CAPÍTULO 5
Propuesta de implementación, caso práctico

5.1. Obtención de información de los activos y la infraestructura

La Dirección General del Colegio de Ciencias y Humanidades es la entidad encarga de dirigir correctamente los procesos educativos, académicos, administrativos y técnicos de los 5 planteles de nivel bachillerato, como entidad central de control se maneja una variedad de activos que deberá ser protegida, este capítulo se centra en el análisis de riesgo de la institución, enfocado en los procesos electrónicos y servicios que brinda la institución. La Dirección General del Colegio de Ciencias y Humanidades contemplan el siguiente organigrama, para desempeñar sus funciones (figura 5.1).

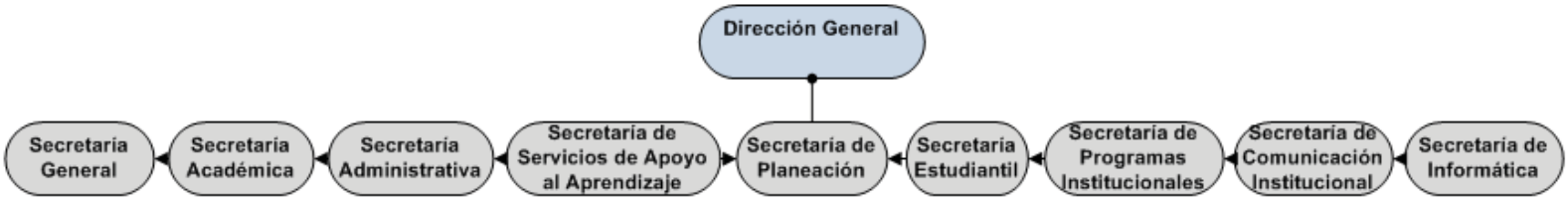

Figura 5. 1 Organigrama Dirección General Colegio de Ciencias y Humanidades.

Una de las Secretarías que conforman el organigrama es la Secretaría de Informática, encargada entre algunas de sus actividades de:

- Evaluar y establecer políticas generales del Colegio de Ciencias y Humanidades en materia de cómputo y telecomunicaciones que apoyen a la Dirección General y a los 5 planteles del colegio, para una toma de decisiones que repercutan en el mejor aprovechamiento de la infraestructura actual.
- Supervisar el uso adecuado de los equipos y redes de cómputo, así como los programas que usan en el colegio.
- Establecer los procesos de capacitación necesarios para el óptimo aprovechamiento de la infraestructura de cómputo y telecomunicaciones.

Estos puntos mencionados, son parte de las actividades que realiza la Secretaría de Informática, tareas relacionadas con este trabajo, que como objetivo plantea "La implementación de un esquema de seguridad perimetral", por lo que la administración, aprobación y mejoras en procesos serán evaluados por la Secretaría de informática.

La fase de la recopilación de información se llevó a cabo empleando:

- Entrevistas y cuestionarios a los responsables de la administración de telecomunicaciones, servidores y sistemas.
- Cuestionarios a los usuarios finales.
- Visitas a sites.
- Recorrido por las instalaciones de la organización.
- Escaneos del segmento de red.

Todo el proceso de identificación de información cae dentro de uno de los pasos de análisis de riesgos, para este caso, el análisis de riesgos está basado en los documentos emitidos por el NIST 800-30 y 800-53, debido a que se utilizan otros documentos de la misma serie SP 800, dedicada a la seguridad de la información y que presenta los mismos beneficios de emplear el análisis de riesgos con base en alguna otra metodología como BS 7799 parte 3, MARGERIT, OCTAVE, COBIT, ISO 27005, entre otros. A continuación se muestra el diagrama del análisis de riesgos basado en la metodología recomendada por NIST 800-30 (figura 5.2).

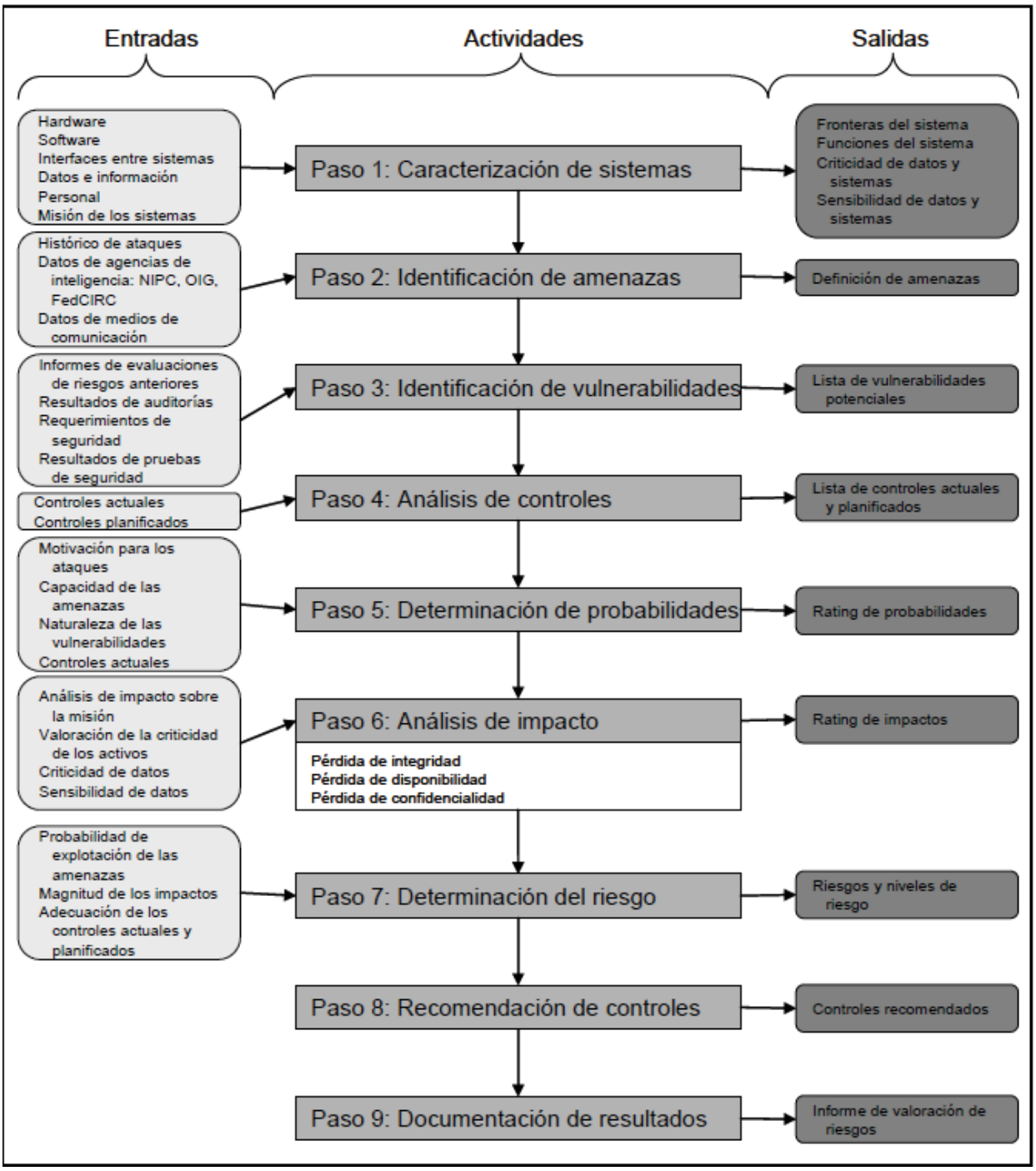

Figura 5. 2 Análisis de Riesgos NIST 800-30.

El análisis de riesgo se centrará en servidores, instalaciones, sistemas y equipos de telecomunicaciones, ya que los controles que se implementarán para gestionar los riesgos serán administrados por la Secretaría de Informática, en caso de que se detecten vulnerabilidades que no puedan ser gestionados por la Secretaría mencionada, sólo se realizará la recomendación pertinente. La obtención de información es uno de los procesos más largos que se realiza al momento de tratar una implementación de seguridad, debido a que muestra el total de activos físicos a proteger. Durante una primera etapa se buscó información a través de documentos, herramientas de escaneo, cuestionarios, entrevistas en sitio a los responsables de servidores e infraestructura por parte de la Secretaría de Informática, solicitando el acceso a la siguiente lista de documentos, políticas y guías de configuración, lo cual corresponde a la documentación técnica de la institución (tabla 5.1).

Tabla 5. 1 Lista de documentos solicitados para revisión .

Documento	Encontrado	Parcialmente	No encontrado
Relación de responsables de activos (Hardware)	X		
Inventario de software utilizado y relación de licencias			X
Inventario de equipos de cómputo	X		
Inventario de la asignación de direcciones IP		X	
Relación de servidores y responsables		X	
Respaldos de servidores			X
Memorias técnicas de la configuración de los servidores			X
Memorias técnicas de la configuración de equipos activos			X
Respaldo de la configuración de equipos activos			X
Informe de seguridad de TI			X
Diagramas de red		X	
Control de modificaciones en configuraciones			X
Memorias técnicas de los sites			X
DRP			X
Guías de hardening para servidores			X
Memorias técnicas de aplicaciones			X
Análisis de riesgo			X
Políticas de instalación para equipos portátiles, servidores y estaciones de trabajo			X
Políticas de monitoreo			X
Políticas de uso de red			X
Política de respaldo			X
Memorias técnicas de cableado estructurado		X	

Es importante aclarar que la lista anterior fueron los puntos solicitados a los responsables, en algunos casos no existe documento que contenga los datos, por lo tanto se contemplan como recomendaciones la elaboración de los mismos, los cuales se justifica su elaboración, con base en el análisis de riesgos.

Continuando con el inventario de activos se listan los componentes que forman parte de la infraestructura tecnológica de la organización (tabla 5.2).

Tabla 5. 2 Resumen de infraestructura.

Activos informáticos	Tipo	Cantidad
Servidores físicos (Hardware)	Servicio	14
Servidores físicos (Software)	Servicio	6
Servidores virtuales (ESX)	Servicio	7
Máquinas virtuales (software)	Servicio	12
Dominios	Servicio	12
Nodos de red	Servicio	270 aproximadamente en uso
Antena WiBox estacionamiento	Servicio	1
Equipos Windows XP	Servicio	171
Equipos Windows vista	Servicio	140
Equipos Windows 7	Servicio	15
Equipos de cómputo UNIX	Servicio	16
Portátiles	Servicio	23
Router	Comunicaciones	2
Switch	Comunicaciones	8
Puntos de acceso	Comunicaciones	3
Cámaras vigilancia IP	Comunicaciones	0
Firewall	Comunicaciones	0
Printserver	Comunicaciones	6
IDS	Comunicaciones	0
Sensores de red	Comunicaciones	1
UPS	Comunicaciones	1
Reguladores	Comunicaciones	40
Sites	Comunicaciones	3
Closet	Comunicaciones	2
Servidores NAT	Comunicaciones	2
Segmentos de red	Comunicaciones	3
Aire acondicionado en sites	Comunicaciones	3
Página web de la institución	Servicio interno y externo	1
Servidores Web otros	Servicio interno y externo	6
Servidores de correo	Servicio interno y externo	1
Antivirus de servidor correo	Servicio interno y externo	1
Antispam en servidor de correo	Servicio interno y externo	1
Servidores de bases de datos	Servicio interno y externo	9
Servidores hotspot	Servicio interno	0
Conexiones a internet	Servicio externo	1
Servidores NAS/SAN	Servicio interno	2
VPN hacia la red interna	Comunicaciones	0
VPN hacia otras entidades	Comunicaciones	2
Servidores de terceros para procesos de la organización.	Servicio externo	1
Cámaras de vigilancia	Monitoreo	8
Personal de seguridad	Vigilancia perimetral	6
Cifrado en medios de almacenamiento	Equipos personales críticos	0
Recursos humanos	Personal	15

De todo el hardware mencionado en la tabla anterior, algunos tienen mayor importancia para la actividad de la institución, los equipos que forman parte de esta categoría se mencionan en la tabla 5.3.

Tabla 5. 3 Relación de equipos críticos para la institución.

Activo	Ubicación	Memoria Técnica
Sw Core FastIron SuperX P 108E-36FO	Site Telecomunicaciones	NO
Sw ServerIron XL P 16E +2FO	Site Servidores	NO
Sw FastIron Edge X424 P 24E + 4FO	Site Servidores	NO
Router Cisco 2800 series P 6E	Site telecomunicaciones	NO
3com 3C16470 P 16E	Soporte	NO APLICA
3com 3C16471 P 24E	Secretaría Administrativa	NO APLICA
Allied AT-8000S P 24E	Closet Salas	NO
Allied AT-8000S P 24E	Control de publicaciones	NO
3com switch 2250 Plus P 50E	Secretaría General	NO
3com 4400 3C172204 P 50E	Medios Digitales	NO
Punto de Acceso Belair	Pasillo Principal	NO
Intel SR2400 Firewall	Site Servidores	NO
Dell PowerEdge 1950 Servidor ESX	Site servidores	NO
Dell PowerEdge 1950 Servidor ESX	Site Servidores	NO
EMC AX150	Site servidores	NO
Silkworm E_200	Site servidores	NO
Dell PowerEdge 1950 centOS vServer	Site servidores	NO
PinetiOn Centro de video vigilancia	Site Telecomunicaciones	----------
IBM System x3550 Servidor Correo	Site Servidores	NO
IBM System x3550 ESX Prueba	Site Servidores	NO
IBM System x3550 Servidor ESX	Site Servidores	NO
Dell PowerEdge 1950 ESX 4	Site Servidores	NO
Dell PowerEdge 1950 ESX 4	Site Servidores	NO
Antena WiBox	Estacionamiento	NO
HP- CPU Cacti	Site Servidores	NO
HP - Pavilion A6100a	Site servidores	NO
HP dx2400	Control presupuestal	NO
HP Proliant ML370	Secretaría General	NO
Aire acondicionado	Site telecomunicaciones	NO APLICA
Aire acondicionado	Site servidores	NO APLICA
Aire acondicionado	Site servidores	NO APLICA
UPS Tripp lite SU6000RT4U 4200W	Site servidores	NO APLICA
UPS ISB 800	Site telecomunicaciones	NO APLICA
UPS Tripp lite omni900lcd 475W	Secretaría de Planeación	NO APLICA

Realizando un análisis de costos en la infraestructura principal de red y servidores, se tiene una inversión en hardware de $2,209,785.69, sin contemplar el costo que representa la información contenida en los diferentes equipos, información que representa la razón de ser de la institución (tabla 5.4).

Tabla 5. 4 Relación de costos de infraestructura crítica.

Equipo	Características	Costo
SERVIDOR	HP PROLIANT	51,173.85
SERVIDOR	INTEL	65,866.84
SERVIDOR	IBM 41U	86,250.00
SERVIDOR	IBM 41U	86,250.00
SERVIDOR	IBM 41U	86,250.00
SERVIDOR	IBM 41U	86,250.00
SERVIDOR	DELL	96,195.00
SERVIDOR	DELL	96,194.99
SERVIDOR	DELL	96,195.00
SERVIDOR	DELL	96,195.00
SERVIDOR	DELL	96,195.00
SERVIDOR	DELL	96,195.00
STORAGE	EMC2	253,000.00
SWITCH	SILKWORM	74,951.01
SWITCH	3COM	7,348.50
SWITCH	3COM	7,348.50
SWITCH	ALLIED	7,348.50
SWITCH	ALLIED	7,348.50
SWITCH	FOUNDRY,FESX424	54,339.80
SWITCH	FOUNDRY,FCSLB16	113,999.99
SWITCH	3COM	10,062.50
SWITCH	FOUNDRY F1-8X1	465,000.00
ROUTER	CISCO 2821	40,825.00
ROUTER	CISCO 2821	40,825.00
ROUTER	CISCO 2801	40,825.00
PUNTO DE ACCESO	BELAIR	52,750.00
UPS	TRIPP LITE	46,000.00
ACONDICIONADOR DE AIRE	CARRIER	16,617.50
ACONDICIONADOR DE AIRE	MITSUBISHI	22,655.00
ACONDICIONADOR DE AIRE	MITSUBISHI	22,655.00
KVM	17FP	5,480.00

La siguiente relación muestra el total de activos lógicos importantes para la institución, administrados por 9 personas, esta tarea contemplando todos los servicios brindados hacia la comunidad, que incluyen servicio web, bases de datos, correo, sensores de red y servidores virtuales, con un total de 31 servicios (tabla 5.5).

Tabla 5. 5 Servicios críticos para la institución.

Servicio	URL
1) Registros Intra CCH	academia.cch.unam.mx/intracch
2) Página web institucional	www.cch.unam.mx
3) Correo institucional	correo.cch.unam.mx
4) Web moodle academia	academia.cch.unam.mx
5) Web moodle Inglés	idiomas.portalacademico.cch.unam.mx/moodle/login/index.php
6) Web moodle Portal Académico	portalacademico.cch.unam.mx
7) Web formación de profesores	132.248.122.4/tacur/
8) Web Control de datos personal Académico	dcdpa.cch.unam.mx
9) Web programa de seguimiento integral	psi.cch.unam.mx
10) Web página Secretaría de Planeación	seplan.cch.unam.mx
11) VMware ESX server 4.0	----------
12) VMWare ESX server 4.0	----------
13) VMware ESX server 4.0	----------
14) VMware ESX server 4.0	----------
15) VMware ESX server 4.0	----------
16) Router Cisco	----------
17) AccessCar	----------
18) ViCenter - Vmware	----------
19) VMware vServer	----------
20) Base de datos portal académico	portalacademico.cch.unam.mx
21) Base de datos PSI	psi.cch.unam.mx
22) Base de datos intraCCH	academia.cch.unam.mx/intracch
23) Base de datos spac-e	spac-e.cch.unam.mx
24) Base de datos portal DGCCH	www.cch.unam.mx
25) Base de datos academia en línea	academia.cch.unam.mx
26) Base de datos DCDPA	dcdpa.cch.unam.mx
27) Base de datos AccessCar	----------
28) Base de datos control presupuestal	----------
29) Base de datos planeación	seplan.cch.unam.mx
30) Enlace internet Red UNAM	----------
31) Cacti - monitor de red	----------
32) Servidor web Secretaría de Planeación	seplan.cch.unam.mx
33) Servidor web spac-e	----------

Cuando se evaluó el estado de la red, contemplando su distribución física, se observó que no existía ningún dispositivo de seguridad implementado, a continuación se muestra el diagrama de red, que se tenía en la institución antes de la implementación del esquema de seguridad propuesto (figura 5.3).

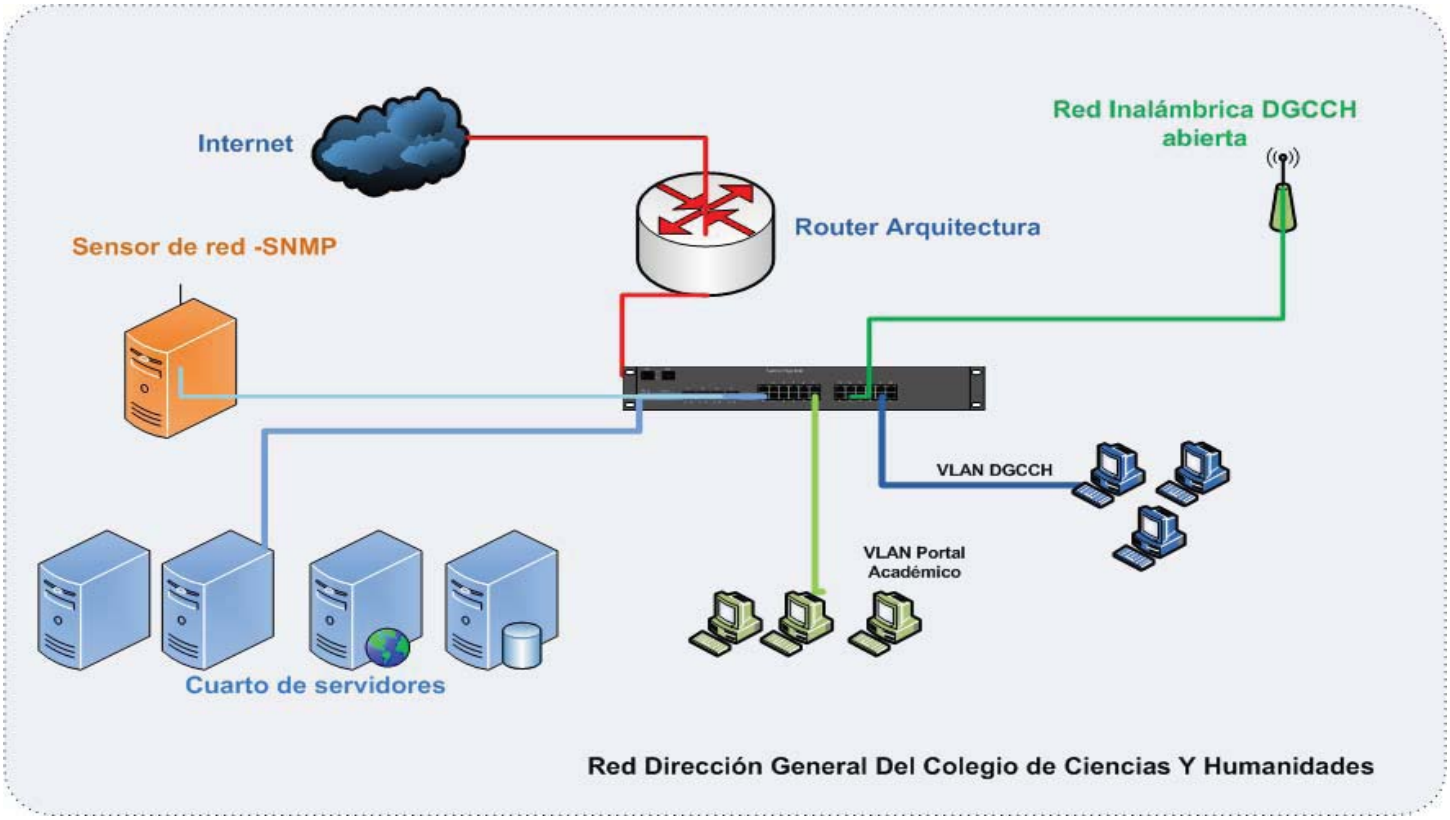

Figura 5. 3 Diagrama de red, antes de la implementación del esquema de seguridad.

Para la mayoría de los servidores y dispositivos activos se planea la elaboración de memorias técnicas, documentos que ayudarán a identificar configuraciones actuales, puertos abiertos, distribución de sistema operativo, características de hardware, conexión física y protocolos que emplean para su administración.

5.2. Análisis de riesgo de la situación actual

La información recabada como parte del análisis de riesgos fue útil para determinar la relación de las posibles amenazas a las que están expuestos los activos, desde los niveles directivos hasta los niveles técnicos. Con base en los activos reportados anteriormente e históricos de actividades arrojados en las entrevistas, escaneo de puertos, se determinaron las amenazas, definidas en el Paso 2 "Identificación de amenazas", que en conjunto con los resultados de prueba de seguridad y entrevistas en sitio, se encontraron las vulnerabilidades definidas en el Paso 3 definido en NIST 800-30, "Identificación de vulnerabilidades" (tabla 5.6).

Tabla 5. 6 Identificación de vulnerabilidades.

Amenaza	Vulnerabilidad
▪ Usuarios internos ▪ Usuarios malintencionados ▪ Usuarios poco capacitados ▪ Usuarios deshonestos ▪ Usuarios negligentes	1. Inexistencia o falta de : • Identificación con credencial del personal que ingresa a la institución. • Controles de acceso físicos a oficinas. • Bitácoras para visitantes en los departamentos. • Controles de acceso a aplicaciones. • Controles de acceso a servidores y equipos activos. • Control de acceso a computadoras. • Control de asignación de direcciones IP's en el segmento de la institución. • Control de tráfico de red. • Control de acceso en la red inalámbrica. • Mecanismos de control perimetral de la red. • Personal que atienda un incidente de seguridad. • Políticas de confidencialidad. • Políticas de uso de la red. • Políticas sobre el manejo de información. • Políticas de seguridad en sistemas operativos. • Políticas de seguridad en servidores. • Políticas de seguridad en dispositivos activos. • Políticas de contraseñas. • Conocimientos de empleados en temas de seguridad. • Actualización de firmware en equipos de red. • Actualizaciones en los sistemas operativos y aplicaciones. • Actualización en antivirus. • Mantenimiento en servidores y equipo de telecomunicación. • Mantenimiento preventivo en equipos de cómputo. • Mantenimiento a equipos de aire acondicionado. • Mantenimiento a estaciones eléctricas. • Corriente eléctrica regulada. • Cifrado en discos duros. • Respaldos de información. • Respaldos de configuración de equipos activos • UPS con capacidad suficiente. • Fuente de corriente eléctrica alterna. • Capacitación. • Separación de funciones de los empleados. • Información en temas de seguridad. • Sites alternos 2. Tableros eléctricos expuestos. 3. Fallas eléctricas. 4. Fallas en equipos de cómputo. 5. Límites de uso de memoria y procesador en servidor. 6. Cableado de red expuesto a los usuarios.

	7. Respaldos en USB sin cifrado. 8. Respaldos en mismo disco duro. 9. Parámetros de configuración por default en equipos activos, servidores y Printserver. 10. Acceso a todas las terminales de administración. 11. Acceso a todos los recursos de red. 12. Acceso total a todos los recursos de Internet. 13. Tiempo de vida útil de un equipo. 14. Uso de la misma contraseña por periodos largos de tiempo. 15. Uso de una contraseña única en varios equipos. 16. Uso de contraseñas no robustas. 17. Uso de protocolos de administración inseguros. 18. Descuidos del personal que labora en la institución. 19. Confianza en otras personas. 20. Uso de IP homologadas para usuarios en general. 21. Fallas por parte del proveedor del servicio de internet. 22. Fallas por parte del proveedor suministro eléctrico.
Usuarios externos ▪ Delincuencia ▪ Hacker ▪ Crackers ▪ Ex empleados ▪ Otras instituciones ▪ Etcétera.	1) Falta de : • Identificación con credencial del personal que ingresa a la institución. • Controles de acceso físicos a oficinas. • Bitácoras para visitantes en los departamentos. • Controles de acceso a aplicaciones. • Controles de acceso a servidores y equipos activos. • Control de acceso a computadoras. • Control de asignación de direcciones IP's en el segmento de la institución. • Control de tráfico de red. • Control de acceso en la red inalámbrica. • Mecanismos de control perimetral de la red. • Personal que atienda un incidente de seguridad. • Políticas de confidencialidad. • Políticas de uso de la red. • Políticas sobre el manejo de información. • Políticas de seguridad en sistemas operativos. • Políticas de seguridad en servidores. • Políticas de seguridad en dispositivos activos. • Políticas de contraseñas. • Conocimientos de empleados en temas de seguridad. • Actualización de firmware en equipos de red. • Actualizaciones en los sistemas operativos y aplicaciones. • Actualización en antivirus. • Mantenimiento en servidores y equipo de telecomunicación. • Mantenimiento preventivo en equipos de cómputo. • Mantenimiento a estaciones eléctricas. • Corriente eléctrica regulada.

	• Cifrado en discos duros. • Respaldos de información. • Respaldos de configuración de equipos activos • UPS con capacidad suficiente. • Fuente de corriente eléctrica alterna. • Capacitación. • Información en temas de seguridad. • Separación de funciones de los empleados. • Sites alternos 2) Tableros eléctricos expuestos. 3) Limites de uso de memoria y procesador en servidor. 4) Cableado de red expuesto a los usuarios. 5) Respaldos en USB sin cifrado. 6) Respaldos en mismo disco duro. 7) Parámetros de configuración por default en equipos activos, servidores y Printserver. 8) Acceso a todas las terminales de administración. 9) Acceso a todos los recursos de red. 10) Acceso total a todos los recursos de Internet. 11) Uso de la misma contraseña por periodos largos de tiempo. 12) Uso de una contraseña única en varios equipos. 13) Uso de contraseñas no robustas. 14) Uso de protocolos de administración inseguros. 15) Descuidos del personal que labora en la institución. 16) Confianza en otras personas. 17) Uso de IP homologadas para usuarios en general. 18) Fallas por parte del proveedor del servicio de internet. 19) Fallas por parte del proveedor suministro eléctrico.
Desastres Naturales	1) Falta de: • Planeación relacionada con la infraestructura de la organización. • Impermeabilizado. • Tuberías aisladas. • Mantenimiento en cableado eléctrico. • Controles de humedad. • Controles de temperatura. 2) Fallas en diseño construcción de los Sites. 3) Tableros eléctricos expuestos. 4) Instalación de red expuesta. 5) Equipos de telecomunicaciones expuestos.
Amenazas Lógicas ▪ Virus ▪ Gusanos ▪ Troyanos ▪ Botnet ▪ Malware ▪ Spyware	1) Falta de : • Dispositivos de seguridad perimetral. • Actualización en software. • Actualización en sistemas operativos. • Actualización en firmware de dispositivos. • Políticas de confidencialidad. • Políticas de uso de la red.

▪ Etcétera.	• Políticas sobre el manejo de información. • Políticas de seguridad en sistemas operativos. • Políticas de seguridad en servidores Windows /Linux. • Políticas de seguridad en dispositivos activos. • Políticas de contraseñas. • Políticas de desarrollo de software seguro. 2) URL con software malicioso. 3) Descarga de ejecutables desde sitios no confiables. 4) Instalación de software pirata. 5) Instalación de software crackeado. 6) Descarga de software de recursos peer to peer (P2P). 7) Configuración por default. 8) Auto arranque de dispositivos extraíbles en terminales y servidores. 9) Debilidades en los protocolos de comunicación. 10) Errores de configuración de los sistemas. 11) Mecanismos de administración remota vulnerables. 12) Contraseñas basadas en palabras de diccionario. 13) Vulnerabilidades de las versiones empleadas en los servidores. 14) Ataques conocidos a sistemas operativos. 15) Puertos abiertos sin utilización. 16) Falta de conocimiento en temas de seguridad.

A continuación se cita una serie de observaciones críticas, relacionado con la infraestructura actual que se tiene:

- Es importante mencionar que la mayoría de los equipos de telecomunicación, comparten una misma contraseña, no recomendables, ya que debilita la seguridad, además de utilizar protocolos de administración inseguros, lo que en conjunto crea un punto crítico de seguridad.
- Se realizaron escaneos desde el exterior de la red institucional, que mostraron acceso a puertos innecesarios en los servidores críticos de la institución, así como acceso a printserver, switch y router, en si todo aquello que tenga un puerto abierto.
- Algunos de los equipos tienen configuraciones por default, permitiendo tener acceso a la configuración, con solo conocer las cuentas preestablecidas por el fabricante.
- No se cuenta con respaldo de la configuración actual que tienen los equipos activos como switch, router y puntos de acceso.
- Por la fecha de adquisición de los equipos, actualmente ninguno de éstos cuenta con garantía, lo que ocasiona que en el momento de fallas de hardware se pierda disponibilidad en los servicios soportados por el hardware dañado, que en puntos críticos puede ocasionar pérdida de servicio o información.
- La red inalámbrica en funcionamiento, no cuenta con algún mecanismo de autenticación y cifrado, lo que permite a cualquier persona hacer uso de los recursos sin ninguna restricción y seguimiento de sus actividades.
- El cableado de red de la institución no se ha actualizado en varios años, se han improvisado conexiones que se quedaron de manera permanente, se recomienda considerar una instalación de cableado estructurado en todo el edificio, para salvaguardar el acceso físico a los medios de transmisión de datos.

- En cuestión al monitoreo y seguridad, se tiene actualmente sólo un sensor que permite verificar el estado de los dispositivos, no se cuenta con un esquema de seguridad perimetral lo que permite a los atacantes tener acceso a todos los puntos de conexión de la institución, servidores y equipos activos. Se recomienda establecer un esquema de seguridad perimetral que permita monitorear el uso de la red con mayor detalle y establecer políticas de acceso sólo a aquellos recursos que deben estar visibles para los usuarios finales.

- Actualmente el equipo UPS ubicado en el site principal, no soportan la carga de corriente requerida, estando por debajo del 50% del total de consumo actual, el UPS actual tiene un soporte de 4200[W], teniendo un consumo de 13000 [W], lo que ocasiona que en fallas eléctricas no se cuente con la protección eléctrica adecuada.
  - 1 Storage EMC AX-150, con una fuente de 315 VA (300 Watts)
  - 1 Switch de fibra Brocade Silkworm 200e de 45 Watts a 60 Watts
  - 1 Switch Foundry X424 de con una fuente de 220 Watts
  - 1 Switch Foundry ServerIron con una fuente de 550 Watts
  - 5 Servers Dell PowerEdge 1950 con dos fuentes, cada una de 670 Watts (6700 Watts en total)
  - 4 Servers IBM X3550 con dos fuentes, cada una de 670 Watts (5360 Watts en total)
  - 1 Server Intel con una fuente de 550 Watts
  - 1 Switch KVM Dell de 40 Watts
  - 1 Consola de administración Dell, entre los 40 y 50 Watts.

  Total en watts 13.820 KW

- La instalación de los equipos de cómputo de los usuarios finales, se realiza siguiendo un procedimiento específico, que limite al usuario final para sólo tener acceso a ciertos recursos del equipo, dicho procedimiento deberá ser revisado para garantizar su óptimo funcionamiento.

- Cuando se presentan incidentes de seguridad reportados por DGTIC, la solución parcial en atención al incidente, es notificar a soporte para su corrección, el tiempo que soporte tome para resolver el incidente, permanecerá en operación la actividad maliciosa del equipo comprometido.

El siguiente punto considerado en la metodología es paso 4: "*análisis de los controles"*, mostrando una lista de controles con los que se cuenta actualmente y aquellos que se planifican a futuro, para minimizar o eliminar la probabilidad de que una amenaza explote una vulnerabilidad (Ver apéndice D).

Para obtener la *probabilidad de ocurrencia y el análisis de impacto*, paso 5 y 6 respectivamente, se determinaron con base en las entrevistas, revisión de instalaciones, visitas en sitio, cuestionarios realizados y decisiones gerenciales. Con base en los siguientes criterios se determinó la prioridad de atención de los riesgos. Al momento de determinar el impacto, la estimación se realizó del tipo cualitativo, se considero un activo importante con base en el tipo de información que maneja, debido a que tratar de estimar su valor económico es muy complicado y variado, pero el hecho de pérdida de disponibilidad, confidencialidad o integridad del activo afecta significativamente el funcionamiento de la institución (tabla 5.7).

Tabla 5. 7 Matriz de nivel de atención de riesgos.

		Probabilidad/ Likelihood		
		Alto(1.0)	Medio (0.5)	Bajo (0.1)
Impacto Impact	Alto(100)	Alto (100x1)	Medio (100x0.5)	Bajo (100x0.1)
	Medio (50)	Medio (50x1)	Medio (50x0.5)	Bajo (50x0.1)
	Bajo (10)	Medio (10x1)	Bajo (0.16)	Bajo(0.08)

Alto (>50 a 100); Medio (>10 a 50); Bajo (1 a 10)

- ***Alto;*** se requiere fuertemente la necesidad de tomar acciones correctivas.
- ***Medio;*** acciones correctivas son necesarias y un plan debe ser desarrollado para incorporar estas acciones en un periodo de tiempo.
- ***Bajo;*** se observó un bajo riesgo y se deberá determinar si se tomarán acciones correctivas o decidir aceptar el riesgo.

Una vez realizado el levantamiento de activos, amenazas, vulnerabilidades, probabilidad de ocurrencia e impacto, se realiza una evaluación de los riesgos para priorizar los niveles de atención, las opciones de los riesgos son:

- ***Mitigación del riesgo;*** implementando controles que reduzcan la probabilidad de ocurrencia.
- ***Transferir el riesgo;*** con base en el análisis de riesgo contemplar la posibilidad de que algunos controles sean realizados por terceros (outsourcing), en algunas veces reduce costos.
- ***Aceptar el riesgo;*** tener conocimiento de los riesgos a los que se está expuesto, aceptando la posibilidad de que se presenten.
- ***Evitar el riesgo;*** las acciones están orientadas a cambiar las actividades o la manera de desempeñar una actividad en particular
- ***Riesgo residual;*** después de implantar los controles necesarios para el tratamiento de los riesgos, por lo general se encuentran remanentes. Lo que se conoce como riesgo residual.

En la tabla 5.8 se muestra la determinación del riesgo, basado en la matriz de nivel de atención de riesgos (tabla 5.7), la cual muestra la probabilidad de explotación de las vulnerabilidades por parte de las diversas amenazas.

Tabla 5. 8 Probabilidad de impacto y ocurrencia.

Vulnerabilidad	Probabilidad de ocurrencia	Impacto	Principio de seguridad afectado	Nivel de atención del Riesgo
Red inalámbrica abierta	Alta	Alto	Confidencialidad	**Alto**
Inexistencia de controles sobre el uso de la red inalámbrica	Alta	Alto	Disponibilidad	**Alto**
Poco control en la administración de direcciones IP	Alta	Alto	Disponibilidad	**Alto**
Inexistencia de control en la información descargada a través de la red de la institución	Alta	Alto	Integridad	**Alto**

Vulnerabilidad	Probabilidad de ocurrencia	Impacto	Principio de seguridad afectado	Nivel de atención del Riesgo
Falta de cuidado del equipo de cómputo	Alta	Alto	Disponibilidad	**Alto**
Limitantes de potencia en UPS	Alta	Alto	Disponibilidad	**Alto**
Falta de mecanismos de control perimetral de la red	Alta	Alto	CIA	**Alto**
Uso de protocolos de administración inseguros	Alta	Alto	CIA	**Alto**
Inexistencia de políticas de uso de red	Alta	Alto	CIA	**Alto**
Inexistencia de políticas para servidores	Alta	Alto	CIA	**Alto**
Inexistencia de respaldos en equipos activos	Alta	Alto	Integridad	**Alto**
Acceso a todos los recursos de red institucional	Alta	Alto	CIA	**Alto**
Uso de una misma contraseña por periodos largos de tiempo	Alta	Alto	CIA	**Alto**
Uso de una contraseña única en varios equipos	Alta	Alto	CIA	**Alto**
Uso de contraseñas no robustas	Alta	Alto	CIA	**Alto**
Confianza en otras personas	Alta	Alto	Confidencialidad	**Alto**
Uso de IP's homologadas para usuarios en general	Alta	Alto	Confidencialidad	**Alto**
Fallas por parte del proveedor del suministro eléctrico	Alta	Alto	Disponibilidad	**Alto**
Puertos abiertos sin uso en estación de trabajo	Alta	Alto	CIA	**Alto**
Inexistencia de respaldos en las diferentes Secretarías	Media	Alto	Confidencialidad	**Medio**
Tableros eléctricos expuestos	Alta	Medio	Disponibilidad	**Medio**
Controles de acceso inseguros para administración de servidores	Media	Alto	Integridad	**Medio**
Vulnerabilidades inherentes del protocolo TCP/IP	Media	Alto	Confidencialidad	**Medio**
Daño en hardware por fallas eléctricas	Media	Alto	Disponibilidad	**Medio**
Inexistencia de control en el tráfico de red generado por la institución	Alta	Medio	Disponibilidad	**Medio**
Fuga de información	Media	Mediano	Confidencialidad	**Medio**
Daño físico a la infraestructura de red	Media	Alto	Disponibilidad	**Medio**
Puertos abiertos sin motivo en servidores críticos	Media	Alto	Confidencialidad	**Medio**
Inexistencia de controles de seguridad en portátiles	Alta	Medio	Confidencialidad	**Medio**
Inexistencia de monitoreo de uso de la red	Alta	Medio	Disponibilidad	**Medio**
Fallas en sistemas de aire acondicionado	Media	Alto	Disponibilidad	**Medio**
Control de acceso débil en aplicaciones	Media	Alto	Confidencialidad	**Medio**
Personal poco capacitado en temas de seguridad	Media	Alto	CIA	**Medio**
Inexistencia de actualizaciones en terminales de trabajo, servidores, antivirus y equipos de red	Media	Alto	CIA	**Medio**
Falta de mantenimiento preventivo en servidores y equipos activos	Alta	Medio	Disponibilidad	**Medio**
Falta de mantenimiento de estaciones eléctricas	Media	Alto	Disponibilidad	**Medio**
Falta de corriente eléctrica regulada	Alta	Medio	Disponibilidad	**Medio**
Inexistencia de fuente de corriente eléctrica alterna	Alta	Medio	Disponibilidad	**Medio**

Vulnerabilidad	Probabilidad de ocurrencia	Impacto	Principio de seguridad afectado	Nivel de atención del Riesgo
Inexistencia de planes de capacitación	Alta	Medio	CIA	**Medio**
Inexistencia de Sites alternos	Alta	Medio	Disponibilidad	**Medio**
Cableado de red expuesto	Alta	Medio	Disponibilidad	**Medio**
Respaldos en mismo disco duro	Alta	Medio	Disponibilidad	**Medio**
Parámetros por default en equipos activos	Media	Alto	CIA	**Medio**
Acceso a todas las terminales de administración	Media	Alto	Integridad	**Medio**
Acceso a todos los recursos de internet	Alta	Medio	CIA	**Medio**
Uso de protocolos de comunicación inseguros	Media	Alto	CIA	**Medio**
Falta de mantenimiento en cableado eléctrico	Media	Alto	Disponibilidad	**Medio**
Inexistencia de controles de humedad	Alta	Medio	Disponibilidad	**Medio**
Inexistencia de controles de temperatura	Alta	Medio	Disponibilidad	**Medio**
Consultas de sitios con software malicioso	Alta	Medio	CIA	**Medio**
Descarga de ejecutables de sitios no confiables	Alta	Medio	CIA	**Medio**
Inexistencia de políticas sobre el uso del equipo de cómputo	Alta	Medio	CIA	**Medio**
Autoarranque de dispositivos extraíbles	Alta	Medio	CIA	**Medio**
Falta de políticas de desarrollo de software seguro	Alta	Medio	CIA	**Medio**
Inexistencia de controles de integridad en equipos activos	Alta	Medio	Integridad	**Medio**
Firmas antivirus deficientes	Media	Medio	Confidencialidad	**Medio**
Inexistencia de políticas de uso de software	Media	Medio	Disponibilidad	**Medio**
Poco control sobre los respaldos	Media	Medio	Confidencialidad	**Medio**
Filtrado de agua a sites	Media	Medio	Disponibilidad	**Medio**
Inexistencia de controles sobre el uso de procesador, memoria, disco duro y ancho de banda	Media	Medio	Disponibilidad	**Medio**
Falta de procedimientos de creación de cuentas	Media	Medio	Disponibilidad	**Medio**
Vulnerabilidades inherentes a las aplicaciones	Media	Medio	Disponibilidad	**Medio**
Tiempo de vida útil de los equipos	Media	Medio	Disponibilidad	**Medio**
Tuberías expuestas	Media	Medio	Disponibilidad	**Medio**
Uso de versiones viejas en aplicaciones	Media	Medio	CIA	**Medio**
Vulnerabilidades conocidas en sistemas operativos	Media	Medio	CIA	**Medio**
Empleo de software sin actualizaciones	Media	Medio	CIA	**Medio**
Inexistencia de auditorías	Alta	Bajo	CIA	**Bajo**
Limitantes de espacio en disco duro en servidores	Baja	Alto	Disponibilidad	**Bajo**
Fallas eléctricas	Baja	Alto	Disponibilidad	**Bajo**
Inexistencia de cultura de seguridad en usuarios finales	Baja	Alto	Integridad	**Bajo**
Inexistencia de control perimetral de los puertos permitidos	Alta	Bajo	Disponibilidad	**Bajo**
Inexistencia de procedimientos de cambios en sistemas	Alta	Bajo	Integridad	**Bajo**
Inexistencia de políticas en sistemas operativos	Alta	Bajo	CIA	**Bajo**

Vulnerabilidad	Probabilidad de ocurrencia	Impacto	Principio de seguridad afectado	Nivel de atención del Riesgo
Inexistencia de cifrado en discos duros	Alta	Bajo	Confidencialidad	**Bajo**
Poca separación de funciones criticas	Baja	Alto	CIA	**Bajo**
USB sin cifrado	Alta	Bajo	Confidencialidad	**Bajo**
Fallas por parte del proveedor de servicios de internet	Baja	Alto	Disponibilidad	**Bajo**
Daños en la configuración de los equipos por poco mantenimiento	Baja	Medio	Integridad	**Bajo**
Descuido en el manejo del hardware	Baja	Medio	Disponibilidad	**Bajo**
Errores de cambios en la configuración de equipos activos y servidores	Baja	Medio	Integridad	**Bajo**
Inexistencia de control a servicios de servidores	Media	Bajo	Confidencialidad	**Bajo**
Inexistencia de políticas de confidencialidad	Baja	Medio	Confidencialidad	**Bajo**
Inexistencia de monitoreo de las aplicaciones	Baja	Medio	Disponibilidad	**Bajo**
Poca educación sobre temas de seguridad a usuarios finales	Baja	Medio	Integridad	**Bajo**
Errores humanos	Baja	Medio	Disponibilidad	**Bajo**
Aprovechamiento de vulnerabilidades de controles físicos	Baja	Medio	Disponibilidad	**Bajo**
Falta de gestión de garantías	Baja	Medio	Disponibilidad	**Bajo**
Interferencias magnéticas	Baja	Bajo	Disponibilidad	**Bajo**
Desastres naturales en la institución	Baja	Bajo	Disponibilidad	**Bajo**

5.3. Alcance y requerimientos de la propuesta

Los controles que pueden mitigar o eliminar los riesgos identificados son señalados para su implementación o planeación, el objetivo de la recomendación de los siguientes controles es reducir el nivel de riesgo, a un nivel aceptable por la dirección.

Después de evaluar el riesgo de cada vulnerabilidad, se determinó con aprobación de la gerencia si el riesgo se mitiga, transfiere o acepta. Como resultado se tiene la propuesta de controles para elaborar una estrategia de seguridad. A la hora de tomar acciones correctivas se encontró que no todos los controles se pueden implementar, el proyecto presentó una serie de restricciones, no necesariamente técnicas que establecen un marco al que debe limitarse, éste contempla decisiones gerenciales y/o mecánicas de trabajo, por ejemplo:

- La cantidad de recursos asignados.
- La forma de planificar el gasto y de ejecutar el presupuesto. En este punto se aprovecharon los recursos con los que cuenta la institución, contemplado gastos mínimos.
- La cultura o forma interna de trabajo puede ser incompatible con ciertos controles.
- Rechazo de controles, por el personal de la institución.

A continuación se realiza un listado de las vulnerabilidades detectadas, con base en el nivel de atención del riesgo, a las cuales se sugiere uno o varios controles que permitan reducir la posibilidad de ocurrencia de los riesgos (tabla 5.9).

Tabla 5. 9 Controles recomendados, con base en el análisis de riesgo.

Vulnerabilidad	Nivel de atención de riesgo	Control sugerido
Red inalámbrica abierta	Alto	Hotspot, servidor RADIUS, cifrado
Inexistencia de controles sobre el uso de la red inalámbrica	Alto	Hotspot, servidor RADIUS, cifrado
Poco control en la administración de direcciones IP	Alto	Inventario de gestión de direcciones IP
Inexistencia de control en la información descargada a través de la red de la institución	Alto	Firewall, filtrado de contenido
Falta de cuidado del equipo de cómputo	Alto	Concientización en temas de seguridad
Limitantes de potencia en UPS	Alto	Evaluación y adquisición de un UPS
Falta de mecanismos de control perimetral de la red	Alto	Firewall, IDS, gestor de uso de red
Uso de protocolos de administración inseguros	Alto	Políticas de configuración de equipos activos
Inexistencia de políticas de uso de red	Alto	Elaboración de políticas de uso de red
Inexistencia de políticas para servidores	Alto	Elaboración de políticas para servidores
Inexistencia de respaldos en equipos activos	Alto	Elaboración de políticas de respaldo
Acceso a todos los recursos de red institucional	Alto	Firewall perimetral, firewall site de servidores, vlan's, NAT's
Uso de una misma contraseña por periodos largos de tiempo	Alto	Políticas de contraseñas
Uso de una contraseña única en varios equipos	Alto	Políticas de contraseñas, concientización en temas de seguridad
Uso de contraseñas no robustas	Alto	Políticas de contraseñas, concientización en temas de seguridad
Confianza en otras personas	Alto	Concientización en temas de seguridad
Uso de IP's homologadas para usuarios en general	Alto	Vlan, NAT
Fallas por parte del proveedor del suministro eléctrico	Alto	Emitir recomendaciones a la Secretaría Administrativa
Puertos abiertos sin uso en estación de trabajo	Alto	Políticas de hardening en estaciones de trabajo
Inexistencia de respaldos en las diferentes secretarías	Medio	Políticas de respaldo
Tableros eléctricos expuestos	Medio	Informar de la observación a la Secretaría Administrativa
Controles de acceso físicos, inseguros para administración de servidores	Medio	Implementar controles biométricos en los sites
Vulnerabilidades inherentes del protocolo TCP/IP	Medio	Políticas de monitoreo
Daño en hardware por fallas eléctricas	Medio	UPS
Inexistencia de control en el tráfico de red generado por la institución	Medio	Gestor de uso de red, balanceadores de carga

Vulnerabilidad	Nivel de atención de riesgo	Control sugerido
Fuga de información	Medio	Políticas de confidencialidad
Daño físico a la infraestructura de red	Medio	Cableado estructurado
Puertos abiertos sin motivo en servidores críticos	Medio	Políticas de hardening en servidores
Inexistencia de controles de seguridad en portátiles	Medio	RFID, bandas magnéticas, cintas de seguridad para portátiles
Inexistencia de monitoreo de uso de la red	Medio	Políticas de monitoreo
Fallas en sistemas de aire acondicionado	Medio	Mantenimiento preventivo
Control de acceso débil en aplicaciones	Medio	Políticas desarrollo de software seguro
Personal poco capacitado en temas de seguridad	Medio	Capacitación del personal
Inexistencia de actualizaciones en terminales de trabajo, servidores, antivirus y equipos de red	Medio	Políticas de hardening en estaciones de trabajo y Políticas de hardening en servidores
Falta de mantenimiento preventivo en servidores y equipos activos	Medio	Mantenimiento preventivo en servidores y equipo activo
Falta de mantenimiento de estaciones eléctricas	Medio	Mantenimiento preventivo en estaciones eléctricas
Falta de corriente eléctrica regulada	Medio	Implementar reguladores en la mayoría de los equipos
Inexistencia de fuente de corriente eléctrica alterna	Medio	Planta eléctrica
Inexistencia de planes de capacitación	Medio	Capacitación del personal
Inexistencia de sites alternos	Medio	Contratos con compañías o acuerdos con otras instituciones
Cableado de red expuesto	Medio	Cableado estructurado
Respaldos en mismo disco duro	Medio	Políticas de respaldo
Parámetros por default en equipos activos	Medio	Políticas de configuración de equipos activos
Acceso a todas las terminales de administración	Medio	Firewall perimetral, firewall Site servidores, listas de control de acceso
Acceso a todos los recursos de internet	Medio	Firewall, gestor de contenido
Uso de protocolos de comunicación inseguros	Medio	Implementación de comunicaciones cifradas
Falta de mantenimiento en cableado eléctrico	Medio	Mantenimiento preventivo en la institución
Inexistencia de controles de humedad	Medio	Sensor de humedad
Inexistencia de controles de temperatura	Medio	Sensor de temperatura
Consultas de sitios con software malicioso	Medio	Gestor de contenido, capacitación al usuario
Descarga de ejecutables de sitios no confiables	Medio	Gestor de contenido, capacitación al usuario
Inexistencia de políticas sobre el uso del equipo de cómputo	Medio	Políticas sobre el uso del equipo de cómputo

Vulnerabilidad	Nivel de atención de riesgo	Control sugerido
Autoarranque de dispositivos extraíbles	Medio	Políticas de hardening en estaciones de trabajo
Falta de políticas de desarrollo de software seguro	Medio	Políticas de desarrollo de software seguro
Inexistencia de controles de integridad en equipos activos	Medio	Memorias técnicas y respaldos de configuración
Firmas antivirus deficientes	Medio	Evaluación y adquisición de un antivirus
Inexistencia de políticas de uso de software	Medio	Políticas de hardening en estaciones de trabajo
Poco control sobre los respaldos	Medio	Políticas de control de cambios y políticas de respaldo
Filtrado de agua a Sites	Medio	Mantenimiento preventivo
Inexistencia de controles sobre el uso de procesador, memoria, disco duro y ancho de banda	Medio	Políticas de hardening en servidores
Falta de procedimientos de creación de cuentas	Medio	Políticas de contraseñas
Vulnerabilidades inherentes a las aplicaciones	Medio	Actualizaciones
Tiempo de vida útil de los equipos	Medio	Mantenimiento preventivo, renovación de hardware
Tuberías expuestas	Medio	Restructuración de instalación eléctrica, mantenimiento
Uso de versiones viejas en aplicaciones	Medio	Actualizaciones
Vulnerabilidades conocidas en sistemas operativos	Medio	Actualizaciones
Empleo de software sin actualizaciones	Medio	Actualizaciones
Inexistencia de auditorías	Bajo	Planificación de auditorias
Limitantes de espacio en disco duro en servidores	Bajo	Evaluación y adquisición de medios de almacenamiento masivo
Fallas eléctricas	Bajo	Mantenimiento general a la red Eléctrica
Inexistencia de cultura de seguridad en usuarios finales	Bajo	Capacitación del personal
Inexistencia de control perimetral de los puertos permitidos	Bajo	Firewall perimetral, IDS
Inexistencia de procedimientos de cambios en sistemas	Bajo	Políticas de control de cambios
Inexistencia de políticas en sistemas operativos	Bajo	Políticas de hardening en estaciones de trabajo
Inexistencia de cifrado en discos duros	Bajo	Cifrado
Poca separación de funciones críticas	Bajo	Definir responsabilidades, separación de funciones
Dispositivos extraíbles sin cifrado	Bajo	Cifrado
Fallas por parte del proveedor de servicios de internet	Bajo	Enlaces redundantes , acuerdos de LSA
Daños en la configuración de los equipos por poco mantenimiento	Bajo	Mantenimiento preventivo

Vulnerabilidad	Nivel de atención de riesgo	Control sugerido
Descuido en el manejo del hardware	Bajo	Capacitación del personal
Errores de cambios en la configuración de equipos activos y servidores	Bajo	Capacitación del personal
Inexistencia de control a servicios de servidores	Bajo	Políticas de hardening en servidores
Inexistencia de políticas de confidencialidad	Bajo	Políticas de confidencialidad
Inexistencia de monitoreo de las aplicaciones	Bajo	Políticas de monitoreo, implementación de herramientas de monitoreo
Poca educación sobre seguridad a usuarios finales	Bajo	Capacitación del personal
Errores humanos	Bajo	Capacitación del personal
Aprovechamiento de vulnerabilidades de controles físicos	Bajo	Implementación de controles de acceso de 2 o más factores
Falta de gestión de garantías	Bajo	Adquisición de periodos de garantía más largos
Interferencias magnéticas	Bajo	----------
Desastres naturales en la institución	Bajo	Prevención

En cuestión a los controles propuestos para la organización, se aprobó el siguiente plan de seguridad, que contempla la siguiente arquitectura de red (figura 5.4).

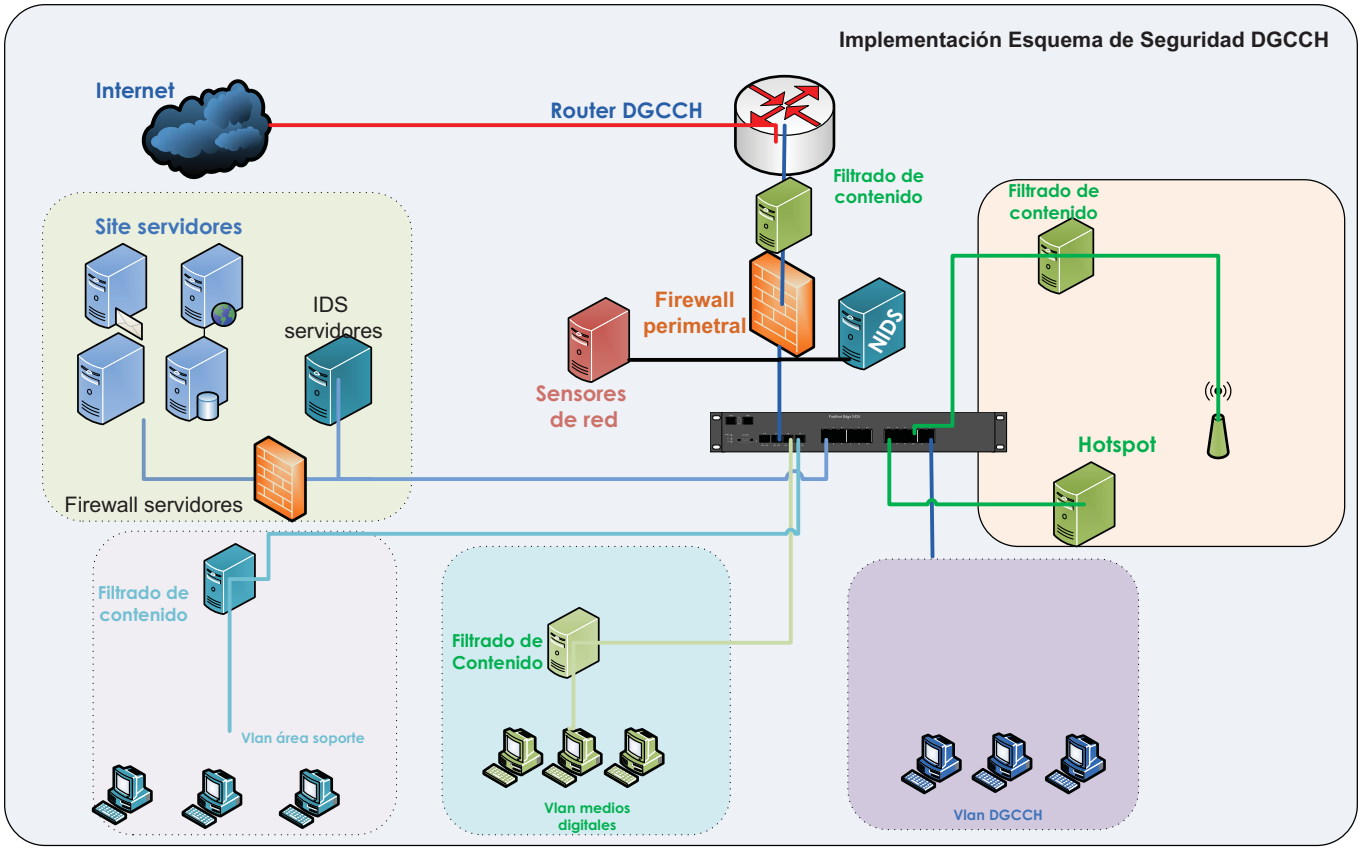

Figura 5. 4 Propuesta de esquema de seguridad para la red.

El esquema de protección planteado, consta de los siguientes mecanismos apoyado de políticas, procedimientos y documentos de respaldo que fortalecen el esquema de seguridad.

a. Esquema de seguridad perimetral

- 2 Firewall (Perimetral y Site de servidores); estableciendo reglas de filtrado apegadas sólo a los requerimientos de servicio.
    - A la fecha de entrega del proyecto, solo se ha configurado el equipo perimetral, por falta de recursos.
- 2 IDS (Perimetral y Site de servidores).
    - A la fecha de entrega del proyecto, solo se ha configurado el equipo perimetral, por falta de recursos.
- 1 Sensor de uso de la red, por tipo de tráfico, host y servicio, (Perimetrales).
- Monitoreo de enlace, por parte del proveedor de servicio "NOC UNAM".
- Zonas de seguridad por secretaría, 3 Segmentos de red por medio de NAT's, y segmento homologado.
- 1 Filtro de contenido perimetral.
- 3 Filtros de contenido independientes.
- Implementación de controles de autenticación y cifrado de los servicios de red inalámbrica.

b. Políticas

- Políticas de seguridad para la red de la organización.
- Políticas de seguridad para sistemas operativos Windows / UNIX.
- Políticas de monitoreo.
- Políticas de respaldo para servidores.

c. Procedimientos

- Establecer responsables de la seguridad lógica de la institución.
- Realización de análisis de riesgos de manera periódica.
- Aplicación para el inventario y asignación de direcciones IP.
- Definición de funciones específicas para cada puesto.
- Procedimiento de actualización de memorias técnicas.
- Procedimiento de instalación y configuración de firewall.
- Procedimientos dé instalación de IDS.
- Procedimiento de instalación de Hotspot.
- Procedimiento de configuración de equipos activos.
- Procedimiento de instalación de sensor de red.
- Procedimiento de configuración de zonas para SAN.
- Procedimiento de instalación servidores ESX.
- Políticas de cambio de contraseñas.
- Hardening en equipos activos.
- Hardening en servidores.
- Procedimiento de instalación sistemas operativos de los usuarios.
- Capacitación al personal de soporte y encargados de la red de la institución.
- Capacitación a los usuarios finales.

- Documentar los procesos y verificarlos periódicamente.

d. Seguridad Física

- Cámaras de circuito cerrado y políticas de monitoreo.
- Empleo de cerraduras físicas, biométricas o electrónicas en sites.
- Planta eléctrica redundante, para site de servidores.
- Instalación de cableado estructurado.
- Monitoreo de condiciones ambientales en sites.

e. Documentos

- Diagramas de red de la institución.
- Memorias técnicas de cableado estructurado.
- Memorias técnicas de los equipos activos (Switch, Router, A.P.).
- Memorias técnicas de servidores.
- Respaldo de la configuración de los equipos activos que lo permitan.
- Respaldo de servidores.

- **Hardware**
  - Contemplar la compra de un SAN para la realización de respaldos de servidores.
  - Configuración de NAS, para respaldos de los datos de los usuarios, cuando requieran mantenimiento los equipos.
  - Implementar un esquema de alta disponibilidad en servidores.
  - Configuración de Firewall con opción de configuración para alta disponibilidad.
  - Redundancia en mecanismos de alimentación eléctrica para site de servidores.
  - Considerar site alternos.

Existen dispositivos que ayudarían a garantizar de mejor manera la continuidad de operación de los servicios brindados, los cuales representan un gasto considerable para la organización. En cuestión de políticas, procedimientos, diagramas y guías de configuración todos contemplan la siguiente información como mínima indispensable:

- Nombre del documento.
- Persona que elaboró.
- Persona que aprobó.
- Fecha de publicación.
- Objetivo del documento.
- Alcance.
- Definiciones.
- Control de Cambios.

5.4. Desarrollo de la implementación

El esquema de seguridad que se implementó no representó un costo considerable a la institución, ya que se aprovecharon todos aquellos recursos de los cuales podrían hacer uso, dentro de éstos se lista el material utilizado para cada control, pero es importante aclarar que muchos de los controles propuestos son procedimientos, los cuales requieren documentación, personal humano y tiempo para su elaboración. El tipo de dispositivos que se propone anteriormente tiene diversidad en costos, fabricantes y prestaciones que brinda, las propuestas de seguridad que se realizaron no representaron un costo adicional hasta el momento de su implementación, pero cabe aclarar que no contempló la totalidad de mecanismos mencionados en la propuesta.

a. ***Firewall perimetral*;** Primer dispositivo contemplando en la implementación, por solicitud de la jefatura se pide contemplar la implantación de este control como una primer barrera de protección derivada de ataques externos.
    - Servidor Intel.
    - 2 interfaces de red de fibra óptica.
    - Personal encargado de la instalación y monitoreo de dichas tareas.
    - Elaboración de procedimiento de instalación.
    - Solución con software libre.

b. ***IDS perimetral;*** Segundo dispositivo instalado, brinda apoyo en la detección de ataques que no pueden ser detectados por el firewall, permite establecer reglas personalizadas.
    - Servidor Dell, independiente subutilizado.
    - Máquina virtual colocada en servidor ESX-A.
    - Se configura mirror en switch core.
    - Personal encargado de la instalación y monitoreo de dichas tareas.
    - Elaboración de procedimiento de instalación.
    - Solución con software libre.

c. ***Sensor de red*;** dispositivo instalado al mismo tiempo que el IDS, capaz de monitorear el comportamiento de protocolos como TCP/UDP/ICMP, y ya dentro de éstos, agruparlos por FTP,HTTP,DNS,telnet,SNMP,POP3 y por host.
    - Servidor Dell, independiente subutilizado.
    - Máquina virtual colocada en servidor ESX-A.
    - Personal encargado de la instalación y monitoreo de dichas tareas.
    - Elaboración de procedimiento de instalación.
    - Solución con software libre.

d. ***Servidores NAT;*** Segmentación de redes virtuales, en áreas que así lo permitan.
    - Configuración de NAT en equipos cisco.
    - Configuración de NAT, empleando software libre.
    - Elaboración de procedimiento de instalación.
    - Personal encargado de la instalación y monitoreo de dichas tareas.

e. ***Filtrado de contenido*;** Empleado como un control en los destinos de búsqueda, de los clientes, permitiendo elegir categorías de bloqueo como pornografía, p2p, proxy, películas, chat, drogas, redes sociales, etcétera.
    - Cuenta creada en OpenDNS para aplicar filtrado de contenido en cada uno de los segmentos de red generados, la herramienta de suscripción anual con todas sus funciones. En este caso sólo se utiliza en la versión libre.
    - Personal encargado de dichas tareas.

f. ***Hotspot***; Control de acceso y confidencialidad de la red inalámbrica.
- Servidor Dell, independiente subutilizado.
- 1 Tarjeta de red PCI express con 2 interfaces ethernet 10/100/1000.
- Configuración de Hotspot en servidor ESX-B.
- Solución con software libre.
- Personal encargado de la instalación y soporte al servicio.
- Elaboración de procedimiento de instalación.

g. Actualización del inventario de las asignaciones de IP y dominios.
- Desarrollo de sistema para el control de asignaciones IP.
  - URL: https://132.248.122.122/ips/inicio.aspx
- Documentación del desarrollo.
- Personal encargado de la supervisión en las asignaciones.

h. Elaboración de memorias técnicas.
- Contempla las memorias técnicas de todos los equipos de comunicación.
- Centralización de contraseñas empleando un gestor de contraseñas.
- Personal humano encargado de dichas tareas.

i. Elaboración de procedimientos para el área de servidores administrados por la Secretaría de Informática.
- Personal humano encargado de dichas tareas.

j. ***Elaboración de respaldos*****.**
- Personal humano encargado de dichas tareas.
- Unidad de almacenamiento externo, NAS y SAN.

k. ***Etiquetar medios de transmisión primarios*****.**
- Personal humano encargado de dichas tareas.

Los controles que se colocaron se complementan con aquéllos que había antes de la implementación, estos mecanismos existentes antes de la implementación son:

- Seguridad física de la red y su entorno.
- Procedimiento en la instalación de sistemas operativos para las máquinas de los usuarios.
- Procedimientos propios de seguridad de cada administrador.

Los controles garantizan un nivel de seguridad, sin embargo, deberán complementarse a través de documentos, guías de configuración, políticas, buenas prácticas que permitan una adecuada gestión de la seguridad.

5.5. Limitantes de la implementación

Cuando se trata de implementar un esquema de seguridad surgen como resultado del análisis de riesgo un sin fin número de mejoras posibles, lo ideal sería que todos los controles plateados se lograran implementar, los principales obstáculos a los que se enfrentan las instituciones al implementar un plan de seguridad eficaz son:

- Falta de presupuesto dirigido meramente a la seguridad de la institución.
- Falta de personal dedicado a la seguridad lógica de la institución.
- Tener definido claramente, las funciones de cada puesto.
- Falta de personal calificado en el área de seguridad.
- Falta de conciencia de los usuarios para utilizar los servicios de cómputo de manera adecuada.
- Cambios tecnológicos constantes.
- Costumbres y formas de trabajo en determinadas áreas.
- Conciencia de los Directivos sobre la importancia de proteger la red de la institución.

Actualmente muchas instituciones cuentan con conexión a Internet, pero pocas se han preocupado por proteger su infraestructura, información y procesos. El hecho de no contar con un área de seguridad en cómputo dentro del organigrama provoca que el administrador de red y el personal asignado al área de sistemas, además de sus tareas diarias, deba lidiar con problemas de seguridad.

En el proyecto realizado actualmente se tiene pendiente la implementación y el desarrollo de algunos controles, el motivo principal de este retraso son los recursos económicos y de personal, que afectan directamente en la adquisición de hardware faltante, el personal dedicado para esta tarea, seguido por las costumbres de trabajo en algunas áreas.

Las actividades que se planea realizar en un futuro, que repercuten en temas de seguridad son:

- Cableado estructurado para toda la institución, con un costo de $452,779.32, el cual incluye el recableado de la totalidad de la instalación en cobre categoría 6E.
- UPS de 10KW en potencia, con un costo aproximado de $97,044.81.
- Cámara de vigilancia IP, sensor de temperatura y humedad $22,096.84.
- Interfaces de red ethernet y de fibra para servidores $13,000.
- La adquisición de un equipo de almacenamiento alternativo NAS, que resguarde una copia de las máquinas virtuales en producción y brinde un soporte de crecimiento en almacenamiento.
- En el caso del IDS por ser una solución de software libre sin licencia se tiene un retardo en las actualizaciones de las firmas de ataque, aproximado a un mes. En caso de que se deseen tener las reglas de filtrado completamente actualizadas se debe pagar una licencia de $30 US anual para un sensor, de 1-5 sensores $499/número de sensores y de más de 6 sensores $399/número de sensores.
- Capacitación.

En la tabla 5.10 se citan todos aquellos riesgos residuales que no fueron atendidos por los recursos relacionados a los mismos, pero que se planean llevar a cabo en un futuro cercano.

Tabla 5. 10 Riesgos residuales.

Vulnerabilidad	Nivel de atención de riesgo	Control sugerido
Falta de cuidado del equipo de cómputo	Alto	Concientización en temas de seguridad
Confianza en otras personas	Alto	Concientización en temas de seguridad
Fallas por parte del proveedor del suministro eléctrico	Alto	Acuerdos de niveles de servicio
Tableros eléctricos expuestos	Medio	Informar de la vulnerabilidad detectada a la Secretaría Administrativa
Controles de acceso inseguros para administración de servidores	Medio	Implementar controles biométricos en los Sites
Fuga de información	Medio	Políticas de confidencialidad
Daño físico a la infraestructura de red	Medio	Cableado estructurado
Inexistencia de controles de seguridad en portátiles	Medio	RFID, bandas magnéticas y cintas de seguridad
Control de acceso débil en aplicaciones	Medio	Políticas desarrollo de software seguro
Falta de corriente eléctrica regulada	Medio	Implementar reguladores en la mayoría de los equipos
Inexistencia de fuente de corriente eléctrica alterna	Medio	Planta eléctrica
Inexistencia de planes de capacitación	Medio	Capacitación del personal
Inexistencia de sites alternos	Medio	Contratos con compañías, acuerdos con otras instituciones
Cableado de red expuesto	Medio	Cableado estructurado
Uso de protocolos de comunicación inseguros	Medio	Implementación de comunicaciones cifradas
Tuberías expuestas	Medio	Restructuración de instalación eléctrica, mantenimiento
Empleo de software sin actualizaciones	Medio	Actualizaciones
Inexistencia de auditorias	Bajo	Planificación de auditorias
Limitantes de espacio en disco duro en servidores	Bajo	Evaluación y Adquisición de medios de almacenamiento masivo
Inexistencia de cultura de seguridad en usuarios finales	Bajo	Capacitación del personal
Inexistencia de cifrado en discos duros	Bajo	Cifrado
Poca separación de funciones criticas	Bajo	Definir responsabilidades, Separación de funciones
USB sin cifrado	Bajo	Cifrado
Fallas por parte del proveedor de servicios de internet	Bajo	Enlaces redundantes , acuerdos de LSA
Descuido en el manejo del hardware	Bajo	Capacitación del personal
Errores de cambios en la configuración de equipos activos y servidores	Bajo	Capacitación del personal
Inexistencia de políticas de confidencialidad	Bajo	Políticas de confidencialidad
Poca educación sobre temas de seguridad a usuarios finales	Bajo	Capacitación del personal

Vulnerabilidad	Nivel de atención de riesgo	Control sugerido
Errores humanos	Bajo	Capacitación del personal
Aprovechamiento de vulnerabilidades de controles físicos	Bajo	Implementación de controles de acceso de 2 o más factores
Falta de gestión de garantías	Bajo	Adquisición de periodos de garantía más largos
Interferencias magnéticas	Bajo	----------
Desastres naturales en la institución	Bajo	Prevención

5.6. Posibilidades de crecimiento

Cuando se implementa un esquema de seguridad que va ligado con un análisis de riesgo, muestra claramente aquellos riesgos residuales que se generan con la implementación de los controles seleccionados, lo que permite contemplar mejoras a mediano y largo plazo. Dentro de las posibilidades de crecimiento que se contemplan para llevar a cabo, se sugiere:

De manera inicial se recomienda contemplar los puntos mencionados en las limitantes de la implementación, como mejoras inmediatas, ya que algunas de ellas su nivel de riesgo es elevado, pero por cuestiones de recursos económicos no fue posible su implementación.

1. Elaboración de análisis de riesgo de manera periódica, basándose en estudios realizados anteriormente, generando un histórico de esquemas de seguridad, que permita observar los puntos de mejora y críticos a la fecha.
2. Revisión y actualización de las políticas de seguridad.
3. Asignar a una persona como responsable de la seguridad de la institución.
4. Aumento de la seguridad física en los sites, implementado controles de acceso de 2 factores.
5. Realizar separación de funciones en todas las actividades críticas de la institución.
6. Establecer un help desk para la atención de incidentes, dentro de la institución.
7. Desarrollar procedimientos de manejo de incidentes, entre ellos de contención de código malicioso.
8. Implementación de plantas de energía eléctricas alternativas y UPS en los sites.
9. Realizar una instalación de cableado estructurado.
10. Segmentación de la red en la totalidad de sus secretarías.
11. Elaboración de un sistema de gestión y respuesta de incidentes de seguridad.
12. Capacitación continúa en cuestiones de seguridad al personal de la institución.
13. Guía de respaldo para base de datos.
14. Actualización de los equipos de telecomunicaciones a equipos administrables.
15. Aplicar un plan de gestión de la seguridad PDCA (Plan - Do - Check - Act).
16. Dar a conocer las políticas de uso de equipos, red y seguridad en red de la institución.
17. Normativa para la publicación de sitios web.
18. Realizar auditorías periódicamente con la finalidad de detectar nuevas vulnerabilidades.

19. Legalizar el uso de software que se tiene de manera ilegal.
20. Revisión de Acuerdos de Niveles de Servicio (LSA) con proveedores de servicio de red y suministro eléctrico.
21. Realizar informes detallados, para sustentar las decisiones derivadas de las iniciativas de seguridad.
22. Migración de todos los servidores a los Sites donde se cuenta con condiciones adecuadas para su funcionamiento y resguardo.
23. Implementar esquema de seguridad para los planteles que integran el Colegio de Ciencias y Humanidades.
    - Aprobación de las políticas de red propuestas desde esta entidad central hacia los planteles que la conforman.
    - Separación de funciones, determinando roles específicos para cada persona.
    - Cifrado de información en equipos portátiles con base en su grado de importancia.
    - Elaboración de planes de contingencia.
    - Capacitación a los encargados de sistemas, en temas relacionados a la seguridad de sistemas operativos Windows y Linux.
    - Capacitar al usuario final en cuestiones de seguridad básicos, ya que él forma el eslabón más débil en la cadena que conforma la seguridad de la información.
24. Gestión, monitoreo y elaboración de estadísticas del uso de la red.