procesadores Virtuales | Windows 2003 Enterprise | 06 GB | 1 HDD 24 GB<br>1 HDD 43 GB |
| 18 | 03 | HYPER-V | 1 X procesadores Virtuales | Windows 2008 Enterprise | 08 GB | 1 HDD 40 GB |
| 19 | 03 | HYPER-V | 3 X procesadores Virtuales | Windows 2008 Enterprise R2 | 03 GB | 1 HDD 100 GB |
| 20 | 03 | HYPER-V | 2 X procesadores Virtuales | Windows 2012 Standard | 08 GB | 1 HDD 100 GB |
| 21 | 03 | HYPER-V | 2 X procesadores Virtuales | Windows 2008 Enterprise R2 | 04 GB | 1 HDD 80 GB |
| 22 | 03 | HYPER-V | 3 X procesadores Virtuales | Windows 2012 Standard | 08 GB | 1 HDD 100 GB |
| 23 | 03 | HYPER-V | 1 X procesadores Virtuales | Windows 2012 Standard | 08 GB | 1 HDD 100 GB |
| 24 | 03 | HYPER-V | 2 X procesadores Virtuales | Windows 2012 Standard | 08 GB | 1 HDD 100 GB |
| 25 | 03 | HYPER-V | 1 X procesadores Virtuales | UBUNTU 12 | 06 GB | 1 HDD 100 GB |
| 26 | 03 | HYPER-V | 2 X procesadores Virtuales | UBUNTU 12 | 04 GB | 1 HDD 100 GB |
| 27 | 03 | HYPER-V | 1 X procesadores Virtuales | Windows 2003 Enterprise | 16 GB | 1 HDD 100 GB |
| 28 | 03 | HYPER-V | 2 X procesadores Virtuales | UBUNTU 12 | 04 GB | 1 HDD 100 GB |
| 29 | 03 | HYPER-V | 2 X procesadores Virtuales | UBUNTU 12 | 04 GB | 1 HDD 100 GB |
| 30 | 06 | HYPER-V | 1 X Procesadores Virtuales | Windows 2012 Standard | 08 GB | 1 HDD 100 GB |
| 31 | 06 | HYPER-V | 2 X Procesadores Virtuales | Windows 2012 Standard | 08 GB | 1 HDD 100 GB |
| 32 | 03 | HYPER-V | 1 X procesadores Virtuales | Windows 2012 Standard | 08 GB | 1 HDD 100 GB |
| 33 | 06 | HYPER-V | 4 X procesadores Virtuales | Windows 2008 R2 enterprise | 08 GB | 1 HDD 100 GB<br>1 HDD 150 GB |
| 34 | 06 | HYPER-V | 2 X procesadores Virtuales | Windows 2012 Standard | 04 GB | 1 HDD 100 GB |
| 35 | 07 | HYPER-V | 1 X Procesadores Virtuales | UBUNTU 12 | 06 GB | 1 HDD 100 GB |

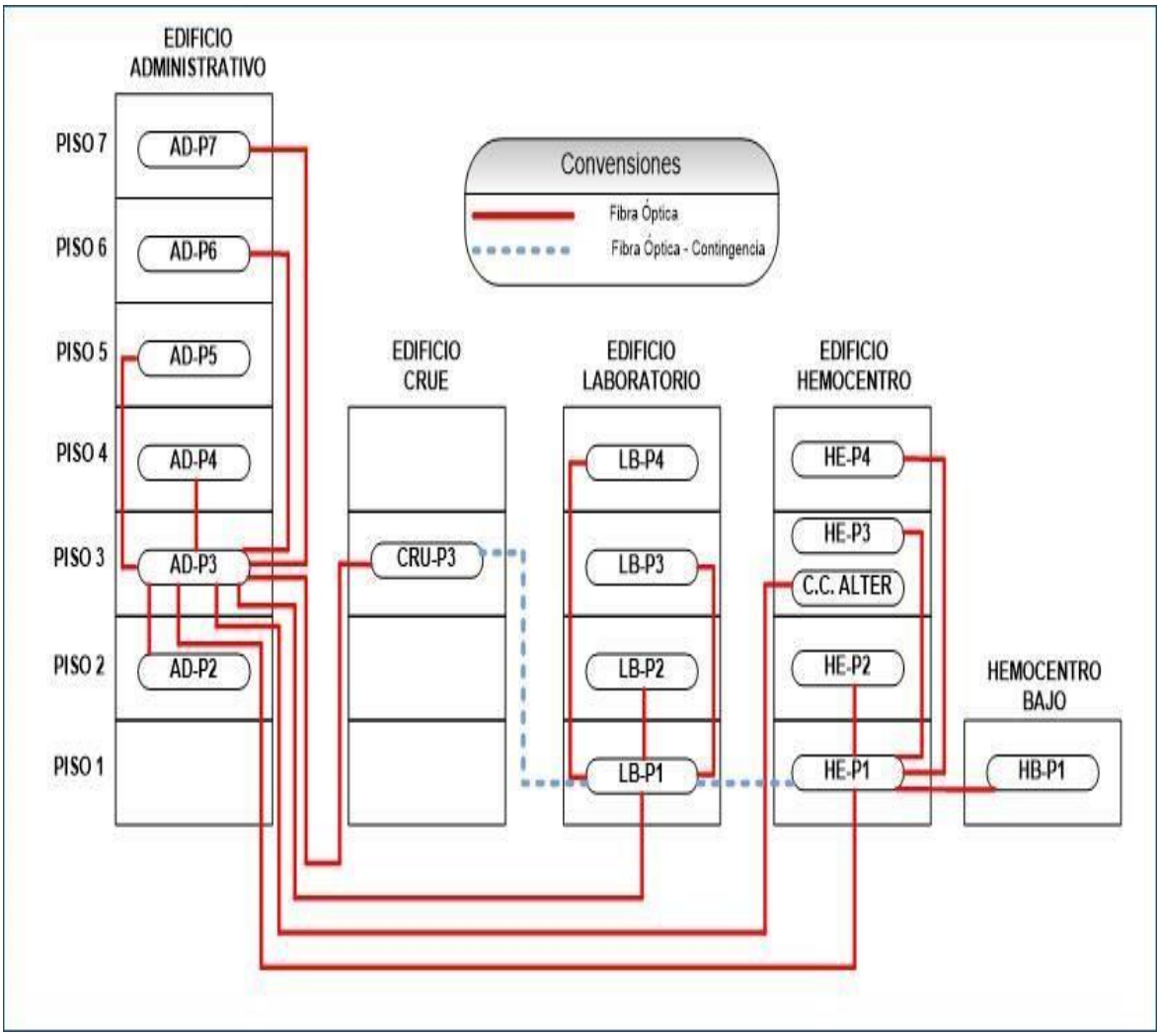
| | | | | | | |
|---|---|---|---|---|---|---|
| 36 | 07 | HYPER-V | 1 X Procesadores Virtuales | UBUNTU 12 | 05 GB | 1 HDD 100 GB |
| 37 | 07 | HYPER-V | 1 X Procesadores Virtuales | UBUNTU 12 | 05 GB | 1 HDD 100 GB |
| 38 | 06 | HYPER-V | 6 X procesadores Virtuales | Windows 2012 Standard | 16 GB | 1 HDD 100 GB |
| 39 | 06 | HYPER-V | 1 X procesadores Virtuales | Windows 2012 Standard | 04 GB | 1 HDD 100 GB |
| 40 | 07 | HYPER-V | 1 X Procesadores Virtuales | UBUNTU 12 | 04 GB | 1 HDD 100 GB |
| 41 | 06 | HYPER-V | 8 X Procesadores Virtuales | Windows 2012 Standard | 71 GB | 1 HDD 100 GB |
| 42 | 06 | HYPER-V | 8 X Procesadores Virtuales | Windows 7 | 1 GB | 1 HDD 100 GB |
| 43 | 06 | HYPER-V | 4 X procesadores Virtuales | Windows 2012 Standard | 08 GB | 1 HDD 100 GB |
| 44 | 06 | HYPER-V | 6 X procesadores Virtuales | Windows 2012 Standard | 12 GB | 1 HDD 100 GB |
| 45 | 06 | HYPER-V | 1 X procesadores Virtuales | Windows 2012 Standard | 04 GB | 1 HDD 100 GB |
| 46 | 07 | HYPER-V | 1 X Procesadores Virtuales | UBUNTU 12 | 06 GB | 1 HDD 100 GB |
| 47 | 07 | HYPER-V | 1 X Procesadores Virtuales | UBUNTU 12 | 04 GB | 1 HDD 100 GB |
| 48 | 06 | HYPER-V | 2 X procesadores Virtuales | Windows 2012 Standard | 8 GB | 1 HDD 100 GB |
| 49 | 06 | HYPER-V | 16 X procesadores Virtuales | Windows 2012 Standard | 51 GB | 1 HDD 100 GB |
| 50 | 06 | HYPER-V | 16 X procesadores Virtuales | Windows 2012 Standard | 51 GB | 1 HDD 100 GB |

**15. Redes y comunicaciones (Switches, routers, canales):** La Secretaría Distrital de Salud (SDS) para interconectar a 1544 usuarios que requieren trabajar en red y que tiene como base de operación el funcionamiento de la red y del dominio saludcapital.gov.co, requiere de una infraestructura de networking que soporte este nivel de usuarios y de la misma manera un diseño y una configuración lógica que garantice un óptimo rendimiento de los equipos activos instalados, la red Ethernet de la entidad cuenta con 1400 puntos dobles certificados y 144 puntos de red sin certificar, bajo una plataforma Microsoft Windows Server 2008 R2 Enterprise, con un Forest y un Active Directory nativo en Windows 2003. La interconexión entre edificios o conexiones troncales, cuenta con un Backbone de fibra óptica de 10Gb con un diseño en estrella con centralización en el centro de cómputo, tercer piso del edificio administrativo. La estructura de interconexión y redes se explican en las siguientes gráficas:

**Grafica 1.4.1. Plano de conexiones de fibra óptica Horizontales (Backbone).**



## Grafica 1.4.2. Conexiones de fibra óptica Horizontales- Verticales (Backbone).



**Infraestructura Física:** Topología en estrella entre los pisos del 2 al 7 del edificio administrativo, Hemocentro, CRUE y Laboratorio.

**Diagrama Infraestructura Física:** Según el grafico está instalado y configurado el Core Black Diamond 8806, compuesto con 6 módulos distribuidos de la siguiente forma:

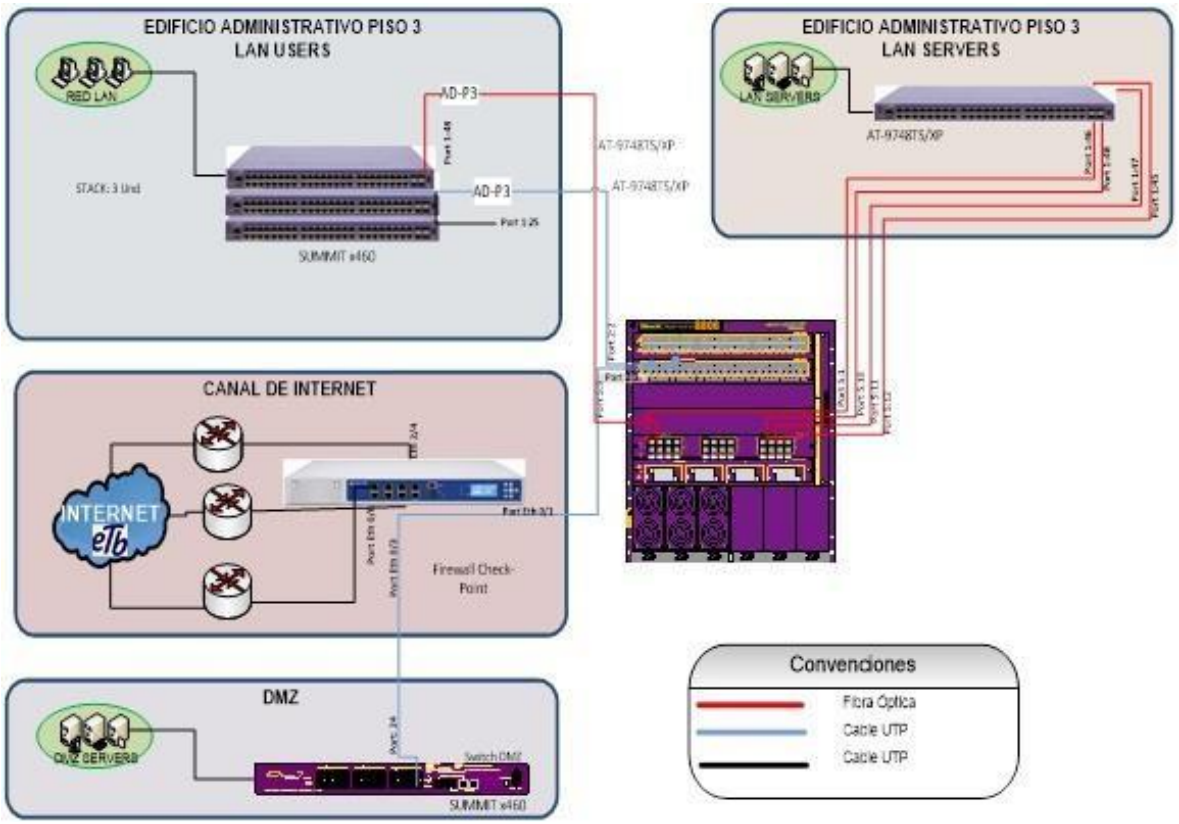
- Módulos 1 y 2 corresponden a Switch de 48 puertos destinados para usuarios finales en el piso 3 del edificio administrativo.
- Módulos 3 y 4 utilizados para la administración y configuración del equipo.
- Módulo 5 con 24 puertos en fibra óptica a 1 G, de los cuales fueron habilitados 12 para las respectivas conexiones de la red.
- Módulo 6 con 4 puertos en fibra óptica a 10 G el cual aún no se conecta.

La distribución de los 13 puertos en fibra dispuesta por el grupo de sistemas fue de la siguiente manera:

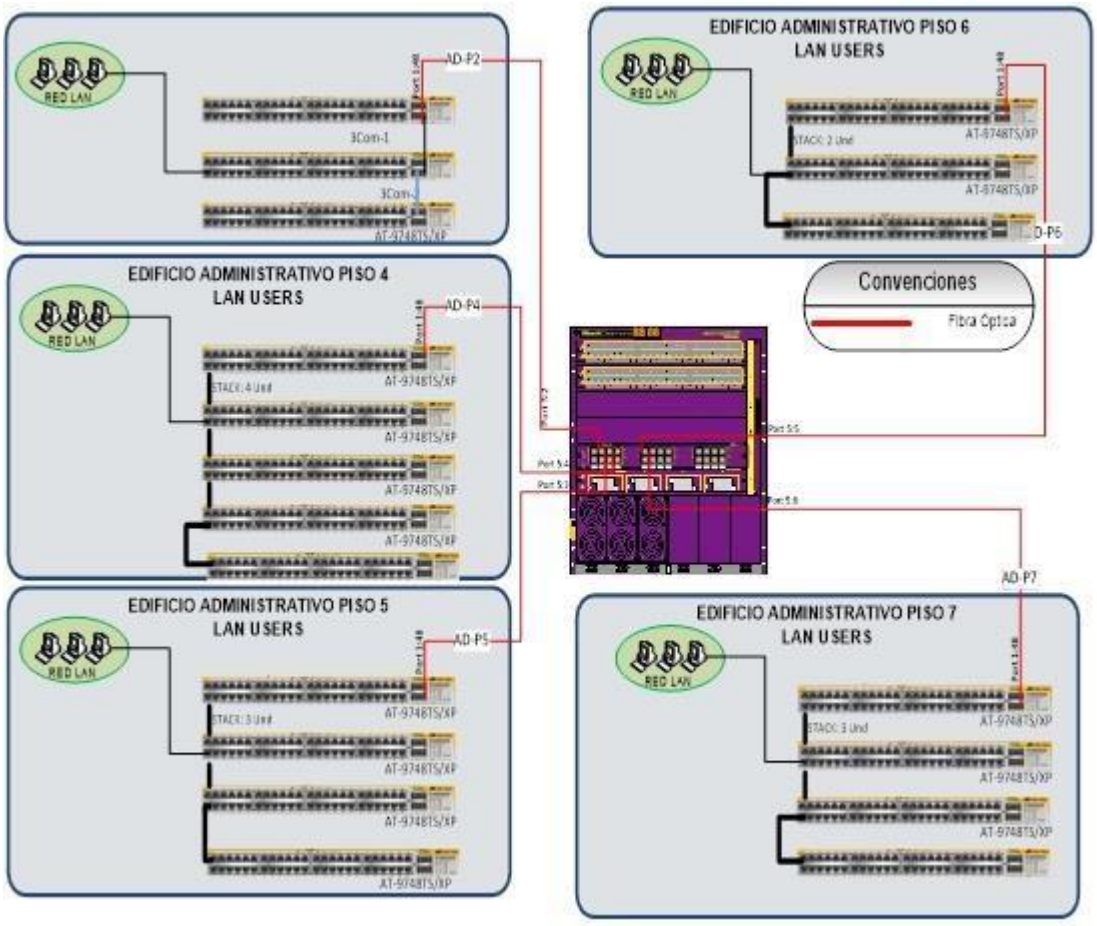
1. Conexión Link Aggregation con el Switch Servidores Centro de Computo AD-P3.
2. Conexión con el piso 2 del edificio administrativo.
3. Conexión con el piso 5 del edificio administrativo.
4. Conexión con el piso 4 del edificio administrativo.
5. Conexión con el piso 6 del edificio administrativo.
6. Conexión con el piso 7 del edificio administrativo.
8. Conexión con el Hemocentro Bajo piso 1.
9. Conexión al Switch Allied Telesis Centro de Computo AD-P3 para usuarios finales.
10. Conexión Link Aggregation con el Switch Servidores Centro de Computo AD-P3.
11. Conexión Link Aggregation con el Switch Servidores Centro de Computo AD-P3.
12. Conexión Link Aggregation con el Switch Servidores Centro de Computo AD-P3.
23. Conexión con el piso 1 del edificio laboratorio.
24. Conexión con el CRUE piso 3.

## Edificio Administrativo Centro de Computo Piso 3

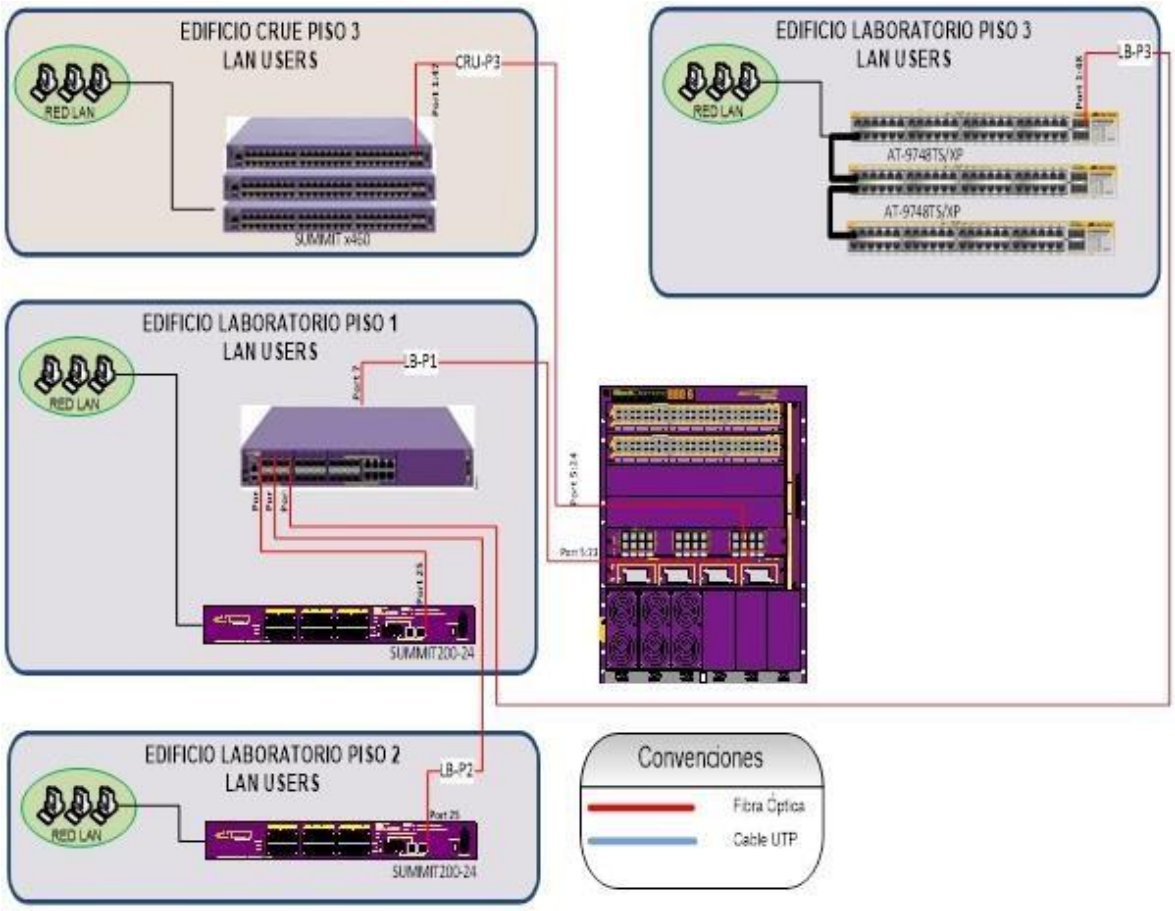
El siguiente grafico es la topología física del centro de cómputo piso 3 Edificio Administrativo



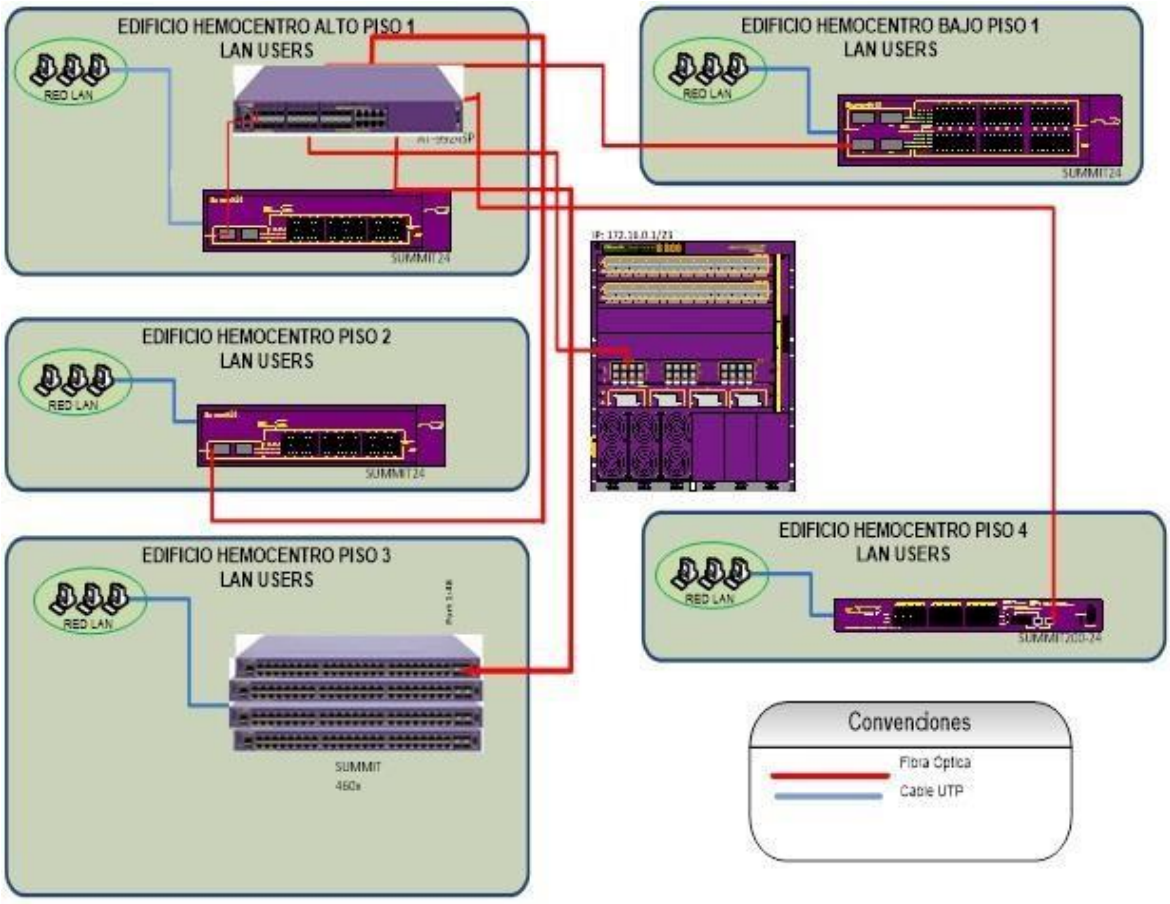
## Edificio Administrativo Pisos 2, 4, 5, 6 y 7



## Edificio CRUE y Laboratorio



## Edificio Hemocentro



Inventario Físico (Activos Físicos): El siguiente cuadro hace la relación de equipos activos (Switch) y seriales instalados en la SDS (activos físicos).

| Ubicación | Piso | Cantidad | Equipo | Modelo | Serial |
|---|---|---|---|---|---|
| Hemocentro | 4 | 1 | 3Com 50 port | 3Com 4210 | |
| | 3 | 1 | Extreme Networks 48 | Summit X 460-24X | 1144G-81093 |
| | | 1 | Extreme Networks 48 | Summit X 460-24X | 1144G-81194 |
| | | 1 | Extreme Networks 48 | Summit X 460-24X | 1144G-81193 |
| | | 1 | Extreme Networks 48 | Summit X 460-24X | 1144G-81094 |
| | 2 | 1 | Extreme Networks 24 | Summit24 | 0049M03035 |
| Hemocentro Alto | 1 | 1 | Extreme Networks 24 | Summit24 | 0049M02608 |
| | | 1 | Extreme Networks 24 | Summit X 460-24X | 1107G-80452 |
| Hemocentro Bajo | 1 | 1 | Extreme Networks 48 | Summit X 460-48t | 1107G-00728 |
| Laboratorio | 3 | 1 | Allied Telesyn 48 | AT-9748TS/XP | 22400000860019 |
| | | 1 | Allied Telesyn 48 | AT-9748TS/XP | 22400000860019 |
| | | 1 | Allied Telesyn 48 | AT-9748TS/XP | 22400000860027 |
| | 2 | 1 | Extreme Networks 24 | Summit200-24 | 0048F14769 |
| | 1 | 1 | 3Com 50 port | 3Com 4210 | |
| | | 1 | Extreme Networks 24 | Summit X 460-24X | 1107G-80458 |
| CRUE | 3 | 1 | Extreme Networks 24 | Summit X 460-24X | 1107G-80457 |
| | | 1 | Extreme Networks 48 | Summit X 460-48t | 1107G-00742 |
| | | 1 | Extreme Networks 48 | Summit X 460-48t | 1107G-00743 |
| Administrativo | 1 | 1 | Extreme Networks 24 | Summit200-24 | |
| | 2 | 1 | Allied Telesyn 48 | AT-9748TS/XP | 20090054060500208 |
| | | 1 | Allied Telesyn 48 | AT-9748TS/XP | 22400000860025 |
| | | 1 | Allied Telesyn 48 | AT-9748TS/XP | |
| | 3 | 1 | Black Diamont 8806 | BD 8806 | 09025-00605 |
| | | 1 | Extreme Networks 48 | Summit X 460-48t | 1107G-00735 |
| | | 1 | Extreme Networks 48 | Summit X 460-48t | 1107G-00730 |
| | | 1 | Extreme Networks 48 | Summit X 460-48t | 1107G-00729 |
| | | 1 | Extreme Networks 48 | Summit X 460-48t | 1107G-00734 |
| | | 1 | Extreme Networks 48 | Summit X 460-48t | 1107G-00731 |
| | 4 | 1 | Allied Telesyn 48 | AT-9748TS/XP | 20090054061000033 |
| | | 1 | Allied Telesyn 48 | AT-9748TS/XP | 20090054060500202 |
| | | 1 | Allied Telesyn 48 | AT-9748TS/XP | 20090054060500196 |
| | | 1 | Allied Telesyn 48 | AT-9748TS/XP | 20090054060500195 |
| | 5 | 1 | Allied Telesyn 48 | AT-9748TS/XP | 20090054060500199 |
| | | 1 | Allied Telesyn 48 | AT-9748TS/XP | 20090054060500144 |
| | | 1 | Allied Telesyn 48 | AT-9748TS/XP | 20090054060500143 |
| | 6 | 1 | Allied Telesyn 48 | AT-9748TS/XP | 22400000860012 |
| | | 1 | Allied Telesyn 48 | AT-9748TS/XP | |
| | | 1 | Allied Telesyn 48 | AT-9748TS/XP | 22400000860013 |
| | 7 | 1 | Allied Telesyn 48 | AT-9748TS/XP | 20090054060500200 |
| | | 1 | Allied Telesyn 48 | AT-9748TS/XP | 20090054061000010 |
| | | 1 | Allied Telesyn 48 | AT-9748TS/XP | 20090054061000042 |

**Esquema de Distribución puertos Switches:** Para todos los Switch de la secretaria de salud aplican las siguientes normas:

1. Los primeros puertos de cada Switch (y si es en un stack serán los de la unidad uno de la pila) se configuraran para la Vlan de impresoras.
2. Los últimos puertos de cada Switch (y si es en un stack serán los de la unidad uno de la pila) se configuraran para la Vlan de de la red inalámbrica.
3. Los puertos siguientes a los de la Vlan de impresoras se configuraran para la Vlan de VOIP.
4. Todos los Switch deberán quedar configurados con PORT SECURITY a la primera MAC que se registre.
5. Los puertos que queden libres en los Switch deberán quedar deshabilitados.

**Estándar de nombres para los Switche:** Este es el estándar definido por la Secretaria Distrital de Salud para los nombres de los Switch.

| Primeros 4 caracteres | Sig. 5 Caracteres | Sig. 2 Caracteres | Ejemplo |
|---|---|---|---|
| Des. De Edificio | Des. Piso | Consecutivo (**) | |
| Labo | Piso3 | | LaboPiso3 |
| Crue | Piso3 | | CruePiso3 |
| Admi | Piso7 | | AdmiPiso7 |
| Hemo | Piso2 | _02 | HemoPiso2_02 |
| (**)Consecutivo si no es un stack, en caso de ser cascadas de SW y así se identifican | | | |

**Arquitectura Lógica**

Según lo establecido por el área de Sistemas de la Secretaria Distrital de Salud, se realizó un estudio preliminar donde se destacaron temas importantes referentes a la conectividad y tráfico transmitido; aplicando IPSUBNETING y dando como resultado la implementación de los siguientes segmentos:

Los puertos asignados para cada VLAN en los dispositivos de borde quedan definidos en el documento de arquitectura servicios switches.

**Edificio administrativo** (como el primer piso no cuenta con rack de comunicaciones este se conecta al del segundo piso).

- ✓ **Piso 2:**
  - ➢ Unidad 1:
    - Del 1 al 2 (VLAN: IMPRESOR)
    - Puerto 3 (VLAN: FINANCIERA)
    - Del 4 al 7 (VLAN: CONTROLVIG)
    - Del 8 al 13 (VLAN: DADMIN)
    - Del 14 al 19 (VLAN: SISTEMAS)
    - Del 20 al 28 (VLAN DESASERV)
    - Del 29 al 44 (VLAN SUBSECRE)
    - Del 45 al 47 (VLAN Default) para la red inalámbrica.
    - Puerto 48 tag para las conexiones de FO.
  - ➢ Unidad 2:
    - Del 1 al 46 (VLAN SUBSECRE)
    - Del 47 al 48 tag para las conexiones de fibra.
- ✓ **Piso 3:**
  - ➢ Unidad 1:
    - Del 1 al 5 (VLAN: IMPRESOR)
    - Del 6 al 10 (VLAN: CONTROLINT)
    - Del 11 al 44 (VLAN: FINANCIERA)
    - Del 45 al 47 (VLAN Default) para la red inalámbrica.
    - Puerto 48 tag para las conexiones de FO.
  - ➢ Unidad 2:
    - Del 1 al 24 (VLAN PLANEACION)
    - Del 25 al 48 (VLAN FINANCIERA)
- ✓ **Piso 4:**
  - ➢ Unidad 1:
    - Del 1 al 4 (VLAN: IMPRESOR)
    - Del 5 al 44 (VLAN: SALUDPUB)

- Del 45 al 47 (VLAN Default) para la red inalámbrica.
- Puerto 48 tag para las conexiones de FO.

➢ Unidad 2:
- Del 1 al 48 (VLAN SALUDPUB)

➢ Unidad 3:
- Del 1 al 48 (VLAN SALUDPUB)

➢ Unidad 4:
- Del 1 al 48 (VLAN SALUDPUB)

✓ **Piso 5:**

➢ Unidad 1:
- Del 1 al 5 (VLAN: IMPRESOR)
- Puerto 6 (VLAN: VOIP)
- Del 7 al 44 (VLAN: DESASERV)
- Del 45 al 47 (VLAN Default) para la red inalámbrica.
- Puerto 48 tag para las conexiones de FO.

➢ Unidad 2:
- Del 1 al 48 (VLAN DESASERV)

➢ Unidad 3:
- Del 1 al 48 (VLAN ASEGURA)

✓ **Piso 6:**

➢ Unidad 1:
- Del 1 al 6 (VLAN: IMPRESOR)
- Del 7 al 45 (VLAN: JURIDICA)
- Del 46 al 47 (VLAN Default) para la red inalámbrica.
- Puerto 48 tag para las conexiones de FO.

➢ Unidad 2:
- Del 1 al 24 (VLAN JURIDICA)
- Del 25 al 26 (VLAN: SUBSECRE)
- Del 27 al 30 (VLAN: DESPACHO)
- Del 31 al 36 (VLAN COMUNICA)
- Del 37 al 48 (VLAN CONTROLINT)

- ✓ **Piso 7:**
  - ➢ Unidad 1:
    - Del 1 al 4 (VLAN: IMPRESOR)
    - Del 5 al 24 (VLAN:THUMANO)
    - Del 25 al 35 (VLAN:PARSOCIAL)
    - Del 36 al 45 (VLAN:DADMIN)
    - Del 46 al 47 (VLAN Default) para la red inalámbrica.
    - Puerto 48 tag para las conexiones de FO.
  - ➢ Unidad 2:
    - Del 1 al 48 (VLAN: DADMIN)
  - ➢ Unidad 3:
    - Del 1 al 18 (VLAN: SUBSECRE)
    - Del 19 al 48 (VLAN:THUMANO)

**Edificio CRUE**

- ✓ **Piso 3:**
  - ➢ Unidad 1:
    - Del 1 al 3 (VLAN: IMPRESOR)
    - Del 4 al 43 (VLAN: DESASERV)
    - Del 44 al 46 (VLAN Default) para la red inalámbrica.
    - Del 47 al 48 tag para las conexiones de FO.
  - ➢ Unidad 2:
    - Del 1 al 10 (VLAN: ASEGURA)
    - Del 11 al 48 (VLAN: CRUE)

**Edificio Laboratorio**

- ✓ **Piso 1:**
  - ➢ Unidad 1:
    - Puerto 1 (VLAN: IMPRESOR)
    - Del 2 al 24 (VLAN: SALUDPUB)
    - Del 25 al 26 tag para las conexiones de FO.
- ✓ **Piso 2:**

- Unidad 1:
  - Puerto 1 (VLAN: IMPRESOR)
  - Del 2 al 24 (VLAN: SALUDPUB)
  - Del 25 al 26 tag para las conexiones de FO.

✓ **Piso 3:**
- Unidad 1: (Allied Telesyn)
  - Del 1 al 3 (VLAN: IMPRESOR)
  - Del 4 al 44 (VLAN: SALUDPUB)
  - Puerto 45 Tag para formar la cascada con el Ext-Net
  - Puerto 48 tag para las conexiones de FO.
- Unidad 1: (Extreme Networks)
  - Del 1 al 25 (VLAN: SALUDPUB)
  - Puerto 26 tag para formar la cascada con el AT

**Edificio Hemocentro**

✓ **Piso 1 (Alto):**
- Unidad 1:
  - Del 1 al 24 (VLAN: SUBSECRE)
  - Del 25 al 26 tag para las conexiones de FO.

✓ **Piso 1 (Bajo):**
- Unidad 1:
  - Del 1 al 46 (VLAN: SUBSECRE)
  - Del 47 al 48 tag para las conexiones de FO.

✓ **Piso 2:**
- Unidad 1:
  - Del 1 al 24 (VLAN: SUBSECRE)
  - Del 25 al 26 tag para las conexiones de FO.

✓ **Piso 3:**
- Unidad 1:
  - Del 1 al 3 (VLAN: IMPRESOR)
  - Del 4 al 8 (VLAN: THUMANO)
  - Del 9 al 44 (VLAN: ASEGURA)
  - Del 45 al 46 (VLAN Default) para le red inalámbrica.

- Del 47 al 48 puertos tag para las conexiones de FO.

➢ Unidad 2:
- Del 1 al 48 (VLAN: ASEGURA)

➢ Unidad 3:
- Del 1 al 48 (VLAN: ASEGURA)

✓ **Piso 4:**

➢ Unidad 1:
- Puerto 1 (VLAN: IMPRESOR)
- Del 2 al 23 (VLAN: DADMIN)
- Puerto 24 (VLAN Default) para le red inalámbrica.
- Del 25 al 26 puertos tag para las conexiones de FO

**16.** Infraestructura Física (Ups, Electricidad, Aire acondicionado).

La operación de toda la plataforma tecnológica de la SDS, requiere de una serie de adecuaciones e instalaciones que permiten el funcionamiento de los diferentes componentes de hardware y software que soportan la misma. Varios de estos elementos y servicios su operación y mantenimiento no depende la Dirección Tecnologías de la información y las comunicaciones - TIC si no de la Dirección Administrativa, como por ejemplo:

- Aire Acondicionado centro de cómputo (soporte y mantenimiento).
- Sistema de detección y extinción de incendios (soporte y mantenimiento).
- Sistema de alimentación eléctrica regulada (mantenimiento y soporte a las UPS y planta eléctrica).
- Sistema de monitoreo y alarmas. (sensores y personal que opera le central de monitoreo).
- Vigilancia privada (personal de la empresa de vigilancia, control de acceso).

Por tal motivo se interactúa con esta dirección para coordinar la operación y mantenimiento de los elementos anteriormente mencionados.

**17.** Seguridad Informática (Lógica y física).

La velocidad de los cambios tecnológicos actuales, la multiplicidad de plataformas, marcas, soluciones, etc., hacen cada día más difícil el tratamiento de la

información de manera eficiente y segura. Sumado a esto, encontramos las barreras de distancia y tiempo comunes a cada uno de nosotros, lo que entorpece aún más la actualización tecnológica.

La seguridad informática consiste en asegurar que los recursos de los sistemas de información (material informático o programas) de la Secretaria Distrital de Salud sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Podemos entender como seguridad un estado de cualquier tipo de información (informático o no) de como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. Para que un sistema se pueda definir como seguro debe tener estas tres características:

- Integridad: La información sólo puede ser modificada por quien está autorizado y de manera controlada.
- Confidencialidad: La información sólo debe ser legible para los autorizados.
- Disponibilidad: Debe estar disponible cuando se necesita.

Dependiendo de las fuentes de amenaza, la seguridad de la entidad puede dividirse en dos partes: seguridad física y seguridad lógica.

**Seguridad física**

Para la Secretaria Distrital de Salud es muy importante ser consciente que por más que nuestra entidad sea la más segura desde el punto de vista de ataques externos (hackers, virus, ataques de DoS, etc.); la seguridad de la misma será nula si no se ha previsto como combatir un incendio o cualquier otro tipo de desastre natural y no tener presente políticas claras de recuperación.

Si bien algunos de los aspectos de seguridad física básicos se prevén, otros, como la detección de un atacante interno a la empresa que intenta acceder físicamente a una sala de cómputo de la misma, no. Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de backup de la sala de cómputo, que intentar acceder vía lógica a la misma. Así, la Seguridad Física consiste en la “aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e

información confidencial". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del centro de cómputo, (tercer piso edificio administrativo) así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

Las principales amenazas que se prevén en Seguridad Física son:

- Desastres naturales, incendios accidentales, tormentas e inundaciones
- Amenazas ocasionadas por el hombre
- Disturbios, sabotajes internos y externos deliberados.

Evaluar y controlar permanentemente la seguridad física de las instalaciones de cómputo y del edificio es la base para comenzar a integrar la seguridad como una función primordial dentro de cualquier organismo.

Tener controlado el ambiente y acceso físico permite:

- Disminuir siniestros
- Trabajar mejor manteniendo la sensación de seguridad
- Descartar falsas hipótesis si se produjeran incidentes
- Tener los medios para luchar contra accidentes

Los siguientes son los elementos que la Secretaria Distrital de Salud tiene instalados y en operación y que contribuyen a mejorar la seguridad física:

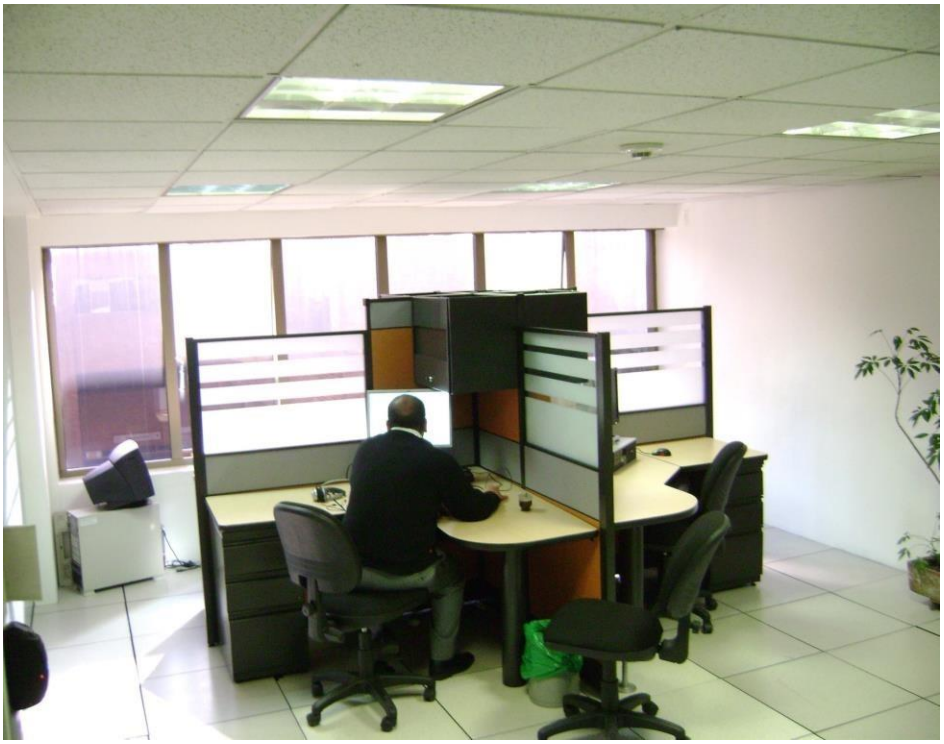
**Control de acceso**

**Planta Física-Edificios:** Para el ingreso a las instalaciones de la entidad esta cuenta con los servicios de una empresa especializada en seguridad y vigilancia, la cual realiza tareas de registro y control al personal externo e interno. En cada uno de los pisos se cuenta con una persona de esta empresa que vigila el acceso del personal y la entrada y salida de elementos con anotaciones en libros de bitácoras. Para los accesos a las dependencias o direcciones ya los funcionarios deben contar para ingresar con sus tarjetas de control de acceso "magnéticas". Independiente a esto se realiza una vigilancia y supervisión por medio de cámaras que están ubicadas en lugares estratégicos "fuera y dentro del edificio, por pisos" las cuales son monitoreadas las 24 horas del día por personal capacitado en una sala de control.

**Centro de Computo:** El centro de cómputo cuenta con un sistema más complejo de control de acceso completamente independientes del sistema de los edificios de la entidad, para el ingreso al centro de cómputo se cuenta con un sistema de exclusa en donde en la primera puerta) permite el acceso a la sala de los administradores del sistema y una segunda puerta que permite el acceso a personas que están registradas y autorizadas, las dos abren con un sistema de control de acceso biométrico “huella digital”, a continuación se describen y muestran los equipos del sistema de control de acceso de la SDS:

A. Tablero de comando del sistema de detección de intrusos con sus respectivos dispositivos de alarma, sensores de movimiento y cámaras de monitoreo.
B. Sistema de control de acceso biométrico con su respectivo sistema de administración instalado en uno de los computadores de los administradores de la plataforma.


C. Divisiones en vidrio templado que separa el centro de cómputo y la sala o puestos de trabajo de los especialistas de la administración.



**Seguridad lógica**

Luego de ver como nuestro sistema puede verse afectado por la falta de seguridad física, es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputo no será sobre los medios físicos sino contra información almacenada y procesada.

Así, la seguridad física sólo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física que la proteja. Estas técnicas las brinda la Seguridad Lógica.

La Seguridad Lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo". Partimos de la premisa ya conocida que "todo lo que no está permitido debe estar prohibido" y esto es lo que debe verificar la Seguridad Lógica.

Los objetivos que se definen son:

- Restringir el acceso a los programas y archivos
- Asegurar que los funcionarios puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.

## 2. GRUPOS FUNCIONALES DE RECUPERACIÓN.

Paralelo a la estructura organizacional de la Secretaria de Salud, es necesario crear una estructura de recuperación que involucre desde la Alta Directiva de la entidad hasta el personal encargado del desarrollo directo de los procedimientos, esto a fin de promover el compromiso de toda la entidad en el desarrollo,

ejecución, mejoramiento y actualización del plan de contingencia de la plataforma de TIC de la SDS y a su vez establecer responsabilidades.

Para que esto sea posible es necesario conformar **Equipos de Recuperación** cuya responsabilidad será la de responder oportunamente en el evento de una contingencia, asegurando que los planes que se establezcan sean llevados a cabo y procurando que se ejecute el proceso de recuperación en el menor tiempo posible.

Con la intención de dar un manejo formal y de manera institucional se crea al interior de la Secretaría Distrital de Salud, el **Comité de Seguridad de la Información (CSI),** de que trata el artículo 21 de la resolución 305 de 2008 expedida por la Comisión Distrital de Sistemas. Este comité está definido mediante resolución No 1074 del 15 de octubre de 2009, emanada del despacho del Secretario Distrital de Salud de Bogotá; conformado por las siguientes personas: Director de planeación y Sistemas o su delegado, Responsable de la Administración de Tecnologías de la información y las Comunicaciones (TICs), responsable de Desarrollo de Software, referente de seguridad informática, ingeniero de la Dirección de Planeación y Sistemas, Director Jurídico o su delegado.
El (CSI) se encarga de validar las Políticas de Seguridad de la Información, así como los procesos, procedimientos y metodologías específicas de seguridad de la información para el adecuado uso y administración de los recursos informáticos y físicos, asignados a los servidores públicos de la Secretaría Distrital de Salud, al igual que de garantizar que exista una dirección y apoyo gerencial, para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso adecuado de los recursos TIC, así como de la formulación y mantenimiento de una política de seguridad de la información en la entidad, dentro de lo cual se encuentra el plan de contingencia de la plataforma tecnológica y de TIC de la entidad.

El (CSI) será el encargado de coordinar todo el personal que interactúa dentro del plan de contingencia de la SDS y de la misma manera proponer, aceptar e implementar cualquier cambio, actualización o socialización del mismo.
Ver anexo: Resolución 1074 del 2009.

### 2.1 Grupo directivo del plan de contingencia

Paralelo a la estructura organizacional de la Secretaria de Salud, es necesario crear una de coordinación del plan de contingencia o desde otra óptica una

estructura de recuperación que involucre desde la Alta Dirección de la Entidad hasta el personal encargado del desarrollo directo de los procedimientos, esto a fin de promover el compromiso de toda la Entidad en el desarrollo del plan y a su vez establecer sus responsabilidades.

El plan de contingencia está coordinado por un grupo interdisciplinario que vela por el cumplimiento, actualización y pruebas del mismo. Para que esto sea posible es necesario conformar una serie de Equipos de Recuperación por rol o núcleo de operación cuya responsabilidad es la de responder en el evento de una contingencia, asegurando que los planes y procedimientos establecidos sean llevados a cabo y en el menor tiempo posible.

El "Grupo Directivo del Plan de Contingencia" es creado por el "*Comité de seguridad de la información"* y es activado después de la detección de cualquier incidente que pueda interrumpir la normal operación de la entidad. Este equipo provee el conocimiento único de la operación de la entidad necesario para revisar y actualizar las estrategias de recuperación y sus procedimientos basados en las circunstancias particulares del incidente. Una vez las estrategias de recuperación han sido revisadas y actualizadas, este equipo coordinará la implementación de la estrategia y procedimientos seleccionados con sus equipos subordinados.

El grupo directivo del plan de contingencia está conformado por los siguientes miembros:

1. **Coordinador General del Plan de contingencia:** Esta función estará a cargo del Director de Tecnología de la Información y de las Telecomunicaciones – TIC.

**Grupos de operación:**

2. **Coordinador grupo de recuperación de Bases de datos:** Función que será desempeñada por el Ingeniero DBA SQL y/o Oracle, profesional de la Dirección de Tecnología de la Información y de las Telecomunicaciones – TIC.
3. **Coordinador grupo de recuperación de Aplicaciones:** Esta actividad será desempeñada por el Coordinador Equipo Ingeniería de Software, profesional de la Dirección de Tecnología de la Información y de las Telecomunicaciones – TIC. apoyado por su grupo de trabajo.
1. **Coordinador grupo de recuperación de Comunicaciones:** Esta actividad será desempeñada por el Ingeniero encargado de administrar la plataforma

de correos electrónicos, Profesional de la Dirección de Tecnología de la Información y de las Telecomunicaciones – TIC apoyado por el ingeniero de redes y el ingeniero encargado de administrar los servidores.

2. **Coordinador grupo de recuperación de Infraestructura:** Esta labor será desempeñada conjuntamente por los profesionales de la Dirección de Tecnología de la Información y de las Telecomunicaciones – TIC.
3. **Coordinador grupo de recuperación de Redes y Canales de Comunicaciones:** Esta actividad será desempeñada por el Ingeniero especialista en redes, profesional de la Dirección de Tecnología de la Información y de las Telecomunicaciones – TIC
4. **Coordinador grupo de recuperación de Infraestructura Física:** Función que será desempeñada por el profesional especializado de la Dirección de Tecnología de la Información y de las Telecomunicaciones – TIC en coordinación con la Dirección Administrativa.
5. **Coordinador grupo de recuperación de Seguridad Informática:** Esta labor será desempeñada por el Ingeniero profesional especializado en seguridad de la Dirección de Tecnología de la Información y de las Telecomunicaciones – TIC con el apoyo del Ingeniero profesional especializado en redes, el coordinador de desarrollos de aplicaciones y líderes de proyectos.

El Grupo Directivo del Plan de Contingencia de la SDS, en cabeza del Director de Tecnología de la Información y de las Telecomunicaciones – TIC será el encargado de definir los criterios de acción para el caso de presentarse un incidente que afecte la normalidad de la operación de la entidad invocar, ejecutar, validar el plan de contingencia y regresar a operación normal.

### 2.2 Grupo de recuperación Bases de Datos.

Este grupo como su nombre lo indica será el encargado en cabeza de su coordinador de reaccionar ante un evento que afecte el normal funcionamiento de las bases de datos (SQL Server - Oracle) que soportan la operación de la SDS, de ejecutar las acciones de recuperación que garanticen retornar a la normal operación de las mismas, para esto se describen los recursos con los que se cuentan para este fin:

- Blade 05 - HP Proliant BL460c G8 Intel(R) Xeon(R) CPU E5-2609 0 @ 2.40GHz (4 Cores) 32 GB 2 HDD 350GB c/u Windows 2008 Enterprise Server.
- Dos PC de alta configuración HP, Modelo DC5750, AMD Athlon dual core 2,60 GHz, RAM 8 Gb, 1 HDD 250 GB.

- Backups totales de las bases de datos de los dos motores usados en la SDS, fulles los días viernes y diferenciales de lunes a jueves generados y administrados con la herramienta BrightStor Ver. 12 y con VTL HP en medios SDLT y LTO3.
- Recurso humano, DBA en cada uno de los motores, SQL y Oracle, servidores y storage, redes y comunicaciones.

## 2.3 Grupo de recuperación Aplicaciones

Este grupo orientado por su coordinador será el encargado ante un evento que afecte el normal funcionamiento de las aplicaciones que soportan la operación de la SDS, de ejecutar las acciones de recuperación que garanticen retornar a la normal operación de las mismas, para esto se describen los recursos con los que se cuentan para este fin:

- Blade 05 - HP Proliant BL460c G8 Intel(R) Xeon(R) CPU E5-2609 0 @ 2.40GHz (4 Cores) 32 GB 2 HDD 350GB c/u Windows 2008 Enterprise Server.
- Backups de todas las aplicaciones y códigos fuente de las mismas que funcionan en la entidad, con fulles de los días viernes y diferenciales de lunes a jueves generados y administrados con la herramienta BrightStor Ver. 12 y con VTL HP en cintas SDLT y LTO3.
- Recurso humano, todos los funcionarios del grupo de desarrollo de la Dirección de Tecnología de la Información y de las Telecomunicaciones – TIC, DBA en cada uno de los motores, SQL y Oracle, servidores y storage, redes y comunicaciones.

## 2.4 Grupo de recuperación Infraestructura (Servidores, Storage)

Este grupo bajo la orientación de su Director de Tecnología de la Información y de las Telecomunicaciones – TIC y de su coordinador de infraestructura, serán los encargados, ante un evento que afecte el normal funcionamiento de los principales componentes de Hardware (servidores y Storage) de la SDS, de ejecutar las acciones de recuperación que garanticen retornar a la normal operación de los mismos, para esto se describen los recursos con los que se cuentan para este fin:

- Blade 05 - HP Proliant BL460c G8 Intel(R) Xeon(R) CPU E5-2609 0 @ 2.40GHz (4 Cores) 32 GB 2 HDD 350GB c/u Windows 2008 Enterprise Server.

- Dos PC de alta configuración HP, Modelo DC5750, AMD Athlon dual core 2,60 GHz, RAM 4 Gb, 1 HDD 250 GB.
- Backups de los System State de los servidores, con fulles de los días viernes y diferenciales de lunes a jueves generados y administrados con la herramienta BrightStor Ver. 12 y con Imágenes de los servidores críticos generadas con Acronis, imágenes que pueden ser restauradas en otras máquinas sin problemas de requerir que estas sean de las mismas características.
- Recurso humano, Ingenieros. servidores y storage, redes y comunicaciones.

2.5 Grupo de recuperación Redes y Canales de Comunicaciones.

Este grupo como su nombre lo indica será el encargado en cabeza del Director de Tecnología de la Información y de las Telecomunicaciones – TIC y el coordinador de infraestructura deben reaccionar ante un evento que afecte el normal funcionamiento de las redes que operan en la entidad así como de los equipos activos que las soportan (Switche Core, Switches de distribución, Switches de borde, routers, Firewall, etc), deberán de ejecutar las acciones de recuperación que garanticen retornar a la normal operación de las mismas, para esto se describen los recursos con los que se cuentan para este fin:

- Un Switch Core de respaldo Extreme Networks, Modelo Black Diamond 3880, con una tarjeta de 8 puertos de FO (1 Gb), dos tarjetas de 32 puertos Ethernet 10/100 c/u, un módulo de administración y sistema de fuentes de poder redundantes, configurado y adecuado para entrar en operación.
- Backups totales de las configuraciones de cada uno de los equipos activos que permiten la restauración de unos equipos en menos tiempo.
- Recurso humano, Ing. servidores y storage, Ingeniero comunicaciones

2.6 Grupo de recuperación Infraestructura Física (Ups, Electricidad, Aire acondicionado).

Este grupo orientado por el Director de Tecnología de la Información y de las Telecomunicaciones – TIC y la Dirección Administrativa, será el encargado ante un evento que afecte el normal funcionamiento de los elementos o sistemas que brindan las condiciones adecuadas para el funcionamiento de los equipos ubicados en el centro de cómputo, de ejecutar las acciones de coordinación con la Dirección Administrativa de recuperación de los mismos

para garantizar el retorno a la normal operación de los elementos y/o sistemas, para esto se describen los recursos con los que se cuentan para este fin:

- Contrato de mantenimiento para la reparación y puesta en servicio del sistema de aire acondicionado del centro de cómputo.
- Contrato de mantenimiento para la reparación y puesta en servicio del sistema de detección y extinción de incendios (FM 200) del centro de cómputo.
- Contrato de mantenimiento para el mantenimiento de parte eléctrica de la planta física de la SDS.
- Contrato de mantenimiento para la reparación y puesta en servicio del sistema eléctrico regulado (UPS) del centro de cómputo.
- Recurso humano, grupo de colabores (Dirección Administrativa).

2.7 Grupo de recuperación Seguridad Informática (Lógica y Física).

Este grupo orientado por el Director de Tecnología de la Información y de las Telecomunicaciones – TIC y el coordinador de infraestructura será el encargado ante un evento que afecte el normal funcionamiento de los elementos o sistemas especializados en seguridad informática (los que prevén cualquier tipo de ataque informático), de ejecutar las acciones de recuperación de los mismos para garantizar el retorno a la normal operación de los elementos y/o sistemas, para esto se describen los recursos con los que se cuentan para este fin:

- Firewall Marca CISCO, Modelo PIX 515E, con seis interfaces Ethernet 10/100, una interfaz de administración, configurado y adecuado para entrar en operación. Este Equipo se está utilizando para controlar y ofrecer el servicio de red inalámbrico.
- Blade 05 - HP Proliant BL460c G8 Intel(R) Xeon(R) CPU E5-2609 0 @ 2.40GHz (4 Cores) 32 GB 2 HDD 350GB c/u Windows 2008 Enterprise Server.
- En este se puede recuperar la plataforma de ISA Server 2006.
- Dos PC de alta configuración HP, Modelo DC5750, AMD Athlon dual core 2,60 GHz, RAM 4 Gb, 1 HDD 250 GB. En estos se puede recuperar la plataforma de ISA Server 2006.
- Backup de las reglas y políticas de seguridad perimetral (firewall) y seguridad interna y de navegación (ISA Server 2006) que se deben implementar en un nuevo equipo que entre en operación.
- Recurso humano, Ingenieros especializados en administración de servidores y storage; Ingenieros especializados en redes y comunicaciones.

## 3. ANALISIS DE RIESGOS

El Análisis de Riesgos consiste en la identificación de los activos (datos, hardware, software, servicios, personal, etc. de valor de la SDS y la determinación del riesgo asociado a cada uno con base en las amenazas y vulnerabilidades que los rodean. El objetivo del Análisis de Riesgo es obtener una visión global del riesgo al que se encuentran expuestos los activos, en función de la probabilidad de que una amenaza pueda llegar a materializarse y el impacto que causaría en la entidad.

Una vez identificados los procesos críticos de la organización y los sistemas informáticos que los soportan, cada uno de éstos últimos contiene activos de información que a su vez dependen de otros componentes críticos como software, hardware e infraestructura diversa diseñados para sostener de forma eficiente dichos procesos críticos. La identificación de los activos y componentes críticos es esencial para conocer qué debe protegerse para clasificarlos mediante criterios basados en su confidencialidad, integridad y disponibilidad.

### 3.1 Marco Conceptual del Análisis de Riesgos

La Gestión de Riesgos en la Secretaria Distrital de Salud, contribuye a la Misión y visión institucional, para ello se establecerán controles frente a los riesgos de seguridad de la información, en lo referente a la plataforma estratégica.

Para el logro de la gestión de riesgos la organización tomó como referencia metodológica la norma AS/NZS 4360 DE 1999 que es base de la norma de ICONTEC (NTC 5254).

La gestión de riesgos de la organización se ha dividido en tres grandes elementos

- Gestión de Activos de Información
- Análisis del Riesgo
- Tratamiento del riesgo

### 3.2 Gestión de los activos de información

Los principios de seguridad de la información, son los parámetros generales, que sirven para garantizar el cumplimiento y entendimiento de las necesidades de seguridad de la organización. Para tal efecto, se ha decidido definir los siguientes principios de seguridad:

| | |
|---|---|
| **Confidencialidad** | Este concepto hace referencia a la prevención de la divulgación no autorizada (confidencialidad), o el acceso no autorizado a cualquier activo de información |
| **Integridad** | Este concepto hace referencia a la prevención sobre la modificación o destrucción de cualquier activo de información, garantizando el no repudio y la autenticidad (integridad) de los mismos. |
| **Disponibilidad** | Se refiere a asegurar el mantenimiento (disponibilidad) de acceso o uso oportuno y confiable de cualquier activo de información de la organización |

### 3.2.1 Activos de Información

Conforme con la norma ISO 27001, un activo de información es “cualquier cosa que tiene valor para la organización”. No obstante, este concepto es bastante amplio, y debe ser limitado por una serie de consideraciones:

- El impacto que para la organización supone la pérdida de cualquier principio de seguridad de cada activo
- El tipo de información que maneja
- Sus productores y consumidores

Para facilitar el trabajo de identificación de los activos de información es indispensable que dichos activos identificados sean categorizados, las siguientes son las categorías definidas para ello (Sugeridas).

| Categoría de Activo | Descripción | Ejemplos de Activo |
|---|---|---|
| **Dato** | Cualquier tipo de información contenida en un medio digital, bien sea en forma de base de datos o en forma de archivos digitales o de intercambio. | Datos, Bases de datos, archivos de documento |
| **Dispositivo** | Cualquier componente de hardware que sea necesario para efectuar o complementar operaciones sobre algún activo de información. | Enrutadores, appliances, POS, lectores de tarjetas |
| **Documento** | Cualquier tipo de información que se encuentre en medio impreso | Documentos impresos |

| Categoría de Activo | Descripción | Ejemplos de Activo |
|---|---|---|
| **Sistema de Almacenamiento de Información** | Hace referencia a cualquier sistema o tecnología para el almacenamiento de datos que sea necesaria para efectuar o complementar alguna operación sobre los activos de información. | Sistemas de almacenamiento de archivos (imágenes, SAN, etc) |
| **Sistema de Información** | Todo sistema que realice operaciones, transacciones y que requiera la interacción de uno o más activos de información para efectuar sus tareas. | Sistemas completos (ERP, sistemas corporativos) |
| **Software** | Cualquier software de cliente final, como suites de ofimática, correo, edición de documentos, etc. | Office, antivirus, etc. |

En caso de ser necesario crear una nueva categoría que tipifique un grupo de activos de información, ésta debe describirse claramente para permitir catalogarlos dentro de la misma.

Si alguno de los activos ya analizados debe ser recategorizado, es importante mantener la historia de su categoría anterior, ya que esto debe reflejarse en los documentos generados y adicionalmente supone una revisión en el análisis de riesgos para el activo recategorizado.

No se considerará activo de información, aquel que no cumpla con ninguno de los criterios especificados anteriormente, ya que no tendrán ningún tipo de tratamiento. Lo mismo sucede cuando no puede ser catalogado dentro de la tipología de activos de información o cuando este no puede ser creado como una nueva categoría.

### 3.2.2 Niveles de Responsabilidad sobre los activos de información

Los niveles de responsabilidad se refieren al papel que juegan los colaboradores de la organización frente a los activos de información, para lo cuales se han definido los siguientes:

| Responsabilidad | Función |
|---|---|
| **Propietario** | Es la Unidad Organizacional donde se genera o produce la información. Sus responsabilidades son:<br><br>• Identificar los activos de información.<br>• Encargarse de la clasificación de sus activos. |

| Responsabilidad | Función |
|---|---|
| **Responsable** | Es un funcionario perteneciente a la Unidad Organizacional propietaria de un grupo de activos de información. Tiene bajo su cargo:<br>• Definir las apropiadas medidas de protección que garanticen la Confidencialidad, Integridad y Disponibilidad del(los) activo(s) de información.<br>• Monitorear que las medidas de protección implementadas sean las adecuadas.<br>• Autorizar y revocar el acceso a aquellas personas que tengan una necesidad de utilizar la información. |
| **Custodio** | Es un funcionario, grupo de funcionarios o una Unidad Organizacional, designados por los propietarios, los cuales se encargan de mantener las medidas de protección establecidas por los responsables sobre los activos de información. |
| **Usuarios** | Son los colaboradores de la organización, quienes están autorizados por el responsable a acceder la información, adicional a ello deben cumplir con todas los requerimientos de control especificados por el propietario o custodio de la información. |

### 3.2.3 Impacto

El impacto es considerado como la consecuencia de que un evento inesperado se presente, causando efectos sobre los activos bien sea a través de una acción deliberada o de una acción accidental, la consecuencia puede generar desde un efecto catastrófico hasta no presentar ningún efecto sobre el o los activos de información de la organización. Normalmente el impacto se mide en términos del efecto o consecuencia que produce afectando los principios de seguridad de la información. La medición del impacto trata de relacionar el efecto o la consecuencia vs el (los) control(es) con los cuales se han tratado de prevenir las condiciones adversas. El impacto puede ser medido de dos maneras: una cualitativa, en la cual son valoraciones subjetivas; u otra cuantitativa como un valor financiero dado a cada activo y cuál es el valor en caso de que dicho activo pueda ser vulnerado.

Para el presente documento, el impacto estará medido de manera cualitativa a través de la siguiente escala, para cada activo conforme a los principios de seguridad:

| Impacto | Valor |
|---|---|
| Mínimo | 1 |
| Bajo | 2 |
| Medio | 3 |
| Alto | 4 |
| Crítico | 5 |

## 3.3 Análisis y Evaluación del Riesgo

Para adelantar el proceso de Gestión de Riesgo, se deben desarrollar las siguientes etapas:

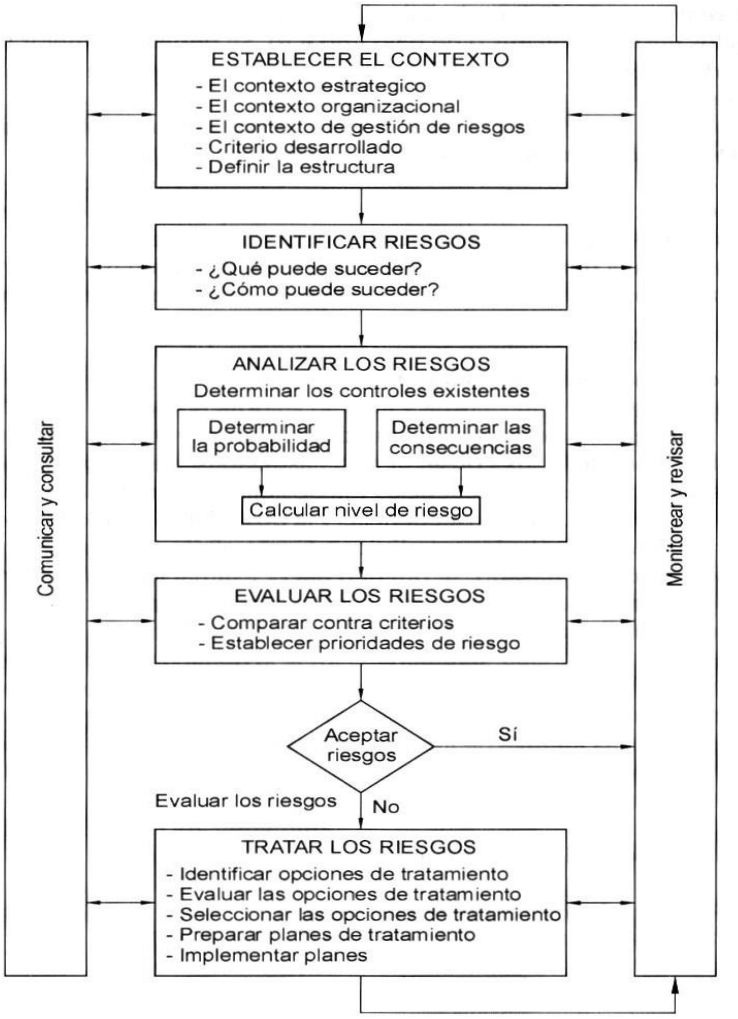



Diagrama de la Norma NTC 5254

### 3.3.1 Identificación de Riesgos

Esta etapa requiere de una visión amplia y de un proceso sistemático debido a que un riesgo no identificado puede afectar de manera significativa un producto o proceso. La identificación debe incluir todos los riesgos que estén o no bajo el control de la institución.

Para identificar el riesgo de un producto o proceso, se debe contestar a las siguientes preguntas:

¿Qué puede suceder?: Lista global de eventos que pueden afectar un producto o proceso, también entendido como las amenazas a un activo de información.

¿Cómo puede suceder?: Determinar las formas de presentarse los diferentes eventos, o las vulnerabilidades que facilitan que se haga efectiva una amenaza.

### 3.3.2 Análisis de riesgos

El análisis busca proporcionar datos que sirvan para la evaluación y el tratamiento de riesgos. Se deben enumerar los riesgos excluidos, siempre que sea posible, a fin de demostrar que el análisis de riesgos es completo.

En la Organización se empleará el análisis cualitativo para obtener un indicador general del nivel de riesgo, este análisis cualitativo emplea escalas numéricas para describir la magnitud de las consecuencias potenciales y la posibilidad de que estas ocurran.

Para estos efectos se evalúan la magnitud de las consecuencias de un evento, si ocurriera, y la probabilidad del evento y sus consecuencias asociadas, en el contexto y los controles existentes. Se combinan las consecuencias y la posibilidad para producir un nivel de riesgo llamado riesgo bruto.

Las variables contempladas para el análisis de riesgo son:
- Activos de Información
- Valoración de los activos
- Amenazas
- Probabilidad de la Amenazas (PA)
- Vulnerabilidades
- Probabilidad de la Vulnerabilidad (PV)
- Probabilidad de Ocurrencia (PO)
- Riesgo Bruto (RB)
- Criticidad Bruta (CB)

Variables adicionales de la matriz de riesgo con:
- Controles Existentes
- Calificación de Gestión (CG)

- Riesgo Neto (RR)
- Criticidad Neta (CR)
- Niveles de Aceptación del Riesgo (NAR)

### 3.3.3 Valoración de los Activos de Información

Así, la identificación de activos de información se hace teniendo en cuenta la importancia que cada "candidato" a ser activo posea dentro del proceso o procedimiento que lo utiliza, y de igual manera la sensibilidad de información que maneja. La valoración de los activos se debe realizar de acuerdo a los criterios de calificación de los activos.

### 3.3.4 Valoración del Riesgo

Con la evaluación de riesgos se pretende separar los riesgos aceptables menores de los mayores, de forma que obtengamos una lista priorizada de riesgos para tomar acciones posteriores. En la Organización se da prioridad a los riesgos que resulten con categoría alta para iniciar el tratamiento de los mismos.

El análisis de riesgo posee su escala de valoración de riesgo, con la cual se da el tratamiento y valoración a los riesgos identificados.

Lo primero que se hace es calcular el riesgo bruto, el cual contempla:

Riesgo Bruto = Impacto (I) * Probabilidad de Ocurrencia (P)

Probabilidad de Ocurrencia (PO): Es el resultado de sumar la probabilidad de una amenaza y la probabilidad de que la vulnerabilidad se concrete y este resultado dividirlo entre dos (2)

$$P_O = (P_A + P_V) /2$$

Al anterior resultado numérico se calcula su escala cuantitativa que se denomina

Criticidad Bruta (CB): Está determinada por la siguiente escala

| **Riesgo Bruto** | **Nomenclatura** | **Criticidad Bruta ($C_B$)** |
|---|---|---|
| **$20 < R_B <= 25$** | C | Crítico |
| **$15 < R_B <= 20$** | A | Alto |
| **$10 < R_B <= 15$** | M | Medio |

| | | |
|---|---|---|
| **$5 < R_B <= 10$** | B | Bajo |
| **$1 < R_B <= 5$** | I | Mínimo |

### 3.3.5 Gestión del Control

La gestión del control es la calificación que se le da a los controles existentes en torno a su efectividad, teniendo como criterios de evaluación la siguiente escala:

| Criterio | Concepto |
|---|---|
| No identificado (1) | La no existencia de controles |
| Identificado (2) | Control o grupo de controles que se sabe deben ser utilizados pero no se encuentra implantado bien sea por que se está planeando o por cualquier otra motivación organizacional |
| Implantado(3) | Control o grupo de controles que solamente se encuentran implantados y operando, pero que no se garantiza la efectividad en su manejo. |
| Funcional(4) | Control o grupo de control que además de ser implantado cuenta con el respaldo de las bunas prácticas y su ejecución se encuentra divulgada y contemplada en procedimientos de apoyo que garantizan su cumplimiento y efectividad |
| Gestionado(5) | Control o grupo de controles integrados y gestionados a partir de un Sistema de Gestión, llevando a cabo un mejoramiento continúo mediante el modelo PHVA contemplado en la norma ISO 27001:2005. Este sería el mayor grado de madurez ya que se contempla no solo implantación, funcionalidad, efectividad sino gestión de mejoramiento continuo |

### 3.3.6 Riesgo Neto

El riesgo neto es la operación que surge entre el valor del riesgo bruto la y evaluación de la gestión de los controles existentes, con el cual se obtiene la criticidad neta resultante del riesgo. El Riesgo Neto se obtiene a través de la siguiente formula.

$$R_N = R_B / C_G$$

La operación anterior da un valor numérico al cual se le calcula su escala cuantitativa denominada

Criticidad Neta (CR): Escala cuantitativa con la que se determina el riesgo después de identificar los controles que se hayan implementado la siguiente escala mide la criticidad neta

| Riesgo Neto | Nomenclatura | Criticidad Neta ($C_R$) |
|---|---|---|
| **20 < $R_N$ <= 25** | C | Crítico |
| **15 < $R_N$ <= 20** | A | Alto |
| **10 < $R_N$ <= 15** | M | Medio |
| **5 < $R_N$ <= 10** | B | Bajo |
| **1 < $R_N$ <= 5** | I | Mínimo |

### 3.3.7 Aceptación del Riesgo

La aceptación del riesgo estará entonces determinada por la siguiente escala:

| Riesgo neto | Nomenclatura | Nivel de Aceptación del Riesgo (NAR) |
|---|---|---|
| **10 < $R_N$ <= 25** | I | Inaceptable |
| **5 < $R_N$ <= 10** | T | Tolerable |
| **1 < $R_N$ <= 5** | A | Aceptable |

### 3.3.8 Identificación de Controles ISO 17799

Después de efectuar el análisis de riesgos para los activos de información desglosados en sus amenazas y vulnerabilidades, es necesario realizar una identificación de los controles de la norma ISO 27001 que son aplicables para cada una de las parejas Amenaza-Vulnerabilidad asociadas a cada activo de información. Esta tarea requiere identificar tanto el Objetivo de Control como los Controles relevantes del Anexo A de la norma en mención.

## 3.4 Tratamiento de riesgos

En el tratamiento del riesgo se incluyen las siguientes etapas:

- Identificar las opciones de tratamiento.
- Evaluar las opciones de tratamiento
- Seleccionar las opciones de tratamiento
- Preparar planes de tratamiento
- Implementar planes.

El siguiente diagrama ilustra el proceso de tratamiento de los riesgos.

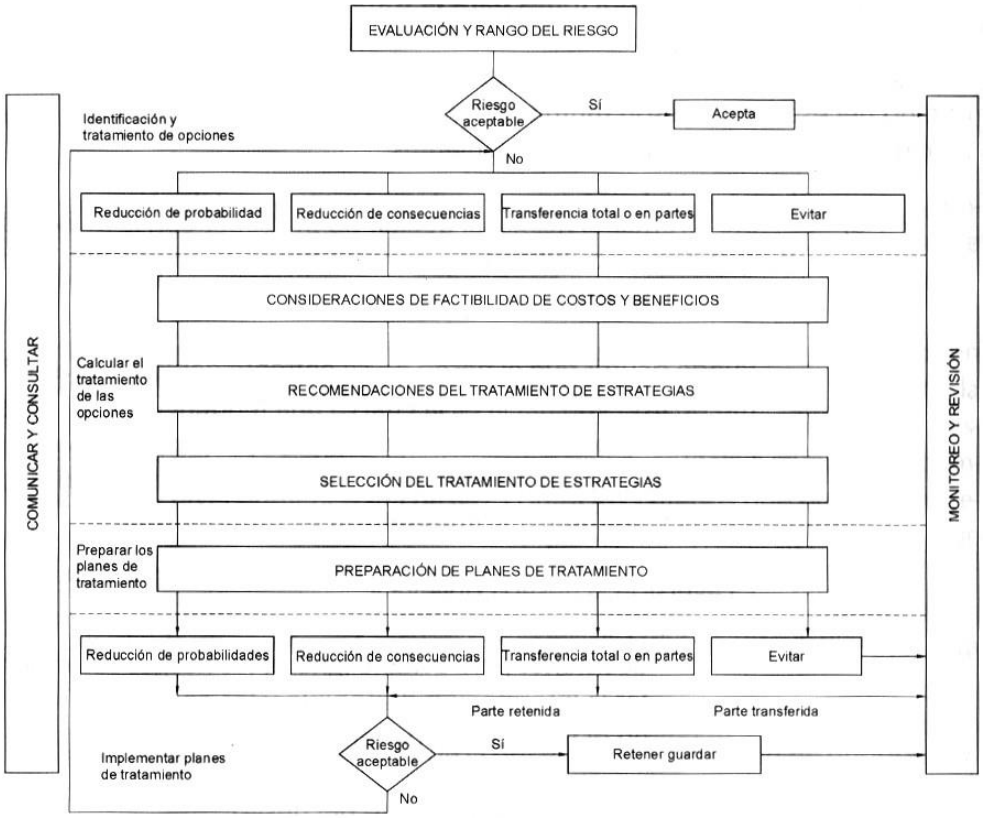



Diagrama de la Norma NTC 5254

Los planes de tratamiento del riesgo se deben plantear en términos de los controles de la Norma ISO 27001 y del manual de buenas prácticas de la norma ISO/IEC17799:2005.

Es importante realizar como etapa inicial del proceso de tratamiento del riesgo la Declaración de Aplicabilidad, como documento de guía y referencia al momento del tratamiento de los riesgos.

Cada vez que se realice el análisis y valoración de los riesgos, o bien se identifiquen nuevos activos de información o nuevos objetivos de control y/o controles para un activo de información previamente analizado, ésta información se debe consignar en el documento respectivo.

### 3.4.1 Planes de Acción para el Tratamiento del Riesgo por Controles

Los planes de acción a generar en la fase de tratamiento del riesgo deben contemplar las posibilidades de reducir (eliminando o minimizando vulnerabilidades asociadas a los activos de información), prevenir, transferir o aceptar el riesgo identificado, teniendo en cuenta la selección de objetivos de control y controles específicos para llevar dicho riesgo a un nivel aceptable. En aquellos casos donde sea identificado un control aplicable, pero que por cualquier circunstancia éste no pueda o no deba ser aplicado para el tratamiento de un riesgo, dicha exclusión debe quedar consignada en la declaración de aplicabilidad.

Es importante aclarar que las vulnerabilidades asociadas a activos de información se pueden eliminar; sin embargo, los riesgos no se eliminan sino que se mitigan o reducen para ser llevados a niveles aceptables.

### 3.4.2 Agrupación de Controles en el Tratamiento

Se han definido dos conceptos de agrupación de los controles de acuerdo con su cobertura y grado de importancia de la siguiente manera:

- Global

Describe los controles que son aplicables a un gran número de activos de información o que tienen un alto nivel de importancia para la organización por el impacto que podría generar su falta de implantación y gestión.

- Específico

Describe los controles que son aplicables a un activo de información o a un grupo específico de ellos que cuentan con características particulares en cada caso. Los controles específicos se han dividido en tres grupos correspondientes a los niveles de aceptación del riesgo establecidos en la matriz de análisis de riesgos (Inaceptables, Tolerables y Aceptables).

Una vez identificado un nuevo control para un activo de información, partiendo de su nivel de aceptación del riesgo (Inaceptables, Tolerables o Aceptables), se debe ubicar dentro de los planes de tratamiento del riesgo y, en consecuencia, definir las acciones a realizar dentro de los mismos. Cada vez que un nuevo control es identificado para un activo de información pueden presentarse dos situaciones; la primera de ellas ocurre cuando el control es completamente nuevo para el nivel de

aceptación del riesgo asociado correspondiente. En éste caso se deben adicionar la nomenclatura del control según la norma ISO 27001 y su descripción.

La segunda situación que se puede presentar cuando un nuevo control es identificado para un activo de información es que se trate de un control ya existente para el nivel de aceptación del riesgo correspondiente, aplicable para otros activos de información previamente analizados. En éste caso, se debe actualizar toda la información relacionada con dicho control adicionando nuevas vulnerabilidades tratadas (de ser necesario), nueva evidencia objetiva (de ser necesario) y el activo de información para el cual fue identificado el control.

### 3.4.3 Guía de Tratamiento del Riesgo

Cada vez que se adiciona un control en el plan de tratamiento del riesgo, de acuerdo con los niveles de aceptación del riesgo del mismo, se debe definir una Guía de Tratamiento que comprende las acciones, actividades y recomendaciones a llevar a cabo para la implementación o mejora de la efectividad del control.

De acuerdo al nivel de aceptación del riesgo se define qué es lo que el control debe hacer o cual debe ser su foco de operación. La siguiente tabla representa las acciones de acuerdo a los niveles de aceptación del riesgo.

| NIVEL ACEPTACION RIESGO | ACCIONES DEL CONTROL(ES) |
|---|---|
| Inaceptable (I) | Minimizar<br>Eliminar<br>Transferir |
| Tolerable (T) | Oportunidad de Mejoramiento<br>Transferir |
| Aceptable (A) | Aceptar<br>Transferir |

Posteriormente, se deben definir todas las actividades necesarias para implantar el control o las recomendaciones para mejorar la efectividad del mismo y llevar así el riesgo a un nivel aceptable. Para efectuar esta tarea se debe tener en cuenta el manual de buenas prácticas de la norma ISO/IEC17799:2005.

Adicionalmente, una vez ha sido implantado el control identificado (bien sea éste nuevo o simplemente mejorado) se debe recalificar la efectividad del control especificada en la matriz de riesgos.

### 3.4.4 Valoración del Plan de Tratamiento del Riesgo

La valoración del tratamiento de un riesgo específico desde el punto de vista del plan de acción, está determinada por dos variables las cuales contemplan la forma en cómo un tratamiento debe ser llevado a cabo, para lo cual se tienen los siguientes criterios:

### 3.4.5 Variable 1: Valoración de la Prioridad de Tratamiento de Riesgo

A continuación se determina la forma en cómo se debe tratar el riesgo y cuál debe ser la prioridad a la hora de implementar los controles que se han identificado para cada uno de los riesgos, a partir de los valores de Criticidad Neta y nivel de Aceptación del Riesgo establecidos durante la fase de análisis de riesgos, se debe establecer la Prioridad de Tratamiento de Riesgo (PTR) de la siguiente manera:

| PRIORIDAD DE TRATAMIENTO DEL RIESGO | CRITICIDAD NETA Y NIVEL ACEPTACION RIESGO |
|---|---|
| Crítica (C) | Inaceptables (CI) |
| Alta (A) | Inaceptables (AI) |
| Media (M) | Inaceptables (MI) |
| Baja (B) | Tolerables, entender como Oportunidad de Mejoramiento |
| Mínima (I) | Aceptables, Revisar Evidencia Objetiva |

Lo anterior se interpreta de la siguiente manera, aquellos riesgos que tienen una criticidad neta (Crítica), y que su Nivel de Aceptación de Riesgo es (Inaceptable), tendrán una prioridad Crítica a la hora del tratamiento del riesgo, de la misma manera se efectúa la lectura para los demás niveles expresados en la tabla.

### 3.4.6 Variable 2: Valoración de la Complejidad de Tratamiento del Riesgo

La siguiente actividad dentro de la fase de tratamiento del riesgo es definir el grado subjetivo de Complejidad (medida en costo estimado, tiempo y esfuerzo) de un tratamiento específico de la siguiente manera:

Alta (A - Requiere alta inversión en dinero y recursos)
Media (M – Requiere inversión moderada en dinero y recursos)
Baja (B - Es Fácilmente ejecutable, probablemente sin inversión)

### 3.4.7 Relación de Vulnerabilidades Tratadas

Es importante que por cada control que se ha identificado se relacionen las vulnerabilidades a las cuales dicho control puede ayudar a mitigar, partiendo de lo identificado en el análisis de riesgos

### 3.4.8 Relación de Evidencia Objetiva

Al momento de implementar los controles definidos para tratar uno o más vulnerabilidades, se recomienda relacionar de la misma manera la evidencia objetiva de que dicho control ha sido implementado, ya que ésta es la prueba de que la acción definida ha sido correctamente ejecutada y garantiza que ha habido continuidad sistemática en su aplicación.

### 3.4.9 Relación de Activos de Información

Teniendo en cuenta que el tratamiento de riesgos está dado en términos de los controles que se recomienda implementar y no en términos de cada activo de información (ya que un control puede aplicar a uno o más activos), es importante como parte del proceso relacionar sobre cual o cuales activos de información dicho control tiene efecto.

## 3.5 Monitoreo

Esta etapa es transversal a todo el proceso de Gestión de Riesgos. Representa un proceso cíclico cuyo resultado puede ser modificado por nuevos cambios en el riesgo, por lo cual hace necesaria su constante revisión para validar la efectividad del proceso, su desarrollo y su permanencia. En la Organización son responsables del monitoreo: El dueño del proyecto, proceso o producto, la Gerencia de Planeación, y la Contraloría.

### 3.5.1 Responsabilidades

- Cada dueño o líder de proceso (Propietario de Información) será el

responsable por la Gestión de Riesgos en el respectivo proceso o proyecto.

- La Gerencia Financiera cumple una labor de promoción y despliegue de la Autogestión de Riesgos en la institución.
- La Auditoría Interna cumple una labor de aseguramiento sobre la base del plan de trabajo.

A nivel de seguimiento, y sin perjuicio de la responsabilidad del líder de proceso o proyecto frente a su plan de mitigación de riesgos particular, se establece un Comité de Seguimiento al Panorama de Riesgos conformado por las Vicepresidencias Ejecutiva y Financiera, la Gerencia de Planeación y la Auditoría Interna que se reunirán trimestralmente. El panorama de riesgo identificado por Sistemas (Seguridad de la Información) deberá constituirse como un insumo de SARO.

## 3.6 Marco Conceptual de la Gestión de Incidentes

La Respuesta a Incidentes es un proceso de asesoramiento para dar soporte reactivo ante violaciones de la integridad de los sistemas de información de la organización.

Al producirse un incidente de seguridad, se debe trabajar para identificar su origen, establecer sus consecuencias, minimizar su impacto y coordinar su resolución. Posteriormente se deben establecer medidas que puedan ayudar a evitar situaciones similares en el futuro.

### 3.6.1 Definición de Incidente de Seguridad

Los incidentes son eventos adversos que amenazan la seguridad de los sistemas de información o redes de computadoras, entendidos como eventos observables, con la intención de producir beneficio económico, fraude, dolo, entre otros. Estos eventos pueden clasificarse de la siguiente manera:

- Conexiones a Sistemas
- Acceso a archivos
- Apagado

Algunos de los eventos adversos más comunes son:

- Acceso no autorizado

- Abuso de permisos y privilegios
- Denegación de servicios
- Uso no autorizado de sistemas para el procesamiento o almacenamiento de datos
- Cambios a las características del hardware, firmware o software del sistema sin consentimiento
- Packet Flooding
- Crashes

En general, todo aquello que atente contra la Integridad, Disponibilidad y Confidencialidad de la Información.

### 3.6.2 Incidentes Internos

Son aquellos incidentes relacionados con las personas, principalmente empleados de la organización que cumplen con una de estas características:

- Administradores experimentados de los sistemas de la organización
- Empleados “inquietos” con conocimientos técnicos superiores
- Empleados disgustados por alguna situación interna de la organización

Los tipos de incidentes internos más comunes son:

- Uso indebido de los recursos informáticos
- Denegación de servicios
- Manipulación de datos
- Eliminación de datos
- Denegación de accesos

Usualmente los atacantes internos requieren de la ayuda de otras personas. Las áreas de Recursos Humanos y Legal juegan un papel decisivo en la conducción de investigaciones sobre ataques internos. Además, el departamento de Relaciones Públicas debe estar informado para llevar a cabo el respectivo manejo de medios cuando sea necesario.

Existen algunas situaciones especiales que deben ser consideradas para prevenir la ocurrencia de incidentes internos de seguridad. Estas situaciones son, entre otras:

- Terminación de contrato de directivos de la organización.

- ❖ Terminación de contrato de personal clave de la organización (experimentado, de larga trayectoria en la misma).
- ❖ Terminación de contrato de algún administrador de sistemas.
- ❖ Terminación de contrato de un oficial de seguridad informática.

### 3.6.3 Objetivos

La respuesta a incidentes de seguridad tiene los siguientes propósitos:

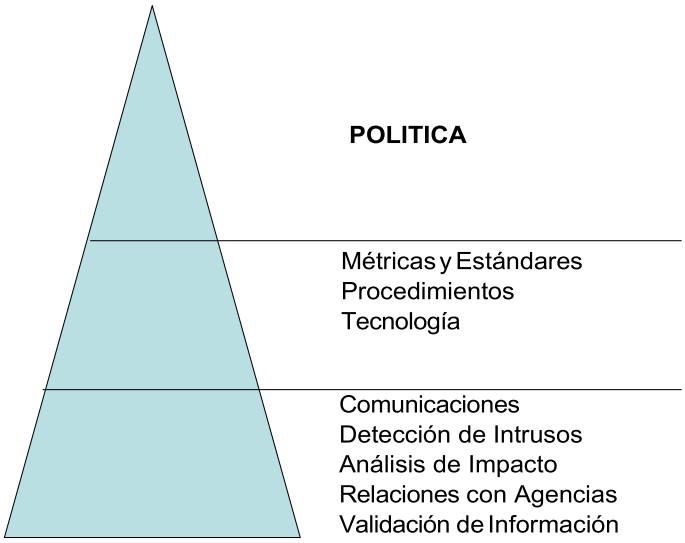
- ❖ Definir un Plan de Respuesta a Incidentes que permita resolver cualquier incidente de la manera más rápida y eficaz posible.
- ❖ Minimizar la cantidad y gravedad de los incidentes de seguridad.
- ❖ Conformar y Administrar un CSIRT principal (Computer Security Incident Response Team, Equipo de respuesta a incidentes de seguridad informática).

### 3.6.4 Justificación

La respuesta apropiada a un incidente debe ser una parte esencial de las directrices de seguridad de la información y de la estrategia de mitigación de riesgos de la organización.
El hecho de responder a los incidentes de seguridad tiene ventajas directas evidentes. No obstante, también pueden existir ventajas financieras indirectas. Cuando la organización es un proveedor de servicios, un plan formal de respuesta a incidentes puede ayudarle a aumentar su negocio, ya que muestra que se toma en serio el proceso de seguridad de la información.

## 3.7 Guía para la Gestión de Incidentes

Desarrollar una arquitectura de respuesta a incidentes de seguridad resulta bastante crítico, puesto que define los componentes de la capacidad de la respuesta a incidentes de la organización y como éstos componentes están interrelacionados. Algunos posibles componentes son: política, procedimientos, tecnología, detección de intrusos y comunicaciones, entre otros.




### 3.7.1 Enfoque Metodológico

El hecho de utilizar una metodología para el análisis y respuesta de incidentes provee los siguientes beneficios:

- Estructura y Organización, lo cual permite controlar, organizar y mantener.
- Eficiencia, lo cual permite responder cuánto dura una respuesta a un incidente y cuánto cuesta.
- Facilidad del proceso de atención del incidente, lo cual facilita la organización y el control en la respuesta a un incidente.
- Manejo de los inesperado, lo cual conlleva al aprendizaje a partir de cada incidente.
- Consideraciones Legales, lo cual permite analizar el impacto de una respuesta incompetente.

### 3.7.2 Definición de un Plan de Respuesta a Incidentes

El plan de Respuesta a Incidentes debe ser fácilmente accesible para todo el personal, en forme de política conforme al documento 1 – Metodología para la creación de Políticas de tal manera que pueda garantizar que, cuando se produzca un incidente, se seguirán los procedimientos correctos.

El ciclo de vida de los incidentes es como se describe a continuación, siguiendo la metodología PDCERF:

- Preparación (Preparation)
- Detección (Detection)
- Contención (Containment)
- Erradicación (Eradication)
- Recuperación (Recovery)
- Seguimiento (Follow Up)

**Preparación.** Incluye las siguientes actividades:

- Generar un conjunto de defensas o controles para mitigar un riesgo o una amenaza potencial.
- Crear conjuntos de procedimientos para manejar los incidentes de la manera más eficiente posible (incluyendo los pasos a seguir, quien debe ser contactado, clasificación especial de la información, prioridades, roles y responsabilidades, límites de riesgo aceptables).
- Obtener recursos y personal necesario para afrontar los problemas.
- Establecer una infraestructura para soportar las actividades relacionadas con la respuesta a incidentes.

Para incidentes internos se deben tener en cuenta las siguientes consideraciones:

- Crear políticas, normas, procedimientos y estándares que definan el comportamiento adecuado y no adecuado para los usuarios de sistemas de información y en general para la utilización de los recursos tecnológicos.
- Hacer de obligatoria aceptación las políticas de seguridad establecidas, como parte del contrato de trabajo y/o del reglamento interno de trabajo.
- Adecuada investigación del pasado de los empleados, en áreas como social, bancaria y penal.
- Asegurarse de la existencia de roles y responsabilidades de los usuarios y manejar un adecuado control de acceso físico y lógico de acuerdo a las políticas y los roles establecidos.

**Detección.** Incluye las siguientes actividades:

- Utilizar software especializado para detectar posibles anomalías (ataques sobre la red, comportamiento inusual de usuarios, accesos en horarios extraños, intentos de acceso no exitosos, inconsistencias en los registros de acceso, fallos de rendimiento de la máquina, intentos de ingeniería social, etc.)
- Acciones y Reacciones Iniciales encaminadas a: analizar todas las anomalías, habilitar o endurecer la auditoria, realizar respaldos de todos los

sistemas comprometidos durante el incidente y documentar todo.
- ❖ Estimar el alcance del incidente.
- ❖ Reportar el incidente.

Para incidentes internos se deben tener en cuenta las siguientes consideraciones:

- ❖ Utilización de detectores de intrusos de host y de red.
- ❖ Revisión de los accesos inusuales, principalmente fallidos, reincidentes y en horarios fuera del trabajo.
- ❖ La detección en este caso no solo puede ser digital, sino también formar parte de un factor humano.

**Contención.** Las siguientes son algunas estrategias de contención:
- ❖ Apagado del sistema (drástico pero en muchos casos importante para prevenir pérdida o corrupción de datos, así como el mantenimiento de evidencia de medios no-volátiles.
- ❖ Desconexión de la red.
- ❖ Modificación dinámica de reglas en los firewalls o elementos de protección.
- ❖ Bloqueo de cuentas de usuario posiblemente comprometidas.
- ❖ Incremento del nivel de monitoreo en la red o de la auditoria de los sistemas.
- ❖ Colocación de Trampas (por ejemplo, honeypots).
- ❖ Bloqueo de servicios potencialmente comprometidos.

**Erradicación.** Las siguientes son algunas estrategias de erradicación:
- ❖ Identificar procedimientos específicos para cada sistema operativo comprometido.
- ❖ Identificar usuarios o servicios potencialmente comprometidos y eliminarlos.
- ❖ Recuperar backups de fecha y fuente confiables con control de integridad.
- ❖ Reinstalar desde medios de fuente confiable con control de integridad.

**Recuperación.** Las siguientes son algunas estrategias de recuperación:
- ❖ Asegurar la no existencia del elemento o agente que causó el incidente inicial (si ha sido identificado).
- ❖ Realizar la recuperación de datos / programas / configuraciones específicas de los sistemas comprometidos.
- ❖ Actualización, instalación de parches, revisión de seguridad de los sistemas comprometidos y réplica en los sistemas similares.
- ❖ Habilitar auditoria en un nivel más alto de lo normal.

**Seguimiento.** Incluye las siguientes actividades:

- Comprobar que todo vuelve a la normalidad y se mantiene estable de esa manera
- Obtener retroalimentación permanente acerca de los sistemas comprometidos y recuperados
- Obtener información importante en caso de procesos legales o administrativos internos
- Obtener métricas nuevas que permitan mejorar día a día la respuesta a incidentes y la orientación de sus esfuerzos
- Aprender las lecciones (técnicas, administrativas, de procedimiento, etc.)

### 3.7.3 Evaluación del Impacto y costos de un incidente

Para la constante retroalimentación del proceso, es importante establecer mecanismos de evaluación del impacto de cada incidente, en la fase de seguimiento cuando el incidente se ha presentado ya o en la fase de preparación cuando el incidente es una posibilidad de acuerdo con lo identificado en el análisis de riesgos. Estos mecanismos generalmente se basan en un BIA (Business Impact Analysis).

Cuando se ha presentado un incidente, es recomendable en la fase de seguimiento alimentar una base de conocimiento de los incidentes ocurridos, sus características técnicas e impacto en la organización de manera que sea posible tomar medidas preventivas para que el incidente no se repita.

## 3.8 Activos de la SDS

Por activos se entiende al conjunto de elementos con valor informativo y operacional que son propiedad de una empresa, institución o individuo, y que reflejan su actividad, corresponde también a Información de diferentes tipos con los que una organización desarrolla su actividad y que suelen ser vitales para el desarrollo del modelo de negocio de la organización.
Los activos pueden agruparse en las siguientes categorías:

- Activos de información: ficheros y bases de datos, documentación del sistema, manuales de usuarios, material de formación, procedimientos operativos o de soporte, planes de continuidad, configuración del soporte de recuperación, información archivada.
- Activos de software: software de aplicación, software del sistema, herramientas, programas de desarrollo y utilidades.
- Archivos físicos: equipos de tratamiento (servidores, monitores, portátiles, módems), equipo de comunicaciones (routers, firewalls, centrales digitales,

máquinas de fax), medios magnéticos (discos y cintas), muebles, etc.
- Servicios: servicios de tratamiento y comunicaciones, servicios generales (calefacción, alumbrado, energía, aire acondicionado).
- Humano: personas, y sus calificaciones, capacidades y experiencia.
- Intangibles: tales como la reputación y la imagen de la organización.

NOTA: Se diligencia con formato de la Comisión Distrital de Sistemas una matriz de inventarios de todos los activos de información de la SDS.

La responsabilidad de cada activo debe estar asignada sobre cada propietario por lo que se procederá a designar un responsable para cada recurso o grupos de recursos el cual asumirá en un futuro la tarea de mantener los controles apropiados y vigentes. El término “propietario” identifica una persona o entidad que cuenta con la responsabilidad gerencial aprobada de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término “propietario” no significa que la persona en realidad tenga algún derecho de propiedad sobre el activo.

El propietario del activo debiera ser responsable de:

- ✓ Asegurar que la información y los activos asociados con los medios de procesamiento de la información sean clasificados apropiadamente.
- ✓ Definir y revisar periódicamente las restricciones y clasificaciones de acceso, tomando en cuenta las políticas de control de acceso aplicables.

La propiedad puede ser asignada a:

- ✓ un proceso comercial;
- ✓ un conjunto de actividades definido;
- ✓ una aplicación; o
- ✓ un conjunto de data definido.
- ✓ Otra información

La información tiene varios grados de criticidad y sensibilidad y debería utilizarse un sistema de clasificación para garantizar una gestión del riesgo adecuada. Una serie de procedimientos organizativos avalarán que en primer lugar, la información se encuentre efectivamente clasificada y que cualquier cambio o creación de un activo de información reciba la tipificación adecuada y la destrucción de cualquier recurso de información sea gestionado de forma acorde al nivel definido.

Siguiendo los criterios definidos en la mayoría de modelos como MAGERIT e ISO17799 se crearán los criterios de clasificación de la información y recursos en función de:

- Nivel de confidencialidad asociada a la información derivados del marco regulador externo o criterios internos.
- Necesidad de disponibilidad del recurso en función del número de personas afectadas por indisponibilidad, funcionamiento irregular, pérdida de imagen y tiempo de recuperación
- Inversión económica de reposición ante la pérdida.
- Nivel de pérdida de integridad del activo (cuanto más alto es el nivel más probable será que éste pierda su integridad)

Se elaborará una Guía de Clasificación de la Información que contendrá todos los procedimientos necesarios para gestionar el ciclo de vida de la información especialmente en lo relativo al denominado sobre-clasificación o clasificación por exceso de información que con el tiempo o por cambios legales pasó a tener niveles inferiores. Igualmente se considerarán el número de categorías de clasificación adecuadas en función de la problemática legal, organizativa y técnica de la compañía. Normalmente se contemplarán los siguientes niveles:

- Desclasificado, considerado público y sin requisitos de control de acceso y confidencialidad.
- Compartido, recursos que son compartidos entre grupos o personas no pertenecientes a la organización.
- Sólo compañía, acceso restringido a los empleados de la organización Confidencial, acceso restringido a una lista específica de personas
- Si el proyecto lo requiere procederá a desarrollarse las Listas de Control de Acceso de información que especificará quién puede acceder a qué.

La Guía de Clasificación contendrá los procedimientos de marcado y tratado de la información de acuerdo con el esquema definido durante el proyecto y adoptado por la entidad. Los procedimientos cubrirán actividades como copia, almacenamiento, transmisión electrónica de documentos, transmisión oral (telefonía móvil, transmisión de voz, máquinas de respuesta automática) y destrucción. El marcado reflejará la clasificación de acuerdo con las reglas establecidas en elementos como informes impresos, pantallas, medios de almacenamiento, mensajes electrónicos y transferencias de ficheros.

| Activo de Información | Valoración Activo (Impacto) | Amenazas | Probabilidad Amenaza | Vulnerabilidades | Probabilidad Vulnerabilidad | Probabilidad de Ocurrencia | Cálculo de Riesgo Neto | Criticidad Neta | Controles Existentes | Calificación de Gestión | Riesgo Residual | Criticidad Residual | Aceptación del Riesgo | Objetivos de Control | Controles |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Bases de datos | 4 | Acceso lógico no autorizado | 4 | Falta de revisión de la auditoría a la actividad sobre el sistema de información | 3 | 4 | 14 | **M** | Se revisa únicamente cuando es necesario, pero no se tienen procedimientos de revisión de logs. | 2 | 7 | **B** | **T** | A.10.10 - Monitoreo | A.10.10.1 - Registros de Auditoría<br>A.10.10.2 - Monitoreo del Uso del Sistema<br>A.10.10.3 - Protección de los Registros de Auditoría |
| Bases de datos | 4 | Acceso no autorizado con privilegios de administrador | 3 | Acceso de los desarrolladores a ambientes productivos | 4 | 4 | 14 | **M** | No existe control | 2 | 7 | **B** | **T** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.11.2 - Gestión de Acceso de Usuarios | A.10.1.2 - Gestión del Cambio<br>A.10.1.3 - Segregación de Funciones<br>A.10.1.4 - Separación de Ambientes |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | de Desarrollo, Prueba y Producción A.11.2.2 - Gestión de Privilegios A.11.2.4 - Revisión de derechos de Acceso |
| Bases de datos | 4 | Acceso no autorizado al sistema con privilegios de administrador | 3 | Falta de revisión de la auditoría a la actividad sobre el sistema de información | 3 | 3 | 12 | **M** | Se revisa únicamente cuando es necesario, pero no se tienen procedimientos de revisión de logs. | 2 | 6 | **B** | **T** | A.10.10 - Monitoreo | A.10.10.1 - Registros de Auditoría A.10.10.2 - Monitoreo del Uso del Sistema A.10.10.3 - Protección de los Registros de Auditoría |
| Bases de datos | 4 | Cambios de la configuración del sistema | 3 | Acceso de los desarrolladores a ambientes productivos | 4 | 4 | 14 | **M** | No existe control | 2 | 7 | **B** | **T** | A.10.1 - Procedimientos y Responsabilidades Operativas A.11.2 - Gestión de Acceso de Usuarios | A.10.1.2 - Gestión del Cambio A.10.1.3 - Segregación de Funciones A.10.1.4 - Separación de Ambientes de Desarrollo, Prueba y Producción A.11.2.2 - Gestión de Privilegios A.11.2.4 - |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | Revisión de derechos de Acceso |
| Bases de datos | 4 | Errores de programación | 3 | Acceso de los desarrolladores a ambientes productivos | 4 | 4 | 14 | **M** | Se tiene un esquema pruebas, para validar los cambios antes de llevarlos a producción. Estas pruebas se realizan en la estación de trabajo del desarrollador. | 2 | 7 | **B** | **T** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.11.2 - Gestión de Acceso de Usuarios | A.10.1.2 - Gestión del Cambio<br>A.10.1.3 - Segregación de Funciones<br>A.10.1.4 - Separación de Ambientes de Desarrollo, Prueba y Producción<br>A.11.2.2 - Gestión de Privilegios<br>A.11.2.4 - Revisión de derechos de Acceso |
| Bases de datos | 4 | Acceso lógico no autorizado al sistema | 4 | Debilidad en las contraseñas | 3 | 4 | 14 | **M** | Aunque almacena las contraseñas cifradas, no se tienen definidas o no se aplican políticas de contraseñas. | 3 | 5 | **I** | **A** | A.11.1 - Requerimientos de Negocio para el Control de Acceso<br>A.11.3 - Responsabilidades del Usuario | A.11.1.1 - Política de Control de Acceso<br>A.11.3.1 - Uso de Contraseñas |
| Bases de datos | 4 | Acceso lógico no autorizado al sistema | 4 | La comunicación no se maneja por un canal encriptado. | 5 | 5 | 18 | **A** | No existe control | 1 | 18 | **A** | **I** | A.10.9 - Servicios de Comercio Electrónico | A.10.9.2 Transacciones el línea A.12.3.1. |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | A.12.3 - Controles criptograficos | Política de uso de los controles criptográficos |
| Bases de datos | 4 | Errores de programación | 3 | Falta de controles sobre la gestión del cambio | 3 | 3 | 12 | **M** | Se tiene un esquema pruebas, para validar los cambios antes de llevarlos a producción. Estas pruebas se realizan en la estación de trabajo del desarrollador. Los cambios son aprobados por el área dueña del aplicativo. | 1 | 12 | **M** | **I** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.12.5 - Seguridad en los procesos de Desarrollo y Soporte | A.10.1.1 - Procedimientos Operativos Documentados<br>A.10.1.2 - Gestión del Cambio<br>A.12.5.1 - Procedimientos de Control de Cambios |
| Bases de datos | 4 | Fallas de software | 3 | Falta de controles sobre la gestión del cambio | 3 | 3 | 12 | **M** | Todos los cambios en la aplicación son aprobados y validados en un ambiente de pruebas. Se dejan actas de los cambios realizados. | 4 | 3 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.12.5 - Seguridad en los procesos de Desarrollo y Soporte | A.10.1.1 - Procedimientos Operativos Documentados<br>A.10.1.2 - Gestión del Cambio<br>A.12.5.1 - Procedimientos de Control de Cambios |
| Bases de datos | 4 | Acceso físico no autorizado al servidor | 2 | Ubicación inadecuada del servidor | 1 | 1 | 4 | **I** | El servidor esta alojado en el Centro de Computo del contratista, el cual cuenta con las medidas de seguridad adecuadas. | 4 | 1 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.1 - Perímetro de Seguridad Física<br>A.9.1.2 - Controles de Acceso Físico<br>A.9.1.6 - Acceso Público, y |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | Areas de Carga y Descarga |
| Bases de datos | 4 | Acceso físico no autorizado al servidor | 2 | Falta de controles de acceso físico | 1 | 2 | 6 | **B** | El acceso físico al servidor esta restringido por la ETB. | 4 | 2 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.1 - Perímetro de Seguridad Física<br>A.9.1.2 - Controles de Acceso Físico<br>A.9.1.6 - Acceso Público, y Areas de Carga y Descarga |
| Bases de datos | 4 | Problemas de temperatura y humedad | 2 | Ubicación en áreas susceptibles a temperaturas y humedad extremas | 2 | 2 | 8 | **B** | En el Centro de Computo del contratista se hace control de las condiciones ambientales | 4 | 2 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.4 - Protección contra amenazas externas y ambientales |
| Bases de datos | 4 | Problemas de temperatura y humedad | 2 | Monitoreo inadecuado de las condiciones ambientales | 1 | 2 | 6 | **B** | En el Centro de Computo de la SDS se hace control de las condiciones ambientales.<br>Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable del mantenimiento de los mismos. | 4 | 2 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.4 - Protección contra amenazas externas y ambientales |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Bases de datos | 4 | Problemas de temperatura y humedad | 2 | Falta de planes de contingencia | 1 | 2 | 6 | **B** | En la actualidad no se tienen definidos planes de contingencia para ninguno de los servidores sobre los que opera este sistema de información.<br>Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable de la contingencia de los mismos. | 4 | 2 | **I** | **A** | A.14.1 - Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio | A.14.1.1 - Incluir la Seguridad de la Información en el proceso de Continuidad del Negocio<br>A.14.1.2 - Continuidad del Negocio y Análisis de Riesgos<br>A.14.1.3 - Desarrollo e Implementación de Planes de Continuidad incluyendo Seguridad de la Información<br>A.14.1.4 - Marco de referencia para la planeación de Continuidad del Negocio<br>A.14.1.5 - Prueba, mantenimiento y reevaluación de los Planes de Continuidad |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | del Negocio |
| Bases de datos | 4 | Acceso lógico no autorizado al sistema | 4 | Falta de controles de acceso lógico | 4 | 4 | 16 | **A** | El mecanismo de acceso a la aplicación es a través de usuario y contraseña, tanto para los usuarios normales, como para los usuarios administradores. | 3 | 5 | **B** | **T** | A.11.2 - Gestión de Acceso de Usuarios<br>A.11.3 - Responsabilidades del Usuario | A.11.2.2 - Gestión de Privilegios<br>A.11.2.3 - Gestión de Contraseñas de Usuario<br>A.11.2.4 - Revisión de derechos de Acceso<br>A.11.3.1 - Uso de Contraseñas<br>A.11.3.2 - Equipos Desatendidos<br>A.11.3.3 - Política de escritorio y Pantalla Limpia |
| Bases de datos | 4 | Acceso lógico no autorizado al sistema | 4 | Préstamo de usuarios y contraseñas | 3 | 4 | 14 | **M** | Los usuarios administradores, tiene un único usuario y contraseña. Para los usuarios normales, no | 3 | 5 | **I** | **A** | A.11.3 - Responsabilidades del Usuario | A.11.3.1 - Uso de Contraseñas |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | se tienen políticas de contraseñas. | | | | | | | |
| Bases de datos | 4 | Errores de programación | 3 | Procedimientos inadecuados del ciclo de vida de desarrollo de sistemas | 3 | 3 | 12 | **M** | Se utilizan metodologías RUP y Agile XP RUP | 4 | 3 | **I** | **A** | A.12.1 - Requerimientos de Seguridad en Sistemas de Información | A.12.1.1 - Requerimientos de Seguridad en Análisis y Especificación |
| Bases de datos | 4 | Errores de programación | 3 | Falta de conocimiento de los desarrolladores | 2 | 3 | 10 | **B** | Los desarrolladores internos son certificados en el tema. Otras aplicaciones son contratadas con terceros especialistas en desarrollo. | 4 | 3 | **I** | **A** | A.8.1 - Previo a la Contratación<br>A.8.2- Durante la Contratación | A.8.1.3 - Términos y Condiciones de Empleo<br>A.8.2.2 - Educación, Capacitación y Concientización en Seguridad de la Información |
| Bases de datos | 4 | Errores de programación | 3 | Supervisión inadecuada al grupo de desarrolladores | 3 | 3 | 12 | **M** | Se realiza seguimiento por medio de cronogramas | 4 | 3 | **I** | **A** | A.10.10 - Monitoreo | A.10.10.1 - Registros de Auditoría<br>A.10.10.2 - Monitoreo del Uso del Sistema<br>A.10.10.3 - Protección de los Registros de Auditoría<br>A.10.10.4 - Registros de Administració |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | n y de Operación A.10.10.5 - Registro de Fallas |
| Bases de datos | 4 | Fallas de hardware | 3 | Monitoreo inadecuado de las condiciones ambientales | 1 | 2 | 8 | **B** | En el Centro de Computo de la SDS se hace control de las condiciones ambientales. Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable del mantenimiento de los mismos. | 4 | 2 | **I** | **A** | A.9.1 - Áreas Seguras | A.9.1.4 - Protección contra amenazas externas y ambientales |
| Bases de datos | 4 | Fallas de hardware | 3 | Mantenimiento inadecuado del servidor | 2 | 3 | 10 | **B** | Se tiene un contrato de mantenimiento de servidores con una empresa externa, sin embargo, la renovación anual del contrato no es inmediata, por lo que existe un periodo de "inestabilidad", entre el vencimiento y la nueva contratación. Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable del mantenimiento de los mismos. | 3 | 3 | **I** | **A** | A.9.2 - Seguridad del equipamiento A.10.2 - Gestión de Servicios Prestados por Terceros | A.9.2.4 - Mantenimiento de Equipos A.9.2.7 - Extracción de la Propiedad A.10.2.1 - Prestación del Servicio |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Bases de datos | 4 | Fallas de hardware | 3 | Falta de planes de contingencia | 1 | 2 | 8 | **B** | En la actualidad no se tienen definidos planes de contingencia para ninguno de los servidores sobre los que opera este sistema de información.<br>Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable de la contingencia de los mismos. | 4 | 2 | **I** | **A** | A.14.1 - Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio | A.14.1.1 - Incluir la Seguridad de la Información en el proceso de Continuidad del Negocio<br>A.14.1.2 - Continuidad del Negocio y Análisis de Riesgos<br>A.14.1.3 - Desarrollo e Implementación de Planes de Continuidad incluyendo Seguridad de la Información<br>A.14.1.4 - Marco de referencia para la planeación de Continuidad del Negocio<br>A.14.1.5 - Prueba, mantenimiento y reevaluación de los Planes de Continuidad |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | del Negocio |
| Bases de datos | 4 | Fallas de software | 3 | Falta de conocimiento del administrador del sistema | 2 | 3 | 10 | **B** | Los desarrolladores internos son certificados en el tema. Otras aplicaciones son contratadas con terceros especialistas en desarrollo. | 4 | 3 | **I** | **A** | A.8.1 - Previo a la Contratación<br>A.8.2- Durante la Contratación | A.8.1.3 - Términos y Condiciones de Empleo<br>A.8.2.2 - Educación, Capacitación y Concientización en Seguridad de la Información |
| Bases de datos | 4 | Fallas de software | 3 | Falta de actualización periódica de versiones o parches sobre el sistema operativo | 2 | 3 | 10 | **B** | Se tiene implementado y en funcionamiento el aplicativo WSUS, con el cual se actualizan los parches de los servidores Windows. | 4 | 3 | **I** | **A** | A.12.5 - Seguridad en los Procesos de Desarrollo y Soporte<br>A.15.2 - Cumplimiento Técnico, de Política de Seguridad y Estándares | A.12.5.1- Procedimientos de Control de Cambios<br>A.12.5.2 - Revisión Técnica de Aplicaciones después de Cambios al Sistema Operativo<br>A.15.2.1 - Cumplimiento |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | con Políticas y Estándares de Seguridad |
| Bases de datos | 4 | Software malicioso | 4 | Supervisión inadecuada al grupo de desarrolladores | 4 | 4 | 16 | **A** | Se realiza seguimiento por medio de cronogramas | 3 | 5 | **B** | **T** | A.10.10 - Monitoreo | A.10.10.1 - Registros de Auditoría<br>A.10.10.2 - Monitoreo del Uso del Sistema<br>A.10.10.3 - Protección de los Registros de Auditoría<br>A.10.10.4 - Registros de Administración y de Operación<br>A.10.10.5 - Registro de Fallas |
| Bases de datos | 4 | Errores humanos | 3 | Falta de documentación | 2 | 3 | 10 | **B** | Se tienen manuales técnicos y de operación. Cuando se contrata un desarrollo se exige la documentación técnica y de operación de la aplicación. | 3 | 3 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas | A.10.1.1 - Procedimientos Operativos Documentados |
| Bases de datos | 4 | Errores humanos | 3 | Falta de conocimiento del administrador del sistema | 2 | 3 | 10 | **B** | Los desarrolladores internos son certificados en el tema. Otras aplicaciones son contratadas con terceros especialistas en desarrollo. | 4 | 3 | **I** | **A** | A.8.1 - Previo a la Contratación<br>A.8.2- Durante la Contratación | A.8.1.3 - Términos y Condiciones de Empleo<br>A.8.2.2 - Educación, Capacitación |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | y Concientización en Seguridad de la Información |
| Bases de datos | 4 | Problemas de operación o administración por ausencia de personal | 2 | Falta de documentación | 2 | 2 | 8 | **B** | La documentación técnica asociada al desarrollo se encuentra en el equipo del administrador | 3 | 3 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas | A.10.1.1 - Procedimientos Operativos Documentados |
| Bases de datos | 4 | Problemas de operación o administración por ausencia de personal | 2 | Falta de contingencias de respaldo de personal crítico | 4 | 3 | 12 | **M** | El administrador del sistema cuenta con un backup para la realización de las tareas propias de su labor | 4 | 3 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas | A.10.1.3 - Segregación de Funciones |
| Bases de datos | 4 | Robo del código fuente de la Aplicación | 3 | Falta de controles de acceso lógico | 4 | 4 | 14 | **M** | El mecanismo de acceso al sistema es a través de usuario y contraseña. Se adquirió la herramienta Visual Source Safe, para el manejo de los códigos fuente, pero aun no esta en operación. | 3 | 5 | **I** | **A** | A.11.2 - Gestión de Acceso de UsuariosA.11.3 - Responsabilidades del Usuario | A.11.2.2 - Gestión de PrivilegiosA.11.2.3 - Gestión de Contraseñas de UsuarioA.11.2.4 - Revisión de derechos de AccesoA.11.3.1 - Uso de Contraseñas A.11.3.2 - Equipos Desatendidos A.11.3.3 - Política de escritorio y Pantalla Limpia |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Bases de datos | 4 | Robo del código fuente de la Aplicación | 3 | Debilidad en las contraseñas | 3 | 3 | 12 | **M** | Aunque almacena las contraseñas cifradas, no se tienen definidas o no se aplican políticas de contraseñas. | 3 | 4 | **I** | **A** | A.11.1 - Requerimientos de Negocio para el Control de Acceso<br>A.11.3 - Responsabilidades del Usuario | A.11.1.1 - Política de Control de Acceso<br>A.11.3.1 - Uso de Contraseñas |
| Bases de datos | 4 | Robo del código fuente de la Aplicación | 3 | Copias no restringidas de datos o software | 4 | 4 | 14 | **M** | No existe control.<br>Se adquirió la herramienta Visual Source Safe, para el manejo de los códigos fuente, pero aun no esta en operación. | 3 | 5 | **I** | **A** | A.7.2 - Clasificación de la información<br>A.11.2 - Gestión de Acceso de Usuarios | A.7.2.1 - Guías de Clasificación<br>A.7.2.2 - Manipulación y Rotulado de la Información<br>A.11.2.2 - Gestión de Privilegios<br>A.11.2.4 - Revisión de Derechos de Acceso |
| Bases de datos | 4 | Robo del código fuente de la Aplicación | 3 | Segregación inadecuada de funciones | 3 | 3 | 12 | **M** | Unicamente los desarrolladores tienen acceso al código fuente.<br>Se adquirió la herramienta Visual Source Safe, para el manejo de los códigos fuente, pero aun no esta en operación. | 4 | 3 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.11.2 - Gestión de Acceso de Usuarios | A.10.1.3 - Segregación de Funciones<br>A.11.2.2 - Gestión de privilegios<br>A.11.2.4 - Revisión de Derechos de Acceso |
| Bases de datos | 4 | Robo del código fuente de la Aplicación | 3 | Falta de comunicación entre las áreas de Recursos Humanos y Dirección de Planeación y Sistemas con respecto a la salida de personal | 4 | 4 | 14 | **M** | No existe control | 1 | 14 | **M** | **I** | A.8.3 - Terminación o Cambio de Empleo | A.8.3.1 - Responsabilidades de Terminación<br>A.8.3.3 - Eliminación |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | de la organización | | | | | | | | | | | de Derechos de Acceso |
| | | | | | | | | | | | | | | | |
| Aplicaciones | 3 | Acceso lógico no autorizado al sistema | 4 | Falta de revisión de la auditoría a la actividad sobre el sistema de información | 3 | 4 | 11 | **M** | Se revisa únicamente cuando es necesario, pero no se tienen procedimientos de revisión de logs. | 2 | 5 | **B** | **T** | A.10.10 - Monitoreo | A.10.10.1 - Registros de Auditoría<br>A.10.10.2 - Monitoreo del Uso del Sistema<br>A.10.10.3 - Protección de los Registros de Auditoría |
| Aplicaciones | 3 | Acceso no autorizado al sistema con privilegios de administrador | 3 | Acceso de los desarrolladores a ambientes productivos | 4 | 4 | 11 | **M** | No existe control | 2 | 5 | **B** | **T** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.11.2 - Gestión de Acceso de Usuarios | A.10.1.2 - Gestión del Cambio<br>A.10.1.3 - Segregación de Funciones<br>A.10.1.4 - Separación de Ambientes de Desarrollo, Prueba y Producción<br>A.11.2.2 - Gestión de Privilegios<br>A.11.2.4 - Revisión de derechos de Acceso |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Aplicaciones | 3 | Acceso no autorizado al sistema con privilegios de administrador | 3 | Falta de revisión de la auditoría a la actividad sobre el sistema de información | 3 | 3 | 9 | **B** | Se revisa únicamente cuando es necesario, pero no se tienen procedimientos de revisión de logs. | 2 | 5 | **I** | **A** | A.10.10 - Monitoreo | A.10.10.1 - Registros de Auditoría<br>A.10.10.2 - Monitoreo del Uso del Sistema<br>A.10.10.3 - Protección de los Registros de Auditoría |
| Aplicaciones | 3 | Cambios de la configuración del sistema | 3 | Acceso de los desarrolladores a ambientes productivos | 4 | 4 | 11 | **M** | No existe control | 2 | 5 | **B** | **T** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.11.2 - Gestión de Acceso de Usuarios | A.10.1.2 - Gestión del Cambio<br>A.10.1.3 - Segregación de Funciones<br>A.10.1.4 - Separación de Ambientes de Desarrollo, Prueba y Producción<br>A.11.2.2 - Gestión de Privilegios<br>A.11.2.4 - Revisión de derechos de Acceso |
| Aplicaciones | 3 | Errores de programación | 3 | Acceso de los desarrolladores a ambientes productivos | 4 | 4 | 11 | **M** | Se tiene un esquema pruebas, para validar los cambios antes de llevarlos a producción. Estas pruebas se realizan en la estación de trabajo del desarrollador. | 2 | 5 | **B** | **T** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.11.2 - Gestión de Acceso de Usuarios | A.10.1.2 - Gestión del Cambio<br>A.10.1.3 - Segregación de Funciones<br>A.10.1.4 - Separación |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | de Ambientes de Desarrollo, Prueba y Producción A.11.2.2 - Gestión de Privilegios A.11.2.4 - Revisión de derechos de Acceso |
| Aplicaciones | 3 | Acceso lógico no autorizado al sistema | 4 | Debilidad en las contraseñas | 3 | 4 | 11 | **M** | Aunque almacena las contraseñas cifradas, no se tienen definidas o no se aplican políticas de contraseñas. | 3 | 4 | **I** | **A** | A.11.1 - Requerimientos de Negocio para el Control de Acceso A.11.3 - Responsabilidades del Usuario | A.11.1.1 - Política de Control de Acceso A.11.3.1 - Uso de Contraseñas |
| Aplicaciones | 3 | Acceso lógico no autorizado al sistema | 4 | La comunicación no se maneja por un canal encriptado. | 5 | 5 | 14 | **M** | No existe control | 1 | 14 | **M** | **I** | A.10.9 - Servicios de Comercio Electrónico A.12.3 - Controles criptograficos | A.10.9.2 Transacciones el línea A.12.3.1. Política de uso de los controles criptográficos |
| Aplicaciones | 3 | Errores de programación | 3 | Falta de controles sobre la gestión del cambio | 3 | 3 | 9 | **B** | Se tiene un esquema pruebas, para validar los cambios antes de llevarlos a producción. Estas pruebas se realizan en la estación de trabajo del desarrollador. Los cambios son aprobados por el área dueña del aplicativo. | 1 | 9 | **B** | **T** | A.10.1 - Procedimientos y Responsabilidades Operativas A.12.5 - Seguridad en los procesos de Desarrollo y Soporte | A.10.1.1 - Procedimientos Operativos Documentados A.10.1.2 - Gestión del Cambio A.12.5.1 - Procedimientos de Control |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | de Cambios |
| Aplicaciones | 3 | Fallas de software | 3 | Falta de controles sobre la gestión del cambio | 3 | 3 | 9 | **B** | Todos los cambios en la aplicación son aprobados y validados en un ambiente de pruebas. Se dejan actas de los cambios realizados. | 4 | 2 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.12.5 - Seguridad en los procesos de Desarrollo y Soporte | A.10.1.1 - Procedimientos Operativos Documentados<br>A.10.1.2 - Gestión del Cambio<br>A.12.5.1 - Procedimientos de Control de Cambios |
| Aplicaciones | 3 | Acceso físico no autorizado al servidor | 2 | Ubicación inadecuada del servidor | 1 | 2 | 5 | **I** | El servidor esta alojado en el Centro de Computo del contratista, el cual cuenta con las medidas de seguridad adecuadas. | 4 | 1 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.1 - Perímetro de Seguridad Física<br>A.9.1.2 - Controles de Acceso Físico<br>A.9.1.6 - Acceso Público, y Areas de Carga y Descarga |
| Aplicaciones | 3 | Acceso físico no autorizado al servidor | 2 | Falta de controles de acceso físico | 1 | 2 | 5 | **I** | El acceso físico al servidor esta restringido por la ETB. | 4 | 1 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.1 - Perímetro de Seguridad Física<br>A.9.1.2 - Controles de Acceso |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | Físico<br>A.9.1.6 - Acceso Público, y Areas de Carga y Descarga |
| Aplicaciones | 3 | Problemas de temperatura y humedad | 2 | Ubicación en áreas susceptibles a temperaturas y humedad extremas | 2 | 2 | 6 | **B** | En el Centro de Computo del contratista se hace control de las condiciones ambientales | 4 | 2 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.4 - Protección contra amenazas externas y ambientales |
| Aplicaciones | 3 | Problemas de temperatura y humedad | 2 | Monitoreo inadecuado de las condiciones ambientales | 1 | 2 | 5 | **I** | En el Centro de Computo de la SDS se hace control de las condiciones ambientales.<br>Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable del mantenimiento de los mismos. | 4 | 1 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.4 - Protección contra amenazas externas y ambientales |
| Aplicaciones | 3 | Problemas de temperatura y humedad | 2 | Falta de planes de contingencia | 1 | 2 | 5 | **I** | En la actualidad no se tienen definidos planes de contingencia para ninguno de los servidores sobre los que opera este sistema de información.<br>Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable de la contingencia de los mismos. | 4 | 1 | **I** | **A** | A.14.1 - Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio | A.14.1.1 - Incluir la Seguridad de la Información en el proceso de Continuidad del Negocio<br>A.14.1.2 - Continuidad del Negocio y Análisis de Riesgos |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | A.14.1.3 - Desarrollo e Implementación de Planes de Continuidad incluyendo Seguridad de la Información<br>A.14.1.4 - Marco de referencia para la planeación de Continuidad del Negocio<br>A.14.1.5 - Prueba, mantenimiento y reevaluación de los Planes de Continuidad del Negocio |
| Aplicaciones | 3 | Acceso lógico no autorizado al sistema | 4 | Falta de controles de acceso lógico | 4 | 4 | 12 | **M** | El mecanismo de acceso a la aplicación es a través de usuario y contraseña, tanto para los usuarios normales, como para los usuarios administradores. | 3 | 4 | **I** | **A** | A.11.2 - Gestión de Acceso de Usuarios<br>A.11.3 - Responsabilidades del Usuario | A.11.2.2 - Gestión de Privilegios<br>A.11.2.3 - Gestión de Contraseñas de Usuario<br>A.11.2.4 - Revisión de derechos de Acceso<br>A.11.3.1 - |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | Uso de Contraseñas<br>A.11.3.2 - Equipos Desatendidos<br>A.11.3.3 - Política de escritorio y Pantalla Limpia |
| Aplicaciones | 3 | Acceso lógico no autorizado al sistema | 4 | Préstamo de usuarios y contraseñas | 3 | 4 | 11 | **M** | Los usuarios administradores, tiene un único usuario y contraseña. Para los usuarios normales, no se tienen políticas de contraseñas. | 3 | 4 | **I** | **A** | A.11.3 - Responsabilidades del Usuario | A.11.3.1 - Uso de Contraseñas |
| Aplicaciones | 3 | Errores de programación | 3 | Procedimientos inadecuados del ciclo de vida de desarrollo de sistemas | 3 | 3 | 9 | **B** | Se utilizan metodologias RUP y Agile XP RUP | 4 | 2 | **I** | **A** | A.12.1 - Requerimientos de Seguridad en Sistemas de Información | A.12.1.1 - Requerimientos de Seguridad en Análisis y Especificación |
| Aplicaciones | 3 | Errores de programación | 3 | Falta de conocimiento de los desarrolladores | 2 | 3 | 8 | **B** | Los desarrolladores internos son certificados en el tema. Otras aplicaciones son contratadas con terceros especialistas en desarrollo. | 4 | 2 | **I** | **A** | A.8.1 - Previo a la Contratación<br>A.8.2- Durante la Contratación | A.8.1.3 - Términos y Condiciones de Empleo<br>A.8.2.2 - Educación, Capacitación y Concientización en Seguridad de la Información |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Aplicaciones | 3 | Errores de programación | 3 | Supervisión inadecuada al grupo de desarrolladores | 3 | 3 | 9 | **B** | Se realiza seguimiento por medio de cronogramas | 4 | 2 | **I** | **A** | A.10.10 - Monitoreo | A.10.10.1 - Registros de Auditoría<br>A.10.10.2 - Monitoreo del Uso del Sistema<br>A.10.10.3 - Protección de los Registros de Auditoría<br>A.10.10.4 - Registros de Administración y de Operación<br>A.10.10.5 - Registro de Fallas |
| Aplicaciones | 3 | Fallas de hardware | 3 | Monitoreo inadecuado de las condiciones ambientales | 1 | 2 | 6 | **B** | En el Centro de Computo de la SDS se hace control de las condiciones ambientales.<br>Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable del mantenimiento de los mismos. | 4 | 2 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.4 - Protección contra amenazas externas y ambientales |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Aplicaciones | 3 | Fallas de hardware | 3 | Mantenimiento inadecuado del servidor | 2 | 3 | 8 | **B** | Se tiene un contrato de mantenimiento de servidores con una empresa externa, sin embargo, la renovación anual del contrato no es inmediata, por lo que existe un periodo de "inestabilidad", entre el vencimiento y la nueva contratación.<br>Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable del mantenimiento de los mismos. | 3 | 3 | **I** | **A** | A.9.2 - Seguridad del equipamento<br>A.10.2 - Gestión de Servicios Prestados por Terceros | A.9.2.4 - Mantenimiento de Equipos<br>A.9.2.7 - Extracción de la Propiedad<br>A.10.2.1 - Prestación del Servicio |
| Aplicaciones | 3 | Fallas de hardware | 3 | Falta de planes de contingencia | 1 | 2 | 6 | **B** | En la actualidad no se tienen definidos planes de contingencia para ninguno de los servidores sobre los que opera este sistema de información.<br>Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable de la contingencia de los mismos. | 4 | 2 | **I** | **A** | A.14.1 - Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio | A.14.1.1 - Incluir la Seguridad de la Información en el proceso de Continuidad del Negocio<br>A.14.1.2 - Continuidad del Negocio y Análisis de Riesgos<br>A.14.1.3 - Desarrollo e Implementación de Planes de Continuidad incluyendo |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | Seguridad de la Información A.14.1.4 - Marco de referencia para la planeación de Continuidad del Negocio A.14.1.5 - Prueba, mantenimiento y reevaluación de los Planes de Continuidad del Negocio |
| Aplicaciones | 3 | Fallas de software | 3 | Falta de conocimiento del administrador del sistema | 2 | 3 | 8 | **B** | Los desarrolladores internos son certificados en el tema. Otras aplicaciones son contratadas con terceros especialistas en desarrollo. | 4 | 2 | **I** | **A** | A.8.1 - Previo a la Contratación A.8.2- Durante la Contratación | A.8.1.3 - Términos y Condiciones de Empleo A.8.2.2 - Educación, Capacitación y Concientización en Seguridad de la Información |
| Aplicaciones | 3 | Fallas de software | 3 | Falta de actualización periódica de versiones o parches sobre el sistema operativo | 2 | 3 | 8 | **B** | Se tiene implementado y en funcionamiento el aplicativo WSUS, con el cual se actualizan los parches de los servidores Windows. | 4 | 2 | **I** | **A** | A.12.5 - Seguridad en los Procesos de Desarrollo y SoporteA.15.2 - Cumplimiento | A.12.5.1- Procedimientos de Control de CambiosA.12.5.2 - |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | Técnico, de Política de Seguridad y Estándares | Revisión Técnica de Aplicaciones después de Cambios al Sistema OperativoA.15.2.1 - Cumplimiento con Políticas y Estándares de Seguridad |
| Aplicaciones | 3 | Software malicioso | 4 | Supervisión inadecuada al grupo de desarrolladores | 4 | 4 | 12 | **M** | Se realiza seguimiento por medio de cronogramas | 3 | 4 | **I** | **A** | A.10.10 - Monitoreo | A.10.10.1 - Registros de Auditoría<br>A.10.10.2 - Monitoreo del Uso del Sistema<br>A.10.10.3 - Protección de los Registros de Auditoría<br>A.10.10.4 - Registros de Administración y de Operación<br>A.10.10.5 - Registro de Fallas |
| Aplicaciones | 3 | Errores humanos | 3 | Falta de documentación | 2 | 3 | 8 | **B** | Se tienen manuales técnicos y de operación. Cuando se contrata un desarrollo se exige la documentación técnica y de operación de la aplicación. | 3 | 3 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas | A.10.1.1 - Procedimientos Operativos Documentados |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Aplicaciones | 3 | Errores humanos | 3 | Falta de conocimiento del administrador del sistema | 2 | 3 | 8 | **B** | Los desarrolladores internos son certificados en el tema. Otras aplicaciones son contratadas con terceros especialistas en desarrollo. | 4 | 2 | **I** | **A** | A.8.1 - Previo a la Contratación<br>A.8.2- Durante la Contratación | A.8.1.3 - Términos y Condiciones de Empleo<br>A.8.2.2 - Educación, Capacitación y Concientización en Seguridad de la Información |
| Aplicaciones | 3 | Problemas de operación o administración por ausencia de personal | 2 | Falta de documentación | 2 | 2 | 6 | **B** | Se tienen manuales técnicos y de operación. Cuando se contrata un desarrollo se exige la documentación técnica y de operación de la aplicación. | 3 | 2 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas | A.10.1.1 - Procedimientos Operativos Documentados |
| Aplicaciones | 3 | Problemas de operación o administración por ausencia de personal | 2 | Falta de contingencias de respaldo de personal crítico | 4 | 3 | 9 | **B** | El administrador del sistema cuenta con un backup para la realización de las tareas propias de su labor | 4 | 2 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas | A.10.1.3 - Segregación de Funciones |
| Aplicaciones | 3 | Robo del código fuente de la Aplicación | 3 | Falta de controles de acceso lógico | 4 | 4 | 11 | **M** | El mecanismo de acceso al sistema es a través de usuario y contraseña. Se adquirió la herramienta Visual Source Safe, para el manejo de los códigos fuente, pero aun no esta en operación. | 3 | 4 | **I** | **A** | A.11.2 - Gestión de Acceso de Usuarios<br>A.11.3 - Responsabilidades del Usuario | A.11.2.2 - Gestión de Privilegios<br>A.11.2.3 - Gestión de Contraseñas de Usuario<br>A.11.2.4 - Revisión de derechos de Acceso<br>A.11.3.1 - Uso de Contraseñas |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | A.11.3.2 - Equipos Desatendidos<br>A.11.3.3 - Política de escritorio y Pantalla Limpia |
| Aplicaciones | 3 | Robo del código fuente de la Aplicación | 3 | Debilidad en las contraseñas | 3 | 3 | 9 | **B** | Aunque almacena las contraseñas cifradas, no se tienen definidas o no se aplican políticas de contraseñas. | 3 | 3 | **I** | **A** | A.11.1 - Requerimientos de Negocio para el Control de Acceso<br>A.11.3 - Responsabilidades del Usuario | A.11.1.1 - Política de Control de Acceso<br>A.11.3.1 - Uso de Contraseñas |
| Aplicaciones | 3 | Robo del código fuente de la Aplicación | 3 | Copias no restringidas de datos o software | 4 | 4 | 11 | **M** | No existe control.<br>Se adquirió la herramienta Visual Source Safe, para el manejo de los códigos fuente, pero aun no esta en operación. | 3 | 4 | **I** | **A** | A.7.2 - Clasificación de la información<br>A.11.2 - Gestión de Acceso de Usuarios | A.7.2.1 - Guías de Clasificación<br>A.7.2.2 - Manipulación y Rotulado de la Información<br>A.11.2.2 - Gestión de Privilegios<br>A.11.2.4 - Revisión de Derechos de Acceso |
| Aplicaciones | 3 | Robo del código fuente de la Aplicación | 3 | Segregación inadecuada de funciones | 3 | 3 | 9 | **B** | Unicamente los desarrolladores tienen acceso al código fuente.<br>Se adquirió la herramienta Visual Source Safe, para el manejo de los códigos fuente, pero aun no esta | 4 | 2 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.11.2 - Gestión de Acceso de Usuarios | A.10.1.3 - Segregación de Funciones<br>A.11.2.2 - Gestión de privilegios<br>A.11.2.4 - Revisión de |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | en operación. | | | | | | Derechos de Acceso |
| Aplicaciones | 3 | Robo del código fuente de la Aplicación | 3 | Falta de comunicación entre las áreas de Recursos Humanos y Dirección de Planeación y Sistemas con respecto a la salida de personal de la organización | 4 | 4 | 11 | **M** | No existe control | 1 | 11 | **M** | **I** | A.8.3 - Terminación o Cambio de Empleo | A.8.3.1 - Responsabilidades de Terminación<br>A.8.3.3 - Eliminación de Derechos de Acceso |
| | | | | | | | | | | | | | | | |
| Mensajeria Exchange Server 2007 | 4 | Acceso lógico no autorizado al sistema | 4 | Falta de revisión de la auditoría a la actividad sobre el sistema de información | 3 | 4 | 14 | **M** | Se revisa únicamente cuando es necesario, pero no se tienen procedimientos de revisión de logs. | 2 | 7 | **B** | **T** | A.10.10 - Monitoreo | A.10.10.1 - Registros de Auditoría<br>A.10.10.2 - Monitoreo del Uso del Sistema<br>A.10.10.3 - Protección de los Registros de Auditoría |
| Mensajeria Exchange Server 2007 | 4 | Acceso no autorizado al sistema con privilegios de administrador | 3 | Acceso de los desarrolladores a ambientes productivos | 4 | 4 | 14 | **M** | Se tiene un esquema pruebas, para validar los cambios antes de llevarlos a producción. Estas pruebas se realizan en la estación de trabajo del desarrollador. | 2 | 7 | **B** | **T** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.11.2 - Gestión de Acceso de Usuarios | A.10.1.2 - Gestión del Cambio<br>A.10.1.3 - Segregación de Funciones<br>A.10.1.4 - Separación de Ambientes de Desarrollo, Prueba y Producción |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | A.11.2.2 - Gestión de Privilegios<br>A.11.2.4 - Revisión de derechos de Acceso |
| Mensajeria Exchange Server 2007 | 4 | Acceso no autorizado al sistema con privilegios de administrador | 3 | Falta de revisión de la auditoría a la actividad sobre el sistema de información | 3 | 3 | 12 | **M** | Se revisa únicamente cuando es necesario, pero no se tienen procedimientos de revisión de logs. | 2 | 6 | **B** | **T** | A.10.10 - Monitoreo | A.10.10.1 - Registros de Auditoría<br>A.10.10.2 - Monitoreo del Uso del Sistema<br>A.10.10.3 - Protección de los Registros de Auditoría |
| Mensajeria Exchange Server 2007 | 4 | Cambios de la configuración del sistema | 3 | Acceso de los desarrolladores a ambientes productivos | 4 | 4 | 14 | **M** | Se tiene un esquema pruebas, para validar los cambios antes de llevarlos a producción. Estas pruebas se realizan en la estación de trabajo del desarrollador. | 2 | 7 | **B** | **T** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.11.2 - Gestión de Acceso de Usuarios | A.10.1.2 - Gestión del Cambio<br>A.10.1.3 - Segregación de Funciones<br>A.10.1.4 - Separación de Ambientes de Desarrollo, Prueba y Producción<br>A.11.2.2 - Gestión de Privilegios<br>A.11.2.4 - Revisión de derechos de Acceso |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Mensajeria Exchange Server 2007 | 4 | Errores de programación | 3 | Acceso de los desarrolladores a ambientes productivos | 4 | 4 | 14 | **M** | Se tiene un esquema pruebas, para validar los cambios antes de llevarlos a producción. Estas pruebas se realizan en la estación de trabajo del desarrollador. | 2 | 7 | **B** | **T** | A.10.1 - Procedimientos y Responsabilidades OperativasA.11.2 - Gestión de Acceso de Usuarios | A.10.1.2 - Gestión del CambioA.10.1.3 - Segregación de FuncionesA.10.1.4 - Separación de Ambientes de Desarrollo, Prueba y ProducciónA.11.2.2 - Gestión de PrivilegiosA.11.2.4 - Revisión de derechos de Acceso |
| Mensajeria Exchange Server 2007 | 4 | Acceso lógico no autorizado al sistema | 4 | Debilidad en las contraseñas | 3 | 4 | 14 | **M** | Aunque almacena las contraseñas cifradas, no se tienen definidas o no se aplican políticas de contraseñas. | 3 | 5 | **I** | **A** | A.11.1 - Requerimientos de Negocio para el Control de Acceso A.11.3 - Responsabilidades del Usuario | A.11.1.1 - Política de Control de Acceso A.11.3.1 - Uso de Contraseñas |
| Mensajeria Exchange Server 2007 | 4 | Acceso lógico no autorizado al sistema | 4 | La comunicación no se maneja por un canal encriptado. | 5 | 5 | 18 | **A** | No existe control | 1 | 18 | **A** | **I** | A.10.9 - Servicios de Comercio Electrónico A.12.3 - Controles criptograficos | A.10.9.2 Transacciones el línea A.12.3.1. Política de uso de los controles criptográficos |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Mensajeria Exchange Server 2007 | 4 | Errores de programación | 3 | Falta de controles sobre la gestión del cambio | 3 | 3 | 12 | **M** | Se tiene un esquema pruebas, para validar los cambios antes de llevarlos a producción. Estas pruebas se realizan en la estación de trabajo del desarrollador. Los cambios son aprobados por el área dueña del aplicativo. | 1 | 12 | **M** | **I** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.12.5 - Seguridad en los procesos de Desarrollo y Soporte | A.10.1.1 - Procedimientos Operativos Documentados<br>A.10.1.2 - Gestión del Cambio<br>A.12.5.1 - Procedimientos de Control de Cambios |
| Mensajería Exchange Server 2007 | 4 | Fallas de software | 3 | Falta de controles sobre la gestión del cambio | 3 | 3 | 12 | **M** | Todos los cambios en la aplicación son aprobados y validados en un ambiente de pruebas. Se dejan actas de los cambios realizados. | 4 | 3 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.12.5 - Seguridad en los procesos de Desarrollo y Soporte | A.10.1.1 - Procedimientos Operativos Documentados<br>A.10.1.2 - Gestión del Cambio<br>A.12.5.1 - Procedimientos de Control de Cambios |
| Mensajería Exchange Server 2007 | 4 | Acceso físico no autorizado al servidor | 2 | Ubicación inadecuada del servidor | 1 | 2 | 6 | **B** | El servidor esta alojado en el Centro de Computo del contratista, el cual cuenta con las medidas de seguridad adecuadas. | 4 | 2 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.1 - Perímetro de Seguridad Física<br>A.9.1.2 - Controles de Acceso Físico<br>A.9.1.6 - Acceso Público, y Areas de Carga y Descarga |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Mensajeria Exchange Server 2007 | 4 | Acceso físico no autorizado al servidor | 2 | Falta de controles de acceso físico | 1 | 2 | 6 | **B** | El acceso físico al servidor esta restringido por la ETB. | 4 | 2 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.1 - Perímetro de Seguridad Física<br>A.9.1.2 - Controles de Acceso Físico<br>A.9.1.6 - Acceso Público, y Areas de Carga y Descarga |
| Mensajeria Exchange Server 2007 | 4 | Problemas de temperatura y humedad | 2 | Ubicación en áreas susceptibles a temperaturas y humedad extremas | 2 | 2 | 8 | **B** | En el Centro de Computo del contratista se hace control de las condiciones ambientales | 4 | 2 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.4 - Protección contra amenazas externas y ambientales |
| Mensajeria Exchange Server 2007 | 4 | Problemas de temperatura y humedad | 2 | Monitoreo inadecuado de las condiciones ambientales | 1 | 2 | 6 | **B** | En el Centro de Computo de la SDS se hace control de las condiciones ambientales.<br>Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable del mantenimiento de los mismos. | 4 | 2 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.4 - Protección contra amenazas externas y ambientales |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Mensajeria Exchange Server 2007 | 4 | Problemas de temperatura y humedad | 2 | Falta de planes de contingencia | 1 | 2 | 6 | **B** | En la actualidad no se tienen definidos planes de contingencia para ninguno de los servidores sobre los que opera este sistema de información.<br>Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable de la contingencia de los mismos. | 4 | 2 | **I** | **A** | A.14.1 - Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio | A.14.1.1 - Incluir la Seguridad de la Información en el proceso de Continuidad del Negocio<br>A.14.1.2 - Continuidad del Negocio y Análisis de Riesgos<br>A.14.1.3 - Desarrollo e Implementación de Planes de Continuidad incluyendo Seguridad de la Información<br>A.14.1.4 - Marco de referencia para la planeación de Continuidad del Negocio<br>A.14.1.5 - Prueba, mantenimiento y reevaluación de los Planes de Continuidad |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | del Negocio |
| Mensajeria Exchange Server 2007 | 4 | Acceso lógico no autorizado al sistema | 4 | Falta de controles de acceso lógico | 4 | 4 | 16 | **A** | El mecanismo de acceso a la aplicación es a través de usuario y contraseña, tanto para los usuarios normales, como para los usuarios administradores. | 3 | 5 | **B** | **T** | A.11.2 - Gestión de Acceso de Usuarios<br>A.11.3 - Responsabilidades del Usuario | A.11.2.2 - Gestión de Privilegios<br>A.11.2.3 - Gestión de Contraseñas de Usuario<br>A.11.2.4 - Revisión de derechos de Acceso<br>A.11.3.1 - Uso de Contraseñas<br>A.11.3.2 - Equipos Desatendidos<br>A.11.3.3 - Política de escritorio y Pantalla Limpia |
| Mensajeria Exchange Server 2007 | 4 | Acceso lógico no autorizado al sistema | 4 | Préstamo de usuarios y contraseñas | 3 | 4 | 14 | **M** | Los usuarios administradores, tiene un único usuario y contraseña. Para los usuarios normales, no | 3 | 5 | **I** | **A** | A.11.3 - Responsabilidades del Usuario | A.11.3.1 - Uso de Contraseñas |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | se tienen políticas de contraseñas. | | | | | | |
| Mensajeria Exchange Server 2007 | 4 | Errores de programación | 3 | Procedimientos inadecuados del ciclo de vida de desarrollo de sistemas | 3 | 3 | 12 | **M** | Se utilizan metodologias RUP y Agile XP RUP | 4 | 3 | **I** | **A** | A.12.1 - Requerimientos de Seguridad en Sistemas de Información | A.12.1.1 - Requerimientos de Seguridad en Análisis y Especificación |
| Mensajeria Exchange Server 2007 | 4 | Errores de programación | 3 | Falta de conocimiento de los desarrolladores | 2 | 3 | 10 | **B** | Los desarrolladores internos son certificados en el tema. Otras aplicaciones son contratadas con terceros especialistas en desarrollo. | 4 | 3 | **I** | **A** | A.8.1 - Previo a la Contratación<br>A.8.2- Durante la Contratación | A.8.1.3 - Términos y Condiciones de Empleo<br>A.8.2.2 - Educación, Capacitación y Concientización en Seguridad de la Información |
| Mensajeria Exchange Server 2007 | 4 | Errores de programación | 3 | Supervisión inadecuada al grupo de desarrolladores | 3 | 3 | 12 | **M** | Se realiza seguimiento por medio de cronogramas | 4 | 3 | **I** | **A** | A.10.10 - Monitoreo | A.10.10.1 - Registros de Auditoría<br>A.10.10.2 - Monitoreo del Uso del Sistema<br>A.10.10.3 - Protección de los Registros de Auditoría<br>A.10.10.4 - Registros de Administració |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | n y de Operación A.10.10.5 - Registro de Fallas |
| Mensajeria Exchange Server 2007 | 4 | Fa llas de hardware | 3 | Monitoreo inadecuado de las condiciones ambientales | 1 | 2 | 8 | **B** | En el Centro de Computo de la SDS se hace control de las condiciones ambientales.Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable del mantenimiento de los mismos. | 4 | 2 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.4 - Protección contra amenazas externas y ambientales |
| Mensajeria Exchange Server 2007 | 4 | Fallas de hardware | 3 | Mantenimiento inadecuado del servidor | 2 | 3 | 10 | **B** | Se tiene un contrato de mantenimiento de servidores con una empresa externa, sin embargo, la renovación anual del contrato no es inmediata, por lo que existe un periodo de "inestabilidad", entre el vencimiento y la nueva contratación.<br>Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable del mantenimiento de los mismos. | 3 | 3 | **I** | **A** | A.9.2 - Seguridad del equipamento A.10.2 - Gestión de Servicios Prestados por Terceros | A.9.2.4 - Mantenimiento de Equipos A.9.2.7 - Extracción de la Propiedad A.10.2.1 - Prestación del Servicio |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Mensajeria Exchange Server 2007 | 4 | Fallas de hardware | 3 | Falta de planes de contingencia | 1 | 2 | 8 | **B** | En la actualidad no se tienen definidos planes de contingencia para ninguno de los servidores sobre los que opera este sistema de información.<br>Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable de la contingencia de los mismos. | 4 | 2 | **I** | **A** | A.14.1 - Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio | A.14.1.1 - Incluir la Seguridad de la Información en el proceso de Continuidad del Negocio<br>A.14.1.2 - Continuidad del Negocio y Análisis de Riesgos<br>A.14.1.3 - Desarrollo e Implementación de Planes de Continuidad incluyendo Seguridad de la Información<br>A.14.1.4 - Marco de referencia para la planeación de Continuidad del Negocio<br>A.14.1.5 - Prueba, mantenimiento y reevaluación de los Planes de Continuidad |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | del Negocio |
| Mensajeria Exchange Server 2007 | 4 | Fallas de software | 3 | Falta de conocimiento del administrador del sistema | 2 | 3 | 10 | **B** | Los desarrolladores internos son certificados en el tema. Otras aplicaciones son contratadas con terceros especialistas en desarrollo. | 4 | 3 | **I** | **A** | A.8.1 - Previo a la Contratación<br>A.8.2- Durante la Contratación | A.8.1.3 - Términos y Condiciones de Empleo<br>A.8.2.2 - Educación, Capacitación y Concientización en Seguridad de la Información |
| Mensajeria Exchange Server 2007 | 4 | Fallas de software | 3 | Falta de actualización periódica de versiones o parches sobre el sistema operativo | 2 | 3 | 10 | **B** | Se tiene implementado y en funcionamiento el aplicativo WSUS, con el cual se actualizan los parches de los servidores Windows. | 4 | 3 | **I** | **A** | A.12.5 - Seguridad en los Procesos de Desarrollo y Soporte<br>A.15.2 - Cumplimiento Técnico, de Política de Seguridad y Estándares | A.12.5.1- Procedimientos de Control de Cambios<br>A.12.5.2 - Revisión Técnica de Aplicaciones después de Cambios al Sistema Operativo<br>A.15.2.1 - Cumplimiento |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | con Políticas y Estándares de Seguridad |
| Mensajeria Exchange Server 2007 | 4 | Software malicioso | 4 | Supervisión inadecuada al grupo de desarrolladores | 4 | 4 | 16 | **A** | Se realiza seguimiento por medio de cronogramas | 3 | 5 | **B** | **T** | A.10.10 - Monitoreo | A.10.10.1 - Registros de Auditoría<br>A.10.10.2 - Monitoreo del Uso del Sistema<br>A.10.10.3 - Protección de los Registros de Auditoría<br>A.10.10.4 - Registros de Administración y de Operación<br>A.10.10.5 - Registro de Fallas |
| Mensajeria Exchange Server 2007 | 4 | Errores humanos | 3 | Falta de documentación | 2 | 3 | 10 | **B** | Se tienen manuales técnicos y de operación. Cuando se contrata un desarrollo se exige la documentación técnica y de operación de la aplicación. | 3 | 3 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas | A.10.1.1 - Procedimientos Operativos Documentados |
| Mensajeria Exchange Server 2007 | 4 | Errores humanos | 3 | Falta de conocimiento del administrador del sistema | 2 | 3 | 10 | **B** | Los desarrolladores internos son certificados en el tema. Otras aplicaciones son contratadas con terceros especialistas en desarrollo. | 4 | 3 | **I** | **A** | A.8.1 - Previo a la Contratación<br>A.8.2- Durante la Contratación | A.8.1.3 - Términos y Condiciones de Empleo<br>A.8.2.2 - Educación, Capacitación |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | y Concientización en Seguridad de la Información |
| Mensajeria Exchange Server 2007 | 4 | Problemas de operación o administración por ausencia de personal | 2 | Falta de documentación | 2 | 2 | 8 | **B** | Se tienen manuales técnicos y de operación. Cuando se contrata un desarrollo se exige la documentación técnica y de operación de la aplicación. | 3 | 3 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas | A.10.1.1 - Procedimientos Operativos Documentados |
| Mensajeria Exchange Server 2007 | 4 | Problemas de operación o administración por ausencia de personal | 2 | Falta de contingencias de respaldo de personal crítico | 4 | 3 | 12 | **M** | El administrador del sistema cuenta con un backup para la realización de las tareas propias de su labor | 4 | 3 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas | A.10.1.3 - Segregación de Funciones |
| Mensajeria Exchange Server 2007 | 4 | Robo del código fuente de la Aplicación | 3 | Falta de controles de acceso lógico | 4 | 4 | 14 | **M** | El mecanismo de acceso al sistema es a través de usuario y contraseña. Se adquirió la herramienta Visual Source Safe, para el manejo de los códigos fuente, pero aun no esta en operación. | 3 | 5 | **I** | **A** | A.11.2 - Gestión de Acceso de Usuarios<br>A.11.3 - Responsabilidades del Usuario | A.11.2.2 - Gestión de Privilegios<br>A.11.2.3 - Gestión de Contraseñas de Usuario<br>A.11.2.4 - Revisión de derechos de Acceso<br>A.11.3.1 - Uso de Contraseñas<br>A.11.3.2 - Equipos Desatendidos<br>A.11.3.3 - Política de escritorio y Pantalla |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | Limpia |
| Mensajeria Exchange Server 2007 | 4 | Robo del código fuente de la Aplicación | 3 | Debilidad en las contraseñas | 3 | 3 | 12 | **M** | Aunque almacena las contraseñas cifradas, no se tienen definidas o no se aplican políticas de contraseñas. | 3 | 4 | **I** | **A** | A.11.1 - Requerimientos de Negocio para el Control de Acceso<br>A.11.3 - Responsabilidades del Usuario | A.11.1.1 - Política de Control de Acceso<br>A.11.3.1 - Uso de Contraseñas |
| Mensajeria Exchange Server 2007 | 4 | Robo del código fuente de la Aplicación | 3 | Copias no restringidas de datos o software | 4 | 4 | 14 | **M** | No existe control.<br>Se adquirió la herramienta Visual Source Safe, para el manejo de los códigos fuente, pero aun no esta en operación. | 3 | 5 | **I** | **A** | A.7.2 - Clasificación de la información<br>A.11.2 - Gestión de Acceso de Usuarios | A.7.2.1 - Guías de Clasificación<br>A.7.2.2 - Manipulación y Rotulado de la Información<br>A.11.2.2 - Gestión de Privilegios<br>A.11.2.4 - Revisión de Derechos de Acceso |
| Mensajeria Exchange Server 2007 | 4 | Robo del código fuente de la Aplicación | 3 | Segregación inadecuada de funciones | 3 | 3 | 12 | **M** | Unicamente los desarrolladores tienen acceso al código fuente.<br>Se adquirió la herramienta Visual Source Safe, para el manejo de los códigos fuente, pero aun no esta en operación. | 4 | 3 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades OperativasA.11.2 - Gestión de Acceso de Usuarios | A.10.1.3 - Segregación de FuncionesA.11.2.2 - Gestión de privilegiosA.11.2.4 - Revisión de |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | Derechos de Acceso |
| Mensajeria Exchange Server 2007 | 4 | Robo del código fuente de la Aplicación | 3 | Falta de comunicación entre las áreas de Recursos Humanos y Dirección de Planeación y Sistemas con respecto a la salida de personal de la organización | 4 | 4 | 14 | **M** | No existe control | 1 | 14 | **M** | **I** | A.8.3 - Terminación o Cambio de Empleo | A.8.3.1 - Responsabilidades de Terminación<br>A.8.3.3 - Eliminación de Derechos de Acceso |
| | | | | | | | | | | | | | | | |
| Infraestructura (Servidores) | 3 | Acceso lógico no autorizado al sistema | 4 | Falta de revisión de la auditoría a la actividad sobre el sistema de información | 3 | 4 | 11 | **M** | Se revisa únicamente cuando es necesario, pero no se tienen procedimientos de revisión de logs. | 2 | 5 | **B** | **T** | A.10.10 - Monitoreo | A.10.10.1 - Registros de Auditoría<br>A.10.10.2 - Monitoreo del Uso del Sistema<br>A.10.10.3 - Protección de los Registros de Auditoría |
| Infraestructura (Servidores) | 3 | Acceso no autorizado al sistema con privilegios de administrador | 3 | Acceso de los desarrolladores a ambientes productivos | 4 | 4 | 11 | **M** | No existe control | 2 | 5 | **B** | **T** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.11.2 - Gestión de Acceso de Usuarios | A.10.1.2 - Gestión del Cambio<br>A.10.1.3 - Segregación de Funciones<br>A.10.1.4 - Separación de Ambientes de Desarrollo, Prueba y Producción |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | A.11.2.2 - Gestión de Privilegios<br>A.11.2.4 - Revisión de derechos de Acceso |
| Infraestructura (Servidores) | 3 | Acceso no autorizado al sistema con privilegios de administrador | 3 | Falta de revisión de la auditoría a la actividad sobre el sistema de información | 3 | 3 | 9 | **B** | Se revisa únicamente cuando es necesario, pero no se tienen procedimientos de revisión de logs. | 2 | 5 | **I** | **A** | A.10.10 - Monitoreo | A.10.10.1 - Registros de Auditoría<br>A.10.10.2 - Monitoreo del Uso del Sistema<br>A.10.10.3 - Protección de los Registros de Auditoría |
| Infraestructura (Servidores) | 3 | Cambios de la configuración del sistema | 3 | Acceso de los desarrolladores a ambientes productivos | 4 | 4 | 11 | **M** | No existe control | 2 | 5 | **B** | **T** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.11.2 - Gestión de Acceso de Usuarios | A.10.1.2 - Gestión del Cambio<br>A.10.1.3 - Segregación de Funciones<br>A.10.1.4 - Separación de Ambientes de Desarrollo, Prueba y Producción<br>A.11.2.2 - Gestión de Privilegios<br>A.11.2.4 - Revisión de derechos de Acceso |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Infraestructura (Servidores) | 3 | Errores de programación | 3 | Acceso de los desarrolladores a ambientes productivos | 4 | 4 | 11 | **M** | Se tiene un esquema pruebas, para validar los cambios antes de llevarlos a producción. Estas pruebas se realizan en la estación de trabajo del desarrollador. | 2 | 5 | **B** | **T** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.11.2 - Gestión de Acceso de Usuarios | A.10.1.2 - Gestión del Cambio<br>A.10.1.3 - Segregación de Funciones<br>A.10.1.4 - Separación de Ambientes de Desarrollo, Prueba y Producción<br>A.11.2.2 - Gestión de Privilegios<br>A.11.2.4 - Revisión de derechos de Acceso |
| Infraestructura (Servidores) | 3 | Acceso lógico no autorizado al sistema | 4 | Debilidad en las contraseñas | 3 | 4 | 11 | **M** | Aunque almacena las contraseñas cifradas, no se tienen definidas o no se aplican políticas de contraseñas. | 3 | 4 | **I** | **A** | A.11.1 - Requerimientos de Negocio para el Control de Acceso<br>A.11.3 - Responsabilidades del Usuario | A.11.1.1 - Política de Control de Acceso<br>A.11.3.1 - Uso de Contraseñas |
| Infraestructura (Servidores) | 3 | Acceso lógico no autorizado al sistema | 4 | La comunicación no se maneja por un canal encriptado. | 5 | 5 | 14 | **M** | No existe control | 1 | 14 | **M** | **I** | A.10.9 - Servicios de Comercio Electrónico<br>A.12.3 - Controles criptograficos | A.10.9.2 Transacciones el línea<br>A.12.3.1. Política de uso de los controles criptográficos |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Infraestructura (Servidores) | 3 | Errores de programación | 3 | Falta de controles sobre la gestión del cambio | 3 | 3 | 9 | **B** | Se tiene un esquema pruebas, para validar los cambios antes de llevarlos a producción. Estas pruebas se realizan en la estación de trabajo del desarrollador. Los cambios son aprobados por el área dueña del aplicativo. | 1 | 9 | **B** | **T** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.12.5 - Seguridad en los procesos de Desarrollo y Soporte | A.10.1.1 - Procedimientos Operativos Documentados<br>A.10.1.2 - Gestión del Cambio<br>A.12.5.1 - Procedimientos de Control de Cambios |
| Infraestructura (Servidores) | 3 | Fallas de software | 3 | Falta de controles sobre la gestión del cambio | 3 | 3 | 9 | **B** | Todos los cambios en la aplicación son aprobados y validados en un ambiente de pruebas. Se dejan actas de los cambios realizados. | 4 | 2 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.12.5 - Seguridad en los procesos de Desarrollo y Soporte | A.10.1.1 - Procedimientos Operativos Documentados<br>A.10.1.2 - Gestión del Cambio<br>A.12.5.1 - Procedimientos de Control de Cambios |
| Infraestructura (Servidores) | 3 | Acceso físico no autorizado al servidor | 2 | Ubicación inadecuada del servidor | 1 | 2 | 5 | **I** | El servidor esta alojado en el Centro de Computo del contratista, el cual cuenta con las medidas de seguridad adecuadas. | 4 | 1 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.1 - Perímetro de Seguridad Física<br>A.9.1.2 - Controles de Acceso Físico<br>A.9.1.6 - Acceso Público, y Areas de Carga y Descarga |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Infraestructura (Servidores) | 3 | Acceso físico no autorizado al servidor | 2 | Falta de controles de acceso físico | 1 | 2 | 5 | **I** | El acceso físico al servidor esta restringido por la ETB. | 4 | 1 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.1 - Perímetro de Seguridad Física<br>A.9.1.2 - Controles de Acceso Físico<br>A.9.1.6 - Acceso Público, y Areas de Carga y Descarga |
| Infraestructura (Servidores) | 3 | Problemas de temperatura y humedad | 2 | Ubicación en áreas susceptibles a temperaturas y humedad extremas | 2 | 2 | 6 | **B** | En el Centro de Computo del contratista se hace control de las condiciones ambientales | 4 | 2 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.4 - Protección contra amenazas externas y ambientales |
| Infraestructura (Servidores) | 3 | Problemas de temperatura y humedad | 2 | Monitoreo inadecuado de las condiciones ambientales | 1 | 2 | 5 | **I** | En el Centro de Computo de la SDS se hace control de las condiciones ambientales.<br>Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable del mantenimiento de los mismos. | 4 | 1 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.4 - Protección contra amenazas externas y ambientales |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Infraestructura (Servidores) | 3 | Problemas de temperatura y humedad | 2 | Falta de planes de contingencia | 1 | 2 | 5 | **I** | En la actualidad no se tienen definidos planes de contingencia para ninguno de los servidores sobre los que opera este sistema de información.Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable de la contingencia de los mismos. | 4 | 1 | **I** | **A** | A.14.1 - Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio | A.14.1.1 - Incluir la Seguridad de la Información en el proceso de Continuidad del NegocioA.14.1.2 - Continuidad del Negocio y Análisis de RiesgosA.14.1.3 - Desarrollo e Implementación de Planes de Continuidad incluyendo Seguridad de la InformaciónA.14.1.4 - Marco de referencia para la planeación de Continuidad del NegocioA.14.1.5 - Prueba, mantenimiento y reevaluación de los Planes de |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | Continuidad del Negocio |
| Infraestructura (Servidores) | 3 | Acceso lógico no autorizado al sistema | 4 | Falta de controles de acceso lógico | 4 | 4 | 12 | **M** | El mecanismo de acceso a la aplicación es a través de usuario y contraseña, tanto para los usuarios normales, como para los usuarios administradores. | 3 | 4 | **I** | **A** | A.11.2 - Gestión de Acceso de Usuarios<br>A.11.3 - Responsabilidades del Usuario | A.11.2.2 - Gestión de Privilegios<br>A.11.2.3 - Gestión de Contraseñas de Usuario<br>A.11.2.4 - Revisión de derechos de Acceso<br>A.11.3.1 - Uso de Contraseñas<br>A.11.3.2 - Equipos Desatendidos<br>A.11.3.3 - Política de escritorio y Pantalla Limpia |
| Infraestructura (Servidores) | 3 | Acceso lógico no autorizado al sistema | 4 | Préstamo de usuarios y contraseñas | 3 | 4 | 11 | **M** | Los usuarios administradores, tiene un único usuario y contraseña. Para los usuarios normales, no | 3 | 4 | **I** | **A** | A.11.3 - Responsabilidades del Usuario | A.11.3.1 - Uso de Contraseñas |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | se tienen políticas de contraseñas. | | | | | | |
| Infraestructura (Servidores) | 3 | Errores de programación | 3 | Procedimientos inadecuados del ciclo de vida de desarrollo de sistemas | 3 | 3 | 9 | **B** | Se utilizan metodologias RUP y Agile XP RUP | 4 | 2 | **I** | **A** | A.12.1 - Requerimientos de Seguridad en Sistemas de Información | A.12.1.1 - Requerimientos de Seguridad en Análisis y Especificación |
| Infraestructura (Servidores) | 3 | Errores de programación | 3 | Falta de conocimiento de los desarrolladores | 2 | 3 | 8 | **B** | Los desarrolladores internos son certificados en el tema. Otras aplicaciones son contratadas con terceros especialistas en desarrollo. | 4 | 2 | **I** | **A** | A.8.1 - Previo a la Contratación<br>A.8.2- Durante la Contratación | A.8.1.3 - Términos y Condiciones de Empleo<br>A.8.2.2 - Educación, Capacitación y Concientización en Seguridad de la Información |
| Infraestructura (Servidores) | 3 | Errores de programación | 3 | Supervisión inadecuada al grupo de desarrolladores | 3 | 3 | 9 | **B** | Se realiza seguimiento por medio de cronogramas | 4 | 2 | **I** | **A** | A.10.10 - Monitoreo | A.10.10.1 - Registros de Auditoría<br>A.10.10.2 - Monitoreo del Uso del Sistema<br>A.10.10.3 - Protección de los Registros de Auditoría<br>A.10.10.4 - Registros de Administració |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | n y de Operación A.10.10.5 - Registro de Fallas |
| Infraestructura (Servidores) | 3 | Fallas de hardware | 3 | Monitoreo inadecuado de las condiciones ambientales | 1 | 2 | 6 | **B** | En el Centro de Computo de la SDS se hace control de las condiciones ambientales. Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable del mantenimiento de los mismos. | 4 | 2 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.4 - Protección contra amenazas externas y ambientales |
| Infraestructura (Servidores) | 3 | Fallas de hardware | 3 | Mantenimiento inadecuado del servidor | 2 | 3 | 8 | **B** | Se tiene un contrato de mantenimiento de servidores con una empresa externa, sin embargo, la renovación anual del contrato no es inmediata, por lo que existe un periodo de "inestabilidad", entre el vencimiento y la nueva contratación. Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable del mantenimiento de los mismos. | 3 | 3 | **I** | **A** | A.9.2 - Seguridad del equipamento A.10.2 - Gestión de Servicios Prestados por Terceros | A.9.2.4 - Mantenimiento de Equipos A.9.2.7 - Extracción de la Propiedad A.10.2.1 - Prestación del Servicio |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Infraestructura (Servidores) | 3 | Fallas de hardware | 3 | Falta de planes de contingencia | 1 | 2 | 6 | **B** | En la actualidad no se tienen definidos planes de contingencia para ninguno de los servidores sobre los que opera este sistema de información.<br>Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable de la contingencia de los mismos. | 4 | 2 | **I** | **A** | A.14.1 - Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio | A.14.1.1 - Incluir la Seguridad de la Información en el proceso de Continuidad del Negocio<br>A.14.1.2 - Continuidad del Negocio y Análisis de Riesgos<br>A.14.1.3 - Desarrollo e Implementación de Planes de Continuidad incluyendo Seguridad de la Información<br>A.14.1.4 - Marco de referencia para la planeación de Continuidad del Negocio<br>A.14.1.5 - Prueba, mantenimiento y reevaluación de los Planes de Continuidad |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | del Negocio |
| Infraestructura (Servidores) | 3 | Fallas de software | 3 | Falta de conocimiento del administrador del sistema | 2 | 3 | 8 | **B** | Los desarrolladores internos son certificados en el tema. Otras aplicaciones son contratadas con terceros especialistas en desarrollo. | 4 | 2 | **I** | **A** | A.8.1 - Previo a la Contratación<br>A.8.2- Durante la Contratación | A.8.1.3 - Términos y Condiciones de Empleo<br>A.8.2.2 - Educación, Capacitación y Concientización en Seguridad de la Información |
| Infraestructura (Servidores) | 3 | Fallas de software | 3 | Falta de actualización periódica de versiones o parches sobre el sistema operativo | 2 | 3 | 8 | **B** | Se tiene implementado y en funcionamiento el aplicativo WSUS, con el cual se actualizan los parches de los servidores Windows. | 4 | 2 | **I** | **A** | A.12.5 - Seguridad en los Procesos de Desarrollo y Soporte<br>A.15.2 - Cumplimiento Técnico, de Política de Seguridad y Estándares | A.12.5.1- Procedimientos de Control de Cambios<br>A.12.5.2 - Revisión Técnica de Aplicaciones después de Cambios al Sistema Operativo<br>A.15.2.1 - Cumplimiento |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | con Políticas y Estándares de Seguridad |
| Infraestructura (Servidores) | 3 | Software malicioso | 4 | Supervisión inadecuada al grupo de desarrolladores | 4 | 4 | 12 | **M** | Se realiza seguimiento por medio de cronogramas | 3 | 4 | **I** | **A** | A.10.10 - Monitoreo | A.10.10.1 - Registros de AuditoríaA.10.10.2 - Monitoreo del Uso del SistemaA.10.10.3 - Protección de los Registros de AuditoríaA.10.10.4 - Registros de Administración y de OperaciónA.10.10.5 - Registro de Fallas |
| Infraestructura (Servidores) | 3 | Errores humanos | 3 | Falta de documentación | 2 | 3 | 8 | **B** | Se tienen manuales técnicos y de operación. Cuando se contrata un desarrollo se exige la documentación técnica y de operación de la aplicación. | 3 | 3 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas | A.10.1.1 - Procedimientos Operativos Documentados |
| Infraestructura (Servidores) | 3 | Errores humanos | 3 | Falta de conocimiento del administrador del sistema | 2 | 3 | 8 | **B** | Los desarrolladores internos son certificados en el tema. Otras aplicaciones son contratadas con terceros especialistas | 4 | 2 | **I** | **A** | A.8.1 - Previo a la Contratación A.8.2- Durante la Contratación | A.8.1.3 - Términos y Condiciones de Empleo A.8.2.2 - Educación, |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | en desarrollo. | | | | | | Capacitación y Concientización en Seguridad de la Información |
| Infraestructura (Servidores) | 3 | Problemas de operación o administración por ausencia de personal | 2 | Falta de documentación | 2 | 2 | 6 | **B** | Se tienen manuales técnicos y de operación. Cuando se contrata un desarrollo se exige la documentación técnica y de operación de la aplicación. | 3 | 2 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas | A.10.1.1 - Procedimientos Operativos Documentados |
| Infraestructura (Servidores) | 3 | Problemas de operación o administración por ausencia de personal | 2 | Falta de contingencias de respaldo de personal crítico | 4 | 3 | 9 | **B** | El administrador del sistema cuenta con un backup para la realización de las tareas propias de su labor | 4 | 2 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas | A.10.1.3 - Segregación de Funciones |
| Infraestructura (Servidores) | 3 | Robo del código fuente de la Aplicación | 3 | Falta de controles de acceso lógico | 4 | 4 | 11 | **M** | El mecanismo de acceso al sistema es a través de usuario y contraseña. Se adquirió la herramienta Visual Source Safe, para el manejo de los códigos fuente, pero aun no esta en operación. | 3 | 4 | **I** | **A** | A.11.2 - Gestión de Acceso de Usuarios<br>A.11.3 - Responsabilidades del Usuario | A.11.2.2 - Gestión de Privilegios<br>A.11.2.3 - Gestión de Contraseñas de Usuario<br>A.11.2.4 - Revisión de derechos de Acceso<br>A.11.3.1 - Uso de Contraseñas<br>A.11.3.2 - Equipos Desatendidos<br>A.11.3.3 - Política de escritorio y |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | Pantalla Limpia |
| Infraestructura (Servidores) | 3 | Robo del código fuente de la Aplicación | 3 | Debilidad en las contraseñas | 3 | 3 | 9 | **B** | Aunque almacena las contraseñas cifradas, no se tienen definidas o no se aplican políticas de contraseñas. | 3 | 3 | **I** | **A** | A.11.1 - Requerimientos de Negocio para el Control de Acceso<br>A.11.3 - Responsabilidades del Usuario | A.11.1.1 - Política de Control de Acceso<br>A.11.3.1 - Uso de Contraseñas |
| Infraestructura (Servidores) | 3 | Robo del código fuente de la Aplicación | 3 | Copias no restringidas de datos o software | 4 | 4 | 11 | **M** | No existe control.<br>Se adquirió la herramienta Visual Source Safe, para el manejo de los códigos fuente, pero aun no esta en operación. | 3 | 4 | **I** | **A** | A.7.2 - Clasificación de la información<br>A.11.2 - Gestión de Acceso de Usuarios | A.7.2.1 - Guías de Clasificación<br>A.7.2.2 - Manipulación y Rotulado de la Información<br>A.11.2.2 - Gestión de Privilegios<br>A.11.2.4 - Revisión de Derechos de Acceso |
| Infraestructura (Servidores) | 3 | Robo del código fuente de la Aplicación | 3 | Segregación inadecuada de funciones | 3 | 3 | 9 | **B** | Unicamente los desarrolladores tienen acceso al código fuente.<br>Se adquirió la herramienta Visual Source Safe, para el manejo de los códigos fuente, pero aun no esta en operación. | 4 | 2 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.11.2 - Gestión de Acceso de Usuarios | A.10.1.3 - Segregación de Funciones<br>A.11.2.2 - Gestión de privilegios<br>A.11.2.4 - Revisión de Derechos de |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | Acceso |
| Infraestructura (Servidores) | 3 | Robo del código fuente de la Aplicación | 3 | Falta de comunicación entre las áreas de Recursos Humanos y Dirección de Planeación y Sistemas con respecto a la salida de personal de la organización | 4 | 4 | 11 | **M** | No existe control | 1 | 11 | **M** | **I** | A.8.3 - Terminación o Cambio de Empleo | A.8.3.1 - Responsabilidades de Terminación<br>A.8.3.3 - Eliminación de Derechos de Acceso |
| | | | | | | | | | | | | | | | |
| Redes y Comunicaciones | 4 | Acceso lógico no autorizado al sistema | 4 | Falta de revisión de la auditoría a la actividad sobre el sistema de información | 3 | 4 | 14 | **M** | Se revisa únicamente cuando es necesario, pero no se tienen procedimientos de revisión de logs. | 2 | 7 | **B** | **T** | A.10.10 - Monitoreo | A.10.10.1 - Registros de Auditoría<br>A.10.10.2 - Monitoreo del Uso del Sistema<br>A.10.10.3 - Protección de los Registros de Auditoría |
| Redes y Comunicaciones | 4 | Acceso no autorizado al sistema con privilegios de administrador | 3 | Acceso de los desarrolladores a ambientes productivos | 4 | 4 | 14 | **M** | No existe control | 2 | 7 | **B** | **T** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.11.2 - Gestión de Acceso de Usuarios | A.10.1.2 - Gestión del Cambio<br>A.10.1.3 - Segregación de Funciones<br>A.10.1.4 - Separación de Ambientes de Desarrollo, Prueba y Producción |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | A.11.2.2 - Gestión de Privilegios<br>A.11.2.4 - Revisión de derechos de Acceso |
| Redes y Comunicaciones | 4 | Acceso no autorizado al sistema con privilegios de administrador | 3 | Falta de revisión de la auditoría a la actividad sobre el sistema de información | 3 | 3 | 12 | **M** | Se revisa únicamente cuando es necesario, pero no se tienen procedimientos de revisión de logs. | 2 | 6 | **B** | **T** | A.10.10 - Monitoreo | A.10.10.1 - Registros de Auditoría<br>A.10.10.2 - Monitoreo del Uso del Sistema<br>A.10.10.3 - Protección de los Registros de Auditoría |
| Redes y Comunicaciones | 4 | Cambios de la configuración del sistema | 3 | Acceso de los desarrolladores a ambientes productivos | 4 | 4 | 14 | **M** | No existe control | 2 | 7 | **B** | **T** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.11.2 - Gestión de Acceso de Usuarios | A.10.1.2 - Gestión del Cambio<br>A.10.1.3 - Segregación de Funciones<br>A.10.1.4 - Separación de Ambientes de Desarrollo, Prueba y Producción<br>A.11.2.2 - Gestión de Privilegios<br>A.11.2.4 - Revisión de derechos de Acceso |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Redes y Comunicaciones | 4 | Errores de programación | 3 | Acceso de los desarrolladores a ambientes productivos | 4 | 4 | 14 | **M** | Se tiene un esquema pruebas, para validar los cambios antes de llevarlos a producción. Estas pruebas se realizan en la estación de trabajo del desarrollador. | 2 | 7 | **B** | **T** | A.10.1 - Procedimientos y Responsabilidades Operativas A.11.2 - Gestión de Acceso de Usuarios | A.10.1.2 - Gestión del Cambio A.10.1.3 - Segregación de Funciones A.10.1.4 - Separación de Ambientes de Desarrollo, Prueba y Producción A.11.2.2 - Gestión de Privilegios A.11.2.4 - Revisión de derechos de Acceso |
| Redes y Comunicaciones | 4 | Acceso lógico no autorizado al sistema | 4 | Debilidad en las contraseñas | 3 | 4 | 14 | **M** | Aunque almacena las contraseñas cifradas, no se tienen definidas o no se aplican políticas de contraseñas. | 3 | 5 | **I** | **A** | A.11.1 - Requerimientos de Negocio para el Control de Acceso A.11.3 - Responsabilidades del Usuario | A.11.1.1 - Política de Control de Acceso A.11.3.1 - Uso de Contraseñas |
| Redes y Comunicaciones | 4 | Acceso lógico no autorizado al sistema | 4 | La comunicación no se maneja por un canal encriptado. | 5 | 5 | 18 | **A** | No existe control | 1 | 18 | **A** | **I** | A.10.9 - Servicios de Comercio ElectrónicoA.12.3 - Controles criptograficos | A.10.9.2 Transacciones el líneaA.12.3.1. Política de uso de los controles criptográficos |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Redes y Comunicaciones | 4 | Errores de programación | 3 | Falta de controles sobre la gestión del cambio | 3 | 3 | 12 | **M** | Se tiene un esquema pruebas, para validar los cambios antes de llevarlos a producción. Estas pruebas se realizan en la estación de trabajo del desarrollador. Los cambios son aprobados por el área dueña del aplicativo. | 1 | 12 | **M** | **I** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.12.5 - Seguridad en los procesos de Desarrollo y Soporte | A.10.1.1 - Procedimientos Operativos Documentados<br>A.10.1.2 - Gestión del Cambio<br>A.12.5.1 - Procedimientos de Control de Cambios |
| Redes y Comunicaciones | 4 | Fallas de software | 3 | Falta de controles sobre la gestión del cambio | 3 | 3 | 12 | **M** | Todos los cambios en la aplicación son aprobados y validados en un ambiente de pruebas. Se dejan actas de los cambios realizados. | 4 | 3 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.12.5 - Seguridad en los procesos de Desarrollo y Soporte | A.10.1.1 - Procedimientos Operativos Documentados<br>A.10.1.2 - Gestión del Cambio<br>A.12.5.1 - Procedimientos de Control de Cambios |
| Redes y Comunicaciones | 4 | Acceso físico no autorizado al servidor | 2 | Ubicación inadecuada del servidor | 1 | 2 | 6 | **B** | El servidor esta alojado en el Centro de Computo del contratista, el cual cuenta con las medidas de seguridad adecuadas. | 4 | 2 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.1 - Perímetro de Seguridad Física<br>A.9.1.2 - Controles de Acceso Físico<br>A.9.1.6 - Acceso Público, y Areas de Carga y Descarga |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Redes y Comunicaciones | 4 | Acceso físico no autorizado al servidor | 2 | Falta de controles de acceso físico | 1 | 2 | 6 | **B** | El acceso físico al servidor esta restringido por la ETB. | 4 | 2 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.1 - Perímetro de Seguridad Física<br>A.9.1.2 - Controles de Acceso Físico<br>A.9.1.6 - Acceso Público, y Areas de Carga y Descarga |
| Redes y Comunicaciones | 4 | Problemas de temperatura y humedad | 2 | Ubicación en áreas susceptibles a temperaturas y humedad extremas | 2 | 2 | 8 | **B** | En el Centro de Computo del contratista se hace control de las condiciones ambientales | 4 | 2 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.4 - Protección contra amenazas externas y ambientales |
| Redes y Comunicaciones | 4 | Problemas de temperatura y humedad | 2 | Monitoreo inadecuado de las condiciones ambientales | 1 | 2 | 6 | **B** | En el Centro de Computo de la SDS se hace control de las condiciones ambientales.<br>Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable del mantenimiento de los mismos. | 4 | 2 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.4 - Protección contra amenazas externas y ambientales |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Redes y Comunicaciones | 4 | Problemas de temperatura y humedad | 2 | Falta de planes de contingencia | 1 | 2 | 6 | **B** | En la actualidad no se tienen definidos planes de contingencia para ninguno de los servidores sobre los que opera este sistema de información.<br>Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable de la contingencia de los mismos. | 4 | 2 | **I** | **A** | A.14.1 - Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio | A.14.1.1 - Incluir la Seguridad de la Información en el proceso de Continuidad del Negocio<br>A.14.1.2 - Continuidad del Negocio y Análisis de Riesgos<br>A.14.1.3 - Desarrollo e Implementación de Planes de Continuidad incluyendo Seguridad de la Información<br>A.14.1.4 - Marco de referencia para la planeación de Continuidad del Negocio<br>A.14.1.5 - Prueba, mantenimiento y reevaluación de los Planes de Continuidad |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | del Negocio |
| Redes y Comunicaciones | 4 | Acceso lógico no autorizado al sistema | 4 | Falta de controles de acceso lógico | 4 | 4 | 16 | **A** | El mecanismo de acceso a la aplicación es a través de usuario y contraseña, tanto para los usuarios normales, como para los usuarios administradores. | 3 | 5 | **B** | **T** | A.11.2 - Gestión de Acceso de Usuarios<br>A.11.3 - Responsabilidades del Usuario | A.11.2.2 - Gestión de Privilegios<br>A.11.2.3 - Gestión de Contraseñas de Usuario<br>A.11.2.4 - Revisión de derechos de Acceso<br>A.11.3.1 - Uso de Contraseñas<br>A.11.3.2 - Equipos Desatendidos<br>A.11.3.3 - Política de escritorio y Pantalla Limpia |
| Redes y Comunicaciones | 4 | Acceso lógico no autorizado al sistema | 4 | Préstamo de usuarios y contraseñas | 3 | 4 | 14 | **M** | Los usuarios administradores, tiene un único usuario y contraseña. Para los usuarios normales, no | 3 | 5 | **I** | **A** | A.11.3 - Responsabilidades del Usuario | A.11.3.1 - Uso de Contraseñas |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | se tienen políticas de contraseñas. | | | | | | | |
| Redes y Comunicaciones | 4 | Errores de programación | 3 | Procedimientos inadecuados del ciclo de vida de desarrollo de sistemas | 3 | 3 | 12 | **M** | Se utilizan metodologias RUP y Agile XP RUP | 4 | 3 | **I** | **A** | A.12.1 - Requerimientos de Seguridad en Sistemas de Información | A.12.1.1 - Requerimientos de Seguridad en Análisis y Especificación |
| Redes y Comunicaciones | 4 | Errores de programación | 3 | Falta de conocimiento de los desarrolladores | 2 | 3 | 10 | **B** | Los desarrolladores internos son certificados en el tema. Otras aplicaciones son contratadas con terceros especialistas en desarrollo. | 4 | 3 | **I** | **A** | A.8.1 - Previo a la Contratación<br>A.8.2- Durante la Contratación | A.8.1.3 - Términos y Condiciones de Empleo<br>A.8.2.2 - Educación, Capacitación y Concientización en Seguridad de la Información |
| Redes y Comunicaciones | 4 | Errores de programación | 3 | Supervisión inadecuada al grupo de desarrolladores | 3 | 3 | 12 | **M** | Se realiza seguimiento por medio de cronogramas | 4 | 3 | **I** | **A** | A.10.10 - Monitoreo | A.10.10.1 - Registros de Auditoría<br>A.10.10.2 - Monitoreo del Uso del Sistema<br>A.10.10.3 - Protección de los Registros de Auditoría<br>A.10.10.4 - Registros de Administració |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | n y de Operación A.10.10.5 - Registro de Fallas |
| Redes y Comunicaciones | 4 | Fallas de hardware | 3 | Monitoreo inadecuado de las condiciones ambientales | 1 | 2 | 8 | **B** | En el Centro de Computo de la SDS se hace control de las condiciones ambientales. Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable del mantenimiento de los mismos. | 4 | 2 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.4 - Protección contra amenazas externas y ambientales |
| Redes y Comunicaciones | 4 | Fallas de hardware | 3 | Mantenimiento inadecuado del servidor | 2 | 3 | 10 | **B** | Se tiene un contrato de mantenimiento de servidores con una empresa externa, sin embargo, la renovación anual del contrato no es inmediata, por lo que existe un periodo de "inestabilidad", entre el vencimiento y la nueva contratación.Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable del mantenimiento de los mismos. | 3 | 3 | **I** | **A** | A.9.2 - Seguridad del equipamentoA.10.2 - Gestión de Servicios Prestados por Terceros | A.9.2.4 - Mantenimiento de EquiposA.9.2.7 - Extracción de la PropiedadA.10.2.1 - Prestación del Servicio |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Redes y Comunicaciones | 4 | Fallas de hardware | 3 | Falta de planes de contingencia | 1 | 2 | 8 | **B** | En la actualidad no se tienen definidos planes de contingencia para ninguno de los servidores sobre los que opera este sistema de información.<br>Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable de la contingencia de los mismos. | 4 | 2 | **I** | **A** | A.14.1 - Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio | A.14.1.1 - Incluir la Seguridad de la Información en el proceso de Continuidad del Negocio<br>A.14.1.2 - Continuidad del Negocio y Análisis de Riesgos<br>A.14.1.3 - Desarrollo e Implementación de Planes de Continuidad incluyendo Seguridad de la Información<br>A.14.1.4 - Marco de referencia para la planeación de Continuidad del Negocio<br>A.14.1.5 - Prueba, mantenimiento y reevaluación de los Planes de Continuidad |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | del Negocio |
| Redes y Comunicaciones | 4 | Fallas de software | 3 | Falta de conocimiento del administrador del sistema | 2 | 3 | 10 | **B** | Los desarrolladores internos son certificados en el tema. Otras aplicaciones son contratadas con terceros especialistas en desarrollo. | 4 | 3 | **I** | **A** | A.8.1 - Previo a la Contratación<br>A.8.2- Durante la Contratación | A.8.1.3 - Términos y Condiciones de Empleo<br>A.8.2.2 - Educación, Capacitación y Concientización en Seguridad de la Información |
| Redes y Comunicaciones | 4 | Fallas de software | 3 | Falta de actualización periódica de versiones o parches sobre el sistema operativo | 2 | 3 | 10 | **B** | Se tiene implementado y en funcionamiento el aplicativo WSUS, con el cual se actualizan los parches de los servidores Windows. | 4 | 3 | **I** | **A** | A.12.5 - Seguridad en los Procesos de Desarrollo y Soporte<br>A.15.2 - Cumplimiento Técnico, de Política de Seguridad y Estándares | A.12.5.1- Procedimientos de Control de Cambios<br>A.12.5.2 - Revisión Técnica de Aplicaciones después de Cambios al Sistema Operativo<br>A.15.2.1 - Cumplimiento |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | con Políticas y Estándares de Seguridad |
| Redes y Comunicaciones | 4 | Software malicioso | 4 | Supervisión inadecuada al grupo de desarrolladores | 4 | 4 | 16 | **A** | Se realiza seguimiento por medio de cronogramas | 3 | 5 | **B** | **T** | A.10.10 - Monitoreo | A.10.10.1 - Registros de Auditoría<br>A.10.10.2 - Monitoreo del Uso del Sistema<br>A.10.10.3 - Protección de los Registros de Auditoría<br>A.10.10.4 - Registros de Administración y de Operación<br>A.10.10.5 - Registro de Fallas |
| Redes y Comunicaciones | 4 | Errores humanos | 3 | Falta de documentación | 2 | 3 | 10 | **B** | Se tienen manuales técnicos y de operación. Cuando se contrata un desarrollo se exige la documentación técnica y de operación de la aplicación. | 3 | 3 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas | A.10.1.1 - Procedimientos Operativos Documentados |
| Redes y Comunicaciones | 4 | Errores humanos | 3 | Falta de conocimiento del administrador del sistema | 2 | 3 | 10 | **B** | Los desarrolladores internos son certificados en el tema. Otras aplicaciones son contratadas con terceros especialistas en desarrollo. | 4 | 3 | **I** | **A** | A.8.1 - Previo a la Contratación<br>A.8.2- Durante la Contratación | A.8.1.3 - Términos y Condiciones de Empleo<br>A.8.2.2 - Educación, Capacitación |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | y Concientización en Seguridad de la Información |
| Redes y Comunicaciones | 4 | Problemas de operación o administración por ausencia de personal | 2 | Falta de documentación | 2 | 2 | 8 | **B** | Se tienen manuales técnicos y de operación. Cuando se contrata un desarrollo se exige la documentación técnica y de operación de la aplicación. | 3 | 3 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas | A.10.1.1 - Procedimientos Operativos Documentados |
| Redes y Comunicaciones | 4 | Problemas de operación o administración por ausencia de personal | 2 | Falta de contingencias de respaldo de personal crítico | 4 | 3 | 12 | **M** | El administrador del sistema cuenta con un backup para la realización de las tareas propias de su labor | 4 | 3 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas | A.10.1.3 - Segregación de Funciones |
| Redes y Comunicaciones | 4 | Robo del código fuente de la Aplicación | 3 | Falta de controles de acceso lógico | 4 | 4 | 14 | **M** | El mecanismo de acceso al sistema es a través de usuario y contraseña. Se adquirió la herramienta Visual Source Safe, para el manejo de los códigos fuente, pero aun no esta en operación. | 3 | 5 | **I** | **A** | A.11.2 - Gestión de Acceso de Usuarios<br>A.11.3 - Responsabilidades del Usuario | A.11.2.2 - Gestión de Privilegios<br>A.11.2.3 - Gestión de Contraseñas de Usuario<br>A.11.2.4 - Revisión de derechos de Acceso<br>A.11.3.1 - Uso de Contraseñas<br>A.11.3.2 - Equipos Desatendidos<br>A.11.3.3 - Política de escritorio y Pantalla |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | Limpia |
| Redes y Comunicaciones | 4 | Robo del código fuente de la Aplicación | 3 | Debilidad en las contraseñas | 3 | 3 | 12 | **M** | Aunque almacena las contraseñas cifradas, no se tienen definidas o no se aplican políticas de contraseñas. | 3 | 4 | **I** | **A** | A.11.1 - Requerimientos de Negocio para el Control de Acceso<br>A.11.3 - Responsabilidades del Usuario | A.11.1.1 - Política de Control de Acceso<br>A.11.3.1 - Uso de Contraseñas |
| Redes y Comunicaciones | 4 | Robo del código fuente de la Aplicación | 3 | Copias no restringidas de datos o software | 4 | 4 | 14 | **M** | No existe control.<br>Se adquirió la herramienta Visual Source Safe, para el manejo de los códigos fuente, pero aun no esta en operación. | 3 | 5 | **I** | **A** | A.7.2 - Clasificación de la información<br>A.11.2 - Gestión de Acceso de Usuarios | A.7.2.1 - Guías de Clasificación<br>A.7.2.2 - Manipulación y Rotulado de la Información<br>A.11.2.2 - Gestión de Privilegios<br>A.11.2.4 - Revisión de Derechos de Acceso |
| Redes y Comunicaciones | 4 | Robo del código fuente de la Aplicación | 3 | Segregación inadecuada de funciones | 3 | 3 | 12 | **M** | Unicamente los desarrolladores tienen acceso al código fuente.<br>Se adquirió la herramienta Visual Source Safe, para el manejo de los códigos fuente, pero aun no esta en operación. | 4 | 3 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.11.2 - Gestión de Acceso de Usuarios | A.10.1.3 - Segregación de Funciones<br>A.11.2.2 - Gestión de privilegios<br>A.11.2.4 - Revisión de Derechos de |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | Acceso |
| Redes y Comunicaciones | 4 | Robo del código fuente de la Aplicación | 3 | Falta de comunicación entre las áreas de Recursos Humanos y Dirección de Planeación y Sistemas con respecto a la salida de personal de la organización | 4 | 4 | 14 | **M** | No existe control | 1 | 14 | **M** | **I** | A.8.3 - Terminación o Cambio de Empleo | A.8.3.1 - Responsabilidades de TerminaciónA.8.3.3 - Eliminación de Derechos de Acceso |
| | | | | | | | | | | | | | | | |
| Seguridad Informática | 4 | Acceso lógico no autorizado al sistema | 4 | Falta de revisión de la auditoría a la actividad sobre el sistema de información | 3 | 4 | 14 | **M** | Se revisa únicamente cuando es necesario, pero no se tienen procedimientos de revisión de logs. | 2 | 7 | **B** | **T** | A.10.10 - Monitoreo | A.10.10.1 - Registros de Auditoría A.10.10.2 - Monitoreo del Uso del Sistema A.10.10.3 - Protección de los Registros de Auditoría |
| Seguridad Informática | 4 | Acceso no autorizado al sistema con privilegios de administrador | 3 | Acceso de los desarrolladores a ambientes productivos | 4 | 4 | 14 | **M** | No existe control | 2 | 7 | **B** | **T** | A.10.1 - Procedimientos y Responsabilidades Operativas A.11.2 - Gestión de Acceso de Usuarios | A.10.1.2 - Gestión del Cambio A.10.1.3 - Segregación de Funciones A.10.1.4 - Separación de Ambientes de Desarrollo, Prueba y Producción |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | A.11.2.2 - Gestión de Privilegios<br>A.11.2.4 - Revisión de derechos de Acceso |
| Seguridad Informática | 4 | Acceso no autorizado al sistema con privilegios de administrador | 3 | Falta de revisión de la auditoría a la actividad sobre el sistema de información | 3 | 3 | 12 | **M** | Se revisa únicamente cuando es necesario, pero no se tienen procedimientos de revisión de logs. | 2 | 6 | **B** | **T** | A.10.10 - Monitoreo | A.10.10.1 - Registros de Auditoría<br>A.10.10.2 - Monitoreo del Uso del Sistema<br>A.10.10.3 - Protección de los Registros de Auditoría |
| Seguridad Informática | 4 | Cambios de la configuración del sistema | 3 | Acceso de los desarrolladores a ambientes productivos | 4 | 4 | 14 | **M** | No existe control | 2 | 7 | **B** | **T** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.11.2 - Gestión de Acceso de Usuarios | A.10.1.2 - Gestión del Cambio<br>A.10.1.3 - Segregación de Funciones<br>A.10.1.4 - Separación de Ambientes de Desarrollo, Prueba y Producción<br>A.11.2.2 - Gestión de Privilegios<br>A.11.2.4 - Revisión de derechos de Acceso |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Seguridad Informática | 4 | Errores de programación | 3 | Acceso de los desarrolladores a ambientes productivos | 4 | 4 | 14 | **M** | Se tiene un esquema pruebas, para validar los cambios antes de llevarlos a producción. Estas pruebas se realizan en la estación de trabajo del desarrollador. | 2 | 7 | **B** | **T** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.11.2 - Gestión de Acceso de Usuarios | A.10.1.2 - Gestión del Cambio<br>A.10.1.3 - Segregación de Funciones<br>A.10.1.4 - Separación de Ambientes de Desarrollo, Prueba y Producción<br>A.11.2.2 - Gestión de Privilegios<br>A.11.2.4 - Revisión de derechos de Acceso |
| Seguridad Informática | 4 | Acceso lógico no autorizado al sistema | 4 | Debilidad en las contraseñas | 3 | 4 | 14 | **M** | Aunque almacena las contraseñas cifradas, no se tienen definidas o no se aplican políticas de contraseñas. | 3 | 5 | **I** | **A** | A.11.1 - Requerimientos de Negocio para el Control de Acceso<br>A.11.3 - Responsabilidades del Usuario | A.11.1.1 - Política de Control de Acceso<br>A.11.3.1 - Uso de Contraseñas |
| Seguridad Informática | 4 | Acceso lógico no autorizado al sistema | 4 | La comunicación no se maneja por un canal encriptado. | 5 | 5 | 18 | **A** | No existe control | 1 | 18 | **A** | **I** | A.10.9 - Servicios de Comercio Electrónico<br>A.12.3 - Controles criptograficos | A.10.9.2 Transacciones el línea<br>A.12.3.1. Política de uso de los controles criptográficos |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Seguridad Informática | 4 | Errores de programación | 3 | Falta de controles sobre la gestión del cambio | 3 | 3 | 12 | **M** | Se tiene un esquema pruebas, para validar los cambios antes de llevarlos a producción. Estas pruebas se realizan en la estación de trabajo del desarrollador. Los cambios son aprobados por el área dueña del aplicativo. | 1 | 12 | **M** | **I** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.12.5 - Seguridad en los procesos de Desarrollo y Soporte | A.10.1.1 - Procedimientos Operativos Documentados<br>A.10.1.2 - Gestión del Cambio<br>A.12.5.1 - Procedimientos de Control de Cambios |
| Seguridad Informática | 4 | Fallas de software | 3 | Falta de controles sobre la gestión del cambio | 3 | 3 | 12 | **M** | Todos los cambios en la aplicación son aprobados y validados en un ambiente de pruebas. Se dejan actas de los cambios realizados. | 4 | 3 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.12.5 - Seguridad en los procesos de Desarrollo y Soporte | A.10.1.1 - Procedimientos Operativos Documentados<br>A.10.1.2 - Gestión del Cambio<br>A.12.5.1 - Procedimientos de Control de Cambios |
| Seguridad Informática | 4 | Acceso físico no autorizado al servidor | 2 | Ubicación inadecuada del servidor | 1 | 2 | 6 | **B** | El servidor esta alojado en el Centro de Computo del contratista, el cual cuenta con las medidas de seguridad adecuadas. | 4 | 2 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.1 - Perímetro de Seguridad Física<br>A.9.1.2 - Controles de Acceso Físico<br>A.9.1.6 - Acceso Público, y Areas de Carga y Descarga |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Seguridad Informática | 4 | Acceso físico no autorizado al servidor | 2 | Falta de controles de acceso físico | 1 | 2 | 6 | **B** | El acceso físico al servidor esta restringido por la ETB. | 4 | 2 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.1 - Perímetro de Seguridad Física<br>A.9.1.2 - Controles de Acceso Físico<br>A.9.1.6 - Acceso Público, y Areas de Carga y Descarga |
| Seguridad Informática | 4 | Problemas de temperatura y humedad | 2 | Ubicación en áreas susceptibles a temperaturas y humedad extremas | 2 | 2 | 8 | **B** | En el Centro de Computo del contratista se hace control de las condiciones ambientales | 4 | 2 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.4 - Protección contra amenazas externas y ambientales |
| Seguridad Informática | 4 | Problemas de temperatura y humedad | 2 | Monitoreo inadecuado de las condiciones ambientales | 1 | 2 | 6 | **B** | En el Centro de Computo de la SDS se hace control de las condiciones ambientales.<br>Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable del mantenimiento de los mismos. | 4 | 2 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.4 - Protección contra amenazas externas y ambientales |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Seguridad Informática | 4 | Problemas de temperatura y humedad | 2 | Falta de planes de contingencia | 1 | 2 | 6 | **B** | En la actualidad no se tienen definidos planes de contingencia para ninguno de los servidores sobre los que opera este sistema de información.<br>Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable de la contingencia de los mismos. | 4 | 2 | **I** | **A** | A.14.1 - Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio | A.14.1.1 - Incluir la Seguridad de la Información en el proceso de Continuidad del Negocio<br>A.14.1.2 - Continuidad del Negocio y Análisis de Riesgos<br>A.14.1.3 - Desarrollo e Implementación de Planes de Continuidad incluyendo Seguridad de la Información<br>A.14.1.4 - Marco de referencia para la planeación de Continuidad del Negocio<br>A.14.1.5 - Prueba, mantenimiento y reevaluación de los Planes de Continuidad |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | del Negocio |
| Seguridad Informática | 4 | Acceso lógico no autorizado al sistema | 4 | Falta de controles de acceso lógico | 4 | 4 | 16 | **A** | El mecanismo de acceso a la aplicación es a través de usuario y contraseña, tanto para los usuarios normales, como para los usuarios administradores. | 3 | 5 | **B** | **T** | A.11.2 - Gestión de Acceso de UsuariosA.11.3 - Responsabilidades del Usuario | A.11.2.2 - Gestión de PrivilegiosA.11.2.3 - Gestión de Contraseñas de UsuarioA.11.2.4 - Revisión de derechos de AccesoA.11.3.1 - Uso de Contraseñas A.11.3.2 - Equipos Desatendidos A.11.3.3 - Política de escritorio y Pantalla Limpia |
| Seguridad Informática | 4 | Acceso lógico no autorizado al sistema | 4 | Préstamo de usuarios y contraseñas | 3 | 4 | 14 | **M** | Los usuarios administradores, tiene un único usuario y contraseña. Para los usuarios normales, no | 3 | 5 | **I** | **A** | A.11.3 - Responsabilidades del Usuario | A.11.3.1 - Uso de Contraseñas |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | se tienen políticas de contraseñas. | | | | | | |
| Seguridad Informática | 4 | Errores de programación | 3 | Procedimientos inadecuados del ciclo de vida de desarrollo de sistemas | 3 | 3 | 12 | **M** | Se utilizan metodologias RUP y Agile XP RUP | 4 | 3 | **I** | **A** | A.12.1 - Requerimientos de Seguridad en Sistemas de Información | A.12.1.1 - Requerimientos de Seguridad en Análisis y Especificación |
| Seguridad Informática | 4 | Errores de programación | 3 | Falta de conocimiento de los desarrolladores | 2 | 3 | 10 | **B** | Los desarrolladores internos son certificados en el tema. Otras aplicaciones son contratadas con terceros especialistas en desarrollo. | 4 | 3 | **I** | **A** | A.8.1 - Previo a la Contratación<br>A.8.2- Durante la Contratación | A.8.1.3 - Términos y Condiciones de Empleo<br>A.8.2.2 - Educación, Capacitación y Concientización en Seguridad de la Información |
| Seguridad Informática | 4 | Errores de programación | 3 | Supervisión inadecuada al grupo de desarrolladores | 3 | 3 | 12 | **M** | Se realiza seguimiento por medio de cronogramas | 4 | 3 | **I** | **A** | A.10.10 - Monitoreo | A.10.10.1 - Registros de Auditoría<br>A.10.10.2 - Monitoreo del Uso del Sistema<br>A.10.10.3 - Protección de los Registros de Auditoría<br>A.10.10.4 - Registros de Administració |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | n y de Operación A.10.10.5 - Registro de Fallas |
| Seguridad Informática | 4 | Fallas de hardware | 3 | Monitoreo inadecuado de las condiciones ambientales | 1 | 2 | 8 | **B** | En el Centro de Computo de la SDS se hace control de las condiciones ambientales. Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable del mantenimiento de los mismos. | 4 | 2 | **I** | **A** | A.9.1 - Areas Seguras | A.9.1.4 - Protección contra amenazas externas y ambientales |
| Seguridad Informática | 4 | Fallas de hardware | 3 | Mantenimiento inadecuado del servidor | 2 | 3 | 10 | **B** | Se tiene un contrato de mantenimiento de servidores con una empresa externa, sin embargo, la renovación anual del contrato no es inmediata, por lo que existe un periodo de "inestabilidad", entre el vencimiento y la nueva contratación. Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable del mantenimiento de los mismos. | 3 | 3 | **I** | **A** | A.9.2 - Seguridad del equipamento A.10.2 - Gestión de Servicios Prestados por Terceros | A.9.2.4 - Mantenimiento de Equipos A.9.2.7 - Extracción de la Propiedad A.10.2.1 - Prestación del Servicio |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Seguridad Informática | 4 | Fallas de hardware | 3 | Falta de planes de contingencia | 1 | 2 | 8 | **B** | En la actualidad no se tienen definidos planes de contingencia para ninguno de los servidores sobre los que opera este sistema de información.<br>Para los servidores y aplicaciones que se tienen en ETB, esta empresa es la responsable de la contingencia de los mismos. | 4 | 2 | **I** | **A** | A.14.1 - Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio | A.14.1.1 - Incluir la Seguridad de la Información en el proceso de Continuidad del Negocio<br>A.14.1.2 - Continuidad del Negocio y Análisis de Riesgos<br>A.14.1.3 - Desarrollo e Implementación de Planes de Continuidad incluyendo Seguridad de la Información<br>A.14.1.4 - Marco de referencia para la planeación de Continuidad del Negocio<br>A.14.1.5 - Prueba, mantenimiento y reevaluación de los Planes de Continuidad |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | del Negocio |
| Seguridad Informática | 4 | Fallas de software | 3 | Falta de conocimiento del administrador del sistema | 2 | 3 | 10 | **B** | Los desarrolladores internos son certificados en el tema. Otras aplicaciones son contratadas con terceros especialistas en desarrollo. | 4 | 3 | **I** | **A** | A.8.1 - Previo a la Contratación<br>A.8.2- Durante la Contratación | A.8.1.3 - Términos y Condiciones de Empleo<br>A.8.2.2 - Educación, Capacitación y Concientización en Seguridad de la Información |
| Seguridad Informática | 4 | Fallas de software | 3 | Falta de actualización periódica de versiones o parches sobre el sistema operativo | 2 | 3 | 10 | **B** | Se tiene implementado y en funcionamiento el aplicativo WSUS, con el cual se actualizan los parches de los servidores Windows. | 4 | 3 | **I** | **A** | A.12.5 - Seguridad en los Procesos de Desarrollo y Soporte<br>A.15.2 - Cumplimiento Técnico, de Política de Seguridad y Estándares | A.12.5.1- Procedimientos de Control de Cambios<br>A.12.5.2 - Revisión Técnica de Aplicaciones después de Cambios al Sistema Operativo<br>A.15.2.1 - Cumplimiento |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | con Políticas y Estándares de Seguridad |
| Seguridad Informática | 4 | Software malicioso | 4 | Supervisión inadecuada al grupo de desarrolladores | 4 | 4 | 16 | **A** | Se realiza seguimiento por medio de cronogramas | 3 | 5 | **B** | **T** | A.10.10 - Monitoreo | A.10.10.1 - Registros de Auditoría<br>A.10.10.2 - Monitoreo del Uso del Sistema<br>A.10.10.3 - Protección de los Registros de Auditoría<br>A.10.10.4 - Registros de Administración y de Operación<br>A.10.10.5 - Registro de Fallas |
| Seguridad Informática | 4 | Errores humanos | 3 | Falta de documentación | 2 | 3 | 10 | **B** | Se tienen manuales técnicos y de operación. Cuando se contrata un desarrollo se exige la documentación técnica y de operación de la aplicación. | 3 | 3 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas | A.10.1.1 - Procedimientos Operativos Documentados |
| Seguridad Informática | 4 | Errores humanos | 3 | Falta de conocimiento del administrador del sistema | 2 | 3 | 10 | **B** | Los desarrolladores internos son certificados en el tema. Otras aplicaciones son contratadas con terceros especialistas en desarrollo. | 4 | 3 | **I** | **A** | A.8.1 - Previo a la Contratación<br>A.8.2- Durante la Contratación | A.8.1.3 - Términos y Condiciones de Empleo<br>A.8.2.2 - Educación, Capacitación |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | y Concientización en Seguridad de la Información |
| Seguridad Informática | 4 | Problemas de operación o administración por ausencia de personal | 2 | Falta de documentación | 2 | 2 | 8 | **B** | Se tienen manuales técnicos y de operación. Cuando se contrata un desarrollo se exige la documentación técnica y de operación de la aplicación. | 3 | 3 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas | A.10.1.1 - Procedimientos Operativos Documentados |
| Seguridad Informática | 4 | Problemas de operación o administración por ausencia de personal | 2 | Falta de contingencias de respaldo de personal crítico | 4 | 3 | 12 | **M** | El administrador del sistema cuenta con un backup para la realización de las tareas propias de su labor | 4 | 3 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas | A.10.1.3 - Segregación de Funciones |
| Seguridad Informática | 4 | Robo del código fuente de la Aplicación | 3 | Falta de controles de acceso lógico | 4 | 4 | 14 | **M** | El mecanismo de acceso al sistema es a través de usuario y contraseña. Se adquirió la herramienta Visual Source Safe, para el manejo de los códigos fuente, pero aun no esta en operación. | 3 | 5 | **I** | **A** | A.11.2 - Gestión de Acceso de Usuarios<br>A.11.3 - Responsabilidades del Usuario | A.11.2.2 - Gestión de Privilegios<br>A.11.2.3 - Gestión de Contraseñas de Usuario<br>A.11.2.4 - Revisión de derechos de Acceso<br>A.11.3.1 - Uso de Contraseñas<br>A.11.3.2 - Equipos Desatendidos<br>A.11.3.3 - Política de escritorio y Pantalla |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | Limpia |
| Seguridad Informática | 4 | Robo del código fuente de la Aplicación | 3 | Debilidad en las contraseñas | 3 | 3 | 12 | **M** | Aunque almacena las contraseñas cifradas, no se tienen definidas o no se aplican políticas de contraseñas. | 3 | 4 | **I** | **A** | A.11.1 - Requerimientos de Negocio para el Control de Acceso<br>A.11.3 - Responsabilidades del Usuario | A.11.1.1 - Política de Control de Acceso<br>A.11.3.1 - Uso de Contraseñas |
| Seguridad Informática | 4 | Robo del código fuente de la Aplicación | 3 | Copias no restringidas de datos o software | 4 | 4 | 14 | **M** | No existe control.<br>Se adquirió la herramienta Visual Source Safe, para el manejo de los códigos fuente, pero aun no esta en operación. | 3 | 5 | **I** | **A** | A.7.2 - Clasificación de la información<br>A.11.2 - Gestión de Acceso de Usuarios | A.7.2.1 - Guías de Clasificación<br>A.7.2.2 - Manipulación y Rotulado de la Información<br>A.11.2.2 - Gestión de Privilegios<br>A.11.2.4 - Revisión de Derechos de Acceso |
| Seguridad Informática | 4 | Robo del código fuente de la Aplicación | 3 | Segregación inadecuada de funciones | 3 | 3 | 12 | **M** | Unicamente los desarrolladores tienen acceso al código fuente.<br>Se adquirió la herramienta Visual Source Safe, para el manejo de los códigos fuente, pero aun no esta en operación. | 4 | 3 | **I** | **A** | A.10.1 - Procedimientos y Responsabilidades Operativas<br>A.11.2 - Gestión de Acceso de Usuarios | A.10.1.3 - Segregación de Funciones<br>A.11.2.2 - Gestión de privilegios<br>A.11.2.4 - Revisión de Derechos de |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | Acceso |
| Seguridad Informática | 4 | Robo del código fuente de la Aplicación | 3 | Falta de comunicación entre las áreas de Recursos Humanos y Dirección de Planeación y Sistemas con respecto a la salida de personal de la organización | 4 | 4 | 14 | **M** | No existe control | 1 | 14 | **M** | **I** | A.8.3 - Terminación o Cambio de Empleo | A.8.3.1 - Responsabilidades de Terminación A.8.3.3 - Eliminación de Derechos de Acceso |
| | | | | | | | | | | | | | | | |

## 4. ESQUEMA DE COPIAS DE RESPALDO

La SDS cuenta internamente con un proceso de respaldo de su información para el cual cuenta con una serie de recursos o elementos de software y hardware que interactúan dentro del mismo. Dentro de este documento *"Plan de Contingencia de la plataforma de TIC de la SDS"*, se expondrá también la arquitectura y el procedimiento de generación de las copias de respaldo de la entidad así como los elementos que conforman el mismo.

Para la definición de la Arquitectura en la SDS se tuvieron en cuenta aspectos actuales de la Infraestructura Tecnológica como el almacenamiento (Storage) relacionado con la SAN (Storage Area Network), los servidores que están involucrados en el proceso, las características y funcionalidades del producto de software *"CA Arcserve Backup r12 SP1"* que actualmente se encuentra en producción. La arquitectura en producción en la entidad trabajara en SAN y LAN.

**Clases de Respaldo**

Los métodos disponibles de respaldo son Total, Diferencial e Incremental, estos métodos permiten obtener y establecer requerimientos de recursos de backup (Tiempo y Medios).

**Tareas de Restauración**

| Método | Full | Diferencial | Incremental |
|---|---|---|---|
| Restaurar - Sistema | 1 Restauración | 2 Restauraciones | > 2 Restauraciones |
| Restaurar– Archivo/Datos | 1 Restauración | 1 Restauración | 1 Restauración |
| Utilización de Medios en Backup | Mayor | Menor que el Full | Menor que el diferencial |
| Ventana de Backup | Mayor Tiempo | Bueno | Mejor |

Por otra parte existen características de la herramienta que buscan mejorar los tiempos de respaldo con la finalidad de obtener ventanas de respaldo más pequeñas y que permitan la utilización máxima de los recursos de almacenamiento.

**Respaldo Total OFF LINE**

El respaldo total de la base de datos OFF LINE, implica que el servicio de la base de datos este abajo. Por consiguiente se requiere que el tiempo en el cual se realiza este respaldo no impacte en el servicio hacia los usuarios.

**Rosado Total ON LINE SQL Server**

Este respaldo incluye todos los objetos de la base de datos. El respaldo en línea permite respaldar las bases de datos sin afectar el servicio, para ello se debe tener en cuenta lo siguiente:

- Se debe tener un usuario con los privilegios de SA
- El servidor a respaldar debe tener instalado el agente de CA ARCSERVE BACKUP para SQL Server

**Respaldo Total ON LINE de Archivos Abiertos**

Este respaldo incluye todos archivos que estén abiertos en el momento del backup, exceptuando los archivos correspondientes a bases de datos y correo electrónico, para ello se debe tener en cuenta lo siguiente:

- El servidor a respaldar debe tener instalado el agente de CA ARCSERVE BACKUP para archivos abiertos

**Retención**

La retención de la información es uno de los aspectos importantes en la definición de los esquemas de respaldo. La necesidad de almacenar información histórica y el acuerdo con los usuarios permite establecer los periodos de protección de información que requiere la organización.

CA Arcserve Backup permite que el usuario defina la retención, defina los pool de medios, estimar el periodo de almacenamiento de los históricos, la utilización de medios y la clase de rotación (sobre escritura o append) que se va a utilizar.

a. Esquema de Rotación estándar. El esquema de rotación estándar utiliza un solo pool de medios, en este se controlan las cintas semanales y mensuales.

b. Esquema de Rotación GFS (GFS = Abuelo, Padre, Hijo). Esta clase de rotación utiliza tres (3) pool de medios (Diario, Semanal y Mensual), Esta rotación permite mejor control de entrada y salida de medios así como la retención de la información.

CA Arcserve Backup incluye seis (6) esquemas de rotación por defecto GFS y permite definir esquemas de rotación propios. Los esquemas predefinidos para GFS son:

a. 5-Day Weekly Full with GFS enabled.
b. 7-Day Full with GFS enabled.
c. 5-Day Incremental/Full on Friday with GFS enabled.
d. 7-Day Incremental/Full on Friday with GFS enabled.
e. 5-Day Differential/Full on Friday with GFS enabled.
f. 7-Day Differential/Full on Friday with GFS enabled.

### 4.1 Arquitectura de la solución de copias de respaldo

Para facilitar la comprensión de la arquitectura en operación, a continuación se describe de manera general cada uno de los componentes y el flujo de la información en dicha Arquitectura con CA Arcserve Backup R12 SP1.

Dominio: El dominio de CA Arcserve Backup es grupo lógico de servidores que permiten la administración de forma centralizada con el mismo usuario. La agrupación de servidores puede contener servidores de diversas plataformas. Cada dominio tiene un nombre y se asigna un servidor primario y un servidor secundario que permiten la validación de los usuarios y da funcionalidad de tolerancia a fallas. El servidor primario se sincroniza con el servidor secundario.

Manager: Permite administrar, configurar, generar las tareas de respaldo y recuperación, administrar la base de datos la cual es MSDE o Microsoft SQL Server de acuerdo al ambiente y el detalle de información a registrar, generar reportes entre otras. Los componentes principales en el manager son:

- Tape Engine: Responsable de la comunicación y control con los dispositivos de almacenamiento
- Database Engine: Registra todas las operaciones realizadas con CA Arcserve Backup, mantiene el histórico de archivos, directorios, drives y maquinas que CA Arcserve Backup ha respaldado o copiado, incluyendo el estado de las tareas procesadas y utilización de los medios.
- Job Engine: Procesa las tareas programadas.

**Opción de Librería TLO**: La opción de librería de Tapes permite la administración de la librería física de cintas desde la configuración, inventario, ingreso o retiro de cintas, lectura, creación de grupos entre otras en librerías que tengan 2 o más drives como es caso de la SDS que cuenta con una librería HP MSL 6026, con dos drive SDLT y dos magazines con 24 slots.

**Opción de SAN:** La opción Storage Area Network (SAN) habilita a los servidores de CA Arcserve Backup para compartir una o más librerías sobre una red de almacenamiento de alta velocidad, permitiendo que el respaldo realizado hacia la librería por cada servidor sea local. La SDS cuenta con tres SAN interconectadas con Fibre Chanel.

**Servidor Primario de Windows:** Es el servidor que inicializa las librerías compartidas y es el responsable de controlar la utilización, detección de cambios en el estado de los dispositivos en el ambiente Windows, en la entidad es el servidor “XXXXXXX” que tiene sistema operativo Windows Server 2003 R2**.**

**Servidor Distribuido o Secundario**: Son los servidores de CA Arcserve Backup que están asignados al servidor primario y conectado a la red de almacenamiento en SAN, compartiendo la librería.

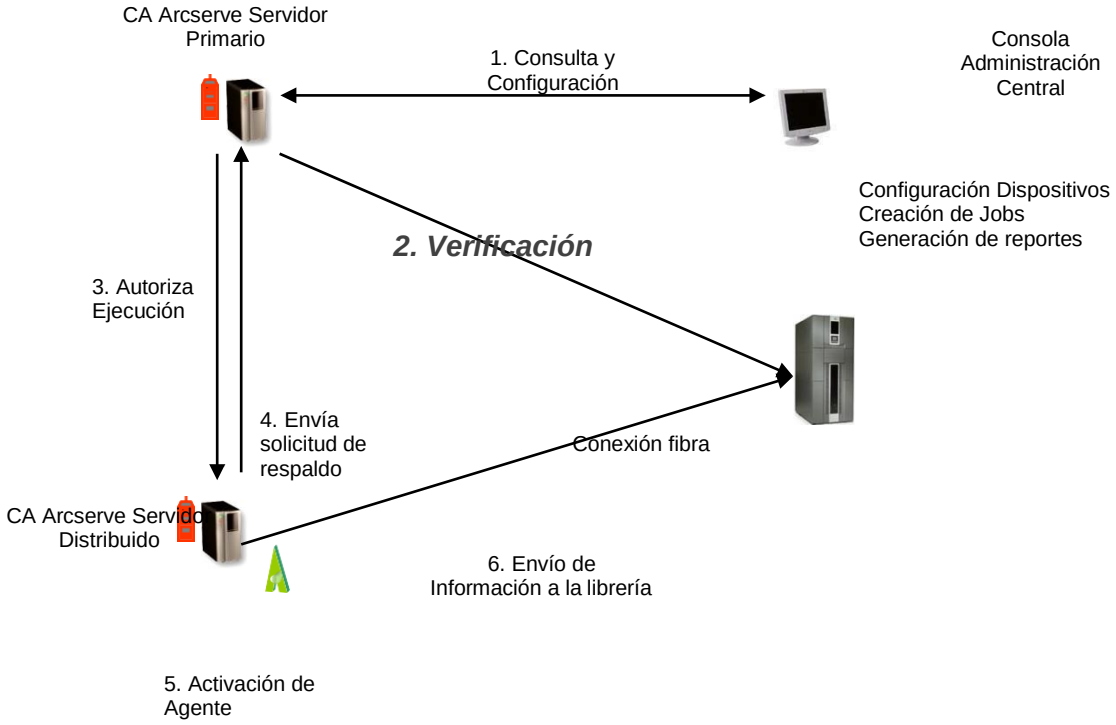
**Agente para SQL:** El agente de Microsoft SQL Server permite realizar el respaldo de las bases de datos en línea, manteniendo el servicio a los usuarios. El agente permite realizar el respaldo a objetos específicos, (Bases de Datos).

**Consola de Administración:** Es la interface de Administración de CA Arcserve Backup y permite:

- ✓ Ver la información de la base de datos
- ✓ Programar requerimientos de respaldo o restauración y acciones
- ✓ Ver el status de las tareas programas
- ✓ Configurar los grupos, dispositivos
- ✓ Generar alarmas
- ✓ Generar reportes

**Flujo de la información:** A continuación se describe el flujo de información entre los diferentes elementos para la ejecución de copias de respaldo sobre los servidores de la SDS a través de los agentes, y el funcionamiento de la estructura de *CA ARCSERVE BACKUP* en ambiente LAN.

**Figura No 1. FLUJO DE INFORMACIÓN**




Los servidores Windows que están involucrados en la solución de respaldo por LAN deben tener como mínimo el siguiente componente de CA Arcserve Backup instalado: CA ARCSERVE BACKUP Client Agent for Windows.

Los servidores Windows que están involucrados en la solución de respaldo y comparten el dispositivo de almacenamiento (respaldo via SAN), en este caso la librería de cintas, deben tener los siguientes componentes de CA Arcserve Backup instalados:

- CA Arcserve Backup Manager – Con este componente se instala el agente de sistema operativo y la opción de administración de la librería.

CA Arcserve Backup SAN

- CA Arcserve Backup TLO
- CA Arcserve Backup DRO
- Agente de Microsoft SQL Server si se requiere
- Agente de Microsoft Exchange Server si requiere
- Agente de Archivos Abiertos si requiere

Los servidores de CA Arcserve Backup en SAN están constituidos por un servidor primario y un número de servidores distribuidos. El servidor primario puede ser cualquier servidor que esté conectado en la SAN, sin embargo se recomienda que este servidor sea un servidor diferente a los servidores de producción, para este caso en particular el servidor primario de CA Arcserve Backup está en Windows y se llama XXXXXX.

El servidor primario tiene la función de controlar el flujo de información entre el grupo de servidores que componen la SAN, previniendo conflictos cuando dos o más servidores utilizan un dispositivo o medio al mismo tiempo y los datos que son enviados desde los servidores que tienen el Agente para Sistema Operativo. Cuando una tarea esta lista para ejecutarse, el dispositivo y el slot correspondiente al medio son reservados, en este punto el dispositivo (unidad de tape) no estará disponible para otra tarea enviada por cualquier servidor de la SAN o la LAN.

Las tareas de copias de respaldo, recuperación, etc., son ejecutadas desde XXXXXXX y los datos son enviados desde el equipo que se está respaldando hacia XXXXXXX, posteriormente los datos pasan directamente a la librería a través de la conexión de fibra. Es importante tener en cuenta que las tareas esperan por su ejecución mientras que una unidad de tape esta disponible.

**Arquitectura de la solución de copias de respaldo:** La arquitectura en operación para las copias de respaldo de los servidores Windows de la SDS se presenta en la siguiente figura:

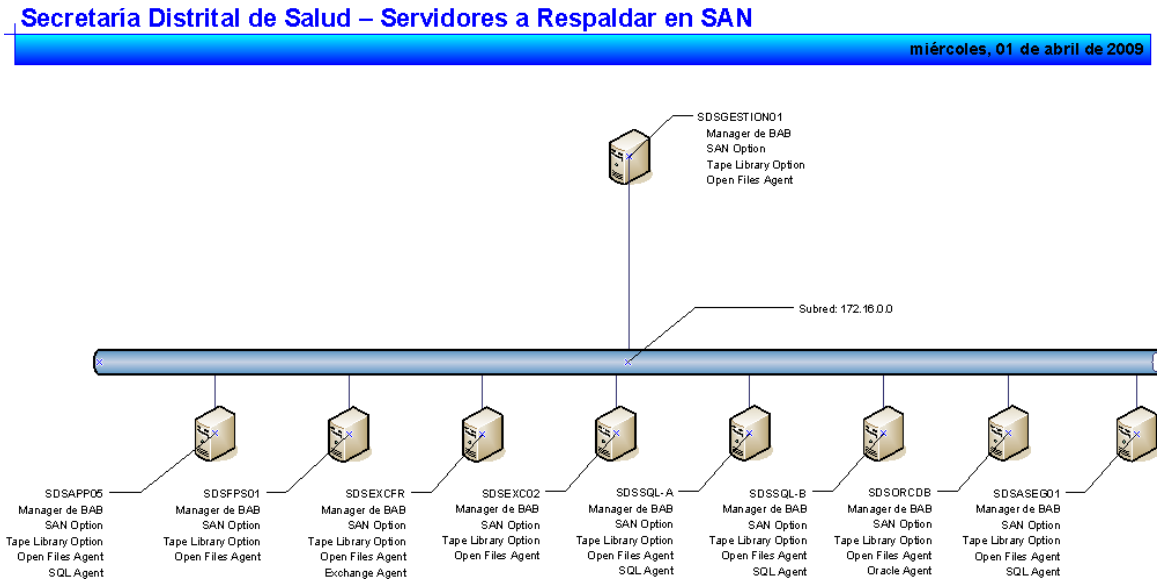



**Figura No. 2 Arquitectura Respaldo Ambiente Windows**

La estructura para las copias de respaldo está constituida por ocho (8) servidores de producción de aplicaciones y un servidor de administración de CA Arcserve Backup, denominado en la figura como XXXXXXX, que actuará como servidor primario de la solución. Así mismo XXXXXX se conecta a una librería de cintas HP MSL6026 con una capacidad inicial de dos (2) unidades de tape SDLT 160 / 320 y veintiséis (26) slots. Además tiene configurada una librería virtual de cintas HP VSL6200 donde se tienen presentadas dos (2) librerías virtuales HP MSL 6060 con 4 unidades LTO3 400 / 800 GB cada una de ellas.

Se debe tener en cuenta que de este punto en adelante se hablará de estas tres librerías (HP MSL6026 con 2 unidades SDLT 160/320 y 2 HP MSL6060 con 4 unidades LTO3 400/800GB cada una) de forma independiente. No se hará referencia si el respaldo irá a VTL o a la librería física debido a que para el sistema operativo y Arcserve las librerías las detecta como físicas. Por último se conectarán 2 unidades externas LTO3 marca IBM con interfaz SAS en el servidor XXXXXXX para poder tomar copia de las cintas de la VTL a cintas reales de tal forma que se puedan enviar a entidades de custodia externas a la entidad.

**Módulos Instalados por Servidor**

Los prerrequisitos para el inicio de la implantación son:

1. Tener habilitado y funcionando correctamente el Servidor Primario de la SAN en plataforma Windows.
2. Validación de cuadro de dispositivos y firmware con base en los certificados por CA Arcserve Backup r12 SP1.
3. Unidades de tape conectadas a los servidores y reconocidas por el sistema operativo.
4. Creación de usuario **–BACKUP-** en el dominio SDS con los permisos y privilegios: Actuar como parte del sistema operativo, iniciar sesión como un servicio, iniciar sesión localmente además debe pertenecer al grupo administradores, operadores de copia de seguridad y administradores de dominio.
5. Conexión vía IP verificada entre los servidores que componen la solución.
6. Licencia de CA Arcserve Backup r12 disponible.
7. Medios de CA Arcserve Backup r12 SP1para instalación disponibles.

**Configuración del Servidor Primario**

Como se indicó el servidor primario para esta solución se definió en el servidor SDSGESTION01, los requerimientos mínimos de este servidor son:

1. Número de Procesadores : 2
2. Memoria disponible : 2 Gb
3. Conexión a la librería vía fibra de un (1) GBit

Las opciones que se instalaron en este servidor son:

1. CA Arcserve Backup Manager (instala la opción de librería)
2. CA Arcserve Backup SAN
3. CA Arcserve Backup TLO
4. CA Arcserve Backup OFA (Archivos Abiertos)

Este servidor también es el soporte para respaldar archivos planos de otros servidores de los cuales este servidor vea los file system correspondientes usando el agente para sistema operativo en estos servidores, permitiendo hacer el respaldo de forma local desde este servidor (XXXXXXX) y liberando los recursos del servidor de producción. La configuración de CA Arcserve Backup sobre este servidor contiene los siguientes elementos:

1. Nombre de Dominio: XXX
2. Servidor de Dominio Primario : XXXXXXX
3. Ruta de instalación CA Arcserve Backup: E:\

4. Base de datos en el Servidor Primario: XXXXX
5. BD en Servidores Distribuidos Remota en XXXXXXX

6. Centralización de Bd: SI, toda la información se encuentra remota en el servidor primario
7. Configuración de librería (se recomienda ejecutar este proceso por la opción automática).
8. Asignación de treinta (30) Slots para Windows
9. Limpieza de Unidades por HW
10. Asignar un password desde el comienzo al usuario XXXXXX.

Las operaciones de inventario sobre la librería, import / export (ingresar o retirar cartuchos de cinta), creación de usuarios, creación de grupos entre otros se realizará desde el servidor primario.

Los servicios de CA Arcserve Backup deben ser iniciados inicialmente en el servidor primario en Windows, y por último en cada uno de los distribuidos, el administrador debe garantizar que la inicialización de la librería desde CA Arcserve Backup finalice correctamente. Una vez se termine este proceso, se iniciaran los servicios en cada uno de los servidores distribuidos de Windows de uno en uno. Para apagar los servidores enmarcados dentro de la solución de respaldos se debe seguir el proceso mencionado antes de forma inversa.

Configuración: Las opciones a instalar y configurar en cada uno de estos servidores son:

| Servidor | Manager BAB | SAN | Agente Exchange | Agente Oracle | Agente SQL | Agente Archivos Abiertos |
|---|---|---|---|---|---|---|
| XXXXXXXX | X | X | | | X | X |
| XXXXXXXX | X | X | | | | X |
| XXXXXXXX | X | X | X | | | X |
| XXXXXXXX | X | X | | | | X |

| | | | | | | |
|---|---|---|---|---|---|---|
| XXXXXXXX | X | X | | | X | X |
| XXXXXXXX | X | X | | | X | X |
| XXXXXXXX | X | X | | X | | X |
| XXXXXXXX | X | X | | | X | X |

La configuración de CA Arcserve Backup sobre estos servidores debe contener los mismos parámetros descritos en el ítem de configuración del servidor primario en Windows teniendo en cuenta las siguientes premisas:

1. La configuración de SAN debe mantener el mismo orden de los servidores ingresado en el servidor primario
2. El nombre de los grupos definidos en la librería debe ser el mismo
3. El password del usuario XXXXX no debe ser modificado en estos servidores
4. El nombre del dominio en el momento de la instalación debe ser el mismo para toda la solución

**Esquemas de Respaldo**

Para la definición de los esquemas de respaldo en los servidores de producción se tendrán en cuenta el escenario que de común acuerdo con el área de sistemas se definió para cada uno de estos servidores. La descripción de este escenario se realizara por servidor, indicando las rutas, información a respaldar, consumo de medios esperado, clase de respaldo, manejo de los medios.

El consumo de los medios se estima con base en la capacidad de los cartuchos sin compresión definida por el fabricante, para nuestro caso cuatrocientos (400) GB, independiente a la capacidad que en la práctica pueda establecerse.

### 4.2 Configuración de la VTL - Librería y Grupos de las Copias de Respaldo

Los grupos de respaldo tienen como función entre otras cosas dividirla librería de forma lógica de tal forma que en el momento del respaldo las unidades de respaldo puedan respaldar la información seleccionada de forma independiente sin tener que esperar a que el trabajo de respaldo termine para poder usar la otra unidad.

Basados en esto se definió la siguiente configuración de grupos para cada una de las librerías así:

- Configuración para la librería real HP MSL6026 con 2 unidades SDLT 160/320

| Slots Asignados | Nombre del grupo | Trabajo de Respaldo Asignado |
|---|---|---|
| 1 al 8 | LIBSQL | |
| 9 al16 | LIBAS1 | |
| 17 al 25 | LIBLAN | |

- Configuración de grupos para 2 unidades externas LTO3 marca IBM conectadas a XXXXXXX

| Unidad | Nombre del grupo | Uso |
|---|---|---|
| Unidad 1 | LTO_1 | Copiar cintas de la VTL a Cintas reales para envío a custodia |
| Unidad 2 | LTO_2 | Copiar cintas de la VTL a Cintas reales para envío a custodia |

- Configuración para la primera librería virtual HP MSL6060 con 4 unidades LTO 3 400 / 800GB

| Slots Asignados | Cantidad de Cintas Emuladas | Prefijo Código Barras | Espacio Usado VTL (GB) | Nombre Grupo | Trabajo de Respaldo Asignado |
|---|---|---|---|---|---|
| 1 al 20 | 16 | SDS | 6400 | VTLASEG | |
| 21 al 35 | 11 | SDS | 4400 | VTLFILE | |
| 36 al 47 | Ninguna | Ninguno | 0 | Libre1 | Ninguno |
| 48 al 60 | Ninguna | Ninguno | 0 | Libre2 | Ninguno |

- Configuración para la Segunda librería virtual HP MSL6060 con 4 unidades LTO 3 400 / 800GB

| Slots Asignados | Cantidad Cintas Emuladas | Prefijo Código Barras | Espacio Usado VTL (GB) | Nombre Grupo | Trabajo de Respaldo Asignado |
|---|---|---|---|---|---|
| 1 al 19 | 6 | SDS1 | 2400 | VTLEXC | |
| 20 al 38 | 6 | SDS1 | 2400 | VTLAPL1 | |
| 39 al 57 | 6 | SDS1 | 2400 | VTLORA | |
| 58 al 60 | Ninguna | Ninguno | 0 | Libre3 | Ninguno |

Teniendo en cuenta que el tamaño total de la VTL es de 19 TB y que actualmente la sumatoria de todos los grupos con sus respectivas cintas creadas es de 18TB tenemos espacio en disco en VTL de 1TB. Dependiendo las cintas que se creen

podemos crear máximo 2 cintas LTO3 de 400GB y sobrarían 200GB. Es importante tener en cuenta que se dejan disponibles los grupos Libre1, Libre2 y Libre3 para poder efectuar respaldos por demanda no programados en la VTL ya sea usando las cintas ya creadas de forma temporal o creando más cintas de respaldo.

Se efectuará un trabajo correspondiente a respaldar los siguientes servidores con los siguientes datos:

La cantidad de datos a respaldar de toda la información anterior es de 1.5TB y la retención para este trabajo de respaldo está estipulado así:
**Único Trabajo:** Se hará respaldo en cada cinta usando el esquema GFS de lunes a viernes con Diferencial de Lunes a Jueves y Full Backup los viernes. Esté trabajo usará una unidad de tape LTO3 400 / 800 GB, generando un esquema de respaldo GFS en un grupo llamado VTLASEG.

| Dia Sem | Lunes | Martes | Miercoles | Jueves | Viernes | Sabado | Domingo |
|---|---|---|---|---|---|---|---|
| 1 | Respaldo Diferencial Diario VTLASEG | Respaldo Diferencial Diario VTLASEG | Respaldo Diferencial Diario VTLASEG | Respaldo Diferencial Diario VTLASEG | Respaldo Full Semanal VTLASEG | Sin Respaldo | Sin Respaldo |
| 2 | Respaldo Diferencial Diario VTLASEG | Respaldo Diferencial Diario VTLASEG | Respaldo Diferencial Diario VTLASEG | Respaldo Diferencial Diario VTLASEG | Respaldo Full Semanal VTLASEG | Sin Respaldo | Sin Respaldo |
| 3 | Respaldo Diferencial Diario VTLASEG | Respaldo Diferencial Diario VTLASEG | Respaldo Diferencial Diario VTLASEG | Respaldo Diferencial Diario VTLASEG | Respaldo Full Semanal VTLASEG | Sin Respaldo | Sin Respaldo |
| 4 | Respaldo Diferencial Diario VTLASEG | Respaldo Diferencial Diario VTLASEG | Respaldo Diferencial Diario VTLASEG | Respaldo Diferencial Diario VTLASEG | Respaldo Full Semanal VTLASEG | Sin Respaldo | Sin Respaldo |
| 5 | Respaldo Diferencial Diario VTLASEG | Respaldo Diferencial Diario VTLASEG | Respaldo Diferencial Diario VTLASEG | Respaldo Diferencial Diario VTLASEG | Respaldo Full Mensual VTLASEG | Sin Respaldo | Sin Respaldo |

**Consumo de Medios:** Con base en la capacidad de los medios es posible estimar que el número de medios a utilizar por respaldo completo es de cuatro (4). Se usará un esquema rotacional GFS con una rotación en cintas diarias de 8 cintas, en cintas semanales 1 y en cintas mensuales 1, de esta forma se concluye que se requieren 16 cintas al año para poder respaldar eficientemente este servidor. Es importante tener en cuenta que se usan 16 cintas ya que los respaldos semanales y mensuales (que son completos) se usarán 4 cintas por cada respaldo.

| Tipo Respaldo | Rotación de Cintas | Cintas a Usar |
|---|---|---|
| Diario | 8 | 8 |
| Semanal | 1 | 4 |
| Mensual | 1 | 4 |
| **Cintas totales** | | **16** |

Con este esquema es posible restaurar la información a cualquier día de la semana de las últimas 2 semanas y/o restaurar la información del día viernes del último viernes y/o restaurar la información último día viernes del mes por el anterior mes.

Para poder tener una retención de información mayor se ejecutarán procesos de copia de cintas de la VTL a cintas reales de tal forma que se puedan enviar a

custodia externa las cintas semanales y mensuales generadas por este trabajo de respaldo.

Se efectuará un trabajo correspondiente a respaldar los siguientes servidores con los siguientes datos:

La cantidad de datos a respaldar de toda la información anterior es de 246 GB y la retención para este trabajo de respaldo está estipulada así:

**Único Trabajo:** Se hará respaldo en cada cinta usando el esquema GFS de lunes a viernes con Diferencial de Lunes a Jueves y Full Backup los viernes. Este trabajo usará una unidad de tape LTO3 400 / 800 GB, generando un esquema de respaldo GFS en un grupo llamado VTLFILE.

| Dia | Lunes | Martes | Miercoles | Jueves | Viernes | Sabado | Domingo |
|---|---|---|---|---|---|---|---|
| Sem | | | | | | | |
| 1 | Respaldo Diferencial Diario VTLFILE | Respaldo Diferencial Diario VTLFILE | Respaldo Diferencial Diario VTLFILE | Respaldo Diferencial Diario VTLFILE | Respaldo Full Semanal VTLFILE | Sin Respaldo | Sin Respaldo |
| 2 | Respaldo Diferencial Diario VTLFILE | Respaldo Diferencial Diario VTLFILE | Respaldo Diferencial Diario VTLFILE | Respaldo Diferencial Diario VTLFILE | Respaldo Full Semanal VTLFILE | Sin Respaldo | Sin Respaldo |
| 3 | Respaldo Diferencial Diario VTLFILE | Respaldo Diferencial Diario VTLFILE | Respaldo Diferencial Diario VTLFILE | Respaldo Diferencial Diario VTLFILE | Respaldo Full Semanal VTLFILE | Sin Respaldo | Sin Respaldo |
| 4 | Respaldo Diferencial Diario VTLFILE | Respaldo Diferencial Diario VTLFILE | Respaldo Diferencial Diario VTLFILE | Respaldo Diferencial Diario VTLFILE | Respaldo Full Semanal VTLFILE | Sin Respaldo | Sin Respaldo |
| 5 | Respaldo Diferencial Diario VTLFILE | Respaldo Diferencial Diario VTLFILE | Respaldo Diferencial Diario VTLFILE | Respaldo Diferencial Diario VTLFILE | Respaldo Full Mensual VTLFILE | Sin Respaldo | Sin Respaldo |

**Consumo de Medios:** Con base en la capacidad de los medios es posible estimar que el número de medios a utilizar por respaldo completo es de uno (1). Se usará

un esquema rotacional GFS con una rotación en cintas diarias de 8 cintas, en cintas semanales 2 y en cintas mensuales 1, de esta forma se concluye que se requieren 11 cintas al año para poder respaldar eficientemente este servidor.

| **Tipo Respaldo** | **Rotación de Cintas** | **Cintas a Usar** |
|---|---|---|
| Diario | 8 | 8 |
| Semanal | 2 | 2 |
| Mensual | 1 | 1 |
| **Cintas totales** | | **11** |

Con este esquema es posible restaurar la información a cualquier día de la semana de las últimas 2 semanas y/o restaurar la información del día viernes de los últimos dos (2) viernes y/o restaurar la información último día viernes del mes por el anterior mes. Para poder tener una retención de información mayor se ejecutarán procesos de copia de cintas de la VTL a cintas reales de tal forma que se puedan enviar a custodia externa las cintas semanales y mensuales generadas por este trabajo de respaldo.

Se efectuará un trabajo correspondiente a respaldar los siguientes servidores con los siguientes datos:

La cantidad de datos a respaldar de toda la información anterior es de 42 GB y la retención para este trabajo de respaldo está estipulado así:

**Único Trabajo:** Se hará respaldo en cada cinta usando el esquema GFS de lunes a viernes con Full Backup de Lunes a Jueves y Full Backup los viernes. Éste trabajo usará una unidad de tape SDLT 160 / 320 GB, generando un esquema de respaldo GFS en un grupo llamado LIBSQL.

| Dia | Lunes | Martes | Miercoles | Jueves | Viernes | Sabado | Domingo |
|---|---|---|---|---|---|---|---|
| Sem | | | | | | | |
| 1 | Respaldo Full Diario LIBSQL | Respaldo Full Diario LIBSQL | Respaldo Full Diario LIBSQL | Respaldo Full Diario LIBSQL | Respaldo Full Semanal LIBSQL | Sin Respaldo | Sin Respaldo |
| 2 | Respaldo Full Diario LIBSQL | Respaldo Full Diario LIBSQL | Respaldo Full Diario LIBSQL | Respaldo Full Diario LIBSQL | Respaldo Full Semanal LIBSQL | Sin Respaldo | Sin Respaldo |
| 3 | Respaldo Full Diario LIBSQL | Respaldo Full Diario LIBSQL | Respaldo Full Diario LIBSQL | Respaldo Full Diario LIBSQL | Respaldo Full Semanal LIBSQL | Sin Respaldo | Sin Respaldo |
| 4 | Respaldo Full Diario LIBSQL | Respaldo Full Diario LIBSQL | Respaldo Full Diario LIBSQL | Respaldo Full Diario LIBSQL | Respaldo Full Semanal LIBSQL | Sin Respaldo | Sin Respaldo |
| 5 | Respaldo Full Diario LIBSQL | Respaldo Full Diario LIBSQL | Respaldo Full Diario LIBSQL | Respaldo Full Diario LIBSQL | Respaldo Full Mensual LIBSQL | Sin Respaldo | Sin Respaldo |

**Consumo de Medios:** Con base en la capacidad de los medios es posible estimar que el número de medios a utilizar por respaldo completo es de uno (1). Se usará un esquema rotacional GFS con una rotación en cintas diarias de 8 cintas, en cintas semanales 2 y en cintas mensuales 1, de esta forma se concluye que se requieren 11 cintas al año para poder respaldar eficientemente este servidor.

| Tipo Respaldo | Rotación de Cintas | Cintas a Usar |
|---|---|---|
| Diario | 8 | 8 |
| Semanal | 2 | 2 |
| Mensual | 1 | 1 |
| **Cintas totales** | | **11** |

Con este esquema es posible restaurar la información a cualquier día de la semana de las últimas dos semanas y/o restaurar la información del día viernes de los últimos dos viernes y/o restaurar la información último día viernes del mes por el anterior mes. Es importante tener en cuenta que este trabajo de respaldo se ejecuta en la unidad real de backup de tal forma que no se ocupe espacio en la VTL. Si se requiere un proceso de retención de información que incluya un mayor tiempo es posible efectuando una rotación de medios mayor.

Se efectuará un trabajo correspondiente a respaldar los siguientes servidores con los siguientes datos:

La cantidad de datos a respaldar de toda la información anterior es de 168 GB y la retención para este trabajo de respaldo está estipulado así:

**Único Trabajo:** Se hará respaldo en cada cinta usando el esquema GFS de lunes a viernes con Full Backup de Lunes a Jueves y Full Backup los viernes. Este trabajo

usará una unidad de tape LTO3 400 / 800 GB, generando un esquema de respaldo GFS en un grupo llamado VTLORA.

| Dia | Lunes | Martes | Miercoles | Jueves | Viernes | Sabado | Domingo |
|---|---|---|---|---|---|---|---|
| Sem | | | | | | | |
| 1 | Respaldo Full Diario VTLORA | Respaldo Full Diario VTLORA | Respaldo Full Diario VTLORA | Respaldo Full Diario VTLORA | Respaldo Full Semanal VTLORA | Sin Respaldo | Sin Respaldo |
| 2 | Respaldo Full Diario VTLORA | Respaldo Full Diario VTLORA | Respaldo Full Diario VTLORA | Respaldo Full Diario VTLORA | Respaldo Full Semanal VTLORA | Sin Respaldo | Sin Respaldo |
| 3 | Respaldo Full Diario VTLORA | Respaldo Full Diario VTLORA | Respaldo Full Diario VTLORA | Respaldo Full Diario VTLORA | Respaldo Full Semanal VTLORA | Sin Respaldo | Sin Respaldo |
| 4 | Respaldo Full Diario VTLORA | Respaldo Full Diario VTLORA | Respaldo Full Diario VTLORA | Respaldo Full Diario VTLORA | Respaldo Full Semanal VTLORA | Sin Respaldo | Sin Respaldo |
| 5 | Respaldo Full Diario VTLORA | Respaldo Full Diario VTLORA | Respaldo Full Diario VTLORA | Respaldo Full Diario VTLORA | Respaldo Full Mensual VTLORA | Sin Respaldo | Sin Respaldo |

**Consumo de Medios:** Con base en la capacidad de los medios es posible estimar que el número de medios a utilizar por respaldo completo es de uno (1). Se usará un esquema rotacional GFS con una rotación en cintas diarias de 4 cintas, en cintas semanales 1 y en cintas mensuales 1, de esta forma se concluye que se requieren 6 cintas al año para poder respaldar eficientemente este servidor.

| Tipo Respaldo | Rotación de Cintas | Cintas a Usar |
|---|---|---|
| Diario | 4 | 4 |
| Semanal | 1 | 1 |
| Mensual | 1 | 1 |
| **Cintas totales** | | **6** |

Con este esquema es posible restaurar la información a cualquier día de la semana de la última semana y/o restaurar la información del día viernes del último viernes y/o restaurar la información último día viernes del mes por el anterior mes. Para poder tener una retención de información mayor se ejecutarán procesos de copia de cintas de la VTL a cintas reales de tal forma que se puedan enviar a custodia externa las cintas semanales y mensuales generadas por este trabajo de respaldo.

La cantidad de datos a respaldar de toda la información anterior es de 101 GB y la retención para este trabajo de respaldo está estipulado así:

**Único Trabajo:** Se hará respaldo en cada cinta usando el esquema GFS de lunes a viernes con Full Backup de Lunes a Jueves y Full Backup los viernes. Este trabajo usará una unidad de tape SDLT 160 / 320 GB, generando un esquema de respaldo GFS en un grupo llamado LIBAS1.

| Dia | Lunes | Martes | Miercoles | Jueves | Viernes | Sabado | Domingo |
|---|---|---|---|---|---|---|---|
| Sem | | | | | | | |
| 1 | Respaldo Full Diario LIBAS1 | Respaldo Full Diario LIBAS1 | Respaldo Full Diario LIBAS1 | Respaldo Full Diario LIBAS1 | Respaldo Full Semanal LIBAS1 | Sin Respaldo | Sin Respaldo |
| 2 | Respaldo Full Diario LIBAS1 | Respaldo Full Diario LIBAS1 | Respaldo Full Diario LIBAS1 | Respaldo Full Diario LIBAS1 | Respaldo Full Semanal LIBAS1 | Sin Respaldo | Sin Respaldo |
| 3 | Respaldo Full Diario LIBAS1 | Respaldo Full Diario LIBAS1 | Respaldo Full Diario LIBAS1 | Respaldo Full Diario LIBAS1 | Respaldo Full Semanal LIBAS1 | Sin Respaldo | Sin Respaldo |
| 4 | Respaldo Full Diario LIBAS1 | Respaldo Full Diario LIBAS1 | Respaldo Full Diario LIBAS1 | Respaldo Full Diario LIBAS1 | Respaldo Full Semanal LIBAS1 | Sin Respaldo | Sin Respaldo |
| 5 | Respaldo Full Diario LIBAS1 | Respaldo Full Diario LIBAS1 | Respaldo Full Diario LIBAS1 | Respaldo Full Diario LIBAS1 | Respaldo Full Mensual LIBAS1 | Sin Respaldo | Sin Respaldo |

**Consumo de Medios:** Con base en la capacidad de los medios es posible estimar que el número de medios a utilizar por respaldo completo es de uno (1). Se usará

un esquema rotacional GFS con una rotación en cintas diarias de 8 cintas, en cintas semanales 2 y en cintas mensuales 1, de esta forma se concluye que se requieren 11 cintas al año para poder respaldar eficientemente este servidor.

| Tipo Respaldo | Rotación de Cintas | Cintas a Usar |
|---|---|---|
| Diario | 8 | 8 |
| Semanal | 2 | 2 |
| Mensual | 1 | 1 |
| **Cintas totales** | | **11** |

Con este esquema es posible restaurar la información a cualquier día de la semana de las últimas dos semanas y/o restaurar la información del día viernes de los últimos dos viernes y/o restaurar la información último día viernes del mes por el anterior mes. Es importante tener en cuenta que este trabajo de respaldo se ejecuta en la unidad real de backup de tal forma que no se ocupe espacio en la VTL. Si se requiere un proceso de retención de información que incluya un mayor tiempo es posible efectuando una rotación de medios mayor.

La cantidad de datos a respaldar de toda la información anterior es de 130 GB y la retención para este trabajo de respaldo está estipulado así:

**Único Trabajo:** Se hará respaldo en cada cinta usando el esquema GFS de lunes a viernes con respaldo Diferencial de Lunes a Jueves y Full Backup los viernes. Este trabajo usará una unidad de tape SDLT 160 / 320 GB, generando un esquema de respaldo GFS en un grupo llamado LIBLAN.

| Dia | Lunes | Martes | Miercoles | Jueves | Viernes | Sabado | Domingo |
|---|---|---|---|---|---|---|---|
| Sem | | | | | | | |
| 1 | Respaldo Full Diario LIBLAN | Respaldo Full Diario LIBLAN | Respaldo Full Diario LIBLAN | Respaldo Full Diario LIBLAN | Respaldo Full Semanal LIBLAN | Sin Respaldo | Sin Respaldo |
| 2 | Respaldo Full Diario LIBLAN | Respaldo Full Diario LIBLAN | Respaldo Full Diario LIBLAN | Respaldo Full Diario LIBLAN | Respaldo Full Semanal LIBLAN | Sin Respaldo | Sin Respaldo |
| 3 | Respaldo Full Diario LIBLAN | Respaldo Full Diario LIBLAN | Respaldo Full Diario LIBLAN | Respaldo Full Diario LIBLAN | Respaldo Full Semanal LIBLAN | Sin Respaldo | Sin Respaldo |
| 4 | Respaldo Full Diario LIBLAN | Respaldo Full Diario LIBLAN | Respaldo Full Diario LIBLAN | Respaldo Full Diario LIBLAN | Respaldo Full Semanal LIBLAN | Sin Respaldo | Sin Respaldo |
| 5 | Respaldo Full Diario LIBLAN | Respaldo Full Diario LIBLAN | Respaldo Full Diario LIBLAN | Respaldo Full Diario LIBLAN | Respaldo Full Mensual LIBLAN | Sin Respaldo | Sin Respaldo |

**Consumo de Medios:** Con base en la capacidad de los medios es posible estimar que el número de medios a utilizar por respaldo completo es de uno (1). Se usará un esquema rotacional GFS con una rotación en cintas diarias de 8 cintas, en cintas semanales 2 y en cintas mensuales 1, de esta forma se concluye que se requieren 11 cintas al año para poder respaldar eficientemente este servidor.

| **Tipo Respaldo** | **Rotación de Cintas** | **Cintas a Usar** |
|---|---|---|
| Diario | 8 | 8 |
| Semanal | 2 | 2 |
| Mensual | 1 | 1 |
| **Cintas totales** | | **11** |

Con este esquema es posible restaurar la información a cualquier día de la semana de las últimas dos semanas y/o restaurar la información del día viernes de los últimos dos viernes y/o restaurar la información último día viernes del mes por el anterior mes. Es importante tener en cuenta que este trabajo de respaldo se ejecuta en la unidad real de backup de tal forma que no se ocupe espacio en la VTL. Si se requiere un proceso de retención de información que incluya un mayor tiempo es posible efectuando una rotación de medios mayor.

ALCALDIA MAYOR
DE BOGOTA D.C.
Secretaría
Salud

**El cómo se definió la presente Arquitectura de Copias de Respaldo**

En el siguiente cuadro se describe el proceso que se llevó a cabo en la fase de desarrollo e implementación de la solución de copias de respaldo de la SDS.

| Segmento: | Tareas a Ejecutar: | Objetivo: | Proceso |
|---|---|---|---|
| **Evaluación** | Datos a respaldar. | Definir qué datos, carpeta a carpeta es necesario respaldar en cada uno de los servidores definidos en cada uno de los sitios | En Datos a Respaldar |
| | Categoría de los datos a respaldar (O.S., e-mail, Database, applications). | Clasificación de cada uno de los datos a respaldar | En Datos a Respaldar |
| | Frecuencia de cambio de los datos a respaldar. | Definición de con qué frecuencia (Horas, Dias, Meses, años) cambian los datos definidos en el punto 1 | En Datos a Respaldar |
| | Geográficamente donde están ubicados los datos a respaldar. | Definición de dónde se encuentran los datos a respaldar | Todos los datos están en la sede de la SDS |
| **Conocimiento del Negocio** | Requerimiento crítico del negocio. | Definición de que datos son totalmente críticos para el negocio (si les pasa algo a estos datos la organización se paraliza) y cuáles no. Es necesario en este punto contar con los datos de los PC de los usuarios. | En Datos a Respaldar |
| | Red. | Definición de cada uno de los segmentos de red, nombres de servidores y velocidad de conexión de la red de los servidores. También es necesario determinar si se implementará una red paralela de almacenamiento | En Diseño SDS |
| | Mapa de conectividad de la red en los servidores. | Definición de la red de conexión entre servidores | En Diseño SDS |

| | | | |
|---|---|---|---|
| | Definir servidores que se van a respaldar. | Definición de los servidores que se van a ser respaldados. En este punto es necesario que aquellos servidores que no sea necesario respaldar, se debe documentar la razón por la cual no es necesario el respaldo. | En Diseño SDS |
| | Definir que opciones requiere dependiendo de lo se compró y las necesidades del cliente. | Asignación de cada una de las opciones adquiridos por Secretaria Distrital de Salud a cada uno de los servidores | En Diseño SDS |
| | Definir que agentes requiere dependiendo de lo que se compró y las necesidades del cliente. | Asignación de cada uno de los agentes adquiridos por Secretaria Distrital de Salud a cada uno de los servidores | En Diseño SDS |
| | Definir requerimientos para la instalación del agente para Oracle | Definición de los requerimientos y viabilidad de los mismos para la implementación del agente para Oracle en las bases de datos de producción | Para respaldar las bases de datos de Oracle las bases de datos deben estar en modo Archive Log… |
| **Lista de Prioridad de los datos del negocio** | Prioridad de cada categoría de los datos. | Definición del nivel de criticidad de los datos a respaldar en una escala de 1 a 5 siendo el 1 el dato más prioritario y el 5 el menos prioritario. | En Arquitectura |
| | Definir el tamaño de los datos a respaldar según las categorías. | Definición del tamaño de los datos a respaldar (la unidad de medida serán MB) | En Datos a Respaldar |
| | Definir la frecuencia de crecimiento de los datos a respaldar | Definición con qué frecuencia crecen los datos a respaldar (la unidad de medida será MB/DIA) | En Datos a Respaldar |
| | Definir la ventana de backup. | Definición del tiempo con el que se cuenta para el respaldo de la información | La ventana de respaldo será de 6pm a 7am |
| **Metodología Implementación** | Identificar el nombre de cada servidor. | Definición del nombre de cada uno de los servidores a respaldar | En Diseño SDS |
| | Identificar en que servidor esta cada aplicación. | Definición de aplicaciones instaladas a respaldar en cada uno de los servidores | En Diseño SDS |

| | | | |
|---|---|---|---|
| | Definición del nombre del dominio de CA Arcserve | Definición de cuál es el nombre del dominio sobre el cual van a ser instalados los manager de BAB | BKP-SDS |
| | Definición del usuario de Arcserve | Definir que usuario usará Arcserve para el tema de la copia de seguridad | sds\-backup- |
| | Definición de la ubicación (unidad) donde se instalará Arcserve | Definir la ubicación de donde se instalará Arcserve | A Excepción de XXXXX todos los productos se instalan en C |
| | Definición del tipo de base de datos del Manager de BAB | Definir el tipo de base de datos en BAB: SQL o SQL Desktop Engine | La base de datos será SQL Server ubicada en CLUSTERSQL |
| | Definición de los grupos | Definir que agrupaciones de Slots se van a configurar en cada uno de los autoloaders | En Arquitectura |
| | Definir el número de trabajos. | Definición del número de trabajos de respaldo a realizar. En esta fase se debe indicar cuál es la fuente y cuál es el destino de la información a respaldar. | En Arquitectura |
| | Definición del esquema de copia de seguridad para cada uno de los trabajos descritos anteriormente | Definir el esquema de copia de seguridad (GFS, Rotacional, Manual, etc.) para cada uno de los trabajos indicados anteriormente | En Arquitectura |
| | Definición de las opciones de cada uno de los trabajos descritos anteriormente | Definir las opciones a configurar por cada uno de los trabajos anteriormente descritos | En Arquitectura |
| | Definición de los filtros | Definir los archivos que serán filtrados en el momento del respaldo. | En Arquitectura |
| | Definir el numero cintas que se van a utilizar dependiendo del método de backup en cada uno de los trabajos diseñados anteriormente | Definir el número de cintas usadas por cada trabajo definido anteriormente | En Arquitectura |
| | Definición del tiempo para la poda automática de la base de datos | Definir el tiempo para borrar los registros antiguos de la base de datos de arcserve. | La poda será cada 30 dias |

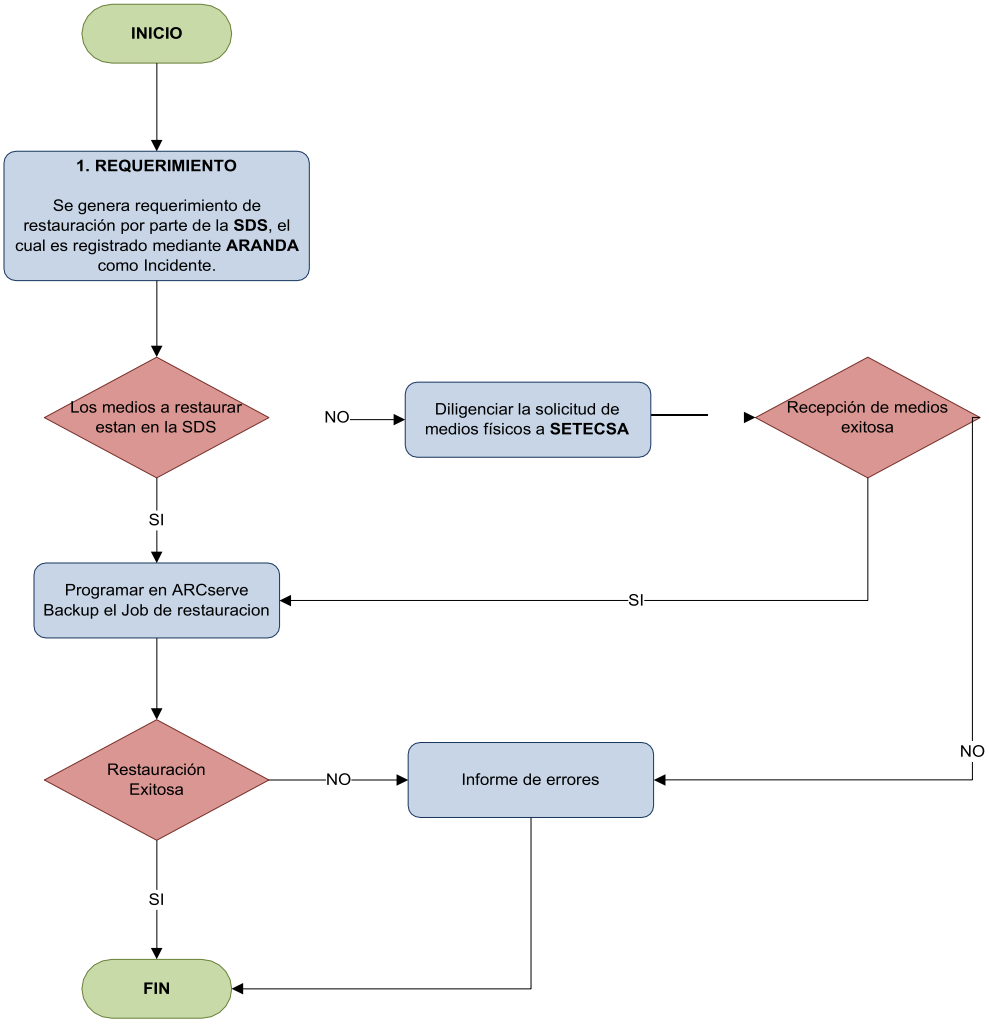
| | | | |
|---|---|---|---|
| | Definición de la Hora para la poda de la base de datos | Definir a que horas se dispara el trabajo de la poda de la base de datos | Se hará a las 12:00pm |

## 4.3 Restauración de Copias de Seguridad

El presente documento se constituye como un instructivo sobre la actividad de restauración de copias de seguridad de acuerdo a la arquitectura actual, la cual se encuentra instalada en algunos servidores bajo la versión r12.0 SP1.Este es un software que permite la copia de seguridad de datos, con sus esquemas de rotación de acuerdo a las necesidades de la Secretaria Distrital de Salud y definida en el documento final de Arquitectura Copias de Seguridad.

**Procedimiento de restauración**

En la siguiente grafica se observa de manera general cual será el proceso de restauración:

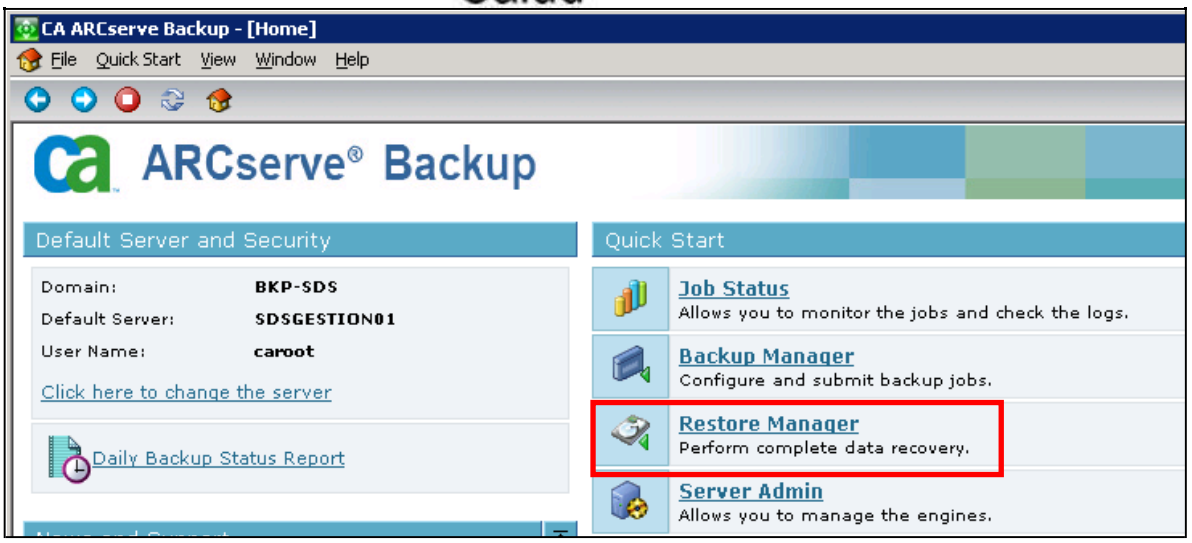


**Configuración JOB de restauración**

Para hacer más intuitivo este procedimiento, vamos a suponer que se borro la información del HOME de ajlopez, en la grafica se borro intencionalmente la info de la carpeta.

Para configurar un Job de restauración la recomendación es hacerlo en el servidor principal de CA ARCServe Backup, para la configuración actual seria:

1. En la ventana principal de CA ARCserve Backup se selecciona la opción *Restore Manager*:

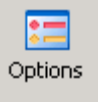



***2*** Enseguida se procede a realizar la selección de la cinta, de acuerdo a la sesión que contiene la información a restaurar, luego se ubica el archivo o archivos a restaurar. Esto se hace seleccionando el ***Source*** en modo: ***Restore by Session.***

***3*** El paso siguiente será ubicar el destino: donde puede ser la ubicación original o una ruta alterna de otro servidor. Para el ejercicio se mantiene la opción: ***Restore files to their original location(s).***

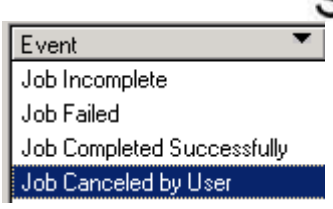
4. Se configura enseguida el ***Schedule***, que será una sola vez, ***once.***

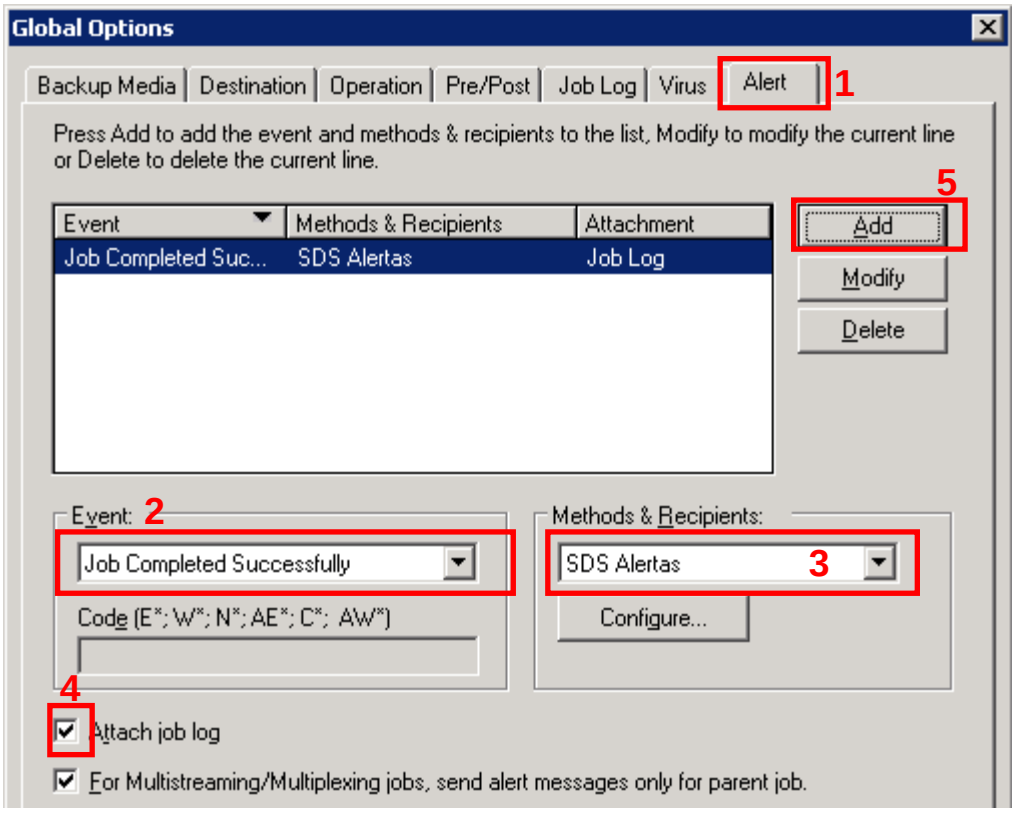
5. Para configurar la notificación al correo del administrador de copias de seguridad, realizaremos la configuración por el menú opciones.




Los parámetros de configuración son:

- Ubicarse en pestaña ***Alert.***
- Señalar el ***Event*** específico.
- Seleccionar los ***Methods & Recipients*** como SDS Alertas
- Seleccionar ***Attach job log.***
- Dar click en ***Add*** para configurar la notificación.
- Repetir todos los pasos anteriores para los eventos:



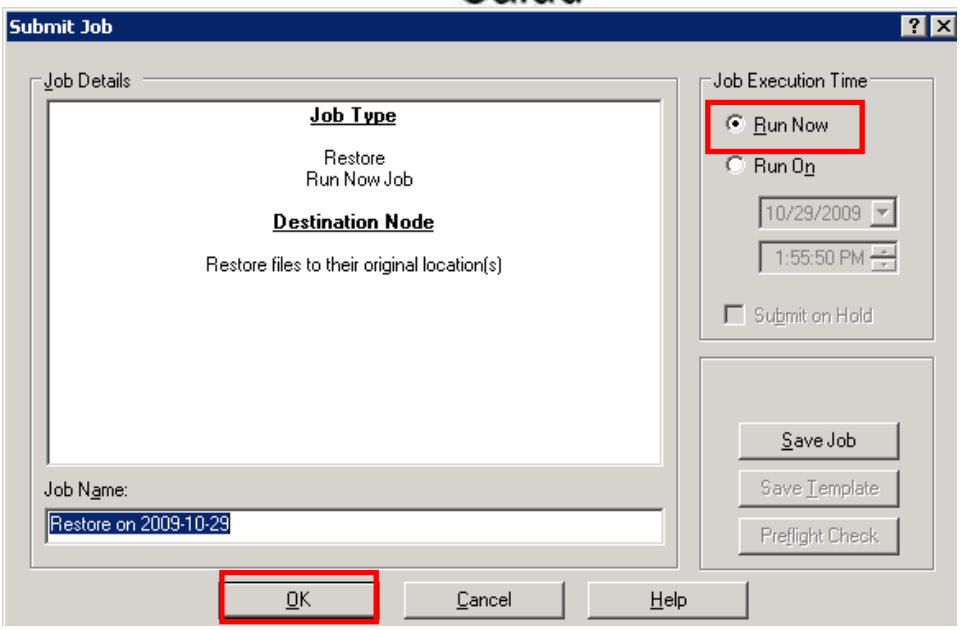

6. Para iniciar la restauración es necesario dar click en el botón ***Start***


7. Enseguida tendremos una pantalla como la siguiente:

En esta pantalla aparece un resumen de la cinta de donde voy a hacer la restauración, el número de serial y demás información básica para iniciar la restauración. Damos click en ***OK.***

8. En la siguiente pantalla de configura una cuenta del dominio que tenga privilegio de Administrador del dominio. Damos click en ***OK.*** Para continuar.

9. En la siguiente pantalla dejamos la opción RUN NOW. Y ejecutamos la restauración.




10. En la pantalla de JOB´s al finalizar exitosamente el proceso de restauración aparece una ventana informando que la operación fue EXITOSA.

11. El administrador de copias de seguridad puede verificar también en su correo electrónico el archivo anexo, donde al final recibirá una línea con el mensaje de ***Restore Operation Successful.***

12. Para verificar la restauración vamos al recurso de red a verificar que sea efectiva la restauración. Luego se notificara al administrador interesado en la restauración y dar por cerrado el incidente.

## 5. SISTEMA DE CONTINUIDAD CON GENERACION DE IMÁGENES

A continuación se describen algunas de las funcionalidades más relevantes del software "*ACRONIS"*, el cual se encuentra actualmente instalado en algunos servidores bajo la versión demo con el objetivo de evaluar los posibles beneficios para la entidad.

Este es un software que permite la Recuperación de Desastres a través de imágenes completas a un servidor, permitiendo la posibilidad de restaurarla en cualquier tipo de hardware, como permitir la conversión a máquinas virtuales.

En el presente documento, se ilustra cual es el servidor central destinado para ser el repositorio de imágenes así como la forma de realizar una restauración de la Imagen, periodicidad, tiempos de ejecución y estándar de los nombres de las imágenes que se generarían.

**Infraestructura física de la solución**

La solución de "*ACRONIS"* instalada como demo en la entidad, está conformado en su parte física por los siguientes elementos:

**Servidor de la Solución de Continuidad**

Este servidor cuenta y excede los requisitos mínimos para la solución de Acronis.

**SUBSISTEMA DE DISCOS SDACRONIS**

El subsistema de discos de este servidor, sobre el que está montada la plataforma tiene las siguientes características:

**Sistema de Archivos:** Sistema de archivos NTFS, sobre los cuales están montado el sistema operativo y la unidad para almacenar las Imágenes de los servidores de la SDS.

**RAID:** El servidor XXXXX, tiene un arreglo RAID 5 (Stripped with Parity), particionado en dos unidades lógicas:

- **Unidad C:\(OS)** de 50 GB sobre la cual se tienen instalados el sistema operativo Windows 2003 Enterprise Server R2 y la aplicación de Acronis True Image Enterprise Server Echo en calidad de DEMO.

- **Unidad E:\ (Data Images)** de 496 GB Destinada para el almacenamiento de las imágenes de los servidores de la entidad.

**Estructura lógica de la solución**

El sistema de **ACRONIS** de la institución, están conformado por los siguientes componentes lógicos:

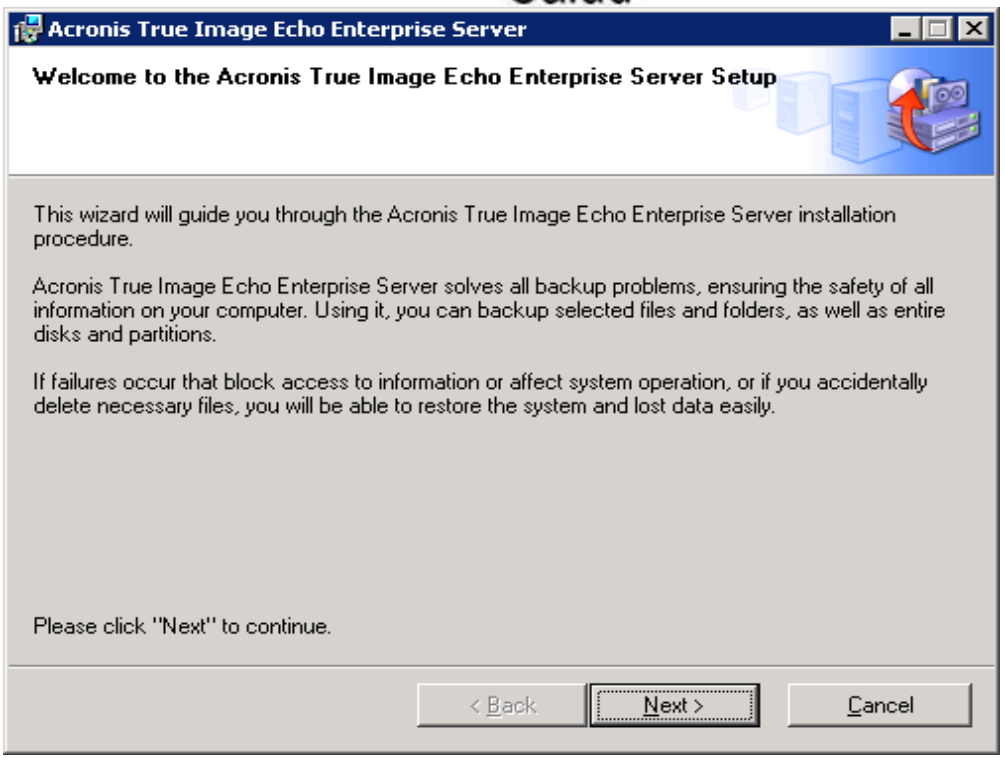
**Dominio:** Este servidor pertenece al dominio **XXXXXXX** (Producción), facilitando así el almacenamiento de las imágenes y restauración de las mismas.

**Componentes del Servidor:** La solución actual de **ACRONIS** en la SDS, se compone de la versión True Image Enterprise Server Echo.

**Instalación del producto**

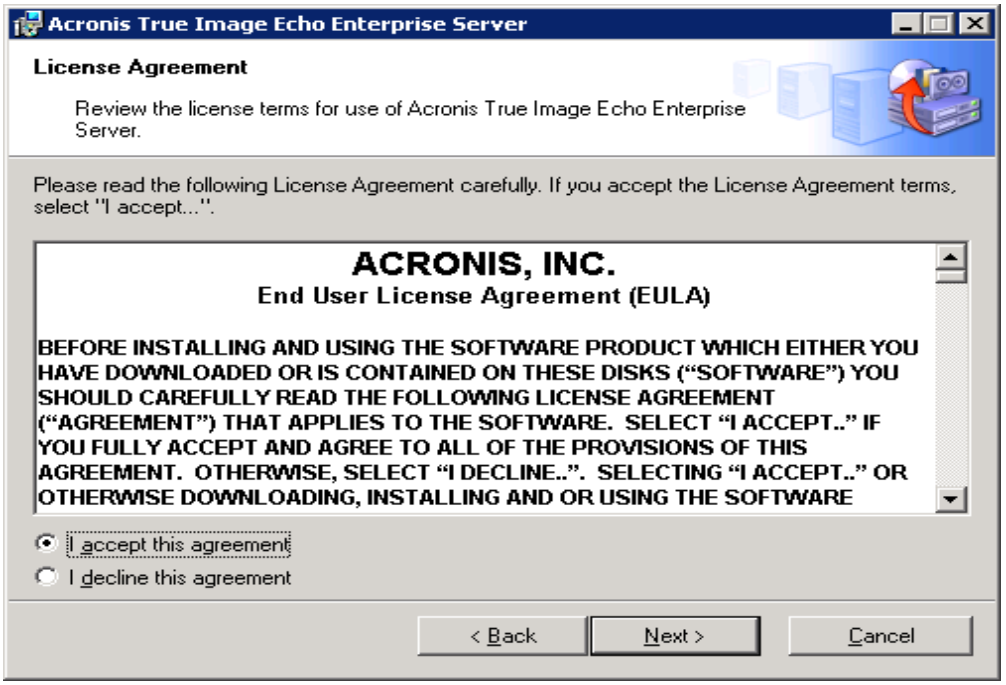
A continuación se da el instructivo paso a paso para instalar el producto True Image Enterprise Server Echo en el servidor en el cual se efectuara el procedimiento de la realización de la Imagen.

En el servidor en el cual se requiere realizar la imagen se debe ejecutar el paquete TrueImageEnterpriseServerEcho_d_en.exe (Trial Version).

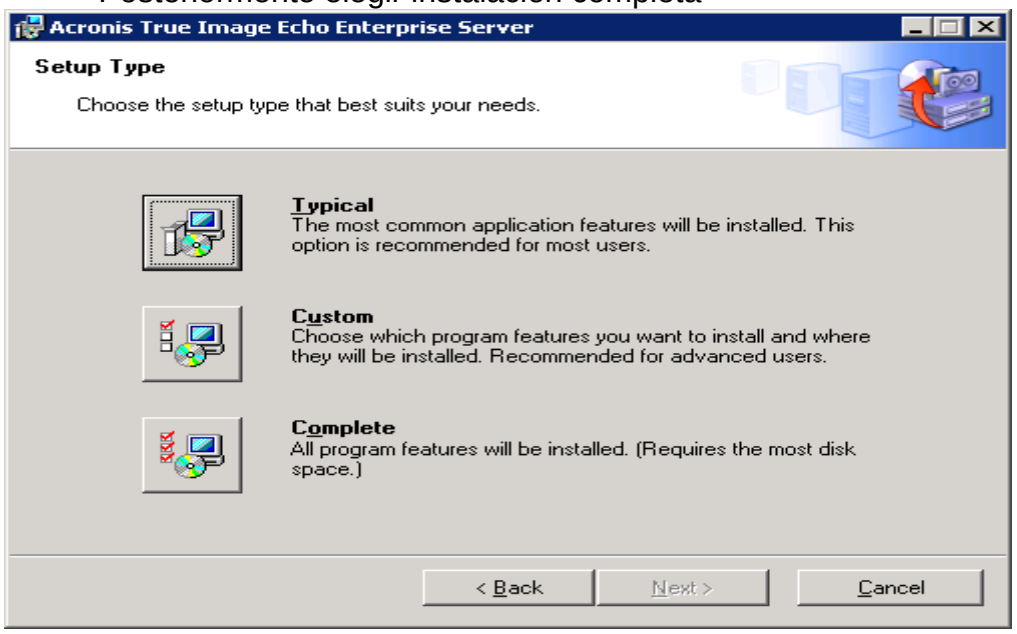



Luego Clic en Next

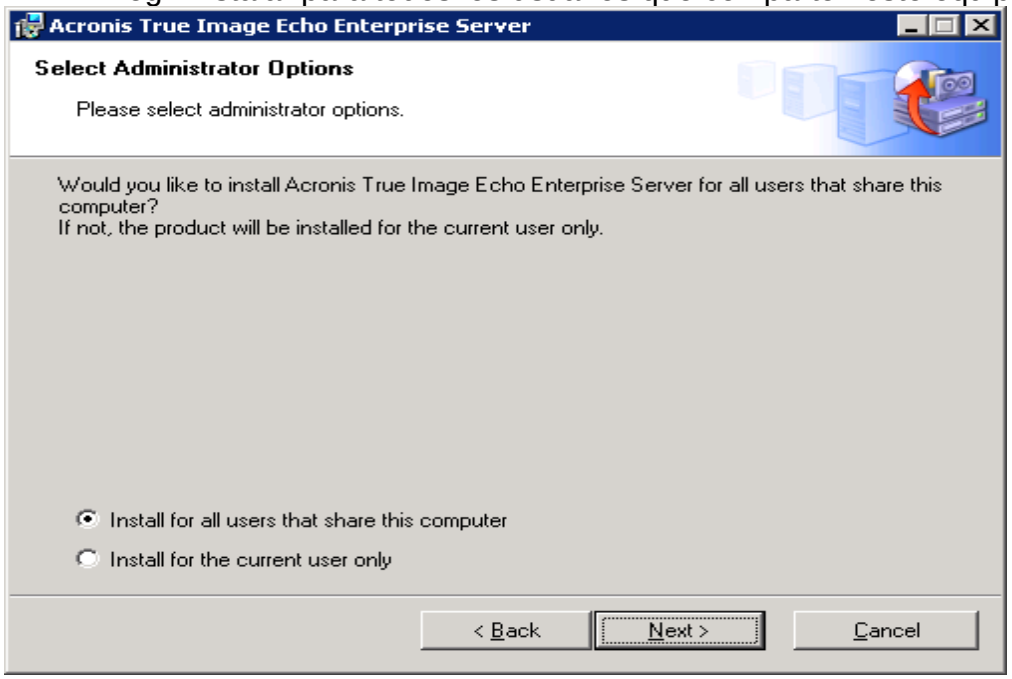
Dar aceptar el acuerdo de licencia y Clic en Next



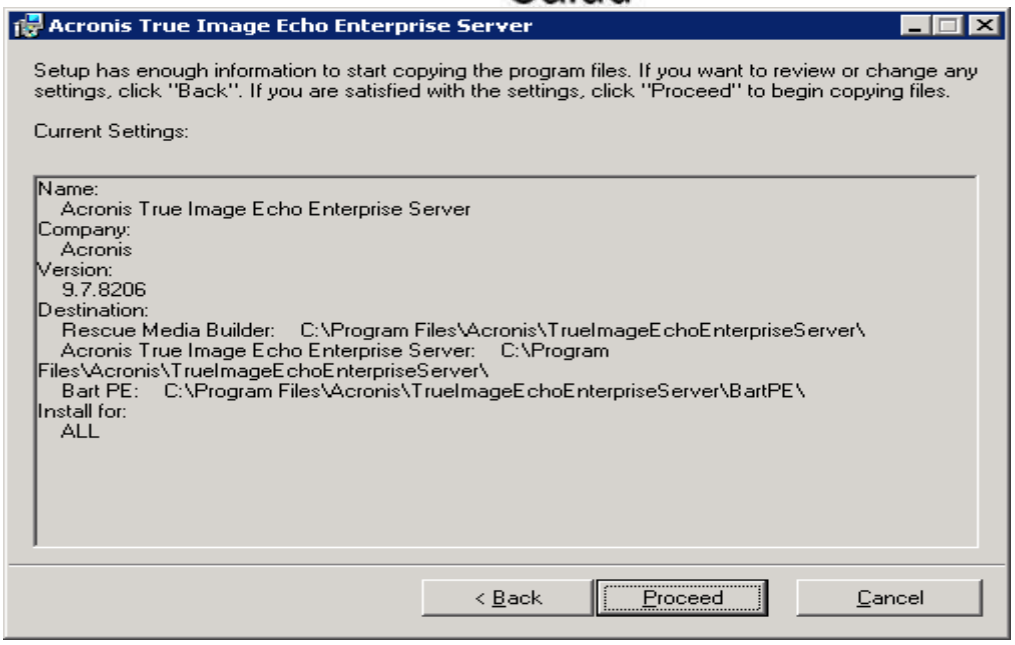
Posteriormente elegir instalación completa

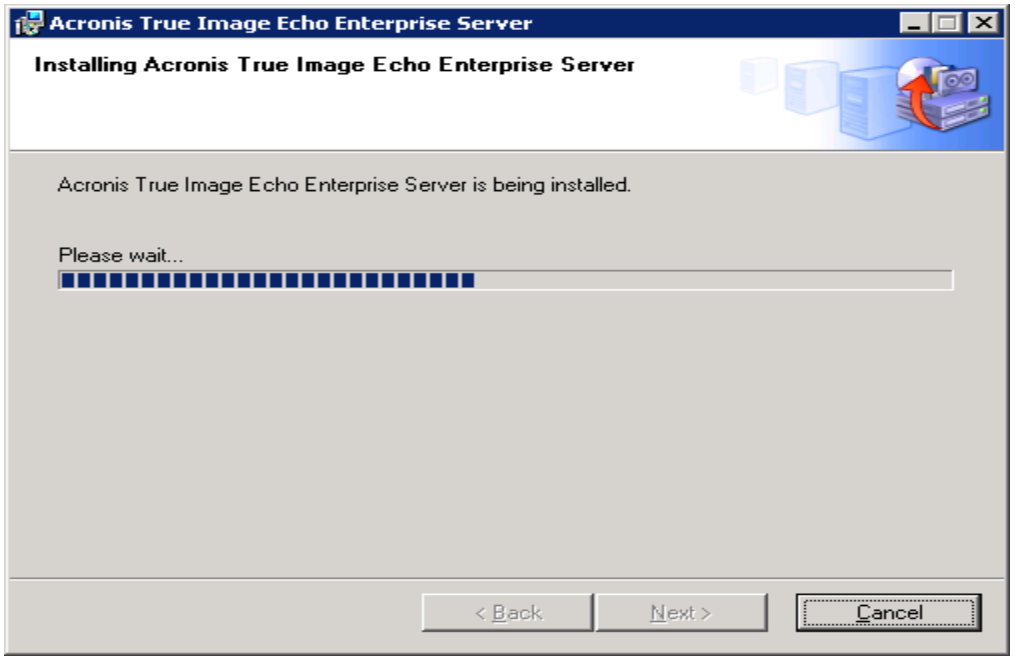



Elegir instalar para todos los usuarios que comparten este equipo

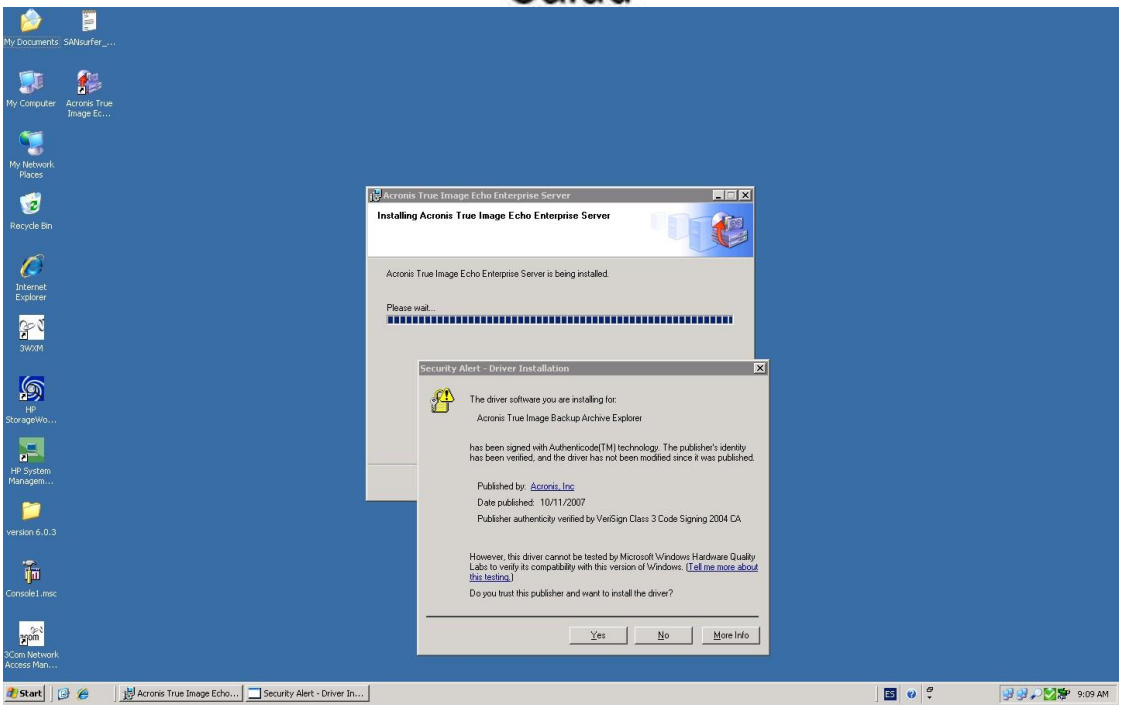



Clic en Proceder

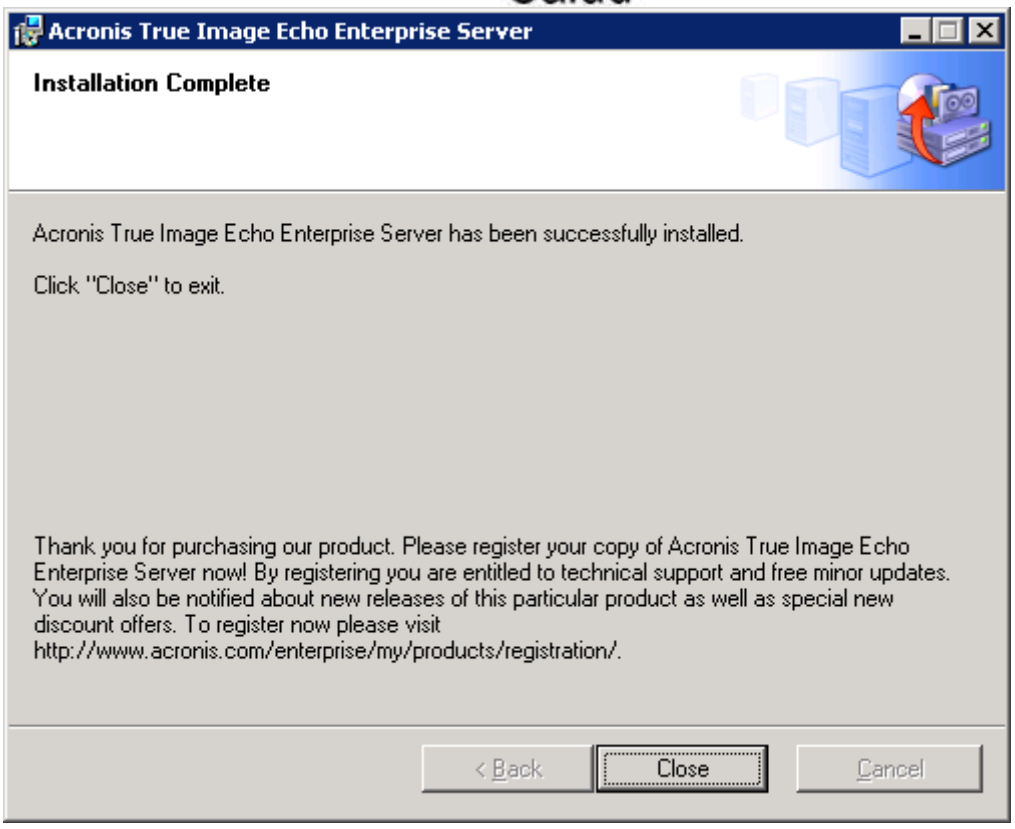


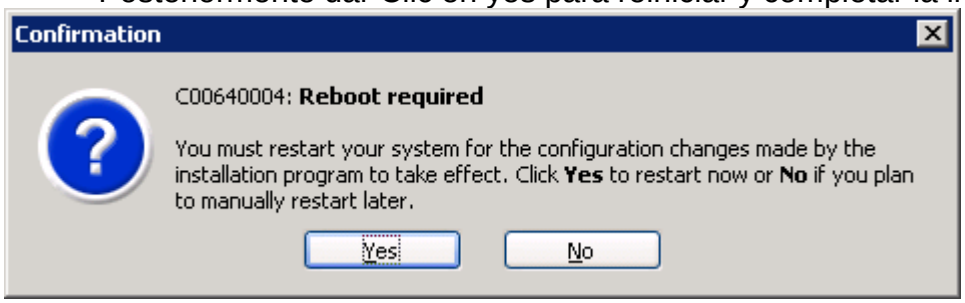

En el cuadro de instalar el driver Acronis True Image Backup Archive Explorer dar Clic en Yes




Por último Clic en el botón de close




Posteriormente dar Clic en yes para reiniciar y completar la instalación



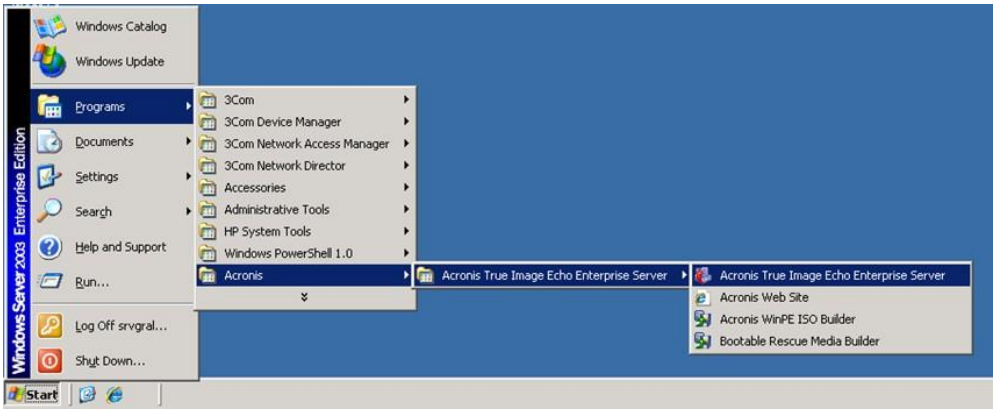

**Realización de las imágenes en los servidores**

Como sigue se dará el procedimiento para el acceso y realización de las imágenes a través del aplicativo **Acronis True Image Echo Enterprise Server DEMO**

ALCALDIA MAYOR
DE BOGOTA D.C.
Secretaría
Salud

## 5 Acceso a ACRONIS TRUE IMAGE ECHO ENTERPRISE SERVER

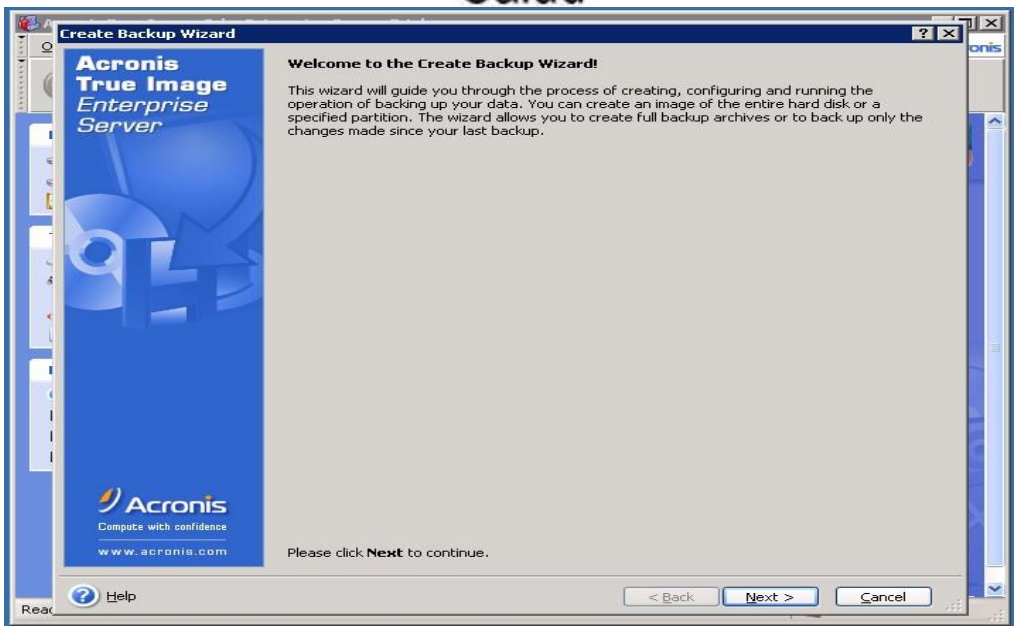
Para acceder al aplicativo dar clic en Inicio / programas / Acronis / Acronis True Image Echo Enterprise Server / Acronis True Image Echo Enterprise Server



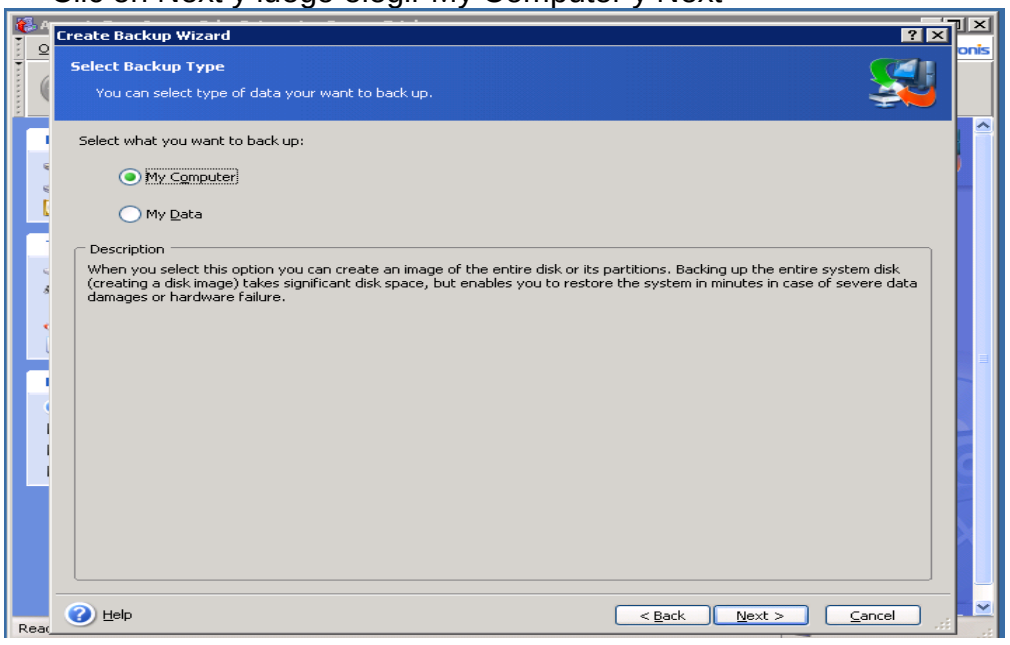


**Realización de la Imagen**

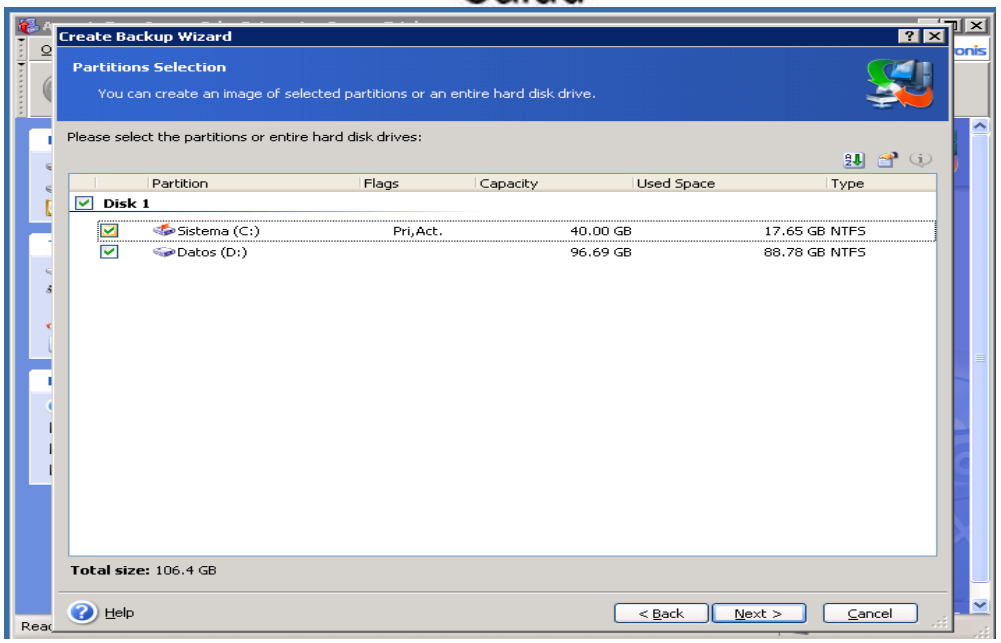
Se elige el icono de Backup



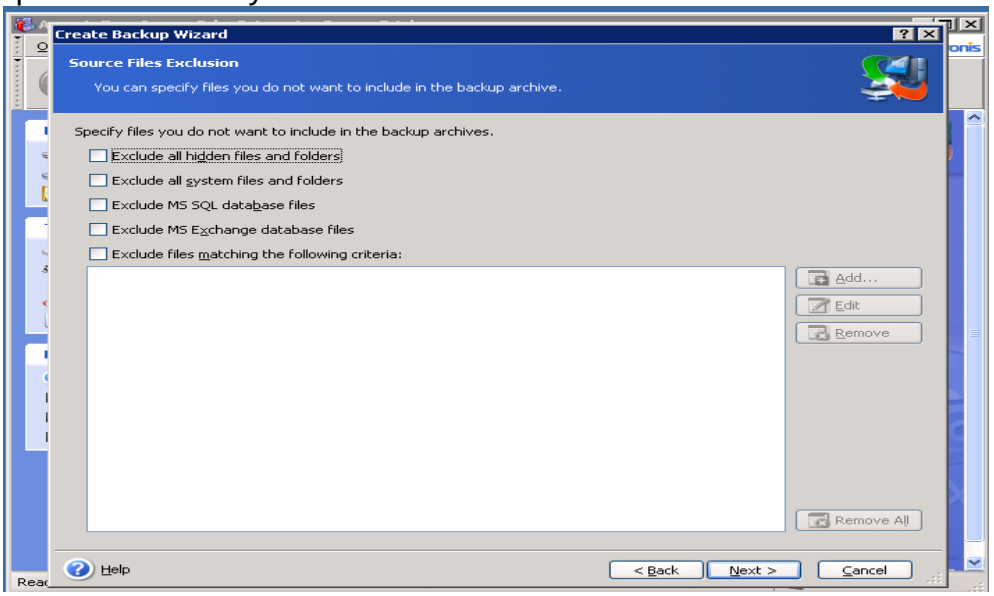

Clic en Next y luego elegir My Computer y Next




Luego elegir los volúmenes a realizar la imagen en este caso se realizara una imagen completa del servidor

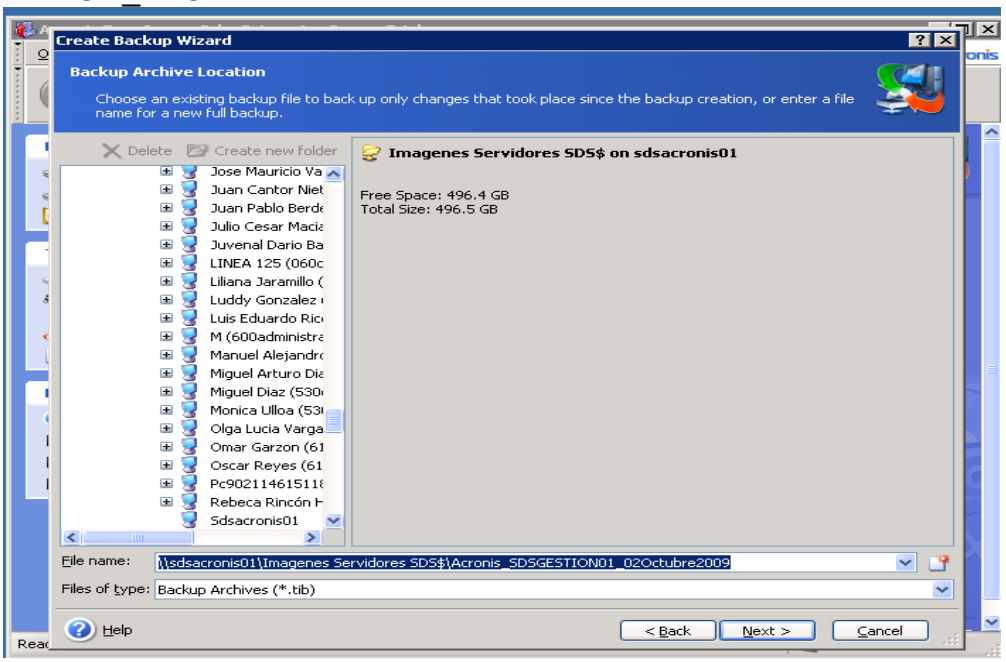



En el próximo cuadro no elegir exclusión alguna para que se realice una imagen completa del mismo y Clic en next

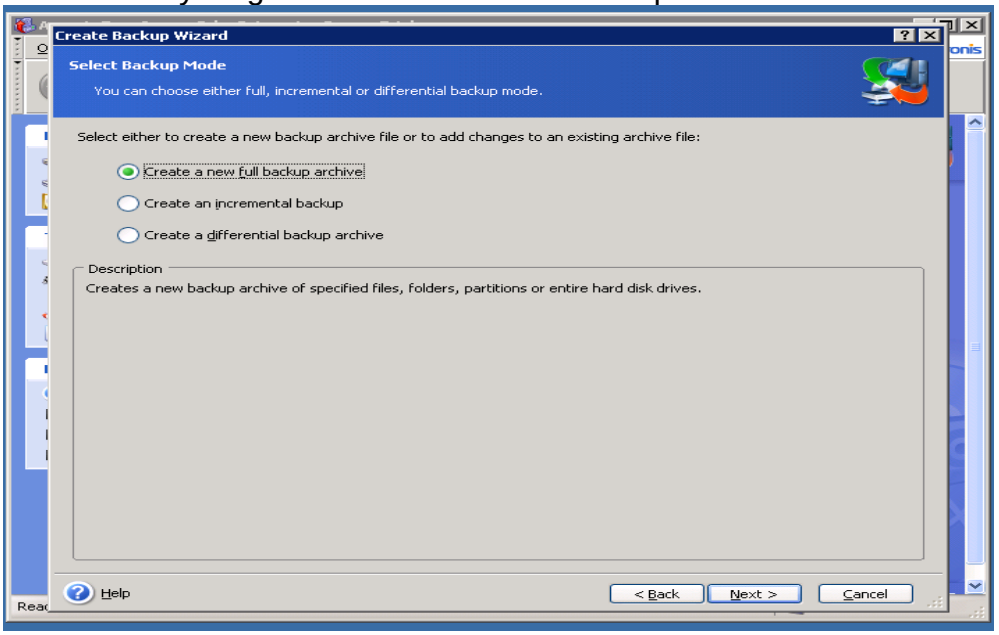



Ahora nos solicitara el destino que servirá para almacenar la imagen del servidor, en este caso elegimos nuestro servidor de Acronis XXXXXX en la carpeta compartida Imagenes Servidores SDS$, luego la carpeta con el nombre del

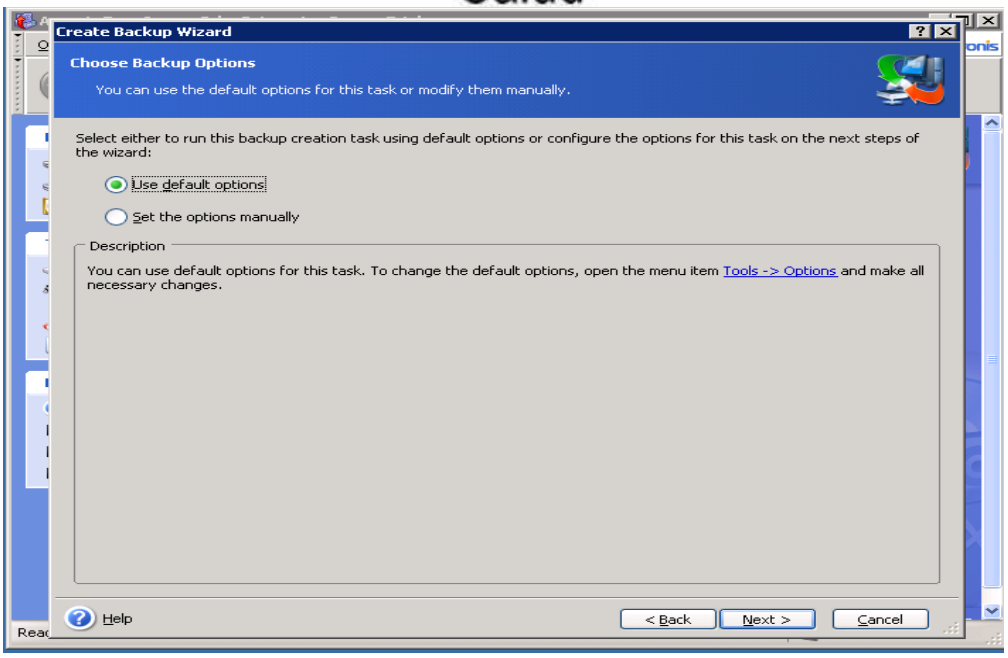
servidor al cual se le esta realizando la imagen, para este ejemplo XXXXX y dentro de ella el nombre del archivo .tib o imagen el cual será: Acronis_NOMBRE SERVIDOR_FECHA



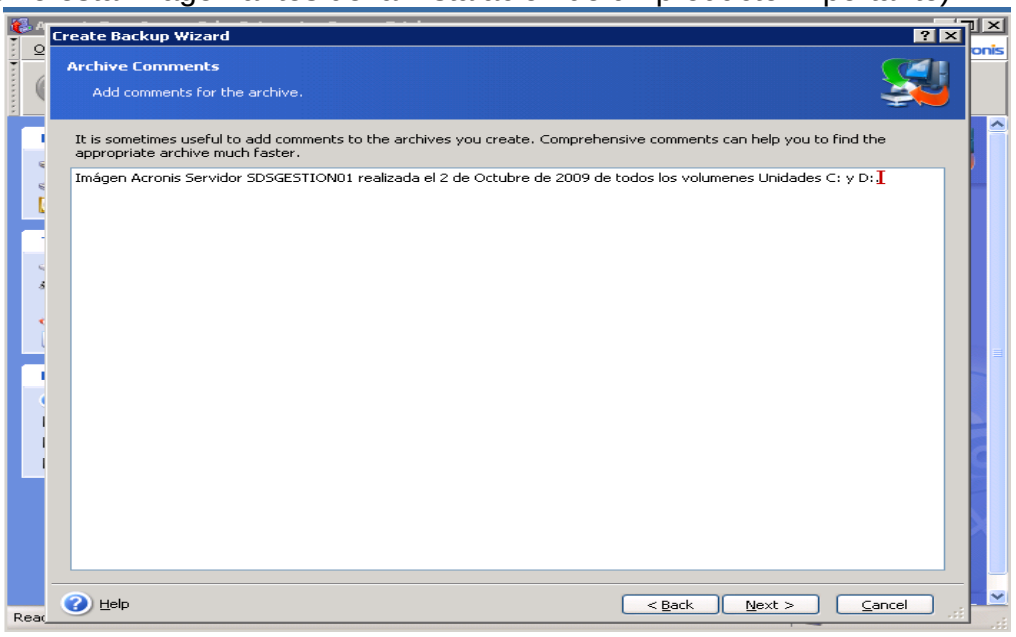

Clic en next y elegir crear un Nuevo full backup



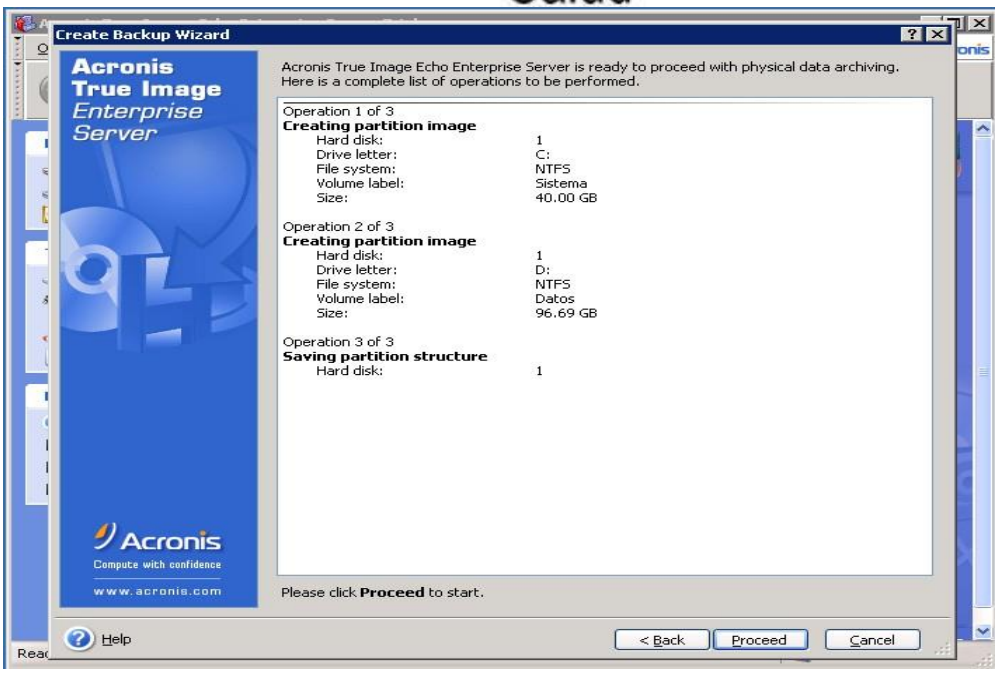

Elegir luego default options y next



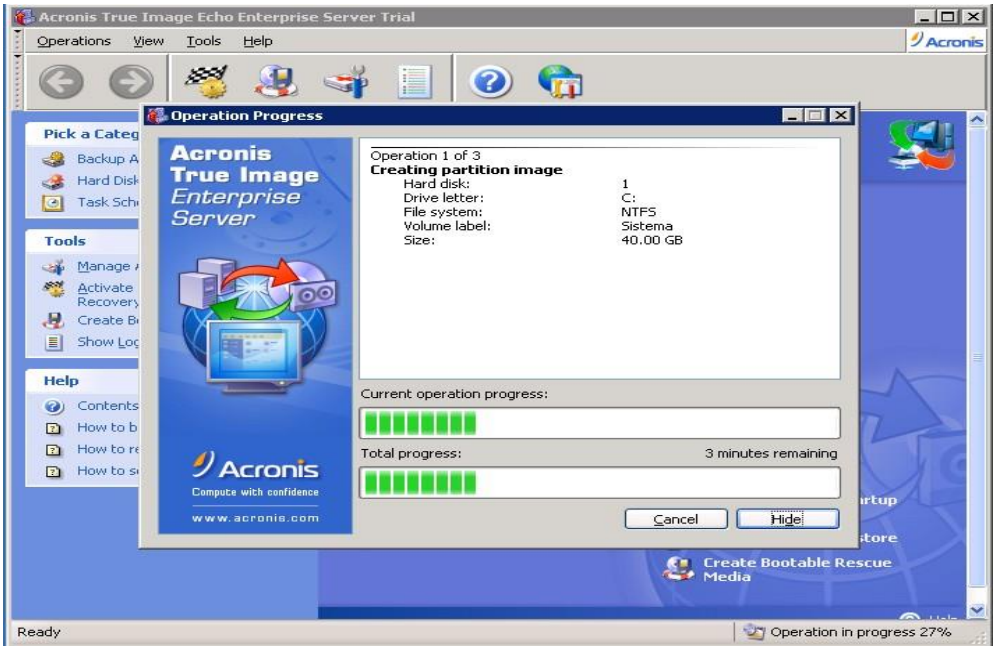

En los comentarios es importante dar una descripción de los volúmenes a los que se le realizo la imagen, la fecha y alguna novedad importante (Por ejemplo si se realizo esta imagen antes de la instalación de un producto importante).

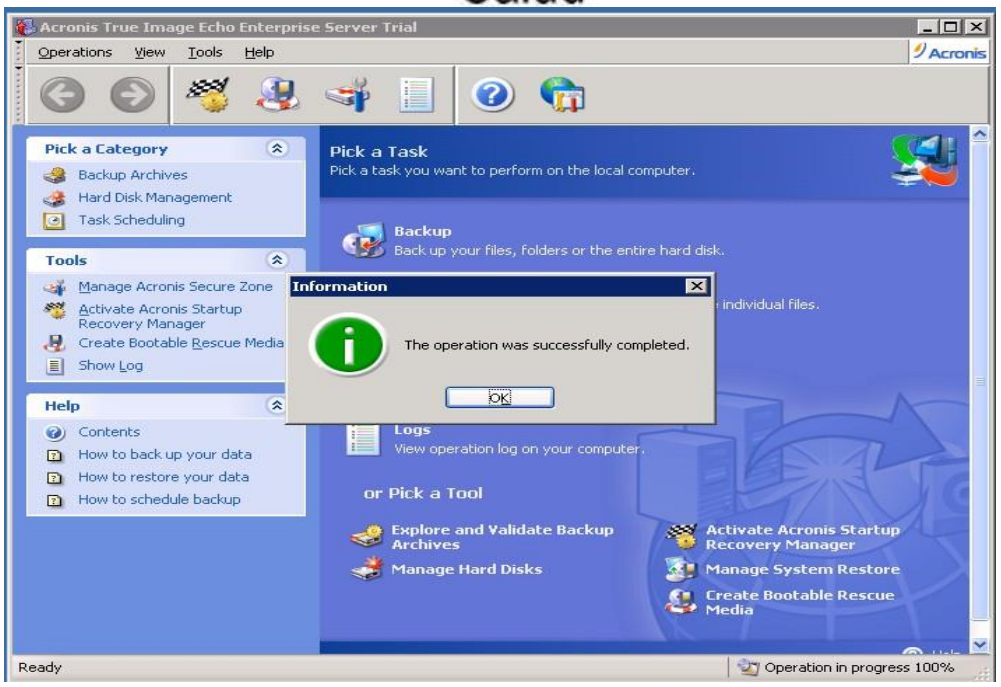



Clic en next y nos mostrará un resumen a lo que le hará la imagen




Clic en Proceed






Visto el archivo imagen desde el servidor XXXXXXX

Para comprobar los logs de seguimiento a la operación entrar por la opción de logs en el panel de acronis


Acronis True Image Echo Enterprise Server Trial
Operations
View
Tools
Help
Acronis
Pick a Category
Backup Archives
Hard Disk Management
Task Scheduling
Tools
Manage Acronis Secure Zone
Activate Acronis Startup Recovery Manager
Create Bootable Rescue Media
Show Log
Help
Contents
How to back up your data
How to restore your data
How to schedule backup
Pick a Task
Pick a task you want to perform on the local computer.
Backup
Back up your files, folders or the entire hard disk.
Recovery
Recover the entire hard disk contents or restore individual files.
Manage Tasks
Tasks
Manage tasks scheduled on your computer.
Logs
View operation log on your computer.
or Pick a Tool
Explore and Validate Backup Archives
Manage Hard Disks
Activate Acronis Startup Recovery Manager
Manage System Restore
Create Bootable Rescue Media
Ready
No operation started

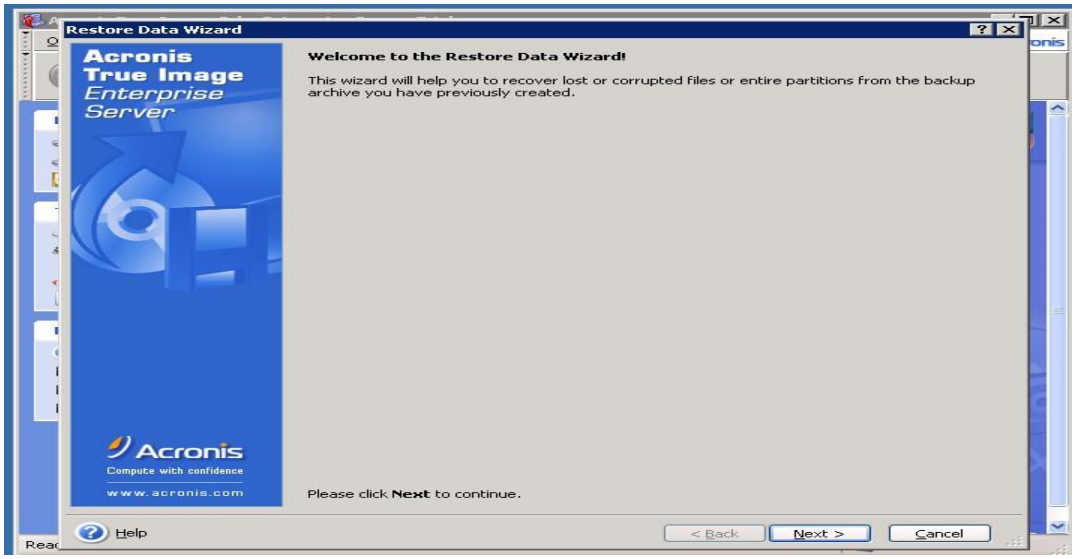
ALCALDIA MAYOR
DE BOGOTA D.C.
Secretaría
Salud

## 5.1 PROCEDIMIENTO PARA LA RESTAURACION DE LAS IMAGENES

A continuación se da el procedimiento para la restauración de la imagen en un servidor

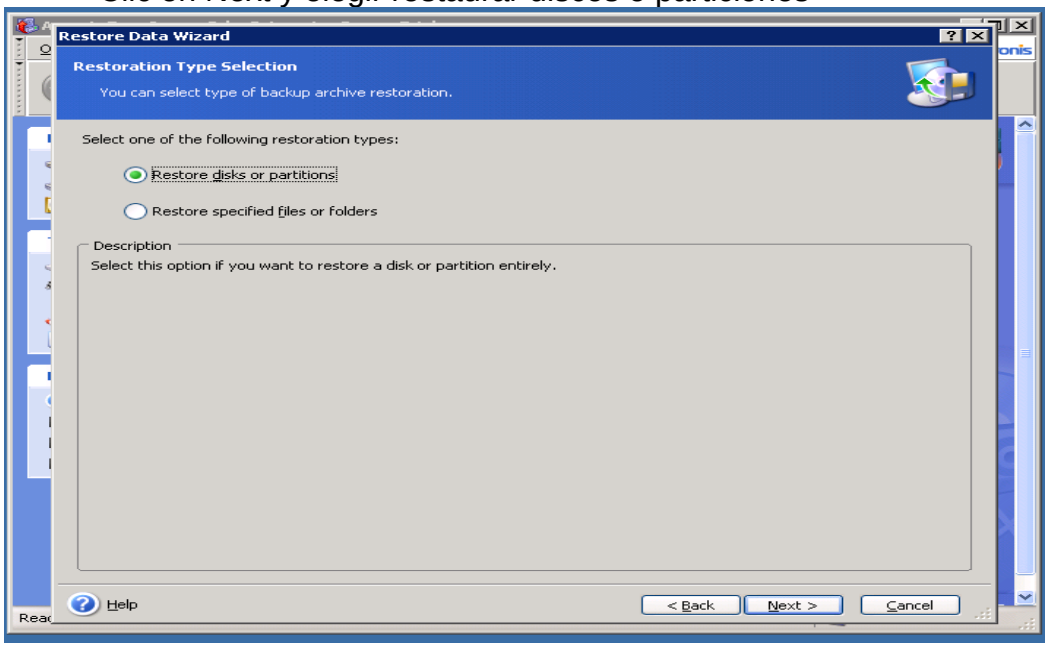
Se elige la opción de Recovery en el panel de Acronis


Clic en Next

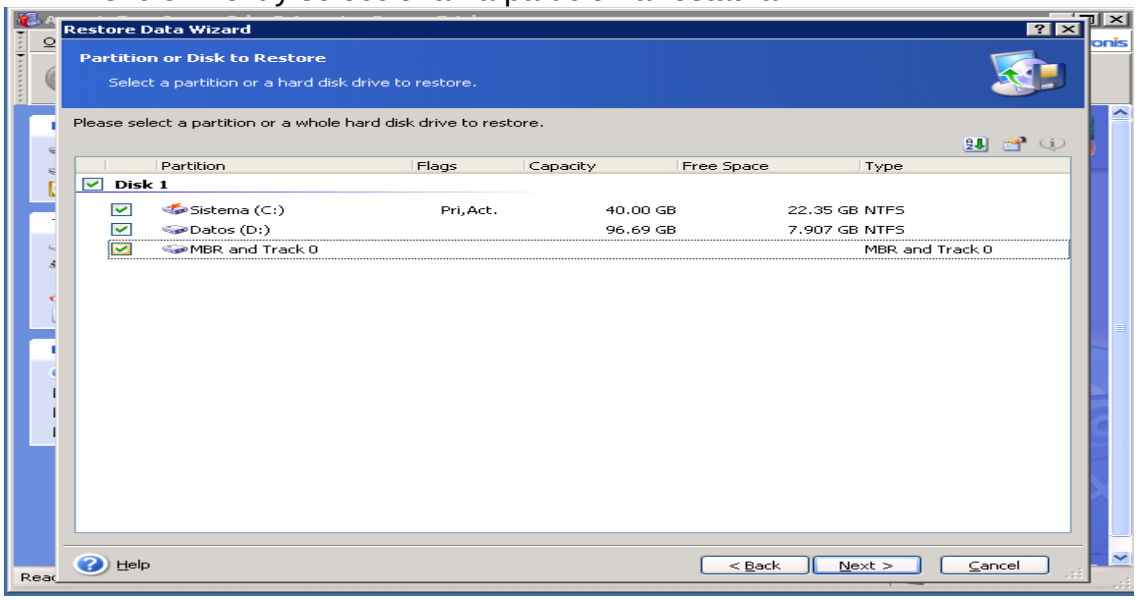


Luego damos la ruta en donde se encuentra el archivo .tib o imagen del especificado servidor

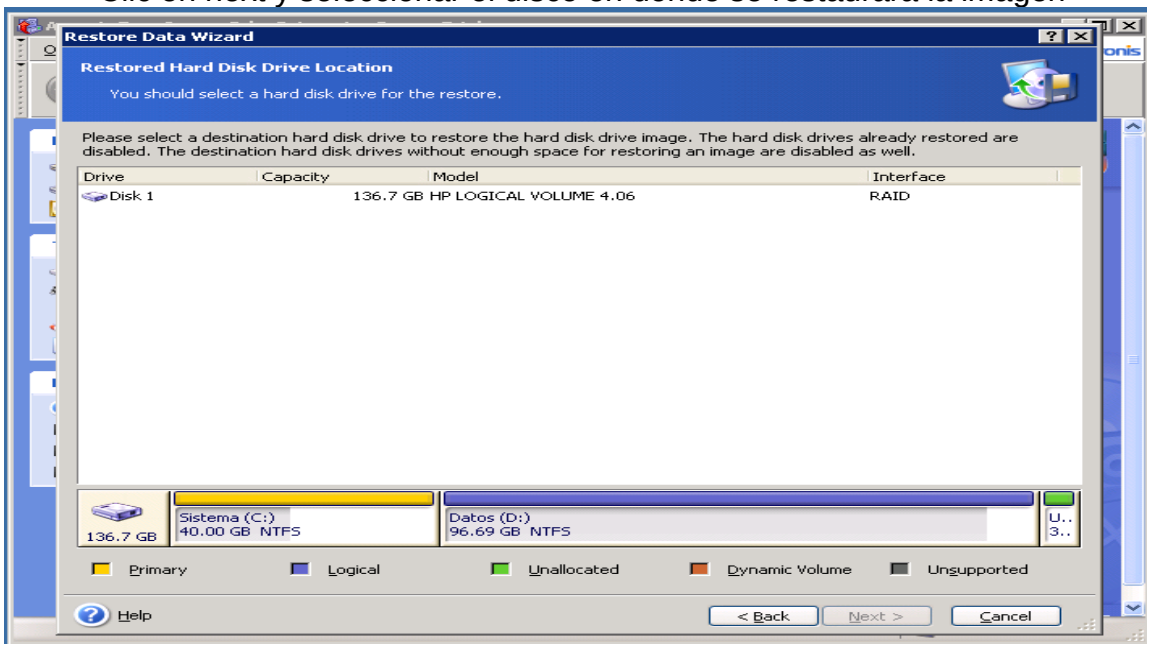
Clic en Next y elegir restaurar discos o particiones



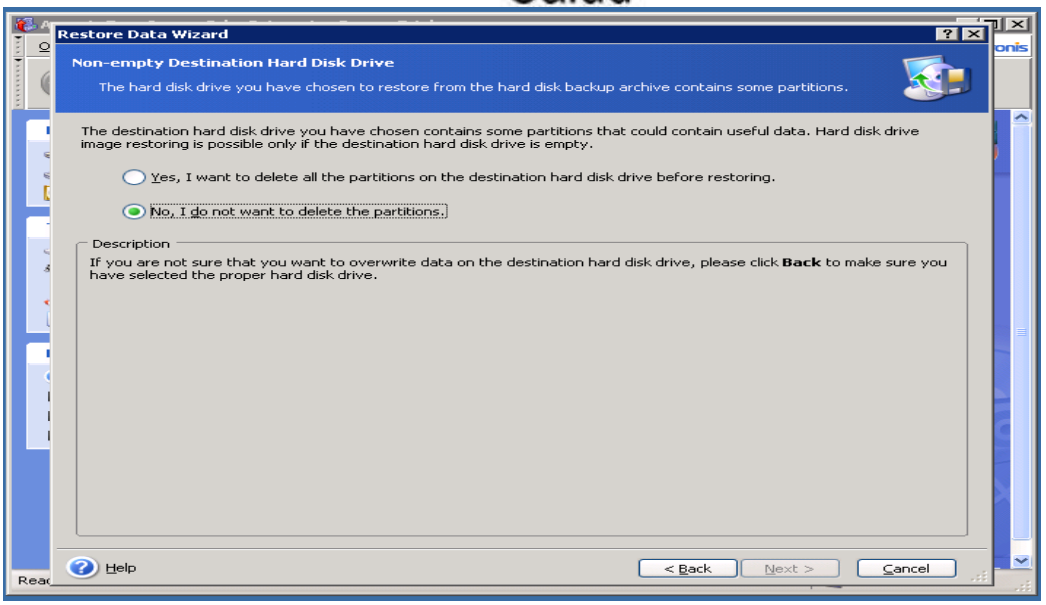
Clic en next y seleccionar la partición a restaurar




Clic en next y seleccionar el disco en donde se restaurara la imagen




Clic en next, luego nos preguntará si se desea o no borrar las particiones en el destino antes de restauración a lo cual es un prerrequisito tener las particiones libres de datos ya que no restauraría la imagen.




Luego Clic en next y posteriormente proceder.

**Programación de las imágenes**

Se ha acordado con la Secretaría Distrital de Salud realizar una imagen a los servidores una vez adquirido el producto cada vez que se analice y se detecte un cambio importante sobre la plataforma.

## 6. PROCESOS DE RECUPERACION

La Dirección de Planeación y Sistemas con el propósito de garantizar la operación de la plataforma de TIC ha creado este documento *"Plan de contingencia de la plataforma de TIC de la SDS",* que se convierte en el procedimiento a seguir ante la presencia de cualquier evento que afecte o interrumpa el normal funcionamiento de la plataforma de TIC. Se ha estructurado de tal manera que brinde continuidad a cualquiera de los núcleos de operación que se definieron en la entidad:

- ✓ Bases de datos (SQL, Oracle).
- ✓ Aplicaciones (Web y livianas).
- ✓ Mensajería (Exchange)
- ✓ Infraestructura (Servidores, Storage).
- ✓ Redes y comunicaciones (Switches, routers, canales).
- ✓ Infraestructura Física (Ups, Electricidad, Aire acondicionado).
- ✓ Seguridad Informática (Lógica y física).

De esta manera modular es más practico hacerle frente a cualquier materialización de una amenaza que afecte total o parcialmente la plataforma de TIC y con la socialización, capacitación y entrenamiento de los grupos definidos por cada núcleo de operación se garantiza que la recuperación de la operación "total o parcial" se realiza en tiempos aceptables en donde el impacto sea mínimo y sin pérdida de la información.

### 6.1. Activación del Plan de Contingencia de la Plataforma de TIC de la SDS

El plan de contingencia de la SDS será activado solo y únicamente por Coordinador General del Plan de contingencia". A él, como coordinador del grupo se le deberá informar cualquier eventualidad que afecte la operación de la entidad, este a su vez lo evaluara con el Coordinador de Ingeniería y tomara la decisión de activar el plan de manera total o parcial (según el núcleo de operación) y se procederá según lo indica el presente documento.

La activación del plan de contingencia durante horario no hábil (en las noches o los fines), habilita el permiso de ingreso a las instalaciones de la entidad de los miembros de los diferentes grupos de recuperación, obviamente previa verificación telefónica, verbal o escrita del Coordinador General, para este fin de formaliza un memorando a la Dirección Administrativa adjuntando un listado con los datos de los miembros de los grupos de recuperación.

Según le eventualidad y su nivel de impacto el plan de contingencia podrá activar uno, dos o más grupos de recuperación según la necesidad. Cada grupo trabajara bajo las instrucciones de su coordinador y si el evento requirió activar otros grupos de recuperación todos entre sí, trabajaran bajo las órdenes del coordinador General del Plan de Contingencia o su delegado.

### 6.2. Procedimiento de recuperación núcleo Bases de Datos

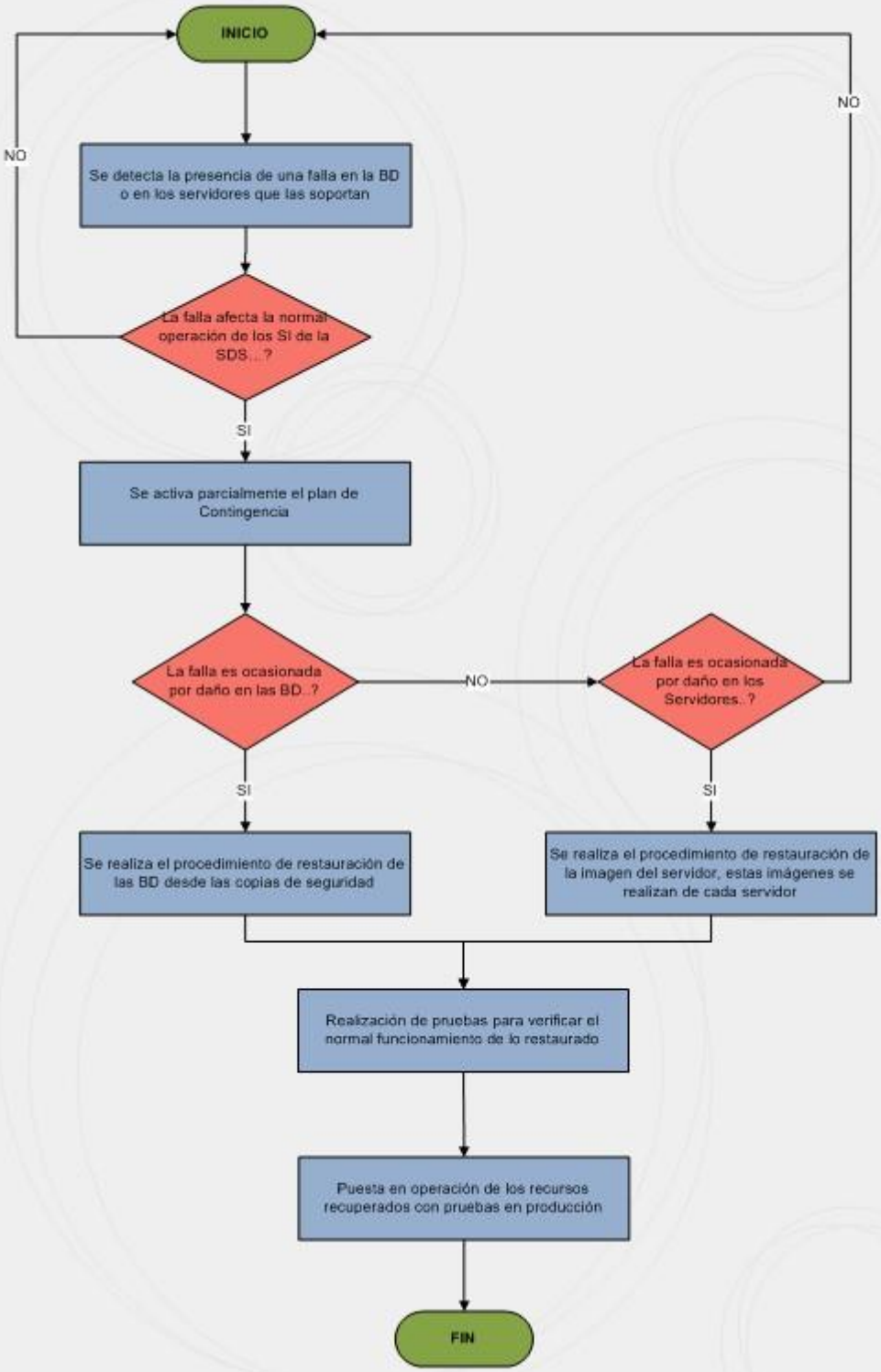
Ante la presencia de un evento que afecte el normal funcionamiento de los motores de bases de datos (SQL Server o Oracle), bien sea por daño irrecuperable de las mismas o daño grave de los servidores donde se alojan estas, se activara el plan de contingencia parcialmente para este núcleo de operación. A continuación se describen los pasos a seguir para la activación y ejecución del plan de recuperación de bases de datos de la SDS:

1. Las personas referentes de BD o la firma proveedora del servicio de administración de BackOffice que detecten el evento avisaran de este al "Coordinador del grupo de recuperación de Bases de datos quien pondrá en conocimiento del mismo al "Coordinador General del Plan de Contingencia de la plataforma de TIC de la SDS", quien activara el plan.
2. Una vez activado el plan se procederá a evaluar los daños o los componentes afectados.
3. Si el evento afecto (daño, borro, etc.) las bases de datos (Oracle O SQL) y el servidor está operativo se procederá a realizar una restauración de las bases de datos desde los medios en donde se generan las copias de respaldo periódicamente.
4. Si las BD a restaurar están en la VTL (esta conserva los BK de las últimas 4 semanas) se restaurara el ultimo backup full (viernes anterior) y el ultimo diferencial generado (noche anterior).
5. Si las bases de datos se respaldaron en la librería física (cintas SDLT) y no se han enviado a custodia, las cintas estarán dentro de la misma y se podrán restaurar las BD que se requieran.
6. Si las BD se respaldaron en cintas y estas ya fueron enviadas a la empresa especializada en custodia de medios, un miembro del grupo de apoyo hará la solicitud a cualquiera de las personas autorizadas para solicitar las cintas a dicha entidad. Esta solicitud por condiciones contractuales se podrá hacer con categoría de urgencia y la empresa entregara las cintas en menos de dos horas para hacer le respectiva restauración.
7. Si el servidor donde alojan las BD sufrió daño grave o irreparable, se activara también el grupo de recuperación de infraestructura y este con la instrucciones de sus coordinadores se procederá a utilizar uno de los cuatro servidores que se tienen de respaldo (fuera del centro de cómputo) para

restaurar la imagen del servidor original con la función *"The Universal Restore de Acronis"* que permite restaurar la imagen en otro servidor de diferentes características de hardware.

8. Después de tener el servidor operativo y completamente configurado (entregado por el grupo de recuperación de Infraestructura) se restauraran las instancias o las BD que se afectaron con el evento. Continuar en el numeral 3.
9. Después de restauradas las BD el coordinador del grupo y DBA de la SDS realizara las respectivas pruebas de operación de las mismas y se dará de alta al servicio afectado.
10. El grupo de restauración después de recuperar la operación redactara un informe al Coordinador General del Plan de Contingencia sobre el evento y de las actividades realizadas para ser analizadas al interior del comité de seguridad y hacer las correcciones, mejoras y/o actualizaciones que se definan como necesarias.

## DIAGRAMA DEL PROCEDIMIENTO DE RECUPERACION DE BASES DE DATOS



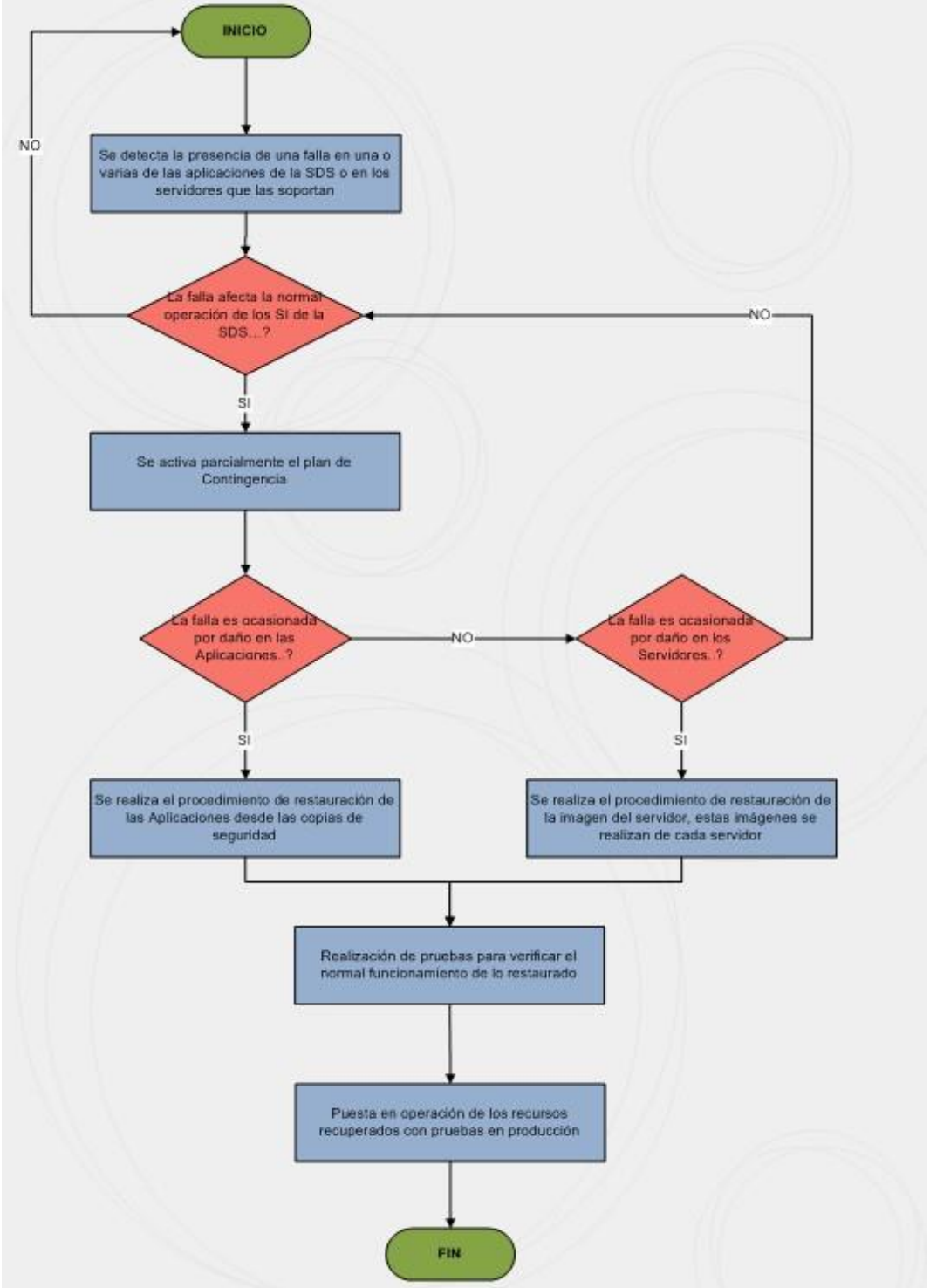
### 6.3. Procedimiento de recuperación núcleo Aplicaciones

Ante la presencia de un evento que afecte el normal funcionamiento de las aplicaciones de la SDS, bien sea por daño irrecuperable de las mismas o daño grave de los servidores donde se alojan estas, se activara el plan de contingencia parcialmente para este núcleo de operación. A continuación se describen los pasos a seguir para la activación y ejecución del plan de recuperación de las Aplicaciones SDS:

1. Las personas referentes de las aplicaciones o la firma proveedora del servicio de administración de BackOffice que detecten el evento avisaran de este al "Coordinador del grupo de recuperación de Aplicaciones" quien pondrá en conocimiento del mismo al "Coordinador General del Plan de Contingencia de la plataforma de TIC de la SDS", quien activara el plan.
2. Una vez activado el plan se procederá a evaluar los daños o los componentes afectados.
3. Si el evento afecto (daño, borro, etc.) las aplicaciones y el servidor está operativo se procederá a realizar una restauración de las aplicaciones desde los medios en donde se generan las copias de respaldo periódicamente.
4. Si las aplicaciones a restaurar están en la VTL (esta conserva los BK de las últimas 4 semanas) se restaurara el ultimo backup full (viernes anterior) y el ultimo diferencial generado (noche anterior).
5. Si las aplicaciones se respaldaron en la librería física (cintas SDLT) y no se han enviado a custodia, las cintas estarán dentro de la misma y se podrán restaurar las aplicaciones que se requieran.
6. Si las aplicaciones se respaldaron en cintas y estas ya fueron enviadas a la empresa especializada en custodia de medios, un miembro del grupo de apoyo hará la solicitud a cualquiera de las personas autorizadas para solicitar las cintas. Esta solicitud por condiciones contractuales se podrá hacer con categoría de urgencia y la empresa entregara las cintas en menos de dos horas para hacer le respectiva restauración.
7. Si el servidor donde se ejecutan las aplicaciones sufrió daño grave o irreparable, se activara también el grupo de recuperación de infraestructura y este, con la instrucciones de sus coordinadores se procederá a utilizar uno de los cuatro servidores que se tienen de respaldo (fuera del centro de computo) para restaurar la imagen del servidor original con la función *"The Universal Restore de Acronis"* que permite restaurar la imagen en otro servidor de diferentes características de hardware.

8. Después de tener el servidor operativo y completamente configurado (entregado por el grupo de recuperación de Infraestructura) se restauraran las aplicaciones que se afectaron con el evento. Continuar en el numeral 3.
9. Después de restauradas las aplicaciones el coordinador del grupo y líder del grupo de desarrollo de la SDS realizara las respectivas pruebas de operación de las mismas y se dará de alta al servicio afectado.
10. El grupo de restauración después de recuperar la operación redactara un informe al Coordinador General del Plan de Contingencia sobre el evento y de las actividades realizadas para ser analizadas al interior del comité de seguridad y hacer las correcciones, mejoras y/o actualizaciones que se definan como necesarias.

## DIAGRAMA DEL PROCEDIMIENTO DE RECUPERACION DE APLICACIONES



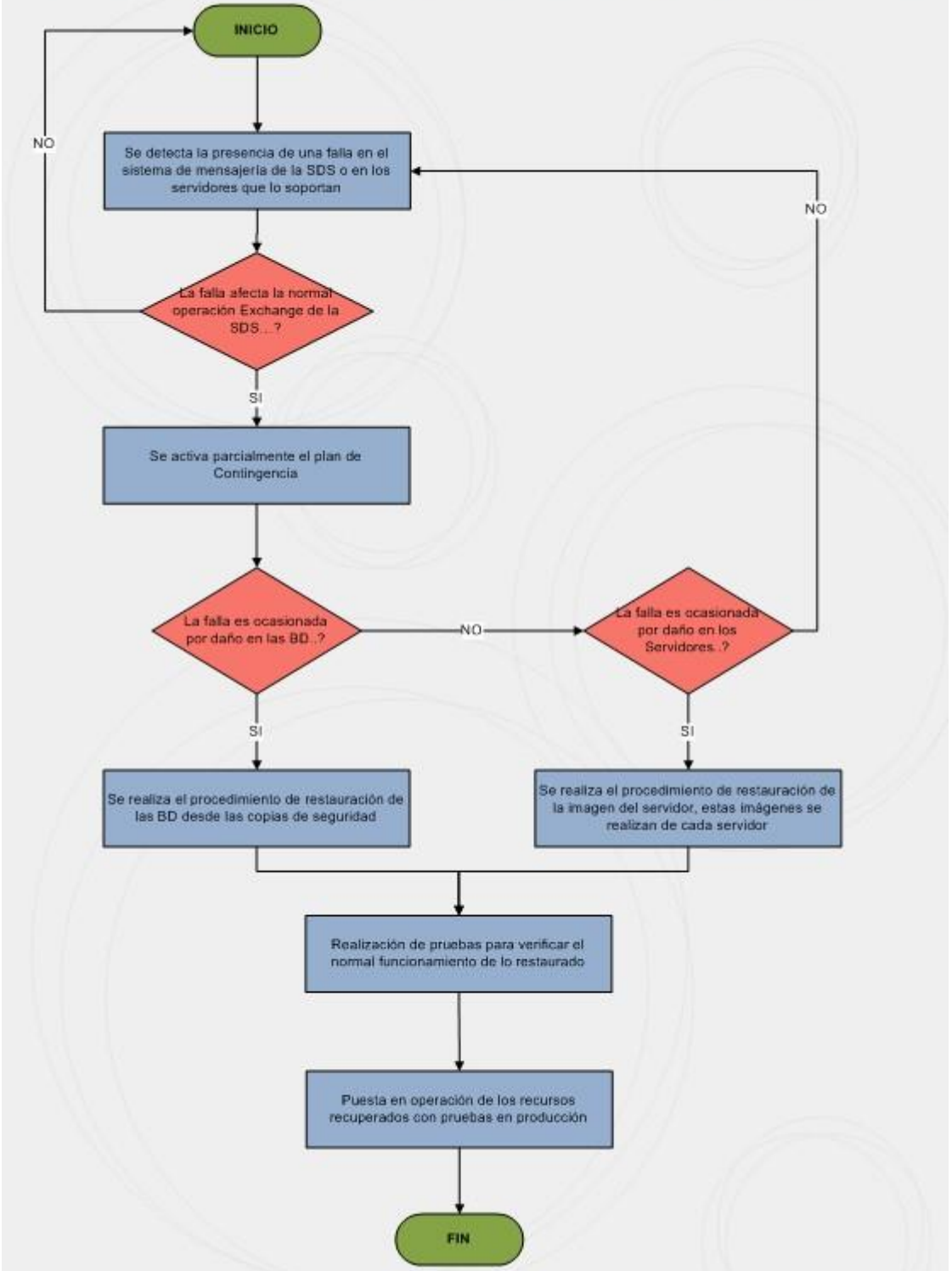
### 6.4. Procedimiento de recuperación núcleo Mensajería

Ante la presencia de un evento que afecte el normal funcionamiento del sistema de mensajería de la SDS (Exchange Server 2010), bien sea por daño irrecuperable de la solución o sus BD o daño grave de los servidores donde se aloja la solución, se activara el plan de contingencia parcialmente para este núcleo de operación. A continuación se describen los pasos a seguir para la activación y ejecución del plan de recuperación del sistema de mensajería SDS:

1. Las personas referentes de Exchange con su especialista, que detecten el evento avisaran de este al "Coordinador del grupo de recuperación de Mensajería" quien pondrá en conocimiento del mismo al "Coordinador General del Plan de Contingencia de la plataforma de TIC de la SDS", quien activara el plan.
2. Una vez activado el plan se procederá a evaluar los daños o los componentes afectados.
3. Si el evento afecto (daño, borro, etc.) la solución, las BD y el servidor está operativo se procederá a realizar una restauración de la solución de mensajería desde los medios en donde se generan las copias de respaldo periódicamente.
4. Si la solución o las BD a restaurar están en la VTL (esta conserva los BK de las últimas 4 semanas) se restaurara el ultimo backup full (viernes anterior) y el ultimo diferencial generado (noche anterior).
5. Si las la solución o las BD se respaldaron en la librería física (cintas SDLT) y no se han enviado a custodia, las cintas estarán dentro de la misma y se podrá restaurar lo que se requiera.
6. Si la solución o las BD se respaldaron en cintas y estas ya fueron enviadas a la empresa especializada en custodia de medios, un miembro del grupo de apoyo hará la solicitud a cualquiera de las personas autorizadas para solicitar las cintas. Esta solicitud por condiciones contractuales se podrá hacer con categoría de urgencia y la empresa entregara las cintas en menos de dos horas para hacer le respectiva restauración.
7. Si el servidor donde se ejecutan la solución de mensajería (Exchange Server 2010) sufrió daño grave o irreparable, se activara también el grupo de recuperación de infraestructura y este, con la instrucciones de sus coordinadores se procederá a utilizar uno de los cuatro servidores que se tienen de respaldo (fuera del centro de cómputo) para restaurar la imagen del servidor original con la función *"The Universal Restore de Acronis"* que permite restaurar la imagen en otro servidor de diferentes características de hardware.

8. Después de tener el servidor operativo y completamente configurado (entregado por el grupo de recuperación de Infraestructura) se restaurara la solución de mensajería que se afectó con el evento. Continuar en el numeral 2.
9. Después de restaurada la solución de mensajería los coordinadores del grupo de recuperación de Mensajería de la SDS realizaran las respectivas pruebas de operación y se dará de alta al servicio afectado.
10. El grupo de restauración después de recuperar la operación redactara un informe al Coordinador General del Plan de Contingencia sobre el evento y de las actividades realizadas para ser analizadas al interior del comité de seguridad y hacer las correcciones, mejoras y/o actualizaciones que se definan como necesarias.

## DIAGRAMA DEL PROCEDIMIENTO DE RECUPERACION DEL SISTEMA DE MENSAJERIA

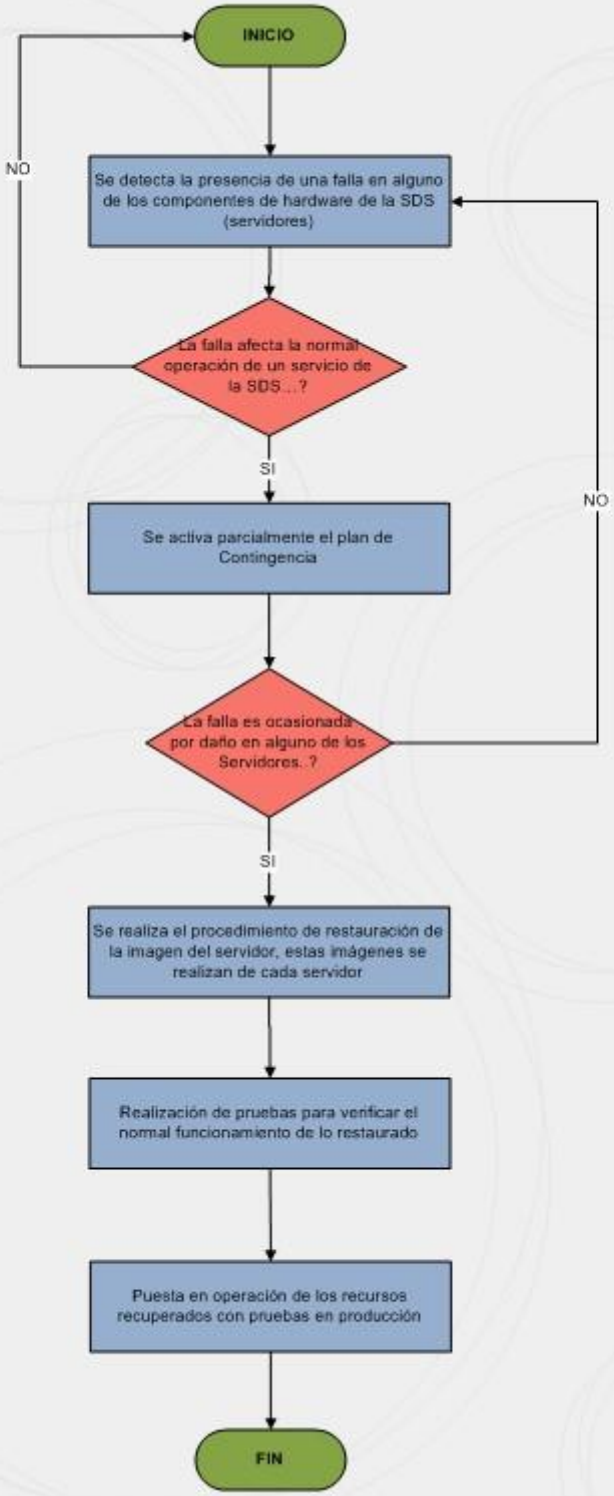


### 6.5. Procedimiento de recuperación núcleo de Infraestructura (servidores, storage)

Ante la presencia de un evento que afecte el normal funcionamiento de los componentes de Hardware que soportan la operación de la SDS (servidores, storage), bien sea por daño irrecuperable del equipo o daño parcial del de los servidores, se activara el plan de contingencia parcialmente para este núcleo de operación. A continuación se describen los pasos a seguir para la activación y ejecución del plan de recuperación de Infraestructura de la SDS:

1. Las personas referentes de Infraestructura (componentes de hardware que están en el centro de cómputo: servidores, Storage) *del servicio de administración de BackOffice* con su especialista en Servers, que detecten el evento avisaran de este a los "Coordinadores del grupo de recuperación de Infraestructura y se activara el plan.
2. Una vez activado el plan se procederá a evaluar los daños o los componentes afectados.
3. Si el evento afecto un elemento irreparablemente y el mismo está por fuera del periodo de garantía, se procederá a realizar una restauración de la imagen del servidor en uno de los servidores que se tienen de respaldo (cuatro, por fuera del centro de cómputo).desde los medios en donde se generan las copias de respaldo de los servidores (imágenes) periódicamente. Si el equipo está dentro de su periodo de garantía el referente de la firma o la persona asignada por los coordinadores realizara simultáneamente la reclamación por garantía ante la firma respectiva. Ver Anexo: listado de los elementos en garantía y su respectivo proveedor.
4. Si la imagen del servidor a restaurar está en el servidor destinado para tal fin "XXXXXX", este conserva las últimas imágenes generadas de cada uno de los diferentes servidores, según documento *"Esquema de generación de Imágenes de los servidores de la SDS"* se restaurara la última Imagen del servidor afectado.
5. Después de tener el servidor operativo y completamente configurado se restauraran las aplicaciones, BD o soluciones que en este estaban operando antes de presentarse el evento.
6. Después de restauradas las aplicaciones, BD o soluciones la realizaran las respectivas pruebas de operación y se dará de alta al servicio afectado.
7. El grupo de restauración después de recuperar la operación redactara un informe al Coordinador General del Plan de Contingencia sobre el evento y de las actividades realizadas para ser analizadas al interior del comité de seguridad y hacer las correcciones, mejoras y/o actualizaciones que se definan como necesarias.

## DIAGRAMA DEL PROCEDIMIENTO DE RECUPERACION DE INFRAESTRUCTURA



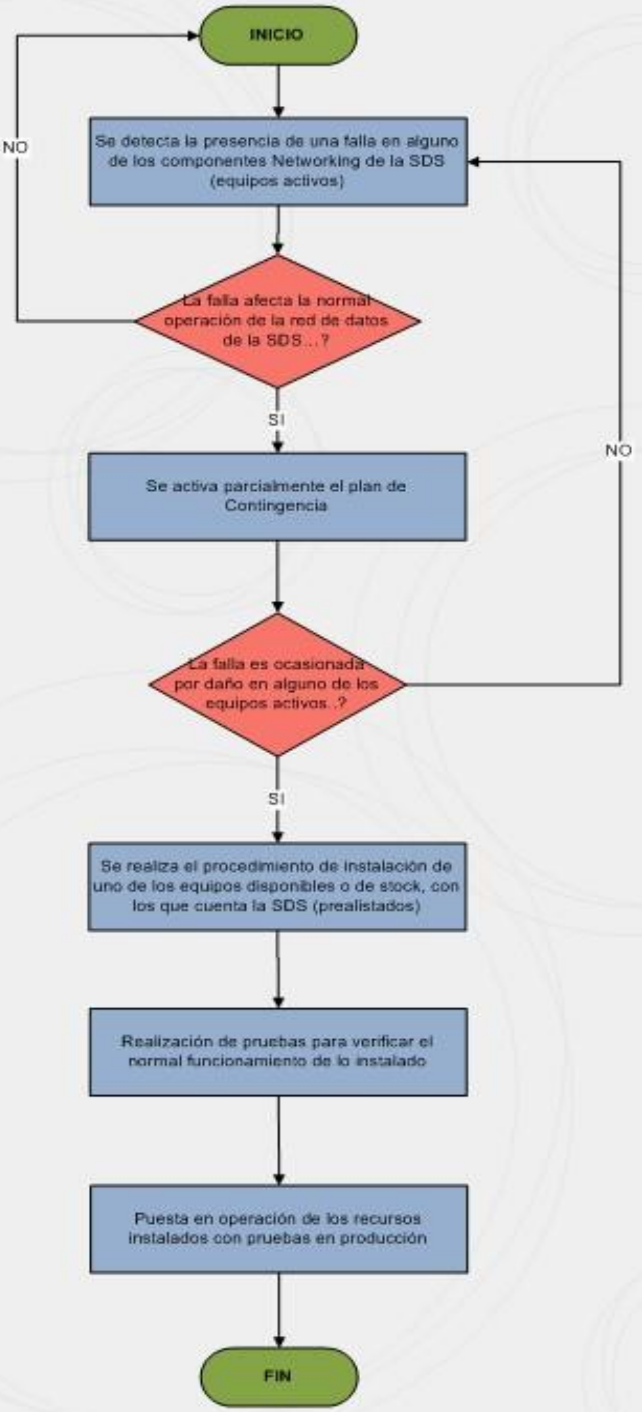
### 6.6. Procedimiento de recuperación núcleo de Redes y Comunicaciones

Ante la presencia de un evento que afecte el normal funcionamiento de los equipos networking o también llamados equipos activos Switch Core, Switches de Distribución, de borde, y Firewall) de la SDS, bien sea por daño irreparable de algún elemento, se activara el plan de contingencia parcialmente para este núcleo de operación. A continuación se describen los pasos a seguir para la activación y ejecución del plan de recuperación de redes y comunicaciones de la SDS:

1. Las personas referentes de Redes y Comunicaciones (componentes Networking) que están distribuidos en los cuatro edificios de la entidad y en cada uno de sus pisos. Ver Tabla de equipos activos en operación, *del servicio de administración de BackOffice,* con su especialista en Redes, que detecten el evento avisaran de este a los "Coordinadores del grupo de recuperación de Redes y Comunicaciones" y se activara el plan.
2. Una vez activado el plan se procederá a evaluar los daños o los componentes afectados.
3. Si el evento afecto un elemento irreparablemente y el mismo está por fuera del periodo de garantía, se procederá a realizar la instalación de uno de los equipos que se tienen de respaldo (cinco, por fuera del centro de cómputo, un Firewall Cisco PIX, Switch Core y tres Switch de borde).cada uno configurado y listo para operar con el estándar de redes de la SDS (Vlan's, interfaces, direccionamiento, etc.). Adicionalmente a esto se cuenta con backup quincenal de la configuración de cada uno de los equipos activos y estos se almacenan en los medios de respaldo. Si el equipo está dentro de su periodo de garantía el referente de la firma o la persona asignada por los coordinadores realizara simultáneamente la reclamación por garantía ante la firma respectiva. Ver Anexo: listado de los elementos activos en garantía y su respectivo proveedor.
4. Si los backup de los equipos activos se respaldaron en cintas y estas ya fueron enviadas a la empresa especializada en custodia de medios, un miembro del grupo de apoyo hará la solicitud a cualquiera de las personas autorizadas para solicitar las cintas. Esta solicitud por condiciones contractuales se podrá hacer con categoría de urgencia y la empresa entregara las cintas en menos de dos horas para hacer le respectiva restauración.
5. Después de tener el equipo activo operativo y completamente configurado se restaurara la solución de redes que se afectó con el evento.
6. Después de restaurada la solución de Redes los coordinadores del grupo de recuperación de Redes y Comunicaciones de la SDS realizaran las respectivas pruebas de operación y se dará de alta al servicio afectado.

7. El grupo de restauración después de recuperar la operación redactara un informe al Coordinador General del Plan de Contingencia sobre el evento y de las actividades realizadas para ser analizadas al interior del comité de seguridad y hacer las correcciones, mejoras y/o actualizaciones que se definan como necesarias.

## DIAGRAMA DEL PROCEDIMIENTO DE RECUPERACION DE REDES Y COMUNICACIONES



### 6.7. Procedimiento de recuperación núcleo de Infraestructura Física

Ante la presencia de un evento que afecte el normal funcionamiento de los equipos que suministran las condiciones ambientales apropiadas para el funcionamiento de todos los equipos y elementos que se encuentran al interior del centro de cómputo (tercer piso edificio Administrativo, Dirección de Planeación y Sistemas), Aire acondicionado, Sistema de detección y extinción de incendios, control de acceso del edificio, sistema de eléctrico regulado “UPS’s y planta eléctrica” de la SDS; bien sea por daño parcial o total de alguno de estos elementos, se activara el plan de contingencia parcialmente para este núcleo de operación. A continuación se describen los pasos a seguir para la activación y ejecución del plan de recuperación de Infraestructura Física de la SDS:

1. Por el diseño del centro de cómputo y de los elementos mencionados (Aire acondicionado, Sistema de detección y extinción de incendios, control de acceso del edificio, sistema de eléctrico regulado “UPS’s y planta eléctrica”), los que normalmente primero detectan un evento que afecte la operación de estos elementos son los miembros *del servicio de administración de BackOffice,* o los miembros del equipo de monitoreo del cuarto de control de la SDS que dependen de la Dirección Administrativa, al detectar el evento avisaran de este al “Coordinador del grupo de recuperación de Infraestructura Física” se activara el plan.
2. Una vez activado el plan se procederá a evaluar los daños o los componentes afectados.
3. Independiente del punto anterior los referentes de los contratos realizaran la solicitud de servicio según el componente y el proveedor, la Coordinadora del núcleo de recuperación de Infraestructura Física, será la responsable de hacer el seguimiento y auditar los resultados de los trabajos realizados por los proveedores en el centro de cómputo. Ver Anexo: Listado de proveedores Dirección Administrativa.
4. El ingeniero determinara si, por demora en los trabajos por parte del proveedor se deberán tomar medidas que afectan la operación total o parcial de la SDS, como:

    - ✓ Apagado total de centro de cómputo.
    - ✓ Apagado parcial del centro de cómputo.
    - ✓ Dejar operativo solo lo critico.

5. Después de tener el equipo operativo se restaurara el sistema que se afectó con el evento. El coordinador del grupo de recuperación de Infraestructura Física de la SDS realizara las respectivas pruebas de operación y se dará de alta al servicio afectado.
6. El grupo de restauración después de recuperar la operación redactara un informe al Coordinador General del Plan de Contingencia sobre el evento y de las actividades realizadas para ser analizadas al interior del comité de seguridad y hacer las correcciones, mejoras y/o actualizaciones que se definan como necesarias.

Nota: Para el caso de presentarse un evento de falla de cualquiera de estos componentes la entidad se enfrenta a un paro no programado de su centro de cómputo, esto implica que los costos y riesgos de no recuperación sean altos y ponen en peligro la continuidad de la entidad.

Es por esta razón, que el diseño, implementación y mantenimientos de los equipos de un centro de cómputo debe ser garantizado y llevado a cabo por profesionales con alta experiencia y profundo conocimiento de la infraestructura y de la normatividad de centros de cómputo.

Con base en lo anterior y en uso de las mejores prácticas se indica que con respecto al sistema de aire acondicionado en el centro de cómputo de la SDS este en sus condiciones óptimas debe estar al frente de los rack (entrada de aire frio) promediando los 16 grados centígrados y en la parte posterior de los rack (salida del aire caliente) es relativo al tipo de equipos pero puede aumentar 6 grados.

El centro de cómputo es el cerebro de los sistemas de voz y datos de la SDS operando 24 horas diarias con requerimientos de alta confiabilidad. Ante un evento que afecten las condiciones óptimas de ambiente del centro de cómputo se generó una tabla con semaforización para el apagado controlado de los servidores y demás componentes de hardware que están en el centro de cómputo según su rol y criticidad de la siguiente manera:

| |
|---|
| Prioridad Alta por Grupo |
| Prioridad Media por Grupo |
| Prioridad Baja por Grupo |

ALCALDIA MAYOR
DE BOGOTA D.C.
Secretaría
Salud

| No. | TIPO | UBICACIÓN |
|---|---|---|
| 1 | FISICO | RACK - C |
| 2 | FISICO | BLADE -9 |
| 3 | FISICO | RACK - C |
| 4 | FISICO | BLADE -10 |
| 5 | FISICO | RACK - C |
| 6 | FISICO | BLADE -1 |
| 7 | FISICO | BLADE -3 |
| 8 | FISICO | RACK - C |
| 9 | FISICO | RACK - B |
| 10 | FISICO | RACK - A |
| 11 | FISICO | RACK - A |
| 12 | FISICO | BLADE -13 |

| No. | TIPO | UBICACIÓN | Nom Maq Virt |
|---|---|---|---|
| 1 | FISICO | BLADE -7 | |
| 2 | FISICO | RACK - C | |
| 3 | FISICO | RACK - C | |
| 4 | FISICO | RACK - C | |
| 5 | FISICO | RACK - B | |
| 6 | FISICO | BLADE -5 | |
| 7 | FISICO | RACK - B | |
| 8 | FISICO | BLADE -11 | |
| 9 | FISICO | RACK - A | |
| 10 | FISICO | BLADE -6 | |

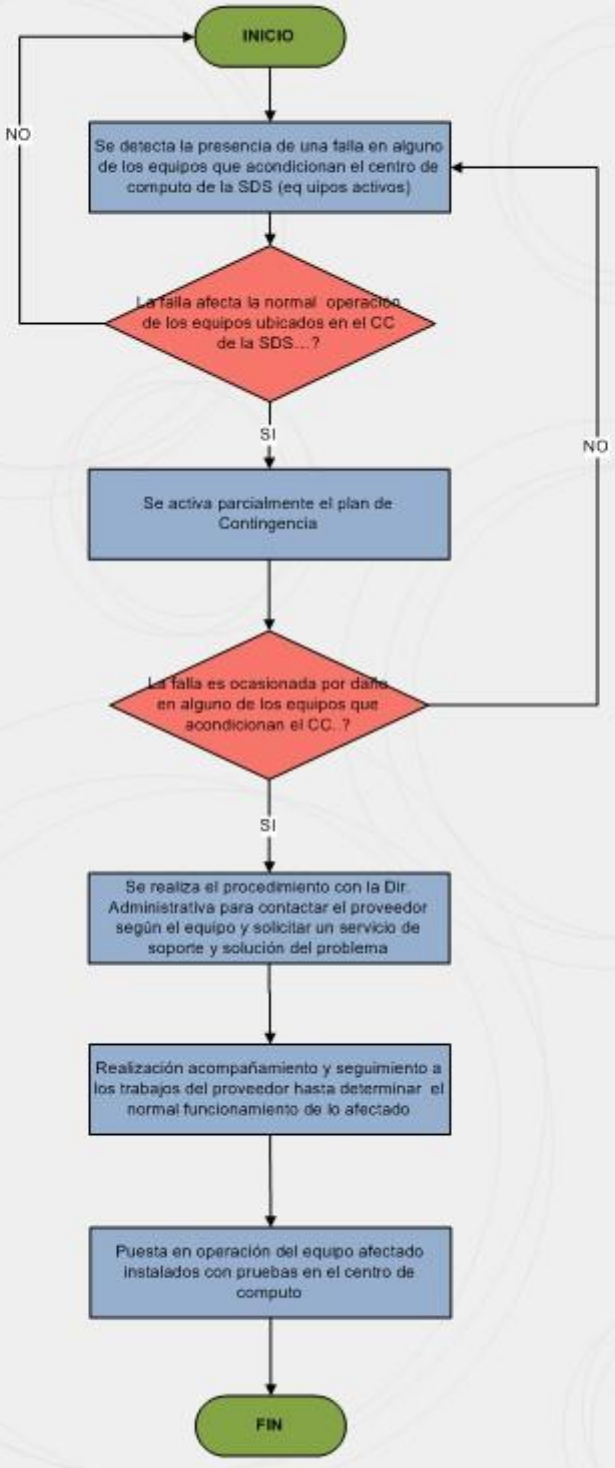
## GRUPO SERVIDORES PRIORIDAD BAJA

| No. | TIPO | UBICACIÓN |
|---|---|---|
| 1 | FISICO | BLADE -14 |
| 2 | FISICO | BLADE -15 |
| 3 | FISICO | BLADE -8 |
| 4 | FISICO | RACK - C |
| 5 | FISICO | BLADE -2 |
| 6 | FISICO | BLADE -4 |
| 7 | FISICO | BLADE -12 |
| 8 | FISICO | RACK - C |
| 9 | FISICO | RACK - A |

Con base en estas tablas de criticidad de los servidores que se encuentran en el centro de cómputo de la SDS se determinara bajo circunstancias especiales cuales mantendrán la operación de la entidad mínima básica o mediana según los roles de cada uno. Como aspecto básico se debe garantizar que los componentes que brindan las condiciones de ambiente al centro de cómputo cuenten con las revisiones y mantenimiento preventivos que determinan su buen funcionamiento.

ALCALDIA MAYOR
DE BOGOTA D.C.
Secretaría
Salud

## DIAGRAMA DEL PROCEDIMIENTO DE RECUPERACION DE INFRAESTRUCTURA FISICA



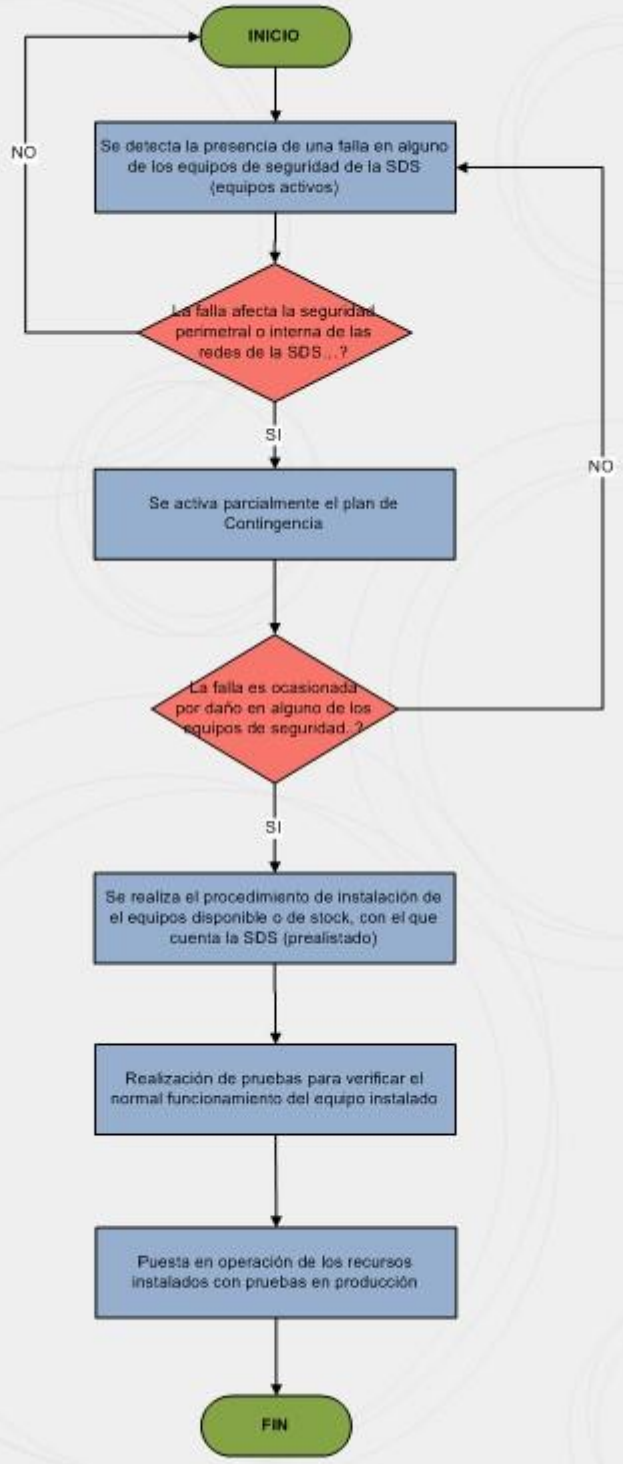
### 6.8. Procedimiento de recuperación núcleo de Seguridad Informática

Ante la presencia de un evento que afecte el normal funcionamiento de los componentes de Hardware que soportan la seguridad Informática de la SDS, bien sea por daño irrecuperable de los equipos o daño parcial de los mismos, se activara el plan de contingencia parcialmente para este núcleo de operación. A continuación se describen los pasos a seguir para la activación y ejecución del plan de recuperación de Infraestructura de la SDS:

1. Las personas de la firma proveedora del servicio de administración de BackOffice, actualmente el Administrador de Seguridad Informática, que detecten el evento que afecta la operación de la entidad, avisaran de este al "Coordinador del grupo de recuperación de Seguridad Informática" y se activara el plan.
2. Una vez activado el plan se procederá a evaluar los daños o los componentes afectados.
3. Si el evento afecto un elemento irreparablemente y el mismo está por fuera del periodo de garantía, se procederá a realizar una instalación del Firewall Cisco PIX que se tiene de respaldo (por fuera del centro de cómputo). Este equipo se tiene configurado y listo para entrar en operación, como guía para las reglas se podrá revisar el backup del Firewall Juniper que se genera periódicamente. Si el equipo está dentro de su periodo de garantía el coordinador realizara simultáneamente la reclamación por garantía ante la firma respectiva. Ver Anexo: listado de los elementos de seguridad Informática en garantía y su respectivo proveedor.
4. Después de tener el equipo operativo y completamente configurado se restauraran las funciones de seguridad interna y perimetral, que estaban operando en este antes de presentarse el evento.
5. Después de restaurado el servicio del equipo se realizaran las respectivas pruebas de operación y se dará de alta al servicio afectado.
6. El grupo de restauración después de recuperar la operación redactara un informe al Coordinador General del Plan de Contingencia sobre el evento y de las actividades realizadas para ser analizadas al interior del comité de seguridad y hacer las correcciones, mejoras y/o actualizaciones que se definan como necesarias.

ALCALDIA MAYOR
DE BOGOTA D.C.
Secretaría
Salud

## DIAGRAMA DEL PROCEDIMIENTO DE RECUPERACION DE SEGURIDAD INFORMATICA



## 7. PRUEBAS Y MANTENIMIENTO DEL PLAN DE CONTINGENCIA DE LA SDS

Para la SDS es necesario definir las pruebas del plan de contingencia, el personal y los recursos necesarios para su realización. Luego se realizan las pruebas pertinentes para intentar valorar el impacto real de un posible evento dentro de los escenarios establecidos como posibles. En caso de que los resultados obtenidos difieran de los esperados, se analiza si la falla proviene de un problema en el ambiente de ejecución, con lo cual la prueba volverá a realizarse una vez solucionados los problemas. Una correcta documentación ayudará a la hora de realizar las pruebas. La capacitación del equipo de contingencia y su participación en pruebas son fundamentales para poner en evidencia posibles carencias del plan.

Antes y después de las pruebas existe una fase de documentación. Esta fase puede implicar un esfuerzo significativo para algunas personas, pero ayudará a comprender otros aspectos del sistema y puede ser primordial para la entidad en caso de ocurrir un desastre. Deben incluirse, detalladamente, los procedimientos que muestren las labores de instalación y recuperación necesarias, procurando que sean entendibles y fáciles de seguir. Es importante tener presente que la documentación del plan de contingencia se debe desarrollar desde el mismo momento que nace, pasando por todas sus etapas y no dejando esta labor de lado, para cuando se concluyan las pruebas y su difusión.

Deben realizarse pruebas para determinar la eficacia del plan de contingencia y de los procedimientos de recuperación ante desastres. Las deficiencias deben resolverse y comprobarse inmediatamente. En un plan de contingencia, el objetivo consiste en ejecutar varias tareas en el menor tiempo posible. Cualquier deficiencia en la documentación, capacitación o, incluso, en los aspectos administrativos, pone en peligro la continuidad del negocio.

La puesta en marcha de los planes a seguir es responsabilidad del Coordinador General del Plan de Contingencia y del encargado de la seguridad, pero también debe existir un compromiso por parte de los usuarios del sistema de información, ejecutivos y todas las personas que de alguna u otra forma ayudan a que el sistema cumpla con los requerimientos para el que fue diseñado, manteniendo sobre todo la integridad y confidencialidad de la información.

La Dirección de Planeación y Sistemas realizara una difusión y mantenimiento**.** Cuando se disponga del plan definitivo ya probado, es necesario hacer su difusión y capacitación entre las personas encargadas de llevarlo a cargo. El

mantenimiento del plan comienza con una revisión del plan existente y se examina en su totalidad realizando los cambios en la información que pudo haber ocasionado una variación en el sistema y realizando los cambios que sean necesarios.

Las primeras pruebas del plan de contingencia de la plataforma de TIC de la SDS, se tienen proyectadas para el mes de noviembre de 2009

### 7.1 RESULTADOS DE LA PRUEBA No 01 DEL 22 DE NOVIEMBRE DE 2009 AL PLAN DE CONTINGENCIA DE LA PLATAFORMA DE TIC´S DE LA SDS

El Plan de Contingencia de la plataforma de TIC de la SDS cumpliendo y en uso de las mejores prácticas tiene contemplado la realización de una serie de pruebas al plan, esto con la intención de garantizar la continuidad de la operación de la entidad y asegurar que todos los miembros de los grupos que intervienen en los procesos de recuperación y otro personal este prevenido y preparado para asumir sus funciones y responsabilidades para cuando el plan sea invocado.

**ACTIVIDADES DESPUÉS DE LA FALLA**

1. **Evaluación de daños:** Al iniciar la prueba el personal encargado del monitoreo de los servicios internos (servidores y aplicaciones), detectan fallas en el funcionamiento de las aplicaciones, al intentar la verificación del estado de las bases de datos de las mismas, ubican la falla grave en el servidor de bases de datos XXXXX el cual al ser verificado se diagnostica como equipos fuera de servicio y con falla grave de hardware de difícil recuperación. Esto implica que las aplicaciones que funciona con estas BD quedan por fuera de operación y un porcentaje del 20 % de los funcionarios que trabajan con estas aplicaciones quedan por fuera de la operación normal de la entidad. Por lo anterior se invoca parcialmente el plan de contingencia con los módulos de recuperación involucrados (Bases de Datos e Infraestructura).
2. **Ejecución de Actividades:** Después de activado parcialmente el plan de contingencia de la plataforma de TIC de la SDS en sus módulos de Bases de Datos e Infraestructura, los miembros inician con los procedimientos de recuperación y con la utilización de los recursos de hardware con que se disponen para el plan de contingencia.

a. El grupo de recuperación de infraestructura realiza la restauración de la imagen del servidor afectado en otro servidor disponible, durante la ejecución del procedimiento de recuperación se estaban tomando los tiempos efectivos.
b. Se realiza la restauración de las bases de datos afectadas, durante la ejecución del procedimiento de recuperación se estaban tomando los tiempos efectivos.
c. Después de tener la maquina con la imagen y las y las BD restauradas con referentes del servicio realizan las pruebas de verificación de los servicio y se restablece totalmente el servicio.

3. **Evaluación de Resultados:** Una vez concluidas las labores de recuperación en los módulos afectados (Bases de datos e Infraestructura) y habiendo recuperado la operación se realizó la evaluación objetiva de todas las actividades realizadas.
    a. Las actividades descritas en los procedimientos después de activado el plan de contingencia de la plataforma de TIC de la SDS, se desarrollaron de buena manera por los miembros de los grupos de recuperación, y fueron efectivas, los miembros sabían que debían hacer y cuál era el objeto de su función dentro del grupo, desde la ubicación de la máquina de respaldo, la restauración de la imagen y la recuperación de las BD hasta las pruebas de recuperación de la operación.
    b. Durante los procedimientos del plan de recuperación de los módulos afectados (Bases de datos e Infraestructura), se realizaron mediciones de los tiempos en cada una de las etapas, Al inicio del proceso de restablecimiento de la imagen del servidor afectado en el servidor disponible, se observó que el tiempo estimado para la restauración era demasiado alto (Aprox. 6 horas), por lo que se evaluó y determino que se podría mejorar configurando con QoS los puertos del Switches que intervenían en el proceso, se configuraron los puertos y el tempo estimado fue de 24 minutos y el tiempo efectivo de recuperación de la imagen fue de 18 minutos. Por lo que se concluye que se debe tener en cuenta para el procedimiento de recuperación de la imagen de los servidores la configuración de los equipos networking. El proceso de restauración de las bases de datos se realiza satisfactoriamente con tiempo efectivo de 40 minutos ya

que las cintas con las copias de respaldo se encontraban en la VTL. Después de recuperada la máquina y las BD los referentes del servicio realizaron las verificaciones de la operación del servicio en 15 minutos y se dios por recuperada la operación.

c. En términos generales la prueba del plan de contingencia de la plataforma de TIC de la SDS fue satisfactoria, los miembros de los grupos de recuperación reaccionaron y procedieron objetivamente y la operación del servicio se restableció en un tiempo total de una hora (1) quince minutos (15), que es bastante bueno teniendo en cuenta la infraestructura afectada.

4. **Retroalimentación del plan de Acción:** Con la evaluación de los presentes resultados se pretende optimizar los procedimientos de recuperación de cada uno de los módulos de recuperación definidos para la entidad, esto para mejorar las actividades que presentaron algún tipo de dificultad, (como la configuración de los puertos en los equipos activos que intervienen asignado QoS a los puertos y la ubicación de los equipos disponibles o de stock para el plan de contingencia) y reforzar los procedimientos que funcionaron correctamente (Bases de datos e Infraestructura).

## 7.2 RESULTADOS DE LA PRUEBA No 02 DEL 23 DE DICIEMBRE DE 2009 AL PLAN DE CONTINGENCIA DE LA PLATAFORMA DE TIC´S DE LA SDS

El Plan de Contingencia de la plataforma de TIC de la SDS cumpliendo y en uso de las mejores prácticas tiene contemplado la realización de una serie de pruebas al plan, esto con la intención de garantizar la continuidad de la operación de la entidad y asegurar que todos los miembros de los grupos que intervienen en los procesos de recuperación y otro personal este prevenido y preparado para asumir sus funciones y responsabilidades para cuando el plan sea invocado.

Esta la segunda prueba del plan de contingencia se aplicó para que se ejecutara este de manera parcial involucrando varios módulos de recuperación y haciendo uso de los recursos que se destinaron para este fin. Sin previo aviso se apagó y se desconectó el servidor XXXXXX en donde se soporta la página Web de la entidad y por donde se accede a la mayoría de las aplicaciones publicadas hacia la nube, esto implica que la mayoría de nuestros clientes externos serian afectados. El servidor se

apagó y se desconectó de la red dejándolo totalmente inoperante simulando un daño total del equipo forzando el inicio del procedimiento de recuperación total de la máquina.

**ACTIVIDADES DESPUÉS DE LA FALLA**

1. **Evaluación de daños:** El personal de la firma proveedora de servicios de Backoffice detectan la caída del servidor XXXXX, el cual al ser verificado se diagnostica con falla grave de hardware y con un tiempo de recuperación muy alto. Esto implica que las aplicaciones que funciona con los link de la página de la entidad quedan por fuera de operación mas todos los demás servicios que se prestan desde el website. Por lo anterior se invoca parcialmente el plan de contingencia con los módulos de recuperación involucrados (Infraestructura y Aplicaciones).
2. **Ejecución de Actividades:** Después evaluar los daños y determinar que el servidor quedo fuera de operación y con daño grave de hardware, se activa parcialmente el plan de contingencia de la plataforma de TIC de la SDS en sus módulos de Infraestructura y Aplicaciones, los miembros de estos grupos inician los procedimientos de recuperación con la utilización de los recursos de hardware y software con que se dispone para el plan de contingencia.
   a. El grupo de recuperación de infraestructura realiza el alistamiento del servidor de stock conectándolo y dejándolo listo para el procedimiento de recuperación en el centro de cómputo.
   b. Inmediatamente se procede a la restauración de la imagen del servidor afectado XXXXXX (backup o imagen generada previamente según esquema de copias de respaldo de imágenes) en el servidor disponible haciendo una réplica idéntica del original con sus unidades C: D: y F: durante la ejecución del procedimiento de recuperación se estuvieron tomando tiempos efectivos por procedimiento.
   c. Después de tener la maquina con la imagen restaurada y como se trata de una maquina con diferentes características a la original (marca, modelo, performance, etc.), se realiza una verificación del sistema operativo, la correcta aplicación de los diferentes drivers para sus componentes y la configuración de red para posteriormente verificar el funcionamiento de los servicios que en este se soportan.
   d. Después de la verificación de todas las variables para la normal operación del servidor se realizan pruebas de la página de la

extranet institucional y se da por recuperado la maquina y todos sus servicios después de un tiempo efectivo de 90 minutos desde la falla del servidor.

3. **Evaluación de Resultados:** Una vez concluidas las labores de recuperación en los módulos afectados (Infraestructura y aplicaciones) y habiendo recuperado la operación se realizo la evaluación objetiva de todas las actividades realizadas.
   a. Las actividades descritas en los procedimientos después de activado el plan de contingencia de la plataforma de TIC de la SDS, se desarrollaron de buena manera. En el procedimiento de restauración de la imagen del servidor se detecto la falta de permisos sobre esa carpeta de los usuarios de infraestructura que deben acceder por la red a las imágenes de los diferentes servidores, esto implico que al momento de intentar conectarse con la unidad donde se almacenan las imágenes se generara un error de acceso, se corrigió este detalle asignando permisos a los diferentes miembros de los grupos de recuperación sobre esta carpeta.
   b. Durante los procedimientos del plan de recuperación de los módulos afectados (Infraestructura y Aplicaciones), se realizaron mediciones de los tiempos en cada una de las etapas. Inicio del procedimiento de recuperación 09:30 AM. Inicio restauración imagen 09:44. Fin de la restauración de la imagen 10:38 AM. Inicio pruebas y puesta a punto de la maquina restaurada 10:45, finalizando a las 10:58. Recuperación de la operación normal 11:00 AM.
   c. En términos generales la prueba del plan de contingencia de la plataforma de TIC de la SDS fue satisfactoria, los miembros de los grupos de recuperación reaccionaron y procedieron objetivamente y la operación del servicio se restableció en un tiempo total de 90 minutos (una hora y 30 minutos), tiempos y resultados que se pueden catalogar como óptimos.
4. **Retroalimentación del plan de Acción:** Con la evaluación de los presentes resultados se pretende optimizar los procedimientos de recuperación de cada uno de los módulos de recuperación definidos para la entidad, esto para mejorar las actividades que presentaron algún tipo de dificultad, como el acceso por la red a las imágenes de los servidores de la SDS.