UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE CIENCIAS Y SISTEMAS

MAESTRÍA EN GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

CICLO ACADÉMICO 2017- 2019

Informe Final de Tesis para optar al Título de

Master en Gestión de la Seguridad de la Información

"PROPUESTA DE OPTIMIZACIÓN DE LA INFRAESTRUCTURA DE SEGURIDAD DE LA ASOCIACIÓN DE MUNICIPIOS DE NICARAGUA (AMUNIC)."

Autores:

Ing. Christian Joel Cuadra Brenes #2017-0005M

Ing. Karina Magdalena Vílchez Roque #2017-0014M

Tutor: MSc. Ing. Reynaldo Antonio Castaño Umaña

Managua, Nicaragua 2019.

Managua, 19 de Febrero 2019

Lic. Carlos Sánchez Hernández

Decano Facultad de Ciencias y Sistemas-UNI

Su despacho.

Estimado Lic. Sánchez,

Por este medio nos dirigimos a usted para solicitar, al comité académico del programa **Maestría en Gestión de la Seguridad de la Información (MGSI)** que usted preside, la aprobación del protocolo de investigación titulado: **"PROPUESTA DE OPTIMIZACIÓN DE LA INFRAESTRUCTURA DE SEGURIDAD DE LA ASOCIACIÓN DE MUNICIPIOS DE NICARAGUA (AMUNIC)".**

Además, solicito la asignación del maestro MSc. Ing. Reynaldo Castaño Umaña como asesor/tutor, para el desarrollo del trabajo final.

Esperando una respuesta afirmativa a esta solicitud para continuar con el desarrollo y elaboración del documento final de tesina, les saludamos

Atentamente,

Ing. Karina Magdalena Vílchez Roque

Maestrante MGSI

Número de carné: UNI: 2017-0014M

Ing. Christian Joel Cuadra Brenes

Maestrante MGSI

Número de carné: UNI: 2017-0005M

C/c. Archivo

UNIVERSIDAD NACIONAL DE INGENIERIA
Facultad de Ciencias y Sistemas
DECANATURA

Managua 03 de mayo de 2019

Ing. Christian Joel Cuadra Brenes

Ing. Karina Magdalena Vilchez Roque

Sus manos

Estimados Maestrantes, reciba un atento saludo de mi parte.

Por medio de la presente le informo que el Protocolo propuesto para elaboración de la Tesis del Programa de Maestría en Gestión de la Seguridad de la Información titulado: "" **PROPUESTA DE OPTIMIZACIÓN DE LA INFRAESTRUCTURA DE SEGURIDAD DE LA ASOCIACIÓN DE MUNICIPIOS DE NICARAGUA (AMUNIC)",** ha sido aprobado ya que cumple con los requisitos de acuerdo al Arto. 48, inciso b) de la normativa para la culminación de estudios de Posgrado.

De acuerdo a su solicitud, el MSc. **Reynaldo Castaño Umaña** será el Profesor encargado del acompañamiento en el proceso de elaboración de su Tesis.

Atentamente;

Lic. Carlos Sánchez Hernández
Decano FCyS-UNI

C/c. MSc. Reynaldo Castaño Umaña. Tutor.
C/c. Archivo FCE mayo 2019

Managua, 18 de noviembre 2019

Lic. Carlos Alberto Sánchez
Decano FCyS-UNI
Su despacho

Estimado Lic. Sánchez:

La presente tiene como objetivo hacer de su conocimiento que he revisado de manera exhaustiva el documento final del trabajo de tesis titulado **"PROPUESTA DE OPTIMIZACIÓN DE LA INFRAESTRUCTURA DE SEGURIDAD DE LA ASOCIACIÓN DE MUNICIPIOS DE NICARAGUA (AMUNIC)."**, elaborado por la *Ing. Karina Magdalena Vílchez Roque y el Ing. Christian Joel Cuadra Brenes*, el cual cumple con las normativas expuestas en los reglamentos de elaboración de trabajos de tesis de nuestra institución y con la calidad académica-profesional para su defensa , por lo cual autorizo su entrega formal y avalo el trabajo realizado.

Cabe destacar la dedicación, esfuerzo y calidad profesional demostrada por los Ingenieros *Vílchez y Cuadra*, durante el desarrollo del presente trabajo, por lo que solicito a los honorables miembros del jurado calificador que usted designe, les sea otorgada la máxima calificación.

Sin más que agregar y deseándole éxitos en sus labores administrativas y académicas, le saludo

MSc. Ing. Reynaldo Castaño Umaña
Docente FCyS-UNI
Tutor

C/c. Archivo

RESUMEN

El presente trabajo de investigación consiste en una Propuesta de Optimización de la Infraestructura Tecnológica de la Seguridad, con la finalidad de proteger los activos informáticos y mejorar la prestación de los servicios que ofrece la Asociación de Municipios de Nicaragua (AMUNIC) a los usuarios, dicho proceso contempla la implementación de controles de seguridad basados en una evaluación de riesgos críticos, identificando las amenazas y vulnerabilidades a los que está expuesta la información de la institución.

Para la realización de la propuesta se tomó como referencia la metodología MAGERIT y criterios de la ISO 27001-2013, con el fin de preservar la integridad, confidencialidad y disponibilidad de los servicios.

La propuesta permite que el estado de los riesgos identificados pasen de critico a aceptables mediante la implementación de controles adecuados, como la creación de VLANs, Implementación de módulo Antispam conforme a las necesidades de AMUNIC, implementación de un Servidor Active Directory, implementación de configuración del WebFiltering en UTM existente e implementación de módulo de Auditoria del SIAFP para el fortalecimiento de la seguridad de la Infraestructura Tecnológica que mejor se adapten en función de su aplicabilidad, adaptabilidad y costos, y creación de un plan de implementación de actividades.

Palabras Claves: Infraestructura, Auditoria, Optimización, Seguridad Informática, Amenazas, Vulnerabilidad, Antispam, Control de Acceso.

Contenido

1. INTRODUCION

La innovación y las tendencias tecnológicas, estimulan en las organizaciones el incremento del rendimiento y productividad, generando su fortalecimiento y la creación de nuevas oportunidades en los mercados globales.

La rapidez con la que cambian los aspectos tecnológicos, trae consigo riesgos de seguridad que deben ser gestionados por las instituciones, no hacerlo, provocaría impacto negativo en dos direcciones: pérdida en el manejo de los activos de información y afectaciones económicas. Aunque hay avances en las inversiones en estos temas, aún existen instituciones que operan con bajos niveles de seguridad.

En este contexto, ubicamos a la Asociación de Municipios de Nicaragua (AMUNIC), la cual tiene una Infraestructura Tecnológica de servicio pre configurada por los proveedores, implementada a través de los niveles de seguridad propios de los sistemas operativos de redes, aplicaciones, dispositivos perimetrales y manejadores de base de datos utilizados. Todo ello, brinda protección básica para la prevención y mitigación de ataques.

Debido al poco nivel de seguridad actual con que cuenta la Infraestructura Tecnológica, se requiere elaborar la presente propuesta de optimización que permita proteger los activos informáticos, mejorar la prestación de servicios, garantizar la disponibilidad y satisfacer la demanda de servicios y recursos que AMUNIC brinda a sus socios.

2. OBJETIVOS

Objetivo General:

Desarrollar una Propuesta de Optimización de la Infraestructura de Seguridad de la Asociación de Municipios de Nicaragua.

Objetivos específicos:

- Realizar un diagnóstico de la Infraestructura Tecnológica de AMUNIC para la identificación de los riesgos asociado a los servicios.

- Proponer controles de seguridad óptimos para la mitigación de los riesgos.

- Elaborar un plan de implementación de la Infraestructura de Seguridad con estimaciones de costos.

3. JUSTIFICACIÓN

La administración de la Infraestructura Tecnológica y servicios informáticos es sumamente importante para AMUNIC, la cual debe tomar en consideración la seguridad del entorno de las aplicaciones y los servicios tales como telefonía IP, red WI-Fi, Sistema de cámaras, Sistema Integral Administrativo Financiero y Planificación (SIAFP), entre otros.

Actualmente, existen una serie de dificultades en materia de seguridad, entre las cuales se puede mencionar la falta de definición de roles en los módulos del SIAFP, deficientes controles en las políticas de uso de equipos, existencia de una red LAN plana, vulnerabilidad ante correos, navegación a internet sin restricciones.

Con la Propuesta de Optimización de la Infraestructura Tecnológica se pretende reducir los riesgos a los que están expuestos los servicios y activos, para lo cual es necesario desarrollar soluciones que sean de carácter correctiva o preventiva de eventos no deseados, logrando de esta forma que la inversión cubra las brechas de seguridad más importantes y por consecuencia, medir la eficacia de los controles de seguridad implementado.

Indudablemente que con la mejora de los procedimientos actuales de control de seguridad se aseguraría la mejora en la calidad de los datos con alta disponibilidad en los sistemas o aplicativos más sensitivos de AMUNIC como es el SIAFP.

Entre las principales razones que son necesarias para la implementación de la Propuesta de Optimización de Infraestructura de seguridad son:

- **Pérdida de productividad**. La pérdida de datos o datos errados, así como intermitencia en los sistemas de información, conlleva a la disminución de la producción.
- **Pérdida de horas-hombres y consumo de tiempo en corregir problemas**. Es una gran cantidad de horas hombres que debe invertir la Institución en solventar los problemas causados por ataques, software malicioso, hacker, etc. Información errónea.
- **Ausencia de políticas y lineamientos** implantados en AMUNIC en lo que a seguridad de la información se refiere.
- **Ausencia de cultura organizacional** que repercute en la seguridad de los activos de información que posee la Institución.

4. MARCO TEORICO

4.1. Bases Teóricas

Las bases teóricas a ser utilizada se describirán en conjunto de teorías, conceptos y proporciones utilizadas que explicarán el problema de investigación, la cual veremos ilustrada en el mapa mental en la figura 1.

Según Blaustein (2014), “Las facilidades y beneficios que ofrecen las redes de computadoras han causado que la mayoría de las instituciones, adopten nuevas tecnologías”.

Estas tecnologías como el Internet han influido en las organizaciones responsabilizándose de la protección contra los posibles daños a los recursos de información y a los usuarios, entre las principales preocupaciones con respecto a la tecnología esta:

- Protección de los recursos de información
- Operaciones eficaces
- Entorno de trabajo no amenazador
- Protección contra la pérdida de información controlada

La protección de los recursos de información es importante para cualquier institución y/o persona donde cada recurso de información conlleva su conjunto específico de necesidades respecto a la preservación de la integridad de la información. En este sentido, la presente investigación hace referencia al estándar ISO 27001:2013, que busca determinar si los controles existentes de Infraestructura Tecnológica de AMUNIC garantizan seguridad de la información.

Figura 1. Mapa mental – AMUNIC - Fuente: Elaboración propia 2018

4.1.1. Infraestructura Informática

Es importante recordar que la seguridad informática y la seguridad de la información, aunque están estrechamente relacionadas, son conceptos diferentes y en el caso de estudio es la primera la que se abordara, no sin antes mencionar la manera en que la infraestructura actual logra implementar dicho concepto.

Según Simón (1996), “Infraestructura de tecnologías de la información (TI) está definida ampliamente como un conjunto de componentes de TI que son la base del servicio de TI; típicamente componentes físicos (computadoras, hardware de red y edificios), pero también varios componentes de red y software.”

4.1.2. Definición de Seguridad de la información

En la actualidad, un término ampliamente utilizado es la Seguridad de la información, que puede asociarse con otras palabras como ciberespacio, ciber amenazas, cibercriminales u otros conceptos compuestos. Aunque se tiene una percepción general sobre lo que representa, en ocasiones puede utilizarse como sinónimo de ciberseguridad, seguridad informática o seguridad en cómputo pero esta idea no es del todo correcta.

La disyuntiva se presenta cuando es necesario aplicar de manera adecuada los conceptos, de acuerdo con las ideas que se pretenden expresar. Si bien existen distintas definiciones para la seguridad de la información, es importante conocer cuándo se utiliza de forma correcta de acuerdo con el contexto, e identificar sus diferencias con los otros términos por ejemplo, el de seguridad de la información.

La norma ISO 27001-2013, define activo de información como los conocimientos o datos que tienen valor para una organización, mientras que los sistemas de información comprenden a las aplicaciones, servicios, activos de tecnologías de información u otros componentes que permiten el manejo de la misma. Por lo tanto, la ciberseguridad tiene como foco la protección de la información digital que "vive" en los sistemas interconectados. En consecuencia, está comprendida dentro de la seguridad de la información.

Según Soriano (s.f), "el concepto de seguridad de la información significa proteger la información y los sistemas de información de un acceso, uso, divulgación, alteración, modificación, lectura, inspección, registro o destrucción no autorizados".

No se puede olvidar que la seguridad lógica 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. La seguridad lógica incluye la protección de la información (datos y software de la red) de posibles incidentes, que van desde la infección de virus hasta el robo o modificación de estos, mediante el uso de medidas y controles como passwords, logins y grupos de usuarios. La seguridad lógica implica también el establecimiento de estrategias de respaldo y recuperación de datos que permitan minimizar el tiempo de restablecimiento de los servicios de la red.

Es inevitable la ocurrencia de fallas, pues no existe seguridad absoluta, se hace necesario que con los medios tecnológicos disponible se establezcan estrategias de seguridad de acuerde a las necesidades de las instituciones.

4.1.3. Dimensiones de la seguridad de la información

La seguridad de la información se articula sobre tres dimensiones ver figura 2, que son los pilares sobre los que aplicar las medidas de protección de la información, según el Instituto Nacional de Ciberseguridad español INCIBE

Figura 2: Triada de Seguridad de la Información

Fuente: INCIBE

La disponibilidad de la información garantiza que los usuarios autorizados tengan acceso a la información y a los resultados relacionados con ella toda vez que se requiera.

La integridad de la información se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

La confidencialidad implica que la información es accesible únicamente por el personal autorizado. Es lo que se conoce como need-to-know. Con este término se hace referencia a que la información solo debe ponerse en conocimiento de las personas, entidades o sistemas autorizados para su acceso.

Sin embargo, también se debe tomar en cuenta las siguientes propiedades:

• **Autenticidad**: asegurar que la información proviene de una fuente genuina y que no es una réplica de información antigua la cual se quiere hacer pasar por información actual.

• **No repudiación**: garantizar que el autor de una transacción electrónica no niegue posteriormente el haberla efectuado.

• **Identificación**: Uno de los requisitos básicos de un buen sistema de seguridad es la correcta identificación de las personas cuando solicitan el acceso.

• **Control de uso**: los procedimientos y políticas de control de uso limitan lo que una persona pueda hacer una vez que tenga acceso a datos o recursos del sistema.

• **Auditabilidad**: poder llevar a cabo la auditoria mediante registros históricos de los eventos (logs).

Todo proceso de optimización conlleva un diagnóstico previo pues es importante conocer las vulnerabilidades que se posee para dar recomendación o propuestas encaminadas a mejorar y tener mejor rendimiento.

4.1.4. Requerimientos de seguridad – Vulnerabilidad, amenazas y ataques

Los requerimientos de seguridad en cualquier institución, son derivados de fuentes como son el conjunto único de amenazas y vulnerabilidades que pudieran ocasionar pérdidas significativas en la institución si ocurrieran.

En un artículo publicado en el sitio web en el Instituto Nacional de Ciberseguridad español INCIBE[1], titulado "Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?" hace énfasis en la existencia de dos tipos de fuentes:

"Una **vulnerabilidad** (en términos de informática) es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos." (INCIBE, 2017)

La vulnerabilidad como tal, no causa daño, es simplemente una condición o conjunto de condiciones que pueden permitir que una amenaza afecte a un activo. Una evaluación de la posibilidad de ocurrencia de las vulnerabilidades y las amenazas, debe ser efectuada en esta fase

Por su parte, "una **amenaza** es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas.

[1] INCIBE: Instituto Nacional de ciberseguridad español

Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas.” (INCIBE, 2017)

Una amenaza tiene el potencial de causar un incidente no deseado, el cual puede generar daño al sistema, la organización y a los activos. El daño puede ocurrir por un ataque directo o indirecto a la información organizacional. Las amenazas pueden originarse de fuentes accidentales o de manera deliberada. Una amenaza para poder causar daño al activo, tendría que explotar la vulnerabilidad del sistema, aplicación o servicio.

El riesgo es la probabilidad de que se produzca un incidente de seguridad, materializándose una amenaza y causando pérdidas o daños.

Los ataques son incidentes provocados por actores internos o externos, entre los ataques más comunes tenemos:

- El espionaje: Acceso ilegitimo a la información desde el punto de vista físico o lógico, utilizando para ello las escuchas de mensaje por canales no protegidos, la lectura o copia de información mediante el acceso a dispositivos de almacenamiento.
- El Sabotaje: Es un ataque destructivo con la finalidad de producir el máximo daño posible; interrupción y borrado, la modificación y generación malintencionada de datos o información, la denegación de servicios o negación de recursos impidiendo a los sistemas de información cumplir con sus funciones.
- Compromiso de medios de autenticación: Cada medio de autenticación (contraseña, medidas biométricas, llaves o tarjetas de identificación) tiene

sus puntos débiles, que pueden ser aprovechado para vulnerar la seguridad y realizar un ataque.

- Compromiso de claves: Implica además de la suplantación de identidad la imposibilidad de demostrar que la persona debidamente autorizada no fue quien realizo el ataque, comprometiendo la integridad y la confiabilidad de dicha persona.

4.1.5. Clasificación de amenazas

Algunas de las fuentes de amenazas más comunes en el ámbito de sistemas de información son:

Malware o código malicioso: permite realizar diferentes acciones a un atacante. Desde ataques genéricos mediante la utilización de troyanos, a ataques de precisión dirigidos, con objetivos específicos y diseñados para atacar a un dispositivos, configuración o componente específico de la red.

Ingeniería social: Utilizan técnicas de persuasión que aprovechan la buena voluntad y falta de precaución de la víctima para obtener información sensible o confidencial. Los datos así obtenidos son utilizados posteriormente para realizar otro tipo de ataques, o para su venta.

APT o Amenazas Persistentes Avanzadas (Advanced Persistent Threats): son ataques coordinados dirigidos contra una empresa u organización, que tratan de robar o filtrar información sin ser identificados. Se suelen ayudar de técnicas de ingeniería social y son difíciles de detectar.

Botnets: conjunto de equipos infectados que ejecutan programas de manera automática y autónoma, que permite al creador del botnet controlar los equipos infectados y utilizarlos para ataques más sofisticados como ataques DDoS.

Redes sociales: el uso no controlado de este tipo de redes puede poner en riesgo la reputación de la empresa.

Servicios en la nube: una empresa que contrate este tipo de servicios tiene que tener en cuenta que ha de exigir los mismos criterios de seguridad que tiene en sus sistemas a su proveedor de servicios.

4.1.6. Fallas de seguridad

Tomando en consideración todo lo antes mencionado, se puede decir que una falla en la infraestructura de TI, es cualquier falla computacional ya sea no intencional o intencional (ejemplo: Ciber ataque) que afecte el funcionamiento normal de una empresa.

Entre las fallas más comunes, una de las destacadas es la falla de red y la seguridad es ahora parte fundamental de las redes de datos, según señala Cisco Networking Academy, ella envuelve un conjunto de protocolos, tecnologías, dispositivos, herramientas y técnicas para asegurar y mitigar los posibles ataques a las redes de datos.

4.1.7. Cortafuegos o Firewall

Para Stalling (s.f), “Los cortafuegos son un medio de protección eficaz para los sistemas basados en las redes de datos, mientras simultáneamente proporcionan acceso al exterior de dichas redes.”

Las principales características de un firewall, según Stalling (s.f), son:

- Todo tráfico entrante y saliente debe pasar a través del cortafuego, esto se consigue bloqueando todos los accesos restantes a la red local, excepto al cortafuego.
- Solo se permitirá el tráfico autorizado, previamente definido por la política de seguridad
- El propio cortafuego debe ser inmune a la penetración.

Es importante hablar sobre la Gestión de la red, usuarios, hardware, software, monitorización de la red y su gestión, tratamiento de alarmas y los informes.

Gestión de Red

Son capaces de controlar, administrar y monitorizar las redes y los dispositivos de interconexión, surgieron como necesidad debido a los niveles de complejidad que han alcanzado las redes, el objetivo es la administración de red.

Gestión de Usuarios

Es la actividad referida a la creación y mantenimiento de cuentas de usuarios, así como la asignación de recursos y mantenimiento de la seguridad en los accesos a la red.

Gestión de Hardware

Actividad que asegura la capacidad de los equipos para cubrir las necesidades de los usuarios, una vez que la información de inventario es recopilada se administra este equipo en la red.

Gestión de Software

Permite a la administración de red determinar si las aplicaciones necesarias se encuentran instaladas y en que equipos de la red se encuentran localizadas.

Monitorización de la actividad de la red

Indica el funcionamiento básico de las herramientas de monitoreo.

Tratamiento de Alarmas

Es necesario comprobar que las fallas de la red generan las alarmas adecuadas.

4.1.8. Corrección de fallas de seguridad informática

La tecnología se ha desarrollado para producir y medir la confianza de los sistemas y esta confianza puede incrementarse de cinco formas según Javier Areitio (2008).

- Aplicando soluciones técnicas con la menor complejidad posible.
- Utilizando componentes más confiables.
- Realizando una arquitectura que limite el impacto de posibles penetraciones, limitando bien la extensión de una vulnerabilidad, o bien implementando capacidades de detección y recuperación.
- Integrando la tecnología en el contexto del entorno operacional.
- Aprovechándose de las contramedidas no técnicas.

4.1.9. Implementación de VLANs

Según Cisco, Una Virtual LAN (VLAN[2]) es una división lógica del dominio de Broadcast a nivel de la Capa 2 del modelo OSI[3]. También podemos decir que una VLAN es una agrupación lógica de dispositivos que se pueden comunicar en sí.

[2] VLAN: Red de Área Local Virtual
[3] OSI: Organización Internacional de Normalización

Mediante la tecnología de VLAN, se puede agrupar los puertos de conmutadores y sus usuarios conectados en grupos de trabajos lógicamente definidos.

Con el objetivo de:

- Mayor flexibilidad en la administración y en los cambios de la red, ya que la arquitectura puede cambiarse usando los parámetros de los conmutadores.
- Aumento de la seguridad, ya que la información se encapsula en un nivel adicional y posiblemente se analiza.
- Disminución en la transmisión de tráfico en la red.

Se describen funcionamientos de la VLAN con respecto a la red LAN:

- Las VLAN funcionan en la capa 2 y la capa 3 del modelo de referencia OSI.
- La Comunicación entre las VLAN es implementada por el enrutamiento de capa 3.
- Las VLAN proporcionan un método para controlar la difusión en la red.
- El administrador de la red asigna puertos a una VLAN.
- Las VLAN pueden aumentar la seguridad de la red, definiendo cuales son los nodos de red que se pueden comunicar entre ellos.

4.1.10. Filtrado de paquetes y Control del acceso y modelos de seguridad

Existen distintos tipos de herramientas de filtrado de contenidos Web, las cuales están desarrolladas para evitar el abuso de los accesos de Internet dentro de las instituciones provocado en ocasiones por los usuarios que acceden a contenidos no apropiados, o que realizan constantemente descargas de gran tamaño, juegos, música, etc., consiguiendo como consecuencia riegos de seguridad, disminución de la productividad de los usuarios, empleo del tiempo en actividades no relacionadas con el trabajo, riesgos legales, gran consumo del ancho de banda de

Internet originando lentitud en el acceso a Internet o a los recursos de la red para el resto de los usuarios, entre otras.

El Filtrado de Paquetes y reglas de políticas de control de acceso está basados en los siguientes criterios:

- Protocolos utilizados.
- Dirección IP de origen y de destino.
- Puerto TCP-UDP de origen y de destino.

Estos criterios, permiten gran flexibilidad en el tratamiento del tráfico, además se puede tener control con otro de los dispositivos de la red como son los Switches, usando los siguientes modelos de seguridad.

- ***Port Security****, según Cisco,* es una función en los *Cisco Switch* destinada a limitar la cantidad de direcciones *MAC* que se pueden conectar a través de un puerto.
- **Lista de Control de Acceso**, según Wikipedia define lista de control de acceso o ACL[4] (del inglés, access control list) es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

Las ACL permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición.

[4] ACL: Listas de Control de Acceso

***MAC**,* control de acceso mandatario. Las reglas incluidas en el sistema deciden sobre los accesos y gobiernan el principio del propietario. Este modelo también se denomina control de acceso basado en reglas, (Areitio, 2008).

4.1.11. Correcciones en las Aplicaciones

Según Villalobos (s.f), en su artículo sobre Principios básicos de seguridad en bases de datos, menciona que la gran mayoría de los datos sensibles del mundo están almacenados en sistemas gestores de bases de datos comerciales tales como Oracle, Microsoft SQL Server entre otros, y atacar una base de datos es uno de los objetivos favoritos para los criminales.

Este autor, sugiere que para evitar ataques en las bases de datos es necesario identificar la sensibilidad, es decir que no se puede asegurar lo que no se conoce. En este sentido, se debe implementar evaluación de vulnerabilidades para luego aplicar un endurecimiento, monitorear, implementar pistas de auditorías en la Base de Datos.

4.1.12. Active Directory

Active Directory (AD[5]), son los términos que utiliza Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. AD principalmente se base en LDAP, DNS, DHCP[6] y kerberos los cuales se describen un poco a continuación:

[5] AD: servidor de Directorio Administrativo
[6] DHCP: El protocolo de configuración dinámica de host

Lightweight Directory Access Protocol (LDAP)

Protocolo ligero de acceso a directorios (LDAP[7]), hacen referencia a un protocolo a nivel de aplicación que permite acceder a un servicio de directorios ordenado y distribuido para buscar diversa información en un entorno de red, LDAP se aloja en una base de datos en donde se realizan cambios, consultas y peticiones administrada a través de una interface gráfica como gestor o línea de comando, un conjunto de objetos, atributos organizados en una manera lógica y jerárquica es el árbol de LDAP.

En la actualidad las implementaciones de LDAP son basadas sobre Sistemas de nombres de dominios o DNS para estructurar los niveles más alto de jerarquía, conforme se desciende en el directorio pueden topar con dispositivos, personas, computadoras, dispositivos de red y/o aplicativos.

Domain Name System (DNS)

El sistema de nombres de dominio (DNS[8]), es un sistema de nomenclatura jerárquica para los equipos de cómputo, así sea un servicio o cualquier otro recurso conectado a una red distribuida.

El sistema gestiona la información y la asocia con un nombre de dominio asignado a cada uno de los dispositivos. La función más crítica de un DNS es traducir o resolver nombres inteligibles para las personas en identificadores binarios asociados con los equipos de una red.

Kerberos

Es un protocolo de autenticación de redes de computadoras, este permite a dos computadoras en una red insegura demostrar su identidad mutuamente de

[7] LDAP: Protocolo ligero de acceso a directorios
[8] DNS: Sistema de nombres de dominio

manera segura, kerberos se basa en criptografía de clave simétrica y requiere un tercero de confianza, además existe extensiones de protocolo para poder utilizar criptografía de clave asimétrica.

Sin embargo, hay una serie de configuraciones para la implementación del Servidor Active Directory como:

- Copias de seguridad para recuperación de desastres.
- Auditoria de acceso a Active Directory.
- Configuración de políticas de contraseñas y bloqueo de cuenta.
- Restricción del escritorio de usuario.
- Tipos de actualizaciones.
- Administración centralizada de actualizaciones.

4.1.13. Cultura de Seguridad

El INCIBE, expresa lo siguiente sobre la Cultura de Seguridad informática. “Concienciamos en materia de prevención de riesgos laborales a nuestros empleados, también es importante concienciarles y formarles en materia de ciberseguridad […] esta formación en ciberseguridad creará una cultura de seguridad en la empresa que servirá para establecer las bases de la protección, tanto de nuestra información confidencial, como la de nuestros clientes y proveedores.”

Por lo que al fomentar el desarrollo de esta cultura de seguridad formando a los usuarios los cuales tenga siempre presente las políticas, normativas y procedimientos de seguridad establecidos en la institución, sin olvidar la supervisión de que se cumplan las buenas prácticas en seguridad y realizando

una constante sensibilización y concientización en seguridad se estará fortaleciendo la seguridad en la institución.

4.1.14. Estándar ISO 27001:2013

Según la norma ISO 27001:2013, “El sistema de gestión de seguridad de la información preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y da confianza a las partes interesadas que los riesgos se gestionan adecuadamente.”

La norma ISO 27001-2013, es una norma que puede ser utilizada tanto a lo interno como a lo externo para evaluar la capacidad de la organización de que, si cumple con los requisitos de seguridad establecidos en ella, por lo que es importante que toda organización que tenga como marco de referencia la norma, es decir que el sistema de gestión de seguridad de información sea parte integral de los procesos y estructura organizacional.

Por lo tanto, la filosofía principal de la norma ISO 27001-2013, se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente como se muestra en la siguiente figura 3

Figura 3: Estructura de ISO 27001

Fuente: Dejan Kosutic - Advisera

Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (software y equipos). Sin embargo, en la mayoría de los casos, ya tienen todo el hardware y software, pero se utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001-2013, estará relacionada con determinar las reglas organizacionales necesarias para prevenir violaciones de la seguridad.

El estándar ISO 27001-2013, fue elaborado para proveer un modelo para el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora del Sistema de Gestión de Seguridad de Información (SGSI) teniendo en cuenta la estructura organizativa, las políticas, procedimientos y los recursos de una organización.

El SGSI basado en ISO 27001-2013, permite prevenir o reducir eficazmente el nivel de riesgo mediante la implantación de los controles adecuados, preparando la organización ante posibles emergencias, garantizando la continuidad del negocio. Por otro lado, podemos ver el SGSI que propone la Norma ISO 27001-2013, puede resumir las siguientes fases que se detallan en la figura 4:

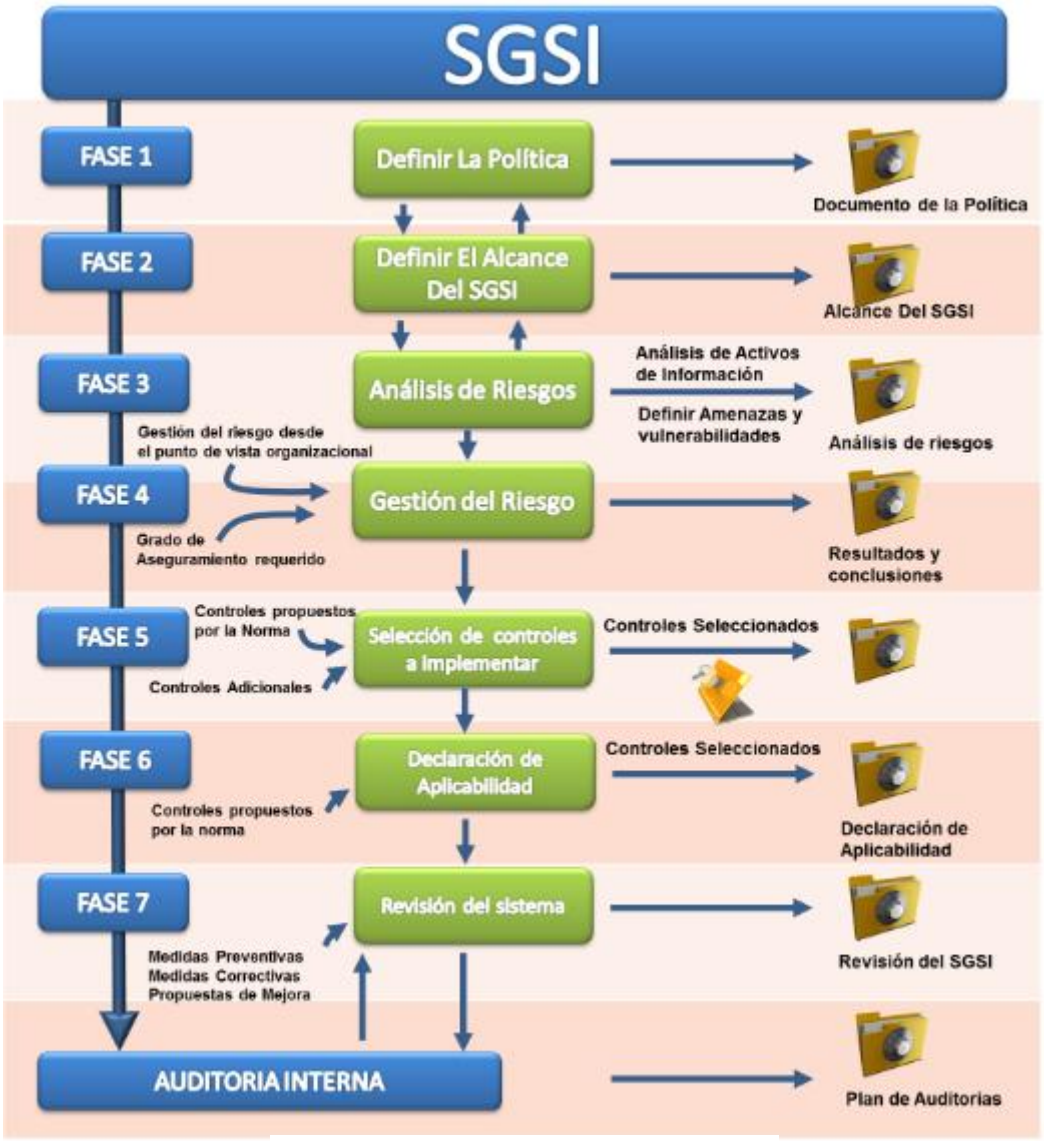


Figura 4: Fases del SGSI – ISO 27001

Fuente: normas-iso.com

De acuerdo a la ISO 27001-2013, se trabajó un Checklist para determinar la seguridad de los controles, ver anexo 3.

La información es uno de los bienes más preciados y de mayor importancia para las organizaciones. En un mundo súper conectado como en el que vivimos, están expuestas a amenazas para la Seguridad de la Información a gran escala y cibera taques destructivos, al margen de su volumen, sector o ubicación geográfica.

Cuando no existen una gestión ni mantenimiento adecuados de los sistemas de seguridad de la información, se corren el riesgo de sufrir graves pérdidas económicas y de que la imagen se deteriore.

Asegurar de que se ha instaurado los controles adecuados para mitigar el riesgo que suponen las amenazas graves para la seguridad de los datos y evitar que se aprovechen los puntos débiles del sistema, ha dejado de ser opcional.

5. DISEÑO METODOLOGICO

En esta investigación se plantearon objetivos metodológicos que a continuación se describe tabla 1:

Objetivo General	Objetivos Específicos	Objetivos metodológicos
Desarrollar una propuesta de optimización de la infraestructura de seguridad de la Asociación de Municipios de Nicaragua.	Realizar un diagnóstico de la Infraestructura Tecnológica de AMUNIC para la identificación de los riesgos asociado a los servicios.	Realizar evaluación de seguridad a la infraestructura de AMUNIC. Implementar Checklist basado en el estándar ISO 27001:2013.
	Proponer controles de seguridad óptimos para la mitigación de los riesgos.	Mejorar los procedimientos de control de seguridad existentes. Proponer la implementación de controles que mitiguen los riesgos.
	Elaborar un plan de implementación de la Infraestructura de Seguridad con estimaciones de costos.	Elaborar un plan de implementación de la infraestructura tecnológica con estimaciones de costos para AMUNIC

Tabla 1: Objetivos Metodológicos

Fuente: Propia

Con este diseño metodológico obtendremos la información que se desea con el fin de responder al planteamiento del problema como lo dice Sampieri en su libro

de Metodología de la Investigación. Por lo que describiremos una serie de elementos y características del estudio a realizar.

De acuerdo al objetivo de investigación, naturaleza del problema, el presente estudio reúne las condiciones suficientes para ser calificado como una *"Investigación Aplicada"*. Es no Experimental.

5.1. Descripción del diseño de la investigación.

No experimental, se basa fundamentalmente en la observación de fenómenos tal y como se dan en su contexto natural para analizarlos con posterioridad.

Por otro lado, la metodología que se usará para proponer los controles de seguridad en la red interna de AMUNIC estará basados en el estándar ISO 27001- 2013 y la metodología MAGARIT.

5.1.1. Descripción del tipo de investigación

Es descriptiva porque, se describirá la situación actual de la problemática (Infraestructura Tecnológica de Seguridad), evaluando a través de un diagnostico las vulnerabilidades que serán parte de los datos a ser recolectados para su posterior análisis.

La dimensión de la investigación usara el método analítico, ya que, mediante la descripción de la situación actual, se permitirá evaluar los dispositivos de red, los servicios y aplicaciones de Infraestructura Tecnológica de Seguridad para

adecuarlos de manera óptima y que estos sean considerados dentro de las políticas de seguridad a ser implementadas en el Active Directory.

5.1.2. Enfoque de Investigación

El enfoque de la investigación será mixto, cualitativo y cuantitativo:

Según Sampieri (2014), Cuantitativo porque consiste en utilizar la recolección y el análisis de datos para contestar preguntas de investigación y probar la hipótesis establecida previamente, y confía en la medición numérica, en el conteo para establecer con exactitud patrones de comportamiento en una población. Se tomará el enfoque cualitativo porque se pretende obtener la recolección de datos para conocer o medir el fenómeno en estudio y encontrar soluciones para la misma; la cual trae consigo la afirmación o negación de la hipótesis establecida en dicho estudio.

5.2. Delimitación y definición de la población de estudio

Para analizar la situación real será necesario entrevistar al responsable de informática para conocer la situación actual. La investigación se hará en usuarios de la Dirección Administrativa Financiera y directores de las áreas y unidades de la Institución.

5.2.1. Población y Muestra

Población:

La población de esta investigación comprende todos los usuarios de la institución, 30 usuarios entre personal de apoyo, técnicos y directores.

Muestra:

Analizaremos áreas sensibles donde están los técnicos y directores, siendo esto una muestra por oportunidad la cual contemplan 12 personas.

5.2.2. Unidad de análisis o muestreo:

Definiremos la Dirección Administrativa Financiera y los directores, como usuarios que ofrecerán una gran riqueza para la recolección y el análisis de los datos para dar respuesta a la problemática.

Se aplicaran criterios para seleccionar muestra de estudio utilizando fuentes de información.

5.3. Descripción de fuentes de información

La investigación según los medios, será de tipo Campo pues se apoyará en información que proviene de entrevistas, cuestionarios y observación, Se establece un plan, según Sampieri en su libro de metodología, para la recopilación de los datos que expresan el tipo de información, los instrumentos que se usaran, ver figura 5.

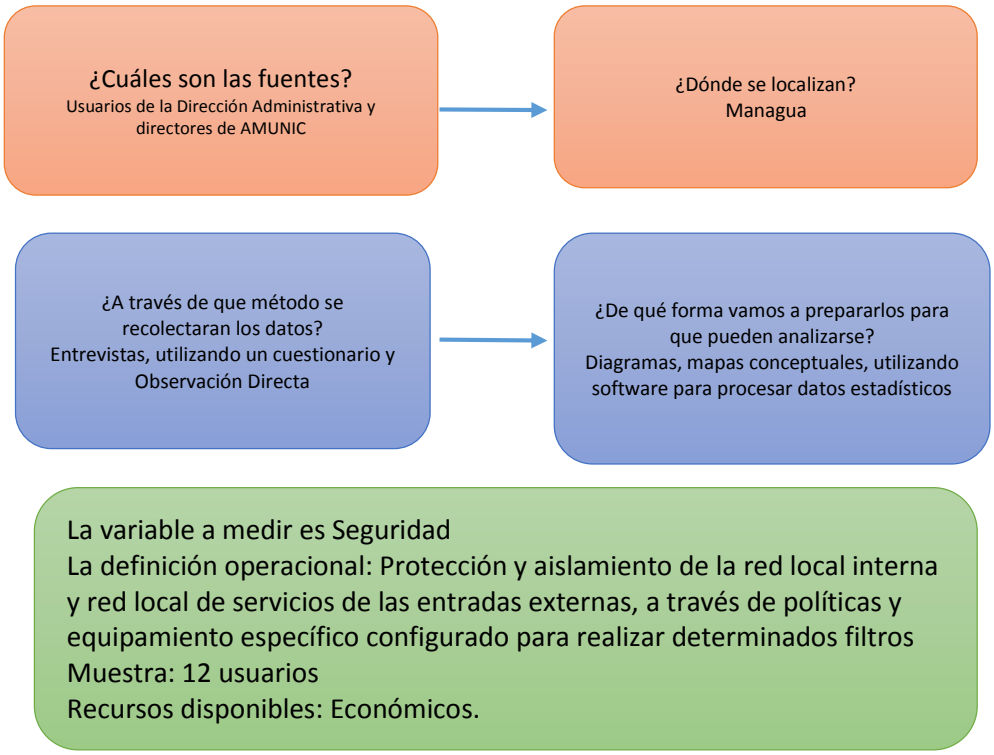


Figura 5: Descripción de las Fuentes de Información

Fuente: Propia 2018

Esta muestra representa el 100% de los usuarios del SIAFP y los directores de áreas y unidades de la institución.

5.3.1. Instrumentos de Recolección de datos

Entrevistas

Sampieri (2014), ilustra el proceso cualitativo del instrumento de la entrevista el cual se aplicará como se describe en la figura 6.

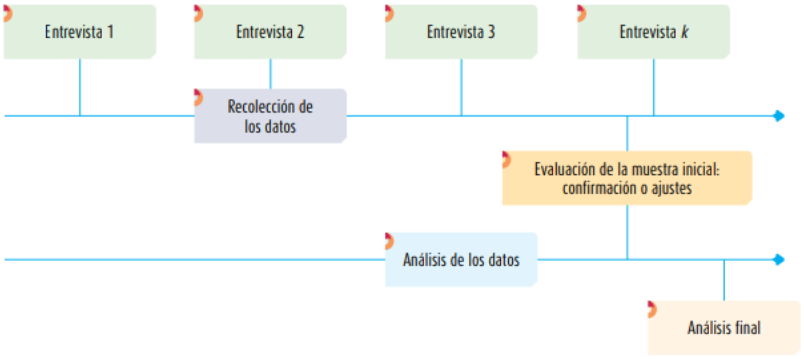


Figura 6: Proceso cualitativo de la entrevista

Fuente: Sampieri, 2014

En el caso en particular se entrevistará, con el modelo de reloj de arena, a los usuarios de la unidad de análisis que se definió previamente en el universo, en ellas se tratara de obtener información referente a la problemática del uso de acceso a los servicios, además de la infraestructura de la red interna, UTM, configuración de los equipos, etc., ver cuestionario en anexo 1,4 y 5.

Observación Directa

Mediante esta técnica, se realizarán visitas a cada oficina para la revisión de la configuración de los dispositivos de red, servidores y UTM.

5.3.2. Variables

Variable Dependiente: Seguridad de la Información e informática

Indicadores:

- Propuesta de segmentación de VLANs
- Configuración de UTM a nivel básico
- Implementación de Servidor AD
- Valoración infraestructura
- Percepción del usuario ante el problema original
- Documento que contemple las medidas de control de seguridad

Definición Conceptual y operacional de la variable:

Variable	Definición conceptual	Definición Operacional	Dimensión	Indicador	Instrumento
Seguridad	Preservar las características de confidencialidad, integridad y disponibilidad de la información, y protección de los sistemas de información e infraestructura tecnológica para lograr el mejor desempeño	Protección y aislamiento de la red LAN, a través de políticas de acceso y equipamiento especifico configurado para realizar determinados filtros	Cumple con el proceso de Seguridad	Propuesta de segmentación de VLANs	Evaluación de Seguridad Informática Interna
				Configuración de WebFiltering y Antispam del UTM a nivel básico	
				Implementación de Servidor AD	
			Diagnóstico	Valorar los riesgos de activos y servicios de la infraestructura tecnológica	Entrevistas
				Percepción del usuario ante el problema original	
			Control	Diseñar Controles de seguridad	Evaluación de Seguridad Informática Interna

Tabla 2: Definición Conceptual y Operacional de Variable

Fuente: Propia

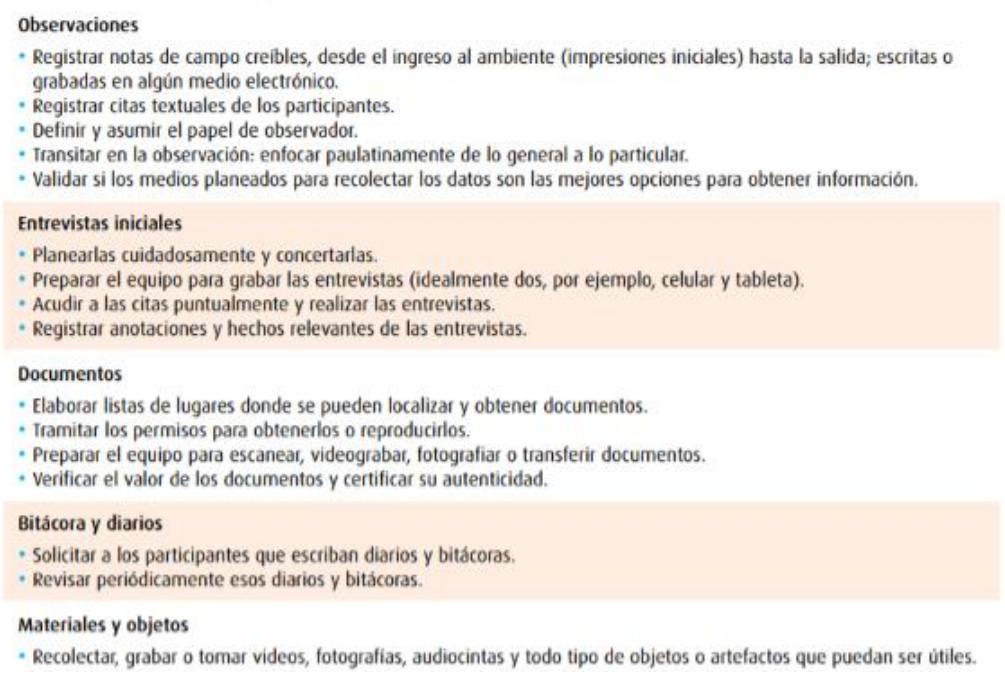
La aplicación de estos indicadores permitirá gestionar una Infraestructura Tecnológica de Seguridad básica a nivel interno de manera integral.

5.3.3. Procedimiento y procesamiento de la recopilación de la información.

Según Giraldo. (s.f), “El procesamiento de la información tiene como fin generar datos agrupados y ordenados que faciliten al investigador el análisis de la información según los objetivos, hipótesis y preguntas de la investigación construidas”.

Una vez que se utilicen los instrumentos para la recopilación de la información y siguiendo los procedimientos para aplicarlos como son las entrevistas, la observación se procesan los datos (dispersos, desordenados, individuales) obtenidos de la unidad de análisis que es parte esencial de la muestra objeto de estudio durante el trabajo de campo, y tiene como fin generar resultado (datos agrupados y ordenados), a partir de los cuales se realizará el análisis según los objetivos de la investigación a realizar.

Siguiendo un ejemplo dado por Sampieri (2014), sobre cómo debe ser el procedimiento en el caso de utilizar métodos como los que se aplicaran en esta investigación en la figura 7.



Observaciones

- Registrar notas de campo creíbles, desde el ingreso al ambiente (impresiones iniciales) hasta la salida; escritas o grabadas en algún medio electrónico.
- Registrar citas textuales de los participantes.
- Definir y asumir el papel de observador.
- Transitar en la observación: enfocar paulatinamente de lo general a lo particular.
- Validar si los medios planeados para recolectar los datos son las mejores opciones para obtener información.

Entrevistas iniciales

- Planearlas cuidadosamente y concertarlas.
- Preparar el equipo para grabar las entrevistas (idealmente dos, por ejemplo, celular y tableta).
- Acudir a las citas puntualmente y realizar las entrevistas.
- Registrar anotaciones y hechos relevantes de las entrevistas.

Documentos

- Elaborar listas de lugares donde se pueden localizar y obtener documentos.
- Tramitar los permisos para obtenerlos o reproducirlos.
- Preparar el equipo para escanear, videograbar, fotografiar o transferir documentos.
- Verificar el valor de los documentos y certificar su autenticidad.

Bitácora y diarios

- Solicitar a los participantes que escriban diarios y bitácoras.
- Revisar periódicamente esos diarios y bitácoras.

Materiales y objetos

- Recolectar, grabar o tomar videos, fotografías, audiocintas y todo tipo de objetos o artefactos que puedan ser útiles.

Figura 7: Procedimiento para la recopilación de la Información

Fuente: Sampieri, 2014

5.3.4. Tipos de análisis que se realizara a la información

El tipo de análisis que se realizara es uno de lo expresado por Sampieri (2014). Método Analítico, este método consiste en la extracción de las partes de un todo, con el objeto de estudiarlas y examinarlas por separado, para ver, por ejemplo, las relaciones entre éstas".

Además, una vez recopilado y ordenado los datos, usaremos escala de valores para luego analizarlas sistemáticamente, agruparlas e interpretarlas y obtener las conclusiones del estudio.

DESARROLLO

6. DIAGNOSTICO

En el presente capítulo, se desarrolla la Propuesta de Optimización de la Infraestructura de Seguridad de la Asociación de Municipios de Nicaragua (AMUNIC), la que parte de un análisis de los riesgos de los activos y vulnerabilidades de los controles existentes en la institución, mismos que están intrínsecamente relacionados a los servicios informáticos que brinda a sus socios internos y externos (Servidores públicos y Autoridades locales).

De manera particular, el diagnóstico técnico de la infraestructura tecnológica, presenta las amenazas, vulnerabilidades y los riesgos de los activos y servicios de AMUNIC y como pueden impactar sobre la información sensible (data) que se administra cuando no se tienen los controles mínimos de seguridad. Para llegar a determinar estos aspectos se utilizó la metodología MAGERIT y aspectos de la ISO 27001-2013.

El diagnóstico presenta una radiografía de los riesgos a los que se expone la institución, por lo que resulta fundamental desarrollar una Propuesta de Optimización de la Infraestructura de Seguridad que tenga como esencia los controles de seguridad de los activos y servicios.

Sin embargo, para la implementación de la Optimización de la Infraestructura Tecnológica es fundamental realizar inversión de carácter técnica y humana, es decir que AMUNIC debe destinar un presupuesto anual para la adquisición de equipos, licencias, selección y contratación de personal para implementar la propuesta.

6.1. Diagnóstico de la infraestructura tecnológica de AMUNIC

Para el desarrollo del diagnóstico de la infraestructura tecnológica se utilizaron entrevistas al 100% de la muestra seleccionada (12 personas), entre ellas, el personal que administra el Sistema Integral Administrativo Financiero y de Planificación (SIAFP) y observación directa de las instalaciones (cuarto de servidores). La observación consiste en la revisión y aplicación de manuales administrativos, diagrama de red y levantamiento de inventario de equipos informáticos. A continuación, se detallan las fuentes de las cuales se obtuvo información:

Fuentes de información:

- Emilce Pineda: Directora Administrativa Financiera
- Freddy Domínguez: Contador General
- Adilia López: Auxiliar Contable
- Uvania García: Responsable de Bodega
- Arlen Jiménez: Asistente Administrativa
- Fanny Arguello: Responsable de Recursos Humanos
- Octavio Laguna: Responsable de Planificación y Comunicación
- Karina Vílchez: Responsable de informática
- Roberto García: Director de Unidad Ambiental
- Norman Corea: Responsable de Unidad de Adquisiciones
- Nubia Luna: Directora Ejecutiva
- Adonis Hernández: Director de Asesoría Económica

La responsabilidad en la ejecución de los controles correctivos y preventivos es compartida por la Unidad de Informática, la Dirección Administrativa Financiera y Dirección Ejecutiva. Sin embargo, la decisión de aprobar la implementación de los controles es responsabilidad de la máxima autoridad administrativa (Dirección Ejecutiva).

6.1.1. Criterios de preguntas a realizar en las entrevistas

El resultado del análisis de riesgo tiene como finalidad la recolección de información. Para la recolección de información se aplicaron técnicas de observación, revisión de documentación, reuniones, consultas y preguntas de entrevistas las que se observan en el formato de los anexos 1, 4 y 5.

Las entrevistas realizadas a la Unidad de Informática y demás áreas de la institución, tuvieron como base los controles detallados en los dominios de la ISO 27001-2013. A continuación, se detalla en forma general los criterios para la identificación de vulnerabilidad sobre las cuales se elaboraron las entrevistas, las cuales están incluidas en el anexo 3 y 5.

Criterios de seguridad para las preguntas de entrevistas de la Unidad de Informática.

- Existencia de Manual de Política de Seguridad de la Información.
- Periodos de actualización del Manual de Política de Seguridad de la Información.
- Socialización del Manual de Política de Seguridad de la Información.
- Existencia del área o responsable de seguridad informática.
- Herramientas de seguridad implementadas.
- Existencia de procedimientos e instructivos propios del área.
- Periodos de actualización de los procedimientos e instructivos.
- Participación y apoyo de las máximas autoridades de la empresa.
- Concientización al personal acerca de temas de seguridad de la información.
- Perfiles y roles de usuarios.
- Clasificación de la información.
- Controles y políticas de seguridad implementadas en la empresa.
- Mecanismos de autenticación.

- Gestión de contraseñas en los diferentes aplicativos.
- Infraestructura tecnológica.
- Software malicioso.
- Mantenimiento de equipos tecnológicos.
- Inventarios tecnológicos.
- Respaldo de información.
- Incidentes de seguridad.
- Plan de contingencia.

Criterios de seguridad para las preguntas de entrevistas en las demás áreas

- Conocimiento acerca del tema de seguridad de la información y seguridad informática.
- Existencia de procedimiento e instructivos propios del área.
- Periodo de actualización de los procedimientos e instructivos.
- Conocimiento de un responsable de seguridad en la Institución.
- Identificación y categoría de los activos de información de cada área.
- Incidentes o eventos de seguridad.
- Control de acceso mediante mecanismos de tarjeta de acceso, llaves entre otros.
- Responsable de solicitar acceso a los diferentes aplicativos y módulos de acuerdo a lo que se utiliza en cada área.
- Concientización en temas de seguridad de la información.
- Importancia de la aplicación de controles de seguridad dentro de la institución.
- Detección de vulnerabilidades de seguridad en los aplicativos.

6.1.2. Resultado de las entrevistas - Situación Actual

De acuerdo a los resultados obtenidos en las diferentes entrevistas realizadas a los usuarios de AMUNIC; así como la utilización de técnicas como la observación

y entrevistas descritas en la metodología, se pudo identificar el estado actual de la institución, referente a temas de seguridad de la información e informática, basado en los controles de la norma ISO 27001-2013 y aspectos de las Normas Técnicas de Control Interno.

Resultados obtenidos de la observación directa

Basado en consultas y revisión de documentos

Políticas de seguridad:

- El 33% de las Áreas y Unidades de AMUNIC, cuenta con procedimientos e instructivos elaborados y aprobados acorde a las Normas Técnicas de Control Interno de la Contraloría General de la República (Unidad de Adquisiciones y Dirección Administrativa Financiera), ver anexo1.

- Mediante entrevistas practicadas a los usuarios y a la Dirección Ejecutiva, reconocen la importancia de asumir compromisos para la implementación de controles de seguridad, anexo 1.

Organización de la seguridad de la información:

- La Unidad de Informática es la responsable de implementar los controles de seguridad aprobados por la Dirección Ejecutiva.

- El responsable de la Unidad de Informática es el encargado de Redes y Base de datos y de la seguridad de estas, es además el responsable de la administración de accesos a los diferentes aplicativos que utilizan los usuarios, por tal razón se la considera como el Responsable de Seguridad Informática, pero no realiza ninguna actividad acorde a la gestión de seguridad de la información, ni ninguna función propia de este cargo, no

existen la definición de actividades a cumplir con respecto a seguridad de la información.

- El 58% de la muestra encuestada de los usuarios tienen la certeza de que cuando se habla del área Seguridad Informática o Seguridad de la Información se están refiriendo a la Unidad de Informática o área de Sistemas, pues se piensa que esta realiza las mismas actividades, y lo único que cambia es el nombre, ver anexo 1.

- El área de Recursos Humanos incluye en el contrato de los usuarios una cláusula que indica que el trabajador se compromete expresamente a guardar confidencialidad y reserva de la información, pero esta cláusula no tiene la relevancia suficiente pues los usuarios no recuerdan que exista ese compromiso de confidencialidad de la información que están manejando.

Gestión de Activos:

- AMUNIC cuenta con inventarios de equipos de computación y dispositivos de almacenamiento, lo cuales son actualizados por la Unidad de Informática y el responsable de Activo Fijo cada vez que se adquiere un nuevo equipo o dispositivo, además de realizar las actualizaciones de inventario anuales.

- El 100% del personal de AMUNIC tienen documento formal donde se indica que tipo de documentación y activo asociado está asignado, en el que estable las responsabilidades con respecto a los activos de equipos de cómputos y dispositivos almacenamientos.

- No se encuentran definidos criterios para la clasificación de la información y manejo de la información, por lo que las áreas no cuentan con un catálogo de clasificación de la información, el cual les permita determinar qué

información es confidencial o de uso interno, está en dependencia de su criterio.

Seguridad de los Recursos Humanos:

- El responsable de Recursos Humanos posee documentación donde se definen las funciones y responsabilidades de los empleados, y realiza el proceso de contratación de nuevos empleados siguiendo los procesos establecidos por la Institución y siguiendo las leyes de contrataciones correspondientes.

- En la revisión de la documentación de recursos humanos se apreció que en los contratos con empleados, contratistas y terceros se incluyen responsabilidades y obligaciones que se deben cumplir en el trabajo o servicio a realizar dentro de la Institución y acorde a las políticas de la misma, pero no incluye las responsabilidades y obligaciones que deben tener en referencia a la seguridad de la información.

- No existe un procedimiento que indique las sanciones en caso de faltas cometidas por los usuarios en la seguridad de los sistemas de procesamiento de información o información física que manejan o manejo incorrecto de los dispositivos tecnológicos; en las políticas internas de AMUNIC no se contemplan.

Seguridad Física y Ambiental:

- AMUNIC tiene instalaciones de una sola planta, para el acceso se tiene un área de vigilancia quien revisa, anota y dirige a las personas a recepción para el ingreso al área o unidad que visita, por lo que se tiene control del ingreso, además de contar con sistema de cámaras.

- No existen detectores de humo, ni alarmas contra incendios en la Institución. Hay extintores en los pasillos y un extintor cerca del cuarto de servidores.

- Las áreas y unidades no se pueden identificar fácilmente, pues no cuentan con el señalamiento apropiado.

Gestión de las Comunicaciones y Operaciones:

- AMUNIC en dependencia del tipo de información designa a una persona como responsables de llevar la documentación externa, asegurándose que la documentación enviada llega al destino indicado. Se lleva un registro donde constan las firmas de las personas externas que recibieron la documentación.

Control de acceso:

- No existe implementado mecanismo que permita bloquear automáticamente las estaciones de trabajo cuando se encuentran desatendidas. Solo el 25% de los usuarios de la muestra entrevistada tiene activada la opción de bloqueo en las computadoras, el 75% de los usuarios no realizan el bloqueo cuando necesitan salir de su puesto de trabajo o no están utilizando el equipo ver anexo 1.

- En los puestos de trabajo se observó que están llenos de documentación sin archivar y muchas veces son documentos confidenciales, a pesar de ello la mayoría de usuarios considera que se guarda la información pertinente para evitar su daño o pérdida en los gabinetes con llaves una vez que la utilizan.

Cumplimiento:

- Todo cumplimiento de responsabilidades y obligaciones dentro de la Institución está relacionado a las normas y política de la Institución, la cual contempla requerimientos legales. No poseen lineamientos de seguridad que eviten incumplimiento por la reproducción, copia o alteración de

información sobre la cual la Institución no tiene derecho de autor, pudiendo esto ocasionar incumplimientos con la ley.

Resultados obtenidos de la entrevista realizada a la Unidad de Informática

Políticas de seguridad:

- Según resultados obtenidos de la aplicación de la entrevista a la Unidad de Informática, ubicada en anexos 3, 4 y 5, AMUNIC ha implementado algunos controles de seguridad, pero, no están documentados ni establecidos en ningún Manual de Políticas de Seguridad de la información.

Organización de la seguridad de la información:

- No existe un Comité de Gestión de Seguridad ni responsable de seguridad de la información que se encargue expresamente de la toma de decisiones referentes a implementaciones de controles y herramientas que permitan mejorar la seguridad de la información.

- Debido a que los equipos de red no son administrables por su antigüedad, no es posible establecer un monitoreo constante de la red.

- La Unidad de Informática es quien se encarga expresamente de la redacción de los términos de referencia para la contratación de personal técnico externo (mantenimientos de equipos, entre otros), en el que incluye un acuerdo de confidencialidad y no divulgación de la información que vaya a ser manejada por proveedores o contratistas.

Gestión de Activos:

- La Unidad de Informática poseen documento donde se detallan las licencias utilizadas para cada servidor y equipo. Actualmente se utilizan dos sistemas operativos en los equipos de cómputo Windows 7 y Windows 10.

- La Unidad de Informática no poseen controles referentes al uso de correo electrónico institucional, equipo de cómputo e internet. Sin embargo, se tienen restricciones conforme a las actividades que desempeña cada usuario, pero estas no están documentadas.

Seguridad Física y Ambiental:

- En el caso de cuarto de servidores (datacenter) a este solo tiene acceso el responsable de informática y las personas que este autorice, por otro lado, llaves del datacenter es centralizada, solo tiene acceso la Dirección Administrativa Financiera (DAF) y la Unidad de Informática por ser considerada un área restringida.

- La Unidad de Informática administra el sistema de cámaras como parte de los controles de seguridad física y reporta a la Dirección Ejecutiva.

- El Rack de comunicaciones, así como las UPS se encuentra dentro del cuarto de servidores, en un espacio físico separado, las llaves las tiene únicamente el responsable de informática y una copia DAF.

- Todos los equipos de red, perimetrales, servidores, DVR, planta telefónica están ubicados dentro del cuarto de servidores, de esa forma se intenta limitar los accesos no autorizados.

- Se cuenta con UPS que les permite tener energía eléctrica 20 minutos después que ocurre el corte de energía, lo que les permite a los usuarios guardar la información y apagar los equipos de cómputos para evitar daños.

- La Unidad de Informática realiza dos veces al año mantenimientos en los equipos de cómputo, y existe documentación donde se detallen qué tipos de mantenimientos se realizan.

- La Unidad de Informática es la responsable de la eliminación de información de las computadoras que fueron utilizados por usuarios que ya no laboran en la Institución, una vez respaldada y entregada copia a Dirección Ejecutiva.

Gestión de las Comunicaciones y Operaciones:

- La Unidad de Informática únicamente cuenta con documentación de respaldos, incluyendo los procedimientos de operación propia de la unidad, como lo son mantenimientos, instructivos o procedimientos de manejo de errores, documentación de recuperación del sistema en caso de fallas, entre otros.

- La Unidad de Informática realiza revisiones de los cambios realizados a los sistemas sean estos en sitio u outsourcing y versiones que se actualizan. El responsable de informática, indica que todos los cambios que se realizan en algún módulo del SIAFP son comunicados y coordinados en el área de Administración Financiera; antes de pasar producción se realizan las pruebas pertinentes para así poder garantizar que los cambios realizados no afectan la utilidad del sistema. Se encuentra documentado el proceso de “Gestión de Cambios”.

- La Unidad de Informática realiza anualmente análisis de la capacidad de los recursos utilizados, pues consideran las necesidades actuales y la vida útil de los recursos.

- No se tiene establecido criterios mínimos de seguridad en la aceptación y aprobación del uso de un sistema de información, los cuales deben ser aplicados antes de la puesta en producción de un nuevo servicio o actualización.

- La Unidad de Informática indica que todos los equipos de cómputo tienen instalado antivirus y garantiza que estos tengan actualizaciones automáticas.

- La gestión del correo es tercerizada por lo cual no se tiene control de spam a las cuentas de correo de los usuarios, por otro lado, en el Firewall existente módulo de Antispam licenciado y pero con pre configuración de proveedor.

- La Unidad de Informática realiza respaldos de información por lineamientos y funciones establecidas por la Dirección Ejecutiva, todos los respaldos son registradas en el documento de “Respaldos de información”, en la que se detalla responsable del respaldo, fecha, hora y nombre del área y usuario.

Control de acceso:

- La Unidad de Informática no posee política que establezca controles de seguridad para el control de accesos a los servicios y equipos de cómputo.

- En el caso de los módulos del SIAFP, la Unidad de Informática, realiza la instalación a solicitud de la Dirección Administrativa Financiera a los usuarios que indique de acuerdo a las funciones y responsabilidades.

- La red de la Institución no se encuentra segmentada, cada usuario de la red puede acceder libremente a las IP de los servidores y poder compartir y ver información sin restricción alguna.

- Existe red inalámbrica (wifi) que es utilizado por todo el personal, la cual posee seguridad básica, cualquier usuario que sepa la clave puede acceder a ella o compartirla sin quedar evidencia alguna.

- Todos los usuarios de la institución manejan como mínimo tres USER ID, los cambios de contraseñas son diferentes para cada aplicativo teniendo lo siguiente:

- Equipos de Cómputo: No pide cambio de contraseña
- Correo Institucional: No pide cambio de contraseña
- SIAFP: tiene usuario y contraseña generales y no pide cambio

Adquisición, desarrollo y mantenimiento de los sistemas de información:

- No existe una política institucional donde se determine los requerimientos de seguridad que deben ser exigidos para el desarrollo o adquisición de un software. Todo se centra en que el sistema funcione de acuerdo a lo que se necesita.

- Para la adquisición e implementación de un nuevo aplicativo la Unidad de Informática se encarga de realizar revisiones y pruebas que garanticen que la modificación, actualización o nuevo aplicativo funciona de acuerdo a las necesidades del usuario final.

- Únicamente el personal de desarrollo e implementación de Sistemas está autorizado a tener acceso al código fuente del sistema en caso de requerirse alguna modificación; previa aprobación de la Dirección Administrativa Financiera.

- Existe documentación formal donde se registran las actividades que se realizan en el Sistema Integral Administrativo Financiero (SIAFP) ya sea desarrollo, pruebas, capacitación y producción.

- No existe una política formal donde se detalla los controles a implementar para prevenir la fuga de información.

- No se realiza ninguna acción de monitoreo y control ante posibles vulnerabilidades técnicas de los sistemas, que permitan dar un trato adecuado a posibles nuevos riesgos de seguridad.

Gestión de incidentes en la seguridad de la información:

- AMUNIC no cuenta con documento de Política y procedimientos de Seguridad de Sistemas, en el que se indique “que ante la sospecha de que la contraseña que haya sido comprometida deberá notificar inmediatamente el incidente de seguridad a la Unidad de Informática, para proceder con el cambio de contraseña”.

- No están documentados los procedimientos para el manejo de riesgo de seguridad, en caso de que se llegue a presentar un incidente la única persona que da las indicaciones es el responsable de Informática.

- En el presente año (2019) se presentó incidente con el hardware firewall de la institución, este quedo inhabilitado de realizar sus funciones debido a un upgrade aplicado, el cual poseía bugs o fallas que causaron la falla total del equipo. Este incidente fue superado gracias al pronto soporte del proveedor y un nuevo hardware fue brindado en calidad de RMA (Return Merchandise Authorization, Autorización de Devolución de Mercancía), volviendo así a su funcionalidad regular y restaurando la seguridad perimetral a sus niveles originales.

- El 100% de los incidentes de seguridad registrados por la Unidad de Informática se ha presentado frecuentemente con el aplicativo SIAFP en el que se han realizado transacciones con errores y no se tiene identificado el usuario quien cometió el error, ya que se carece de implementación de roles en el sistema.

- El resto de incidentes registrados es cuando se quedan sin el servicio de Internet, ver anexo 1.

Gestión de la continuidad:

- En la Gestión de continuidad de la Institución referida a la parte informática no se tiene documentado ningún proceso o plan de continuidad. Sin embargo, si se tiene identificado cuales son los eventos que causan o podrían causar interrupciones en procesos normales y el impacto que puede tener la paralización de las actividades que conllevan la explotación de la vulnerabilidad.

- La Unidad de Informática realiza respaldo según la planificación aprobada en el año para proteger información sensible, en caso de daño de activos (Discos duros, equipo de cómputo, servidor, etc.) permitiendo de esa manera recuperarse en el menor tiempo posible y continuar con las actividades propias del negocio si se refiere a la información, y en el caso de daño de servidores se cuenta con otro equipo.

- En caso de los servidores, no se cuenta con el instructivo “contingencia servidores”. ante un posible problema o daño en uno o varios servidores.
  Nombre de Servidores:
    - Servidor de Base de Datos y aplicativo (SIAFP)
    - Servidor de Contingencia

Resultados obtenidos de las entrevistas realizadas a los Usuarios del SIAFP y directores.

Usuarios del Sistema Integral Administrativo Financiero y de las áreas y unidades, ver preguntas en el anexo 1.

Organización de la seguridad de la información:

- Todos los controles implementados actualmente no son objeto de monitoreo. Sin embargo, el 100% de los usuarios reportan los posibles problemas o incidentes que ocurran en sistema o servicio, de lo contrario

se asume que todo funciona correctamente y estos son notificados a la Unidad de Informática.

Gestión de las Comunicaciones y Operaciones:

- Cada usuario del Sistemas tiene claro cuáles son sus funciones y responsabilidades a cumplir de acuerdo al cargo que tienen y funciones adicionales que pueden ser encargadas por la Dirección Administrativa Financiera.

- Los usuarios del Sistema Integral Administrativo Financiero (SIAFP) manifestaron que no existe monitoreo de las transacciones realizadas en el sistema, siendo esto un inconveniente a la hora de detectar inconsistencias o errores en los procesos. El 83% de los usuarios consideran alto el nivel de importancia de tener monitoreo o pistas de auditoria de las transacciones realizadas, ver anexo 1.

- El 100% de los responsables de áreas y unidades manifiestan que no existe control sobre el bloqueo de los medios removibles en los equipos de cómputos de los usuarios, lo que es una amenaza de fuga de información, y no se realizan ningún tipo de monitoreo que garantice que no se fugue dicha información.

Control de acceso:

- El 100% de los usuarios del Sistema Integral Administrativo Financiero (SIAFP), utilizan contraseñas para acceder al sistema con longitud máxima de 3 caracteres, y son del conocimiento de todos, en especial de aquellos que hacen uso del mismo módulo, antes los incidentes de transacciones erradas no se tiene certeza de quién utilizó o registró la transacción.

- El 100% de los usuarios para otras contraseñas usan un mínimo 6 caracteres las cuales son establecidas por ellos mismos, estas son

utilizadas para el acceso a sus equipos y aplicativos y no guardan la confidencialidad debida de sus contraseñas, pues de vez en cuando las comparten con sus compañeros.

- Todos los responsables de áreas y unidades dicen almacenar información impresa confidencial y cuentan con la seguridad física requerida, pues la información no se encuentra accesible para cualquier usuario.

Gestión de incidentes en la seguridad de la información:

- Ante los incidentes de seguridad, el 54% notifica directamente a la Unidad de Informática, 38% notifica a su jefe inmediato para que sean ellos los encargados de comunicar a Informática para resolver el inconveniente con el área pertinente y 8% a Dirección Ejecutiva. Anexo1.

Gestión de Activos:

- En base a la observación y resultado de las entrevistas a los responsables de áreas y unidades, la gestión de los archivos de información física no utiliza ningún criterio de etiquetado y manejo de la información, pues se archiva la información de acuerdo a las necesidades de cada persona, solo ciertas carpetas cuentan con el nombre que hace referencia a lo que contiene.

Seguridad de los Recursos Humanos:

- La máxima autoridad administrativa tiene conocimientos en temas relacionados con la seguridad de la información e informática, además de conocer de la existencia de los controles implementados para mitigar incidentes.

- La Dirección Administrativa Financiera es la responsable del control de Activos, cuentan con procedimientos donde indica que antes del término de contrato laboral deben devolver los activos fijos que se les ha entregado al

inicio de sus labores. Cada jefe de área o unidad o la persona que designe Dirección Ejecutiva se encarga de recibir los materiales de oficinas utilizados por el usuario, para tener la certeza de que aquellos materiales de oficina que son devueltos sean los mismos que se le asignaron al inicio de las labores y estén en buen estado.

Seguridad Física y Ambiental:

- El 100% del personal de las áreas y unidades, en especial los directores entrevistados tienen conocimientos de que está prohibido sacar equipos de propiedad de la Institución, salvo autorización de Dirección Ejecutiva, y el único control referido a seguridad es la revisión del personal de seguridad y hoja de salida de equipo, formato que maneja la Dirección Administrativa Financiera, esta medida está dentro de la política interna y manejo de activos, y los únicos autorizados para sacar equipos en este caso laptops de manera permanente son los responsables de áreas y unidades por temas de reuniones o trabajos asignados por Dirección Ejecutiva.

El resultado de las entrevistas en donde se evaluaron los dominios de la ISO 27001-2013, se observan las vulnerabilidades en los niveles organizativos, Políticas de Seguridad de la información, criptografía, seguridad de las comunicaciones, adquisición, desarrollo y mantenimiento de los sistemas de información y la gestión de continuidad de negoción con un 0% de cumplimiento de los controles establecidos en la norma.

Por su parte, en los aspectos de gestión de incidentes de seguridad de la información se tiene un cumplimiento del 85.71%, en cuanto a la gestión durante y después; no así en el antes. Ver tabla 3, figura 8 y anexo 3

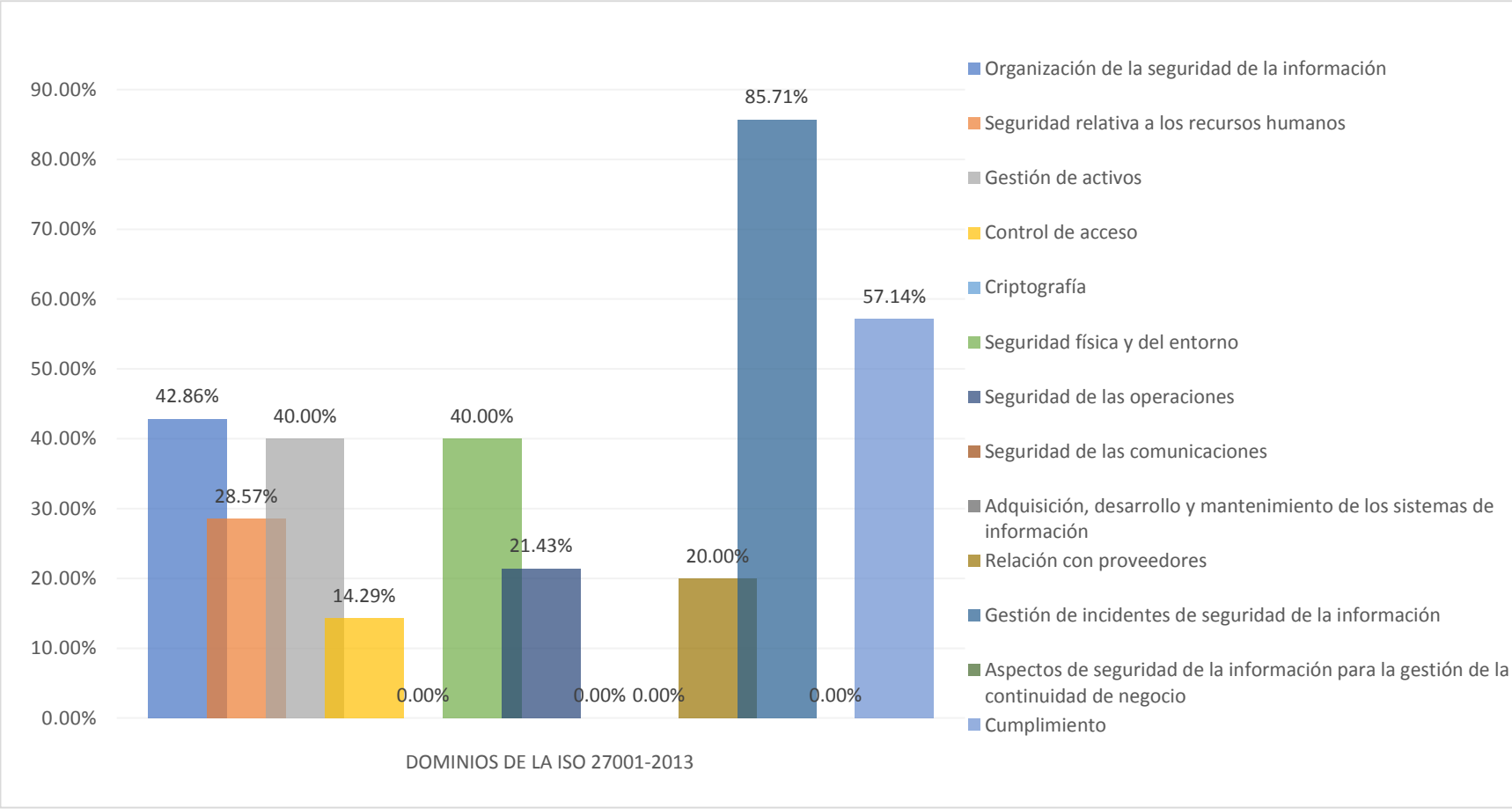
Dominio ISO 27001-2013	Cumplimiento
Políticas de seguridad de la información	0,00%
Organización de la seguridad de la información	42,86%
Seguridad relativa a los recursos humanos	28,57%
Gestión de activos	40,00%
Control de acceso	14,29%
Criptografía	0,00%
Seguridad física y del entorno	40,00%
Seguridad de las operaciones	21,43%
Seguridad de las comunicaciones	0,00%
Adquisición, desarrollo y mantenimiento de los sistemas de información	0,00%
Relación con proveedores	20,00%
Gestión de incidentes de seguridad de la información	85,71%
Aspectos de seguridad de la información para la gestión de la continuidad de negocio	0,00%
Cumplimiento	57,14%

Tabla 3: Cumplimiento de Dominios ISO 27001-2013

Fuente: Elaboración Propia

Figura 8: Cumplimiento de Dominios ISO 27001-2013 - AMUNIC

Fuente: Propia



6.2. Evaluación de Infraestructura tecnológica Actual

Los alcances técnicos de la Propuesta de Optimización de la Infraestructura de Seguridad, plantea una mejora por medio de controles y mecanismos de seguridad.

Cabe destacar que, aunque se tiene una Infraestructura Tecnológica establecida, esta tiene controles básicos como son las configuraciones de los dispositivos perimetrales por el proveedor, las normas no están documentadas, no se puede monitorear la red por limitaciones técnicas de los equipos (switch no administrados).

A continuación, una representación del inventario existente de los dispositivos de la institución en la tabla 4: Inventario de equipos existentes - AMUNIC:

Tabla 4: Inventario de Equipos existentes - AMUNIC

Cantidad	Equipo	Marca/Modelo	Características	Aplicaciones	Modalidad	IP	Ubicación	Sistema Operativo
1	Servidor	HP DL380G5	Procesador: Intel Xeon RAM: 12GB Disco Duro: 5 discos de 160GB	Correo	Producción	192.168.0.20	Cuarto de Servidores	Linux
1	Servidor	HP DL380G6	Procesador: Intel Xeon RAM: 16GB Disco Duro: 10 discos de 160GB	SIAFP y Base de Datos Oracle	Producción	192.168.0.30		Windows
1	Servidor	HP DL380G5	Procesador: Intel Xeon RAM: 10GB Disco Duro: 5 discos de 64GB	SIAFP (respaldo) Oracle	Contingencia	192.168.0.30		Windows
1	Firewall	Checkpoint 5100		Proxy		192.168.0.8		Linux
1	Firewall	Checkpoint1300		Proxy		192.168.0.9		Linux
2	Router	Linksys WRT54G	1 Puerto WAN 10/100 Mbps Ruteo por RIP-1, RIP-2, static IP routing			192.168.0.10		

Cantidad	Equipo	Marca/Modelo	Características	Aplicaciones	Modalidad	IP	Ubicación	Sistema Operativo
			Compatibilidad con protocolos Ethernet, Fast Ethernet, IEEE 802.11b, IEEE 802.11g Soporte para DHCP, DMZ port, IP address filtering, MAC address filtering, NAT, Stateful Packet Inspection (SPI), VPN passthrough, auto-uplink (auto MDI/MDI-X), firewall, switching Soporte WEP, WPA y WPA2 para Wireless 4 puerto LAN 10/100 Mbps					
7	Switch	Cisco Linksys SR224G	Velocidad de 100 Mbps 24 puertos 10/100 2 puertos gigabit 2 puertos miniGBIC para expansión de fibra Auto negociación					

Cantidad	Equipo	Marca/Modelo	Características	Aplicaciones	Modalidad	IP	Ubicación	Sistema Operativo
1	UPS Servidor	Smart 2200(torre)						
1	UPS Servidor	Smart 2200	UPS (Rack)					
1	UPS Servidor	Smart 2200 XL	UPS (Rack)					
1	UPS	3000	UPS (Rack)					
1	PBX	GrandsTream	PBX (Rack) con 25 teléfonos IP					
1	Teclado		Teclado					
1	Mouse		Mouse					
1	Monitor	WF 1907	Monitor					
1	DVR	Turbo HD	DVR (Rack)					
6	CPU (Monitor, teclado, Mouse)	DELL OPTIPLEX 3040	Procesador: Ci7 RAM: 8GB Disco Duro: 1TB	SIAFP Correo Institucional Internet Antivirus			Dirección Administrativa Financiera DAF	Windows 7 Ultímate
3	CPU (Monitor, teclado, Mouse)	DELL OPTIPLEX 7020	Procesador: Ci7 RAM: 8GB Disco Duro: 1TB	Correo Institucional Internet Antivirus			Unidad de Gestión Ambiental	Windows 10
3	CPU (Monitor, teclado, Mouse)	DELL OPTIPLEX 7020	Procesador: Ci7 RAM: 8GB Disco Duro: 1TB	Correo Institucional Internet Antivirus			Unidad de Adquisiciones	Windows 10
3	Laptop	Toshiba Satellite S55-C5138	Procesador: Ci7 RAM: 8GB Disco Duro: 500GB	Correo Institucional Internet			Dirección Económica	Windows 10

Cantidad	Equipo	Marca/Modelo	Características	Aplicaciones	Modalidad	IP	Ubicación	Sistema Operativo
				Antivirus				
2	Disco Duro Externo	Wester Digital/Iomega	2TB					
1	Disco Duro Externo	ADATA	3T					
1	Disco Duro Externo	ADATA	2T					
5	Access Point	Cisco Linksys WAP54G	WPA2					
1	SIAFP	Sistema Integral Administrativo Financiero y Planificación	Cliente/ Servidor	Módulos: Contabilidad Banco Caja Activo Fijo Cuentas por Cobrar Nomina Almacén Cuentas por pagar			Instalado en los equipos de la Dirección Administrativa Financiera DAF	Form Developer 6.0
1	Licencia de UTM	Licencia de Checkpoint		Licencia de: IPS Antispam Boot Antivirus WebFiltering				

Cantidad	Equipo	Marca/Modelo	Características	Aplicaciones	Modalidad	IP	Ubicación	Sistema Operativo
35	Licencia de Antivirus	Licencia de Antivirus Kaspersky	Endpoint Advanced Security					

En el caso de los equipos de cómputo (CPU), es una representación de los equipos existentes en la diferentes áreas y unidades, en total se tienen 25 Equipos CPU completos con su monitor, teclado, mouse y ups, de igual manera el caso de las laptops son un total de 18 laptops, además de 11 impresoras en uso, 5 scanner y 2 cámaras.

6.3. Análisis de los equipos actuales

Análisis de los dispositivos de la red actual

La evaluación de la red, son especificaciones que se obtuvieron de documentación proporcionada por la Unidad de Informática y la Dirección Administrativa Financiera. En la figura 9, se tiene una descripción general de la infraestructura de red actual.

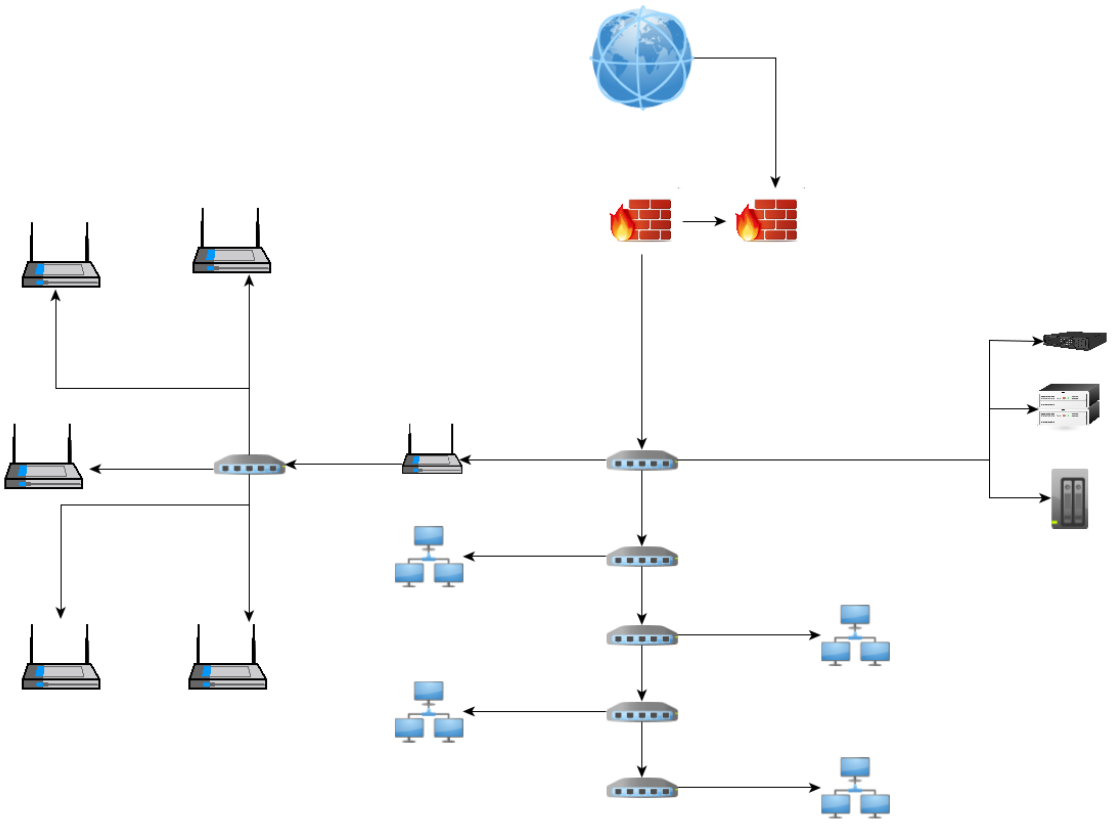


Figura 9. Diagrama de Red - AMUNIC

En el diagrama de red se identifican varios equipos de cómputo siendo estos de escritorio y otros equipos portátiles (Laptop), que dentro de la Infraestructura Tecnológica se denominan equipo de cómputo.

La conexión en la red se da a través de switches de 24 puertos. Los que proporciona la conexión de los switches a los teléfonos IP quienes conectan a los equipos de cómputo y en otros casos la conexión del switch a las impresoras de red, hay un Router que brinda conexión a los Puntos de Acceso (AP) para dar el servicio de red inalámbrica.

Además, se tiene una planta telefónica que provee servicio actualmente a la misma cantidad de equipo de cómputo 25, los demás periféricos como scanner e impresoras se conectan de manera directa a los equipos de cómputo, las cámaras de vigilancia ip esta conectadas también a los switches.

Debido a la cantidad de equipos de cómputo en la institución (alrededor de 25) se optó por utilizar switches de 24 puertos Cisco modelo Linksys SR224G, con una velocidad de 100Mbps por puerto y con dos interfaces de 1Gbps. Sin embargo, debido a que no existe una segmentación de la red, encontrándose absolutamente todos los equipos en la misma VLAN, se ha estado teniendo problemas en la perdida de servicio, tanto al momento de transferir archivos, imprimir o acceder a los servicios de correo y sistemas.

Equipos como switch, firewall, Router, servidores, están en un mismo lugar cuarto de servidores (datacenter). El cableado es relativamente nuevo, hace 2 años que se instaló debido al cambio de local que se tuvo, este es categoría 6.

Análisis de servicios y aplicaciones

En el análisis de servicios a nivel técnico se tiene la siguiente información:

La velocidad del servicio de Internet es de 10Mbps, la cual es ocupada para las siguientes actividades:

- Actualización de sistemas operativos de la Institución.
- Actualización de base de datos de Antivirus empresarial.
- Acceso a soportes remotos por parte de los servicios tercerizados.
- Navegación general de la institución.

El servicio de Correo Electrónico Institucional, es un servicio que esta tercerizado por temas de recursos técnicos y financiero. Además de la disponibilidad del mismo 24/7.

En cuanto al servicio de Soporte técnico a usuarios, en general es un soporte personalizado en aplicaciones ofimáticas tanto de uso como de algún inconveniente que estas puedan ocasionar, como los problemas de hardware.

El tema del soporte técnico a los módulos del SIAFP, se da en uso de la aplicación, capacitación de procedimientos, resolución de incidentes en el registro de la información, siempre asegurando la integridad de la información y la autorización correspondiente por parte de la Dirección Administrativa Financiera, las cuales están registradas a través de correos electrónicos.

El SIAFP no tiene roles establecidos en los usuarios, las contraseñas son generales y pocos seguras pues son de menos de 10 caracteres y son letras, se dan incidentes en las transacciones involuntarias que han tenido que ser corregidas con reclasificaciones en los comprobantes, pero sin saber el usuario que lo hizo, es decir los errores, modificaciones o eliminación de los registros de la información que se puedan dar no dejan constancia de los cambios para auditorias financieras y cumplir de esta manera con las Normas Técnicas de Control Interno.

Otra aplicación existente en la institución es el software antivirus que se maneja para todos los equipos de cómputo es de tipo licenciado, el cual brinda la protección necesaria, ya que no se han registrado incidentes de virus en los equipos, en las configuraciones internas del antivirus se tiene habilitado el escaneo de las unidades extraíbles automáticamente una vez que se ingresen. No obstante, no se tiene control alguno sobre las aplicaciones que puedan instalar en los equipos de cómputo y que estos puedan ser víctima de virus, malware, robo o compromiso de información.

El hecho de tener una evaluación de la situación actual ayudará a tener claro los aspectos que deben ser considerados en la propuesta, es decir todos aquellos elementos a ser mejorados para brindar servicio de calidad en la institución.

Es importante contar con el análisis de riesgo de los activos para la toma de decisión oportuna y de esta manera proponer los mecanismos de seguridad necesarios para optimizar la infraestructura tecnológica existente.

6.4. Identificación y evaluación de riesgos

En el análisis cuantitativo de riesgos se realizó la evaluación de la probabilidad y el impacto de los riesgos, para determinar la magnitud y la prioridad.

Servicios Brindados:

- Internet
- Correo
- Soporte técnico a usuarios
- Servicio de Acceso al SIAFP

La frecuencia con se brindan estos servicios es diario a excepción del soporte de acceso al SIAFP, el cual se brinda de acuerdo a las solicitudes.

Como se indicó anteriormente, la metodología usada para el análisis de riesgo es MAGERIT, la cual maneja seis elementos básicos:

- Activos
- Amenazas
- Vulnerabilidades
- Impactos
- Riesgo
- Salvaguardas (Funciones, Servicios y Mecanismos)

A continuación, se muestra resultados del análisis realizado a la institución en el que muestra cinco de los seis elementos de la metodología, vulnerabilidades y riesgos de los servicios y activos de la infraestructura tecnológica existente.

Identificación de Activos:

En la tabla 5 se identifican activos con sus categorías: Software, Hardware, Comunicaciones, Equipos Auxiliares, Instalaciones, Información y Personal, además se muestra la relación de cada uno de los activos en la figura 10.

Tabla 5: Identificación de Activo y sus categorías

Software	SIAFP
	Sistemas Operativos
	Antivirus
	Otras aplicaciones
Hardware	Servidores
	Firewall
	Impresoras
	Computadoras: PC y Laptop

	Scanner
	Router
	Access Point
	Switch
	UPS
	Estabilizadores
	Cámaras
Comunicaciones	Telefonía IP
	Red Wifi
	Red LAN
	Internet
	Cableado
	Enlace del Proveedor
Equipos Auxiliares	UPS
	Aires Acondicionados
	Cableado Eléctrico
	Sistema de Vigilancia
Instalaciones	Edificio
	Mobiliario
	Vehículos
Información	BD del SIAFP
	Documentos Financieros
	Documentos legales
	Manuales Institucionales
	Formatos
	Respaldos de Información
Personal	Personal TIC
	Personal de Dirección

Árbol de los activos

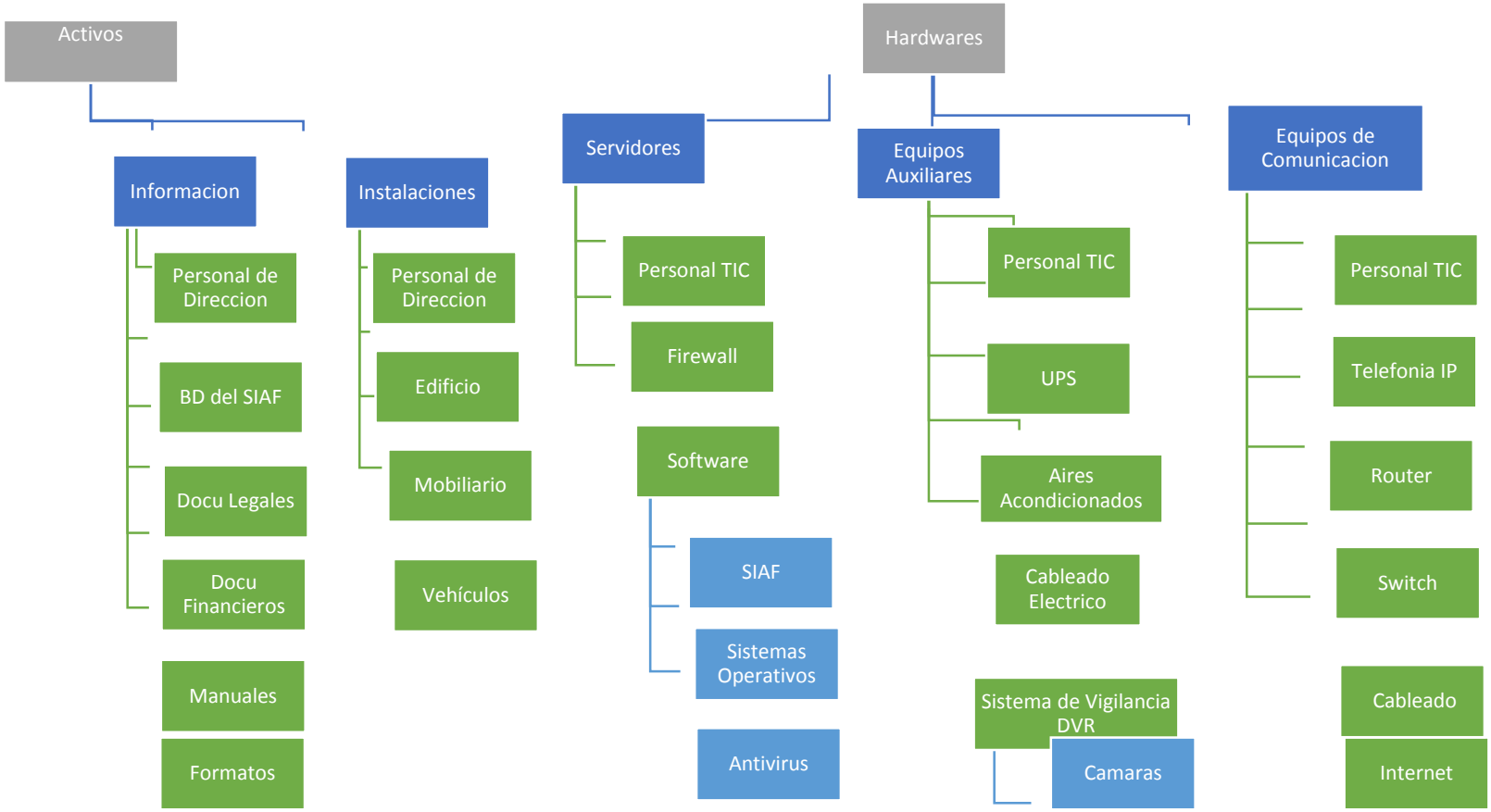


Figura 10: Árbol de Activos de AMUNIC

Fuente: Elaboración Propia

Valoración de Activos:

Según la metodología MAGERIT define que “La valoración se puede ver desde la perspectiva de la ‘necesidad de proteger’ pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes.” (MAGERIT 3.0, p 24)

De acuerdo con los preceptos estipulados en la norma ISO 27001-2013, los activos de información deben ser valorados con base a la disponibilidad, confidencialidad e integridad. La valoración que cada activo recibió se relaciona con base a las entrevistas o información suministrada por el responsable del activo. Ver en tabla 6

Abreviación utilizada:

DIMENSIONES	
CONFIDENCIALIDAD	C
INTEGRIDAD	I
DISPONIBILIDAD	D
AUTENTICIDAD	A
VALOR CUALITATIVO	VC

Las Escalas utilizadas son:

Escala utilizada para Valor	
1	No necesario
2	Poco necesario
3	Necesario
4	Muy Necesario
5	Imprescindible

Escala utilizada para Dimensiones	
1	Nada grave
2	Poco grave
3	Problemático
4	Grave
5	Muy grave

El valor del Activo (Valor), corresponde a la suma de la confidencialidad, disponibilidad, integridad, autenticidad, uso y acceso, donde seis (6) es la calificación más baja y 30 la calificación más alta. Además, el tipo de activo es la clasificación que se le dio cuando se identificó el activo.

Tabla 6: Valoración del Activo

Activo	**Valor**	**Dimensiones**						**Tipo de activo**	**VC**	**Valor Cuantitativo**
		C	I	D	A	Uso	Acceso			
SIAF	30	5	5	5	5	5	5	Software	4	U$ 25,000.00
Sistemas Operativos	14	2	3	3	2	2	2	Software	3	U$100.00
Antivirus	18	2	1	3	2	5	5	Software	2	U$1,200.00
Servidores	30	5	5	5	5	5	5	Hardware	4	U$15,000.00
UPS	20	3	3	3	3	3	5	Hardware	4	U$ 7,000.00
Firewall	30	5	5	5	5	5	5	Hardware	5	U$9,000.00
Router	21	3	3	4	3	4	4	Hardware	3	U$100.00
Impresoras/ Scanner	8	1	1	1	1	2	2	Hardware	3	U$150.00
PC Escritorio	18	3	3	3	3	3	3	Hardware	3	U$1250.00
Laptop	8	1	1	1	1	2	2	Hardware	2	U$1100.00
Cableado	13	1	1	3	2	3	3	Comunicaciones	3	U$3500.00
Switch	19	3	1	3	3	4	5	Comunicaciones	3	U$500.00
Telefonía IP	15	2	2	2	3	3	3	Comunicaciones	2	U$50.00
Planta Telefónica	15	2	2	2	3	3	3	Comunicaciones	2	U$2,000.00
Cámaras de Vigilancia	29	5	5	5	4	5	5	Comunicaciones	3	U$200.00
DVR	29	5	5	4	4	5	5	Comunicaciones	2	U$1,000.00
BD sistema	30	5	5	5	5	5	5	Comunicaciones	5	U$350,000.00
Documentos legales	30	5	5	5	5	5	5	Información	5	U$50,000.00
Documentos financieros	30	5	5	5	5	5	5	Información	5	U$70,000.00

Activo	Valor	Dimensiones						Tipo de activo	VC	Valor Cuantitativo
		C	I	D	A	Uso	Acceso			
Manuales	28	4	5	4	5	5	5	Información	3	U$6,000.00
Formatos	13	3	2	2	2	2	2	Información	3	U$500.00
Edificio	16	1	1	3	1	5	5	Otros	3	U$320,000.00
Vehículos	6	1	1	1	1	1	1	Otros	2	U$100,000.00
Personal TIC	30	5	5	5	5	5	5	Otros	4	U$115,000.00
Personal Dirección	28	3	5	5	5	5	5	Otros	4	U$8,000

Con respecto a la valoración de los activos podemos observar en la tabla anterior que los activos más valiosos son la aplicación del SIAFP, la base de datos, los servidores, Firewall, la documentación legal y financiera y el personal de TI. Elementos a considerar en la propuesta de optimización para brindar la seguridad necesaria para la continuidad del negocio.

Identificación de Amenazas

Las amenazas son los eventos inesperados con potencial para causar daños, la siguiente lista son amenazas que se encontraron en el análisis de los activos y según las entrevistas realizadas a los usuarios, a la Unidad de Informática, además se puede ver las amenazas a las que están expuestos los servicios en la tabla 7 (Matriz Servicios - Amenazas).

Fallos no intencionados:

- Errores de los usuarios.
- Errores del administrador del sistema.
- Errores de configuración.
- Difusión de software dañino.
- Alteración de la información.
- Destrucción de la información.

- Fugas de información.
- Vulnerabilidades de los programas.
- Errores de mantenimiento/actualización de software.
- Errores de mantenimiento/actualización de hardware.
- Caída del sistema por agotamiento de recursos.
- Pérdida de equipos.

Ataques deliberados o intencionados

- Suplantación de identidad.
- Abuso de privilegios de acceso.
- Uso no previsto.
- Difusión de software dañino.
- Acceso no autorizado.
- Modificación de la información (SIAFP).
- Destrucción de la información.
- Revelación de la información.
- Manipulación de programas.
- Manipulación de hardware.
- Denegación de servicios.
- Robo de equipos.
- Personal no disponible.
- Ataque destructivo.
- Bypass de las reglas de navegación.

Tabla 7: Matriz Servicios - Amenazas

Servicios	Amenazas
INTERNET	Errores de configuración Bypass de las reglas de navegación Fugas de información Uso no previsto Acceso no autorizado Difusión de Software Dañino Denegación de servicios
SOPORTE A USUARIOS	Manipulación de programas Errores de mantenimiento/actualización de software Aumento de vulnerabilidades del sistema Operativo Vulnerabilidades de los programas Falta de respaldos en copias de seguridad Perdida, Robo o daño de dispositivos de almacenamiento externos Inserción de dispositivos no autorizados Falla de los equipos Corte de Energía Sobrecalentamiento de equipos Acceso de personal no autorizado Hacking Puertos Abiertos Visibilidad nula de los equipos de red Descarga de archivos maliciosos Acceso no autorizado a otros equipos de usuario Congestionamiento de la red

Servicios	Amenazas
SIAFP	Manipulación, Revelación, Fuga de información Ataque destructivo Acceso no autorizado Abuso de privilegios de acceso Alteración de la información Destrucción de la información Modificación de la información Vulnerabilidades de los programas Suplantación de identidad Falta de respaldos en copias de seguridad Perdida, Robo o daño de dispositivos de almacenamiento externos Inserción de dispositivos no autorizados Falla de los equipos Corte de Energía Sobrecalentamiento de equipos Acceso de personal no autorizado Hacking Puertos Abiertos Visibilidad nula de los equipos de red Descarga de archivos maliciosos Acceso no autorizado a otros equipos de usuario Congestionamiento de la red

Servicios	Amenazas
CORREO	Abuso de privilegios de acceso Alteración de la información Destrucción de la información Abuso de privilegios de acceso Modificación de la información Suplantación de identidad Denegación de servicios Falta de respaldos en copias de seguridad Falla de los equipos Sobrecalentamiento de equipos Hacking Visibilidad nula de los equipos de red Transporte de información por conexiones no segura Descargas de archivos maliciosos Congestionamiento de la red Acceso no autorizado a otros equipos de usuario
TELEFONÍA	Falla de los equipos Corte de Energía Sobrecalentamiento de equipos Acceso de personal no autorizado Puertos abierto Hacking Visibilidad nula de los equipos de red Congestionamiento de la red

Identificación de Vulnerabilidad

Como resultado del levantamiento de la información de las posibles amenazas que pueden materializarse, se tienen las siguientes vulnerabilidades manifestadas por los entrevistados e identificadas durante las visitas a AMUNIC y que pueden ser explotadas para convertir una amenaza en un riesgo real, llegando a causar daños graves en la institución. Ver tabla 8

- No tener implementada Políticas de seguridad a través de GPO (Global Policy Object).
- Configuraciones a nivel de proveedores del Firewall.
- Falta de capacitación por parte del proveedor.
- Ausencia de un sistema de extinción automática de fuegos.
- Ausencia de control de cambios de configuración eficiente y efectiva.
- Ausencia de VLAN.
- Ausencia de Active Directory.
- Ausencia de reglas avanzadas de Antispam.
- No hay control de instalación de programas en las PC o laptop.
- Falta de plan de mantenimiento de equipos.
- Ausencia de generador de energía.
- Ausencia de control de acceso Físico.
- Incorrecta configuración de puertos.
- Equipos de red obsoletos no permiten monitoreo.
- Ausencia de WebFiltering.
- No se cuenta con actualización de Software.
- Ausencia de planes de Respaldo.
- Uso de dispositivos de almacenamiento externos para transporte de información.
- Contraseñas inseguras para el acceso a los módulos del SIAFP.
- Roles y privilegios del SIAFP por defecto permite registro, modificación, eliminación información.

- Mal Sistema de ventilación.
- Ausencia de certificados SSL.

Tabla 8: Matriz Servicios – Vulnerabilidad

Servicios	**Vulnerabilidad**
INTERNET	Configuraciones a nivel de proveedores del Firewall Falta de capacitación por parte del proveedor Ausencia de Active Directory Ausencia de generador de energía Mal sistema de ventilación Ausencia de control de acceso físico Incorrecta configuración de puertos Equipos de red obsoletos no permite monitoreo Ausencia de WebFiltering
SOPORTE A USUARIOS	Ausencia de Active Directory No se cuenta con actualización del software No hay control de instalación de programas en las PC o laptop Ausencia de reglas avanzadas de Antispam Ausencia de planes de Respaldo Uso de dispositivos de almacenamiento externos para el transporte de información Falta de mantenimiento de equipos Ausencia de generador de energía Ausencia de control de acceso físico Ausencia de WebFiltering

Servicios	Vulnerabilidad
SIAFP	Ausencia de VLANs Ausencia de Active Directory Contraseñas inseguras para el acceso a los módulos del SIAFP. Roles y privilegios del SIAFP por defecto permite registro, modificación, eliminación información. Falta de plan de mantenimiento Ausencia de control de cambios de configuración eficiente y efectiva. Ausencia de planes de Respaldo Uso de dispositivos de almacenamiento externos para el transporte de información. Falta de mantenimiento de equipos Ausencia de generador de energía Mal sistema de ventilación Ausencia de control de acceso físico Incorrecta configuración de puertos Ausencia de certificados SSL
CORREO	Ausencia de Active Directory Ausencia de reglas avanzadas de Antispam Ausencia de planes de Respaldo Incorrecta configuración de puertos Ausencia de certificados SSL
TELEFONÍA	Ausencia de VLANs Ausencia de generador de energía Mal sistema de ventilación Ausencia de control de acceso físico Incorrecta configuración de puertos

Evaluación del impacto

Producto de la investigación realizada se cuenta con un análisis cualitativo del impacto de las amenazas. Ver tabla 9.

Tabla 9: Amenazas - Impacto

Amenaza	Impacto
Fallos no intencionados	Alteración/perdida o fuga de información
	Daño/pérdida de activos o indisponibilidad de otros servicios
	Costos excesivos
	Información para toma de decisiones errada o inoportuna
	Interrupción del servicio
	Pérdida de credibilidad, competitividad o imagen de la institución
	Pérdida de productividad de los servidores de AMUNIC
Ataques deliberados o intencionados	Alteración/pérdida o fuga de información
	Daño/pérdida de activos o indisponibilidad de otros servicios
	Fraude / Robo o malversación de fondos
	Interrupción del servicio
De origen Industrial	Alteración/pérdida o fuga de información
	Daño/pérdida de activos o indisponibilidad de otros servicios
	Costos excesivos

Amenaza	Impacto
	Interrupción del servicio
	Ingresos deficientes
	Pérdida de productividad de los servidores de AMUNIC
Desastres Naturales	Interrupción del servicio
	Pérdida de credibilidad, competitividad o imagen de la institución

El hecho de que las vulnerabilidades (fallas, omisiones o deficiencias de seguridad) identificas puedan ser aprovechadas tiene un alto impacto para la institución pues la pérdida, daño y la integridad de la información se ven comprometidas, afectando la credibilidad e imagen de la institución.

Evaluación del Riesgo

A la vista de los impactos y riesgos a que están expuesto los activos y servicios, hay que tomar en cuenta una serie de decisiones condicionadas por diversos factores como son: la gravedad del impacto y/o del riesgo y las obligaciones a las que por ley esté sometida la Institución.

Ante este escenario, es fundamental tomar decisiones de controles y medidas para mitigar el impacto de los riesgos de los activos y servicios que impidan la continuidad del negocio. Ver tabla 10.

Escala de calificación de los riesgos según MAGERIT:

Magnitud = Probabilidad x Impacto

	Nivel	Descriptor	Descripción	Frecuencia
Probabilidad	**1**	**Raro**	El evento puede ocurrir solo en circunstancia excepcional	No se ha presentado en los últimos 5 años
	2	**Improbable**	El evento puede ocurrir en algún momento	Al menos una vez en los últimos 5 años
	3	**Posible**	El evento podría ocurrir en algún momento	Al menos una vez en los últimos 2 años
	4	**Probable**	El evento probablemente ocurra en la mayoría de las circunstancias	Al menos una vez en último año
	5	**Casi Seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año

	Nivel	Descriptor	Descripción
Impacto	1	Insignificante	El hecho tendría consecuencias mínimas
	2	Menor	Si el hecho llegara a presentarse tendría bajo impacto
	3	Moderado	Si el hecho llegara a presentarse tendría medianas consecuencias
	4	Mayor	Si el hecho llegara a presentarse tendría altas consecuencias
	5	Catastrófico	Si el hecho llegara a presentarse tendría catastróficas consecuencias

B: Zona de Riesgo Baja	0-5	Administrar mediante procedimientos de rutinas	No Accion
M: Zona de Riesgo Moderada	6-10	Debe especificarse responsabilidad general	Preventiva
A: Zona de Riesgo Alta	11-15	Necesita atención de alta gerencia	Seguimiento
E: Zona de Riesgo Extrema	16-25	Requiere acción inmediata	Correctiva

Tabla 10: Evaluación del Riesgo

No	Riesgo	Probabilidad	Impacto	Magnitud del Riesgo	Tratamiento
Software					
R1	Incorrecta implementación de políticas de Firewall	5	4	20	Correctiva
R2	Instalación de software no licenciado y autorizado	4	3	12	Seguimiento
R3	Recursos Compartidos por defecto	5	4	20	Correctiva
R4	No tener implementada Políticas de seguridad a través de GPO (Global Policy Object)	5	4	20	Correctiva
R5	Información comprometida del SIAFP	5	5	25	Correctiva
R6	Aplicaciones clientes por defecto y desactualizadas	2	3	6	Preventiva

No	Riesgo	Probabilidad	Impacto	Magnitud del Riesgo	Tratamiento
R7	Acceso no autorizado a los sistemas	4	5	20	Correctiva
R8	Ingreso de correos masivos al servidor de correo	1	4	4	No Acción
R9	Ingreso de phishing causando identidades robadas de los usuarios	2	5	10	Preventiva
Datos					
R10	Pérdida masiva de Datos	2	5	10	Preventiva
R11	Filtración de información	5	5	25	Correctiva
R12	Infección de Malware	3	5	15	Seguimiento
Hardware					
R13	Interrupción de Servicio	1	4	4	No acción
R14	Daño de equipos	3	2	6	Preventiva
Redes y Comunicaciones					
R15	Daño, Pérdida o Robo de Equipos	2	5	10	Preventiva
R16	Explotación de Vulnerabilidades	5	5	25	Correctiva

No	Riesgo	Probabilidad	Impacto	Magnitud del Riesgo	Tratamiento
	de los software y equipos				
R17	Pérdida de reputación por Hacking	5	5	25	Correctiva
R18	Acceso no autorizado a los servicios	5	4	20	Correctiva
R19	Manipulación de la información	3	3	9	Preventiva
R20	Robo de información	3	5	15	Seguimiento
R21	Lentitud en la red	5	3	15	Seguimiento
R22	Acceso no autorizado a otros equipos de usuario	4	5	20	Correctiva

Este análisis más que identificar los **riesgos** a los que los activos y servicios de la institución están expuesto, busca cuantificar y predecir el impacto que tendrán en la continuidad del negocio.

Este proceso de la gestión de riesgo es continúo porque permitirá tener resolución a los problemas que se puedan presentar sobre todo las vulnerabilidades que puedan ser explotadas, tomando como referencia las lecciones aprendidas, datos históricos documentados y de esta manera proporcionar una base racional para la toma de decisiones.

Una vez identificado los elementos, se tomó como referencia los controles de seguridad de la ISO 27001-2013, para analizar el grado de aplicabilidad que se tiene en la Infraestructura Tecnológica de AMUNIC, lo que dará insumo para proponer los controles de seguridad en los que la institución tiene debilidad.

En este sentido en la tabla 11, se muestran los riesgos críticos a los que los activos y servicios de la institución están expuestos, y su tratamiento estará basada en mitigar y reducir los riesgos que contribuirán a la confidencialidad, integridad y disponibilidad de los servicios y continuidad del negocio.

Tabla 11: Riesgos Críticos - Propuesta

No	Riesgo	Magnitud del Riesgo	Problemática	Hardware/Software	Propuesta
R3	Recursos Compartidos por defecto	20	Latencia en la red en cada transacción que circule Imposibilidad de configuración de VLAN debido a limitaciones de Hardware No se puede realizar monitoreo por restricción de hardware	Switch no administrable	Cambio de Hardware Configuración de VLAN para lograr una correcta segmentación de la red, evitando cuellos de botellas y aumentando la seguridad Configuración de Syslog
R16	Explotación de Vulnerabilidades de los software y equipos	25			
R22	Acceso no autorizado a otros equipos de usuario	20			
R4	No tener implementada Políticas de seguridad a través de GPO (Global Policy Object	20	Imposibilidad de aplicación de políticas generales de seguridad debido a la ausencia de un active Directory	No existe servidor para la instalación del Active Directory	Se debe adquirir un servidor con licencia de Windows server 2016 para poder hacer uso de las características de un active Directory y
R11	Filtración de Información	25			

No	Riesgo	Magnitud del Riesgo	Problemática	Hardware/Software	Propuesta
					de esa manera, permitir la implementación de políticas de forma centralizada
R5	Información comprometida del SIAFP	25	Imposibilidad de seguimiento de transacciones debido a la ausencia del módulo auditor del SIAFP No fue realizada la programación del módulo auditor del sistema SIAFP No se tiene definidos los roles de usuario en los módulos del SIAFP	Ausencia de Modulo auditor	Contratación de outsourcing para la creación del módulo de auditoria del sistema SIAFP. Incluyendo soporte anual

No	Riesgo	Magnitud del Riesgo	Problemática	Hardware/Software	Propuesta
R1	Incorrecta implementación de políticas de Firewall	25	La seguridad está a nivel básico y a criterio del proveedor no de la institución El módulo Antispam está configurado en modo básico, por tanto, no existen todas las medidas necesarias para evitar correos spam, phishing o de malware Puertos Abiertos Imposibilidad de bloqueo de sitios no autorizados debido a la ausencia de un WebFiltering El módulo de WebFiltering está		Mejorar la configuración a niveles aceptables y con criterios de la institución de acuerdo a las necesidades, como la restricción de los puertos abiertos. Realizar la implementación completa del sistema Antispam, además de que se brinde una capacitación para el debido manejo del modulo Realizar la implementación completa del módulo de WebFiltering,
R17	Pérdida de Reputación por Hacking	25			

No	Riesgo	Magnitud del Riesgo	Problemática	Hardware/Software	Propuesta
			configurado en modo básico, de tal manera que no se puede tener una gestión completa de los sitios no autorizados. Además, dicha gestión va de la mano con la implementación del Active Directory		además de que se brinde una capacitación para el debido manejo del modulo

El diagnóstico muestra elementos que serán considerados para la elaboración de la Propuesta de Optimización de la Infraestructura de Seguridad de AMUNIC, la cual tiene como objetivo reducir los riesgos según el tratamiento de acción correctiva a los que está expuesta la institución. Dentro de los elementos a considerar tenemos:

- Creación de VLAN
- Implementación de módulo Antispam conforme a las necesidades de la empresa
- Implementación de un Servidor Active Directory
- Implementación de Configuración del WebFiltering en el UTM existe
- Implementación de módulo de Auditoria del SIAFP

Es importante destacar que en el análisis de la Infraestructura Tecnológica de Seguridad de AMUNIC, los riesgos con acciones preventivas, seguimiento y los que no implican ningún tratamiento (No acción), son controlados de acuerdo a los datos históricos.

7. PROPUESTA DE OPTIMIZACIÓN

Propuesta de optimización de la infraestructura tecnológica de AMUNIC

Para la elaboración de la Propuesta de Optimización de la Infraestructura de Seguridad de AMUNIC, se toma como línea base el diagnóstico de la situación actual con sus cinco elementos que buscan mejorar la seguridad de la Infraestructura Tecnológica de la institución.

Se considerará necesario dentro de la Infraestructura Tecnológica propuesta, la adquisición, actualización y configuración de dispositivos, licencias, entre otros elementos que se detallaran en cada punto a desarrollar en la propuesta.

7.1. Creación de VLAN

Resultado del diagnóstico, la obsolescencia de los dispositivos de red como los switches existente no permiten controlar y monitorear la red, lo que la hace vulnerable, ya que permite el acceso a cualquier dispositivo que este en la red (red plana) totalmente sin seguridad.

La Separación de paquetes de diferentes áreas es algo que se logrará con la creación de VLAN. Actualmente, debido a que la red es plana, todos los usuarios son capaces de acceder a todos los equipos de la red. No obstante, al implementar VLANs, los usuarios estarán limitados a acceder únicamente a las VLAN o equipos que se les permita, reduciendo así la posibilidad de filtración de información y accesos no autorizados.

La saturación de la red con la implementación de VLANs, la red reduciría sustancialmente la lentitud en la red, esto debido a que en la actualidad todos los usuarios, impresoras, servidores y teléfonos IP transitan en la misma red, causando saturación innecesaria, lo que ha llevado a inconvenientes, por ejemplo: lentitud de acceso al sistema SIAFP o retraso en las impresiones y envíos de correos, expresados a través de las entrevistas a los usuarios del SIAFP.

La adquisición de nuevos switches administrables es la solución de seguridad para la institución, estos serán configurados con las buenas prácticas de seguridad. En dichos switches se declararán las siguientes VLANs:

- DAF (Dirección Administrativa Financiera)
- Informática
- Servers
- Dirección Ejecutiva
- Unidad de Gestión Ambiental (UGA)
- Dirección de Asesoría Económica
- Adquisiciones
- Comunicación

Dichas VLANs serán asignadas a los puertos en los que los usuarios de esas áreas determinadas estarán conectados y posteriormente se implementara port security para bloquear el puerto y cualquier usuario ya sea interno o externo que intente realizar conexión a través de un puerto que no le corresponde, para una mejor compresión se puede ver Figura 11 y tabla 12.

Adicionalmente, se crearán ACL para lograr mayor seguridad, por ejemplo:

- Únicamente la red de informática tiene acceso a la red de administración de los switch.
- Las VLANs de los usuarios se encontrarán aisladas, de tal manera que los tráficos no puedan ser vistos por usuarios de otras VLANs.
- La VLAN de informática será capaz de acceder a nivel administrativo a la red de servers.

La figura 11, referida a la distribución muestra como todas las VLANs existentes lograrán tener acceso al datacenter donde se encuentran los servidores y la planta telefónica.

Adicionalmente, la VLAN de Informática (Vlan 11) tendrá acceso a las VLAN 10 y 13, que pertenecen a la Dirección Administrativa Financiera y a Dirección Ejecutiva, ya que estas áreas necesitan soporte remoto por medio de RDP. Además, tanto la VLAN de Informática como la de la Dirección Ejecutiva contaran con acceso a la Vlan 19, que es usada exclusivamente para el Sistema de circuito cerrado y sus cámaras, esto por fines de gestión.

Gráfico de distribución de VLANs

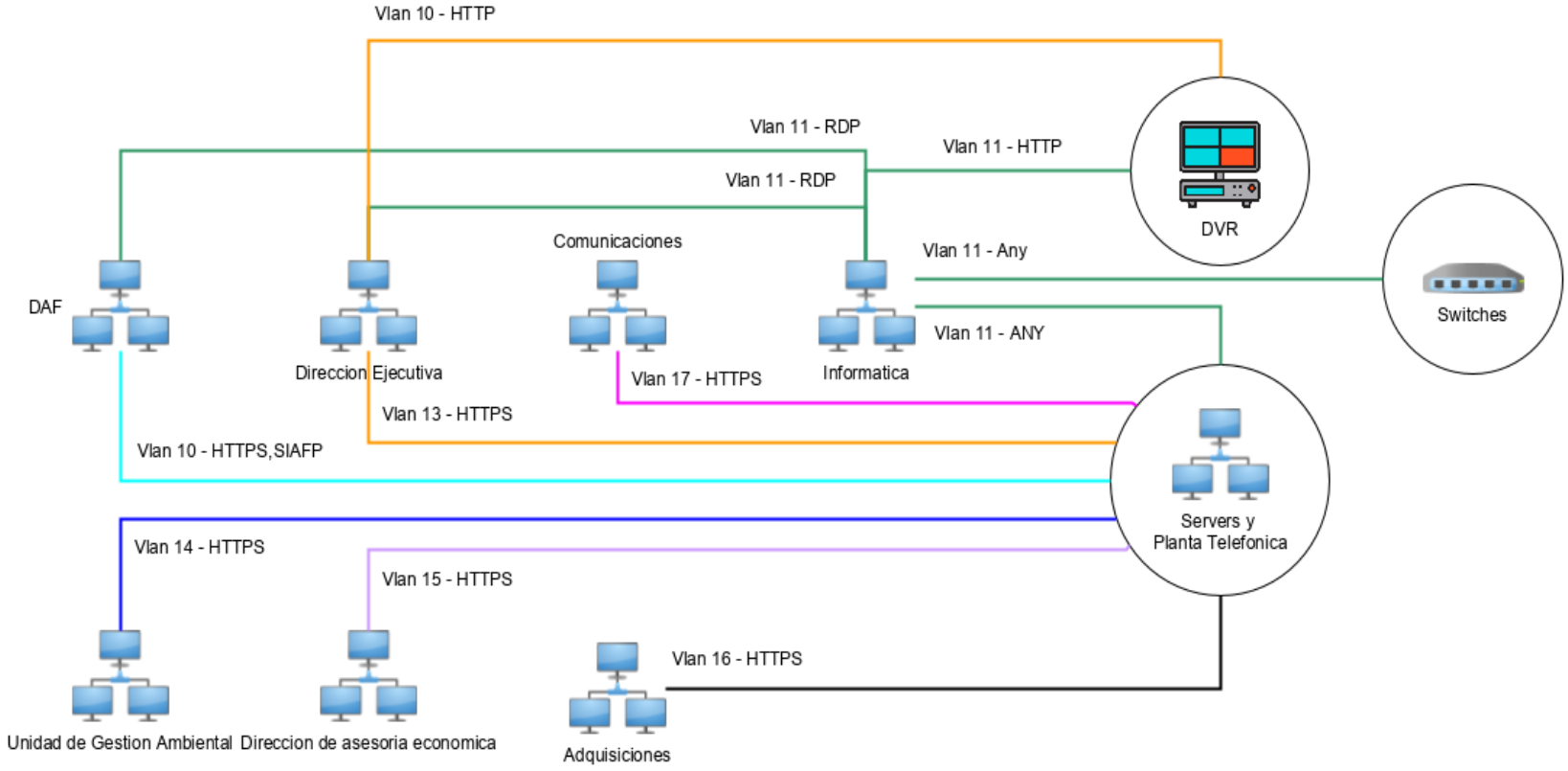


Figura 11: Distribución de VLANs – AMUNIC

Fuente: Elaboración Propia

Tabla 13: Distribución de VLANS

Vlan ID	Rango de IP	Nombre	Acceso hacia	Acceso desde	ACL Aplicadas			
					Origen	Destino	Puerto	Protocolo
10	192.168.10.0/24	DAF (Dirección Administrativa Financiera)	Servers	Informática	Vlan 10	Email Server	443	TCP
					Vlan 10	App Server	1521	TCP
11	192.168.11.0/24	Informática	Dirección Ejecutiva DAF (Dirección Administrativa Financiera)	DAF (Dirección Administrativa Financiera) Informática Servers Dirección Ejecutiva Unidad de Gestión Ambiental (UGA) Dirección de Asesoría Económica Adquisiciones Comunicaciones Informática	Vlan 11 Vlan 11	Vlan 10 Vlan 13 Vlan 12	Any	Any

Vlan ID	Rango de IP	Nombre	Acceso hacia	Acceso desde	ACL Aplicadas			
					Origen	Destino	Puerto	Protocolo
12	192.168.12.0/24	Servers	Dirección Ejecutiva	Dirección Ejecutiva	Email Server App Server	Vlan 13	443 1521	TCP
			Unidad de Gestión Ambiental (UGA)	Unidad de Gestión Ambiental (UGA)	Email Server	Vlan 14	443	TCP
			Dirección de Asesoría Económica	Dirección de Asesoría Económica	Email Server	Vlan 15	443	TCP
			Adquisiciones	Adquisiciones	Email Server	Vlan 16	443	TCP
			Comunicaciones	Comunicaciones	Email Server	Vlan 17	443	TCP
			DAF (Dirección Administrativa Financiera)	DAF (Dirección Administrativa Financiera)	Email Server App Server	Vlan 18	443 1521	TCP
			Informática	Informática	Vlan 12	Vlan 18	Any	Any

Vlan ID	Rango de IP	Nombre	Acceso hacia	Acceso desde	ACL Aplicadas			
					Origen	Destino	Puerto	Protocolo
13	192.168.13.0/24	Dirección Ejecutiva	Servers	Informática	Vlan 13	Vlan 18	Any	TCP
14	192.168.14.0/24	Unidad de Gestión Ambiental (UGA)	Servers		Vlan 14	Email Server	443	TCP
15	192.168.15.0/24	Dirección de Asesoría Económica	Servers		Vlan 15	Email Server	443	TCP
16	192.168.16.0/24	Adquisiciones	Servers		Vlan 16	Email Server	443	TCP
17	192.168.17.0/24	Comunicaciones	Servers		Vlan 17	Email Server	443	TCP
18	192.168.18.0/24	Planta Telefónica	DAF (Dirección Administrativa Financiera) Informática Servers Dirección Ejecutiva Unidad de Gestión Ambiental (UGA)	DAF (Dirección Administrativa Financiera) Informática Servers Dirección Ejecutiva Unidad de Gestión Ambiental (UGA) Dirección de Asesoría Económica	Vlan 10 Vlan 11 Vlan 12 Vlan 13 Vlan 14 Vlan 15 Vlan 16 Vlan 17	Vlan 18	SIP	UDP

Vlan ID	Rango de IP	Nombre	Acceso hacia	Acceso desde	ACL Aplicadas			
					Origen	Destino	Puerto	Protocolo
			Dirección de Asesoría Económica Adquisiciones Comunicaciones Informática	Adquisiciones Comunicaciones Informática				
19	192.168.19.0/24	DVR	Informática Dirección Ejecutiva	Informática Dirección Ejecutiva	Vlan 11 Vlan 13	Vlan 19	80	TCP
20	172.10.20.0/24	Management	Management	Informática	Vlan 11	Vlan 20	Any	TCP

La propuesta contempla la adquisición de nuevos switches, los que serán completamente administrables, con el objetivo de monitorear el tráfico y poder tener control de colisión de paquetes o problemas con los puertos o con los propios switches.

Por otra parte, se reutilizará el cableado existente el que tiene dos años de haberse instalado y está certificado, de igual manera se hará uso del rack, servidores, Router ya instalados, en este sentido, se tiene la propuesta de la red con la adquisición de los switches, un servidor para servicio de Active Directory y la reutilización de los demás dispositivos. Ver figura 12

En cuanto a la adquisición de los switches y de acuerdo a las necesidades, estos deben tener los siguientes criterios tecnológicos para el tema de la creación de VLANs y cumplir con los requerimientos de seguridad demandados por la institución.

Criterio/Tecnología

- Creación y gestión de VLAN
- Creación y gestión de ACL
- Implementación de port security
- Facilidad de gestión
- Puertos de fibra
- Velocidad de conexión
- 24 puertos
- Habilitado para monitoreo SNMP
- Habilitado para monitoreo Syslog
- Soporte para protocolo Spanning Tree
- Capa de funcionamiento (Layer 2 o Layer 3)
- Licenciamiento perpetuo
- Soporte de fabricante

- Soporte local
- Costo

Teniendo en cuenta los criterios de tecnología y las debilidades para el control y seguridad en la red actual, se requieren la adquisición de seis switches que serán actualizados, cuatro de ellos serán switches para distribución y el otro será utilizado a modo de switch Core que además tendrá redundancia , con las siguientes características de interés para la institución:

- **Administrable** a través de línea de comando por protocolo Telnet o SSH y administración web a través de HTTP y HTTPS: Permitiendo una gran facilidad de administración para el administrador, ya sea por cualquiera de los protocolos antes mencionados
- **24 puertos ethernet** con velocidad hasta de 10/100/1000 mbps: Mejora de la velocidad de conexión actual (100Mbps) manteniendo la misma cantidad de puertos.
- **2 puertos ethernet/SFP+ de 10Gbps** (solo con cable categoría 6e): Mejora de la velocidad de conexión actual (1Gbps) manteniendo la misma cantidad de puertos.
- **2 puertos SFP+ de 10Gbps**: Con el uso de estos dos puertos se puede crear puertos dedicados con velocidad aumentada para la interconexión de los switches.
- **Switching capa 2 y capa 3**: Se pueden realizar las tareas de switching tanto en capa 2 como en capa 3, aumentando así el control y facilidad de gestión.
- **Tamaño en rack de 1U**: Debido al espacio limitado en el datacenter, se necesita un switch que ocupe únicamente 1U
- **Tamaño de tabla de MAC de hasta 16,000**: Tomando en consideración la cantidad de direcciones MAC que existen actualmente en la institución, esta característica permitirá un enorme crecimiento de la institución a un futuro.
- **Soporte de hasta 4,000 VLANS**: Se pueden gestionar hasta 4,000 VLANS en cada switch, lo cual permitiría hacer un enorme crecimiento en la institución en caso de necesitarlo a futuro.

- **Posibilidad de monitoreo con SNMP versiones 1, 2c y 3**: Se obtendrá la capacidad de monitorear los switches, además de hacerlo de manera segura con la versión 2c o 3 del protocolo SNMP, que son generalmente empleados por la mayoría de sistemas de monitoreo
- **Protocolo spanning tree (STP)**: Con el apoyo del protocolo Spanning Tree, se podrá realizar la redundancia completa e interconexión de todos los switches.
- **Soporte de ACL**: Se podrán crear ACL para la mejor gestión y seguridad de la red de la compañía.
- **Soporte de QoS**: En caso de ser necesario, se podría aplicar QoS (Quality of Service) a servicios específicos dentro de la institución, como, por ejemplo, a la telefonía.
- **Protección de amenazas avanzadas**: Con esta característica se obtendrá una capa adicional de seguridad, al realizar un monitoreo de movimientos anómalos dentro de la red.
- **Licenciamiento vitalicio**: debido a que este es un proyecto de gran dimensión, se necesita adquirir equipos que puedan trabajar sin necesidad de pagar licenciamiento anual o por módulos. Con el modo de licenciamiento de Cisco, se realizar la compra del iOS una única vez con las características deseadas y se podría renovar soporte con el fabricante de manera opcional en caso de necesitarlo.

En la Figura 14 se puede apreciar el nuevo diagrama de Red propuesto con la adquisición de equipos de infraestructura tecnológica, conexiones y tecnologías. El propósito de la nueva infraestructura de red de AMUNIC es:

- Lograr alta disponibilidad en el backbone: Con la ayuda de dos switches Core interconectados por medio de fibra de 10Gbps, donde se encontrará un HSRP (Hot Standby Router Protocol); además, se tendrá un etherchannel de 30Gbps dedicado entre ambos switches.

- Redundancia de los switches de acceso: Los switches de acceso se encontrarán interconectados por medio de cables de cobre Categoría 6, para sacar provecho de 1Gbps de velocidad en los puertos y lograr así una redundancia completa, de tal manera que, si uno de estos switches llegase a colapsar, el resto de los equipos tendrán aun conexión tanto hacia Internet como al Datacenter.
- Redundancia de conexión con el Datacenter: El datacenter se encontrará en redundancia con dos switches, a través de fibra de 10Gbps para lograr redundancia en caso de perder uno de los mismos.

Propuesta de Topología de Red

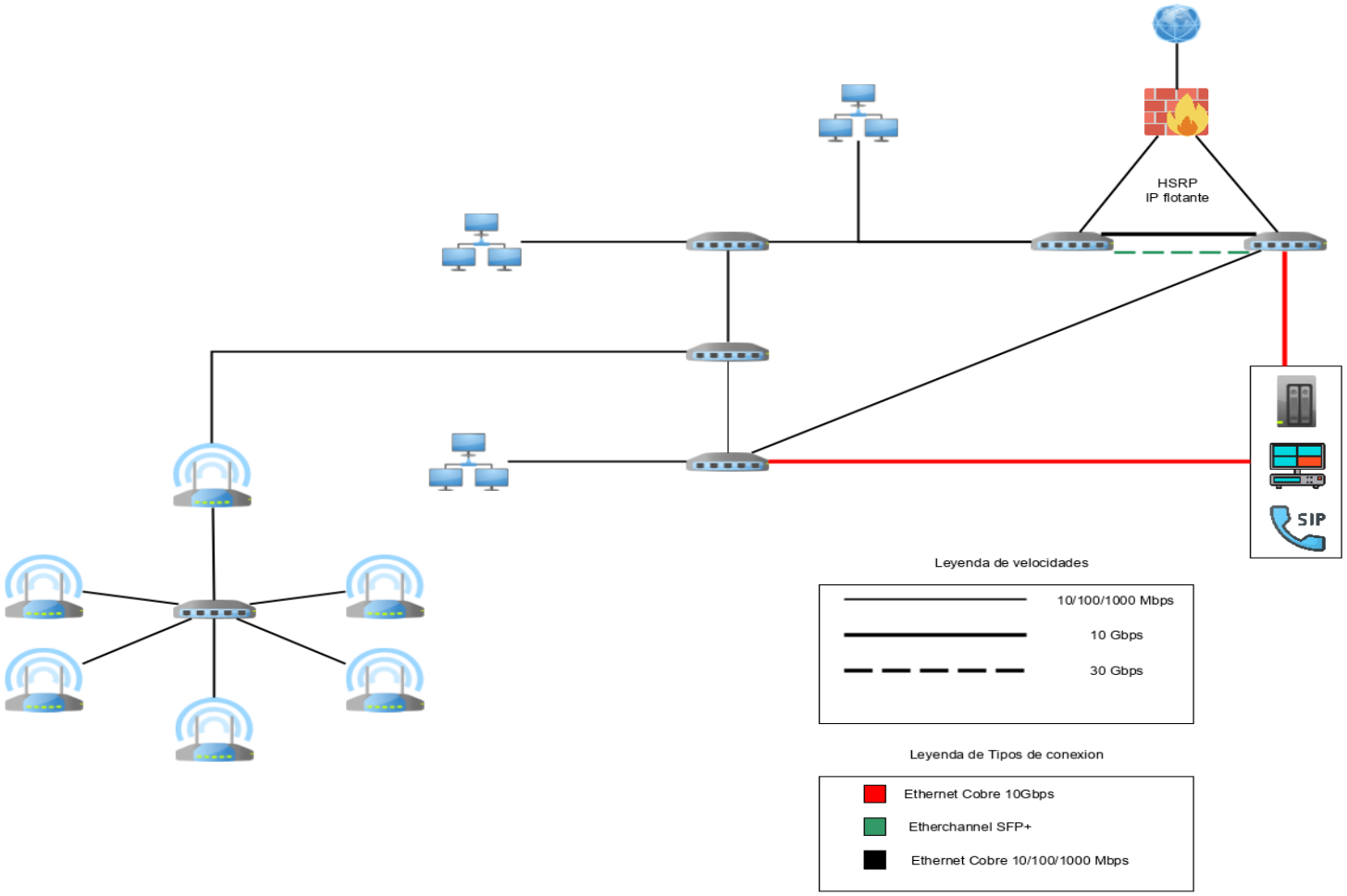


Figura 12: Propuesta de Red – AMUNIC; Fuente: Elaboración propia

7.2. Implementación de módulo Antispam conforme a las necesidades de AMUNIC

Actualmente, el equipo firewall posee un módulo Antispam configurado de manera básica, por lo que no es capaz de suplir las necesidades de seguridad de la Institución.

Una vez que el Antispam sea reconfigurado para poder cumplir con estas necesidades, lograr reducir el riesgo de ingreso de phishing, infección de virus, que la información sea comprometida (pérdida o daño), esto con la activación de las siguientes características:

- Configuración del módulo Antispam para realizar las RDNS, SPF, DMARC, DKIM, BATV:
  - **RDNS (Reverse DNS):** es una medida de seguridad para asegurar que los correos provenientes de determinados dominios llegan desde la dirección IP correcta
  - **SPF (Sender Policy Framework):** Permite revisar los DNS autoritativos de los dominios que envían correos, de tal manera que se puede corroborar si el IP que envía correos está realmente autorizado a hacerlo.
  - **DMARC (Domain Message Authentication Reporting):** Un método para evitar que el dominio propio sea usado con fines de spoofing, ya que permite hacer una consulta DNS para verificar si el servidor que envía los correos está correctamente autenticado para enviarlos.
  - **DKIM (DomainKeys Identified Mail):** Con este método, se puede identificar rápidamente un email spoofing, ya que permite al equipo Antispam verificar si el correo recibido está firmado por el servidor autorizado para enviarlos.
  - **BATV (Bounce Address Tag Validation):** Permite verificar la dirección de rebote de los correos tanto enviados como recibidos, para evitar correos que no posean el parámetro bien definido.

- **Configuración de prevención de bulk email:** Con esta protección, se logra evitar que entren incontables cantidades de correos spam hacia el servidor de correo.
- **Inspección de correos tanto entrantes como salientes:** Debido a que tantos atacantes externos pueden enviar correos phishing, también puede existir una cuenta de correo comprometida enviando correos desde dentro, por tanto, todos los correos salientes también deben de ser analizados y estar dentro del umbral de cantidades de correo aceptados.
- **Configuración de RBL gratuitas, pero de confianza, incluyendo barracuda:** El uso de listas RBL permite filtrar de antemano correos maliciosos, ya que se cuenta con una base de datos en tiempo real que reporta tanto dominios como direcciones IP maliciosas.
- **Correos spam puestos en cuarentena:** El Antispam debe tener la posibilidad de almacenar los correos en una cuarentena de donde puedan ser fácilmente reportados como falsos positivos de ser necesarios.
- **Activación de filtros por direcciones de email, expresiones regulares:** Cuando se está recibiendo correos masivos de muchas direcciones de correo maliciosas, se puede crear una expresión regular que sea capaz de leer el encabezado del correo y detener todo correo que cumpla con la regla, previniendo así correos masivos aun cuando son de muchas direcciones diferentes.

7.3. Implementación de un Servidor Active Directory

El diagnóstico realizado a la actual Infraestructura Tecnológica nos brinda datos de las vulnerabilidades, entre ellas está la ausencia de políticas de seguridad en la infraestructura, en la cual no se tiene control de acceso a los servicios por la falta de un servidor de Active Directory (AD), para reducir el riesgo a la que está expuesta tanto los equipos de cómputo como la información, en este sentido la Propuesta de Optimización de la Infraestructura de Seguridad de AMUNIC, establece la implementación de un Servidor Active Directory.

Se debe adquirir licencia de Windows server 2016 para poder hacer uso de las características de un Active Directory, este será instalada en un nuevo equipo para permitir la implementación de políticas de forma centralizada, como:

- Instalación del sistema operativo siguiendo las buenas prácticas ofrecidas por el fabricante.
- Instalación del servicio de active Directory y configuración del mismo, nuevamente siguiendo las buenas prácticas ofrecidas por el fabricante.
- Creación de las siguientes políticas de dominio:
  - Política de contraseñas, auto bloqueo de equipos en cinco minutos, usuarios son automáticamente enviados al grupo de usuarios avanzados y sacados del grupo administradores.
  - Bloqueo de CMD y ejecutar, deshabilitar cuentas locales para mantener únicamente cuentas de dominio.
  - Deshabilitar capturas de pantalla
  - Deshabilitar acceso a dispositivos USB y CD de almacenamiento.
  - Implementación de fondo de pantalla institucional
- Creación de grupos de usuarios, incluyendo los grupos de permisos de navegación.

En la implementación del Servidor Active Directory, se tomará en consideración un modelo de política de control de acceso como lo muestra el anexo 2.

7.4. Implementación de Configuración del WebFiltering en el UTM existe

La implementación de la configuración del WebFiltering en el UTM existe, permitirá minimizar el riesgo, tener control de navegación, restringir acceso a sitios especifico, evitando pérdida de información por correos electrónicos externos, almacenamiento en línea, descargas, entre otras amenazas a las que se está expuesto sino se tiene el control de navegación de los usuarios.

Realizar la implementación completa del módulo de WebFiltering en el UTM, es parte de la propuesta, sin olvidar al eslabón más débil en la seguridad que es el usuario final, para esto se tiene el plan de capacitación institucional el que se incluye temas de seguridad de la información, por otro lado, se tendrá la debida transferencia de conocimiento en el manejo del módulo para la correcta administración.

Políticas de navegación por medio de perfiles de Active Directory

El firewall se unirá al controlador de dominio una vez que este se implemente, de tal manera que sea capaz de leer la lista de grupos y así, realizar perfiles de navegación basado en los grupos. Se crearán tres grupos de navegación:

- Proxy Bloqueo
- Proxy Directores
- Proxy Regular

Donde se definen las siguientes restricciones específicas:

- **Proxy Bloqueo**

Ningún sitio puede ser accedido y no se puede descargar

- **Proxy Regular**

Cualquier sitio web con alguna de las siguientes clasificaciones estará bloqueado de acceso:

- Juegos/Apuestas
- Desnudo
- Páginas personales
- Redes Sociales
- Sospechosas
- Armas
- Paginas con contenido multimedia (Sitios de video como Youtube, música online, etc.)

Límite de descarga: 300MB

Nota: El contenido multimedia de videos es liberado de 12PM a 1PM.

- **Proxy Directores**

Son capaces de acceder cualquier sitio web y descargar archivos de cualquier tamaño.

- **Restricciones adicionales**
  - Ninguno de los grupos anteriores excepto el de Dirección Ejecutiva pueden acceder a correos web de terceros, únicamente al correo web de la empresa.

- Los sitios que han sido etiquetados como Phishing no pueden ser accedidos por ningún usuario.
- Todo el tráfico entrante y saliente es analizado de virus por el motor de seguridad del firewall.
- Los objetos que han sido clasificados como sospechosos son bloqueados.
- Las aplicaciones potencialmente peligrosas son bloqueadas.
- Las siguientes extensiones no pueden ser descargadas si fueron encontradas como sospechosas por el sistema de seguridad: exe, zip, msi, cab.
- Las siguientes aplicaciones han sido bloqueadas: P2P, torrent, Drives personales (Dropbox, OneDrive, Google Drive, etc), anonimizadores, acceso remoto, VPN.

7.5. Implementación de módulo de Auditoria del SIAFP

La necesidad de controlar las transacciones realizadas con el fin de mantener la integridad, confidencialidad y disponibilidad de los registros contables, y basados en el principio 7 de las Normas Técnicas de Control Interno de la Contraloría General de la Republica, en que se establece que la entidad identifica riesgos para el logro de sus objetivos y los analiza como base para determinar cómo deben ser administrados e identificando riesgos internos como factores tecnológicos el que los sistemas de información están expuestos a las modificaciones de datos, y utilizando la información resultante de la entrevistas y los registros de bitácora de incidentes de transacciones del Sistema se hace necesario la creación de un módulo de auditoria del SIAFP para controlar todas la gestión en ellas.

Por otro lado, la ausencia de los roles y la aplicación de segregación de funciones hace necesario la implementación del módulo auditor para reducir los riesgos.

La implementación de mecanismos de seguridad que permitan el monitoreo del funcionamiento y uso del sistema y demás servicios tecnológicos instalados en la institución, pueden controlar la integridad de la información que estos almacenan o comunican a través de los medios y la disponibilidad de los activos y servicios de información ya que actualmente se considera según los resultados de la auditoria externa a AMUNIC que la gestión de seguridad realizada sobre estos activos no está siendo adecuadamente realizada.

Potenciar los controles de seguridad en el SIAFP, permite obtener del sistema datos claros y precisos, conforme a lo requiere la institución y los clientes, minimizando incidentes de seguridad como daño de aplicaciones, equipos tecnológicos hasta incluso robo o alteración de información, lo que puede costarle mucho dinero.

El módulo auditor del SIAFP tiene como finalidad la supervisión continua de todas las actividades relativas al SIAFP, estas estarán en el marco del cumplimiento de los procedimientos y estándares establecidos por las Normas Técnicas de Control Interno y el Manual Administrativo Financiero Institucional en el que existen los controles de registro, aprobación y autorizado de toda la gestión administrativa.

En este sentido, la Propuesta de Optimización de Infraestructura de Seguridad, establece los controles preventivos a la seguridad del SIAFP en los que se contemplan la implementación del servidor AD y la implementación de VLAN.

En los controles de detección tenemos el desarrollo del módulo auditor en que se registrará el usuario, ip de equipo, nombre del equipo, hora del registro, es decir el registro de la actividad diaria para detectar errores u omisiones, establecimiento

y análisis de ficheros de log para la revisión del funcionamiento del SIAP y de esta manera conocer el origen de la transacción.

Como controles correctivos para facilitar la vuelta a la normalidad cuando se produce un determinado incidente se tienen las copias o respaldos que se realizan a la base de datos, por otro lado con la implementación de controles de detección a través de pantallas de Sistemas se pueden realizar las reversiones para reparar el error antes del cierre mensual, en caso contrario se realizará justificación y notas aclaratorias para fin de auditorías financieras del error encontrado y subsanado en movimientos de otros meses.

El desarrollo del módulo auditor del SIAFP debe contener los siguientes controles tanto a nivel de aplicación como de base de datos:

- Control de entrada de datos: procedimientos de validación y corrección de datos.
- Controles de tratamientos de datos para asegurar que no se dan de alta, modifican o borran datos no autorizados para garantizar la integridad de los mismos mediante procesos no autorizados.
- Controles de salidas de datos: relativos a la corrección y adecuación de las salidas suministradas por el sistema, establecimiento de procedimientos de distribución de salidas, de gestión de errores en las salidas, etc.

Controles en bases de datos:

- Definición de procedimientos para la descripción sobre los cambios de datos, así como para el mantenimiento del diccionario de datos.
- Controles sobre el acceso a datos y de concurrencia.
- Controles para asegurar la integridad de los datos: fundamentalmente información de control para garantizar el correcto funcionamiento de las transacciones.

7.6. Evaluación de los controles propuestos

En la tabla 14, se ve como a través de la implementación de cada una de las propuestas de Optimización de la Infraestructura Tecnológica de Seguridad de AMUNIC, se logra mitigar y reducir el riesgo que los activos y servicios de la institución a lo que se encontraban expuestos, contribuyendo a la confidencialidad, integridad y disponibilidad de los servicios con los mecanismos de seguridad y mejores prácticas.

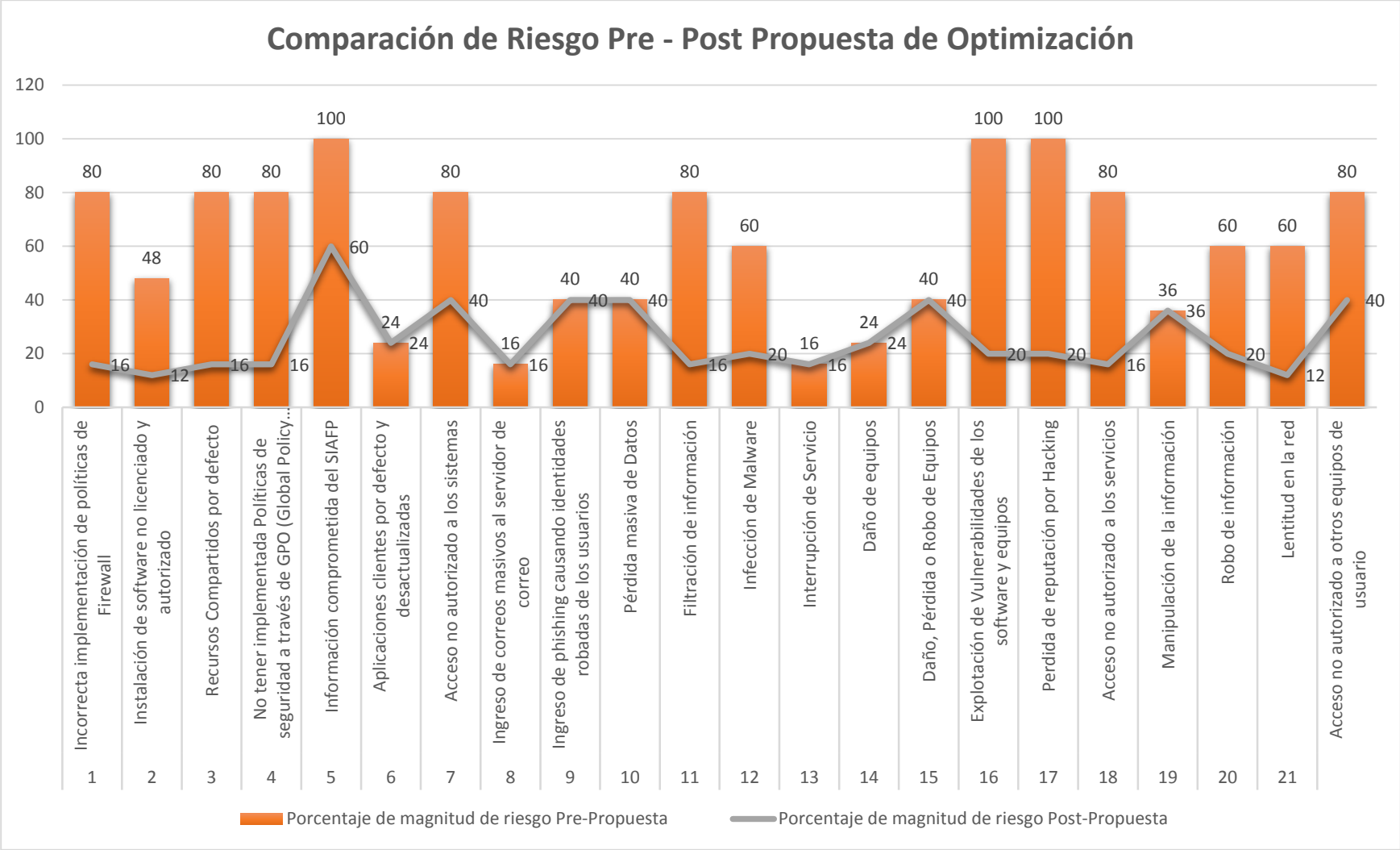
Tabla 14: Evaluación de Riesgos

No	Riesgo	Probabilidad	Impacto	Magnitud del Riesgo	Tratamiento
Software					
R1	Incorrecta implementación de políticas de Firewall	1	4	4	No acción
R2	Instalación de software no licenciado y autorizado	1	3	3	No acción
R3	Recursos Compartidos por defecto	1	4	4	No acción
R4	No tener implementada Políticas de seguridad a través de GPO (Global Policy Object	1	4	4	No acción
R5	Información comprometida del SIAFP	3	5	15	Seguimiento
R6	Aplicaciones clientes por defecto y desactualizadas	2	3	6	Preventiva
R7	Acceso no autorizado a los sistemas	2	5	10	Preventiva
R8	Ingreso de correos masivos al servidor de correo	1	4	4	No Acción

No	Riesgo	Probabilidad	Impacto	Magnitud del Riesgo	Tratamiento
R9	Ingreso de phishing causando identidades robadas de los usuarios	1	5	10	Preventiva
Datos					
R10	Pérdida masiva de Datos	2	5	10	Preventiva
R11	Filtración de información	1	5	5	No acción
R12	Infección de Malware	1	5	5	No acción
Hardware					
R13	Interrupción de Servicios	1	4	4	No acción
R14	Daño de Equipos	3	2	6	Preventiva
Redes y Comunicaciones					
R15	Daño, Pérdida o Robo de Equipos	2	5	10	Preventiva
R16	Explotación de Vulnerabilidades de los software y equipos	1	5	1	No acción
R17	Perdida de reputación	1	5	5	No acción
R18	Acceso no autorizado a los servicios	1	4	4	No acción
R19	Manipulación de la información	3	3	9	Preventiva
R20	Robo de información	1	5	5	No acción
R21	Lentitud en la red	1	3	3	No acción
R22	Acceso no autorizado a otros equipos de usuario	2	5	10	Preventiva

Sin lugar a dudas, la implementación de la Propuesta de Optimización de Infraestructura de Seguridad, da como resultado, mejoras en los dominios de la ISO 27001-2013, reduciendo la probabilidad de explotación de las vulnerabilidades en dominios como, seguridad de las comunicaciones y aspectos de seguridad de la información y al igual que la mitigación de los riesgos críticos el que el estado es aceptable, fortaleciendo la infraestructura tecnológica de seguridad de la institución. Ver figura 13.

Figura 13: Comparativas de Riesgo Pre – Post Propuesta de Optimización



8. PLAN DE IMPLEMENTACION DE LA INFRAESTRUCTURA TECNOLÓGICA

En este capítulo es importante, considerar cada uno de los elementos de la Propuesta de Optimización de la Infraestructura de Seguridad de AMUNIC y es fundamental asegurar que cada uno de los activos y servicios evaluados, contengan una serie de tareas, tiempo, recursos tecnológicos, humanos y financieros para obtener los resultados deseados. Ver tabla 16

8.1. Definiendo Prioridades

La definición de prioridades de cada solución en este plan de implementación es basada de acuerdo a estos aspectos (ver tabla 15):

- Impacto en lograr una modernización, eficiencia y efectividad en la administración de las operaciones diarias.
- Impacto en proporcionar información oportuna y de calidad para apoyar la gestión institucional, tanto a nivel de control administrativo como en el nivel gerencial.
- Impacto en la mejora de la seguridad de la infraestructura tecnológica de AMUNIC.
- Urgencia operativa.

Se entenderá:

1 como alta	**2** como media	**3** como baja prioridad.

Proyecto	Prioridad	Impacto en lograr una modernización	Impacto en proporcionar información oportuna	Impacto en la mejora de la seguridad de la infraestructura tecnológica	Urgencia operativa
Creación de VLAN	1	1	2	1	2
Implementación de un Servidor Active Directory	1	1	3	1	1
Implementación de Configuración del WebFiltering en el UTM existe	1	2	3	1	2
Implementación de módulo de Auditoria del SIAFP	1	1	1	1	1
Implementación de módulo Antispam conforme a las necesidades de AMUNIC	2	2	1	1	2

Tabla 15: Definición de Prioridades

Tabla 16: Relación de controles, tareas, costos y recurso técnicos - humanos

Solución	**Tareas**	**Estimación de costos**	**Recursos técnicos**	**Recursos humanos**
Creación de VLAN	IP Planning	U$ 50.00	* PC de técnico	*Personal de Informática * Técnico de redes
	Configuración inicial de los switches según las buenas prácticas, incluyendo comunidad de lectura/escritura	U$ 6,800.00 U$ 80,000.00	*Compra de Switches de distribución (4) *Compra de Switches core (2 para asegurar redundancia) * PC de técnico	*Personal de Informática * Técnico de redes
	Hardening de configuración de switches	U$ 5,000.00	*Switches de distribución y core * PC de técnico	*Personal de Informática * Técnico de redes
	Configuración de las VLANS necesarias y VTP Server		*Switches de distribución * PC de técnico	*Personal de Informática * Técnico de redes
	Configuración de la redundancia de los switches por spanning tree		*Switches de distribución *PC de técnico	*Personal de informática * Técnico de redes

Solución	Tareas	Estimación de costos	Recursos técnicos	Recursos humanos
			* Cables de red Cat 6	
	Configurar la redundancia de conexión con el datacenter		*Switches de distribución * PC de técnico * Cables de red Cat 6	*Personal de Informática * Técnico de redes
	Configuración de IP helper		*Switches de distribución *PC de técnico *Servidor DHCP	*Personal de Informática * Técnico de redes
	Configuración de reenvió de logs a servidor de monitoreo		*Switches de distribución * PC de técnico *Servidor Syslog	*Personal de informática * Técnico de redes
	Pruebas de interconexión		*Switches de distribución *PC de técnico * Cables de red Cat 6	*Personal de Informática * Técnico de redes
	Inclusión de verificación SPF	U$ 200.00	*Equipo Antispam	*Personal de Informática

Solución	Tareas	Estimación de costos	Recursos técnicos	Recursos humanos
Implementación de módulo Antispam conforme a las necesidades de AMUNIC			*PC de Técnico	*Técnico de seguridad
	Inclusión de verificación RDNS		*Equipo Antispam *PC de Técnico	*Personal de Informática *Técnico de seguridad
	Configuración de listas RBL		*Equipo Antispam *PC de Técnico	*Personal de informática *Técnico de seguridad
	Inclusión de BATV			
	Inclusión de DKIM			
	Inclusión de DMARC			
	Monitoreo de comportamiento SPAM para correos entrantes y salientes		*Equipo Antispam * PC de técnico	*Personal de Informática *Técnico de seguridad
	Implementación de cuarentena para revisión posterior de correos		*Equipo Antispam *PC de Técnico	*Personal de Informática *Técnico de seguridad
	Implementación de listas blancas y listas negras tanto por dominio de correo como por IP		*Equipo Antispam *PC de Técnico	*Personal de Informática *Técnico de seguridad

Solución	**Tareas**	**Estimación de costos**	**Recursos técnicos**	**Recursos humanos**
Implementación de un Servidor Active Directory	Instalación del sistema operativo siguiendo las buenas prácticas ofrecidas por el fabricante	U$ 4,100.00	*Compra del Server *Licencia de Windows Server 2016	*Personal de Informática *Ingeniero de servidores
	Instalación del servicio de Active Directory y configuración del mismo siguiendo las buenas prácticas ofrecidas por el fabricante	U$ 1,500.00	* Server * PC de Prueba	*Personal de Informática *Ingeniero de servidores
	Creación de las políticas de dominio			
	Creación de grupos de usuarios, incluyendo los grupos de permisos de navegación			
	Prueba de políticas de AD			
Implementación de Configuración	Uso de grupos de navegación del AD	U$200.00	* Equipo UTM *PC de Técnico	*Personal de informática *Técnico de seguridad

Solución	Tareas	Estimación de costos	Recursos técnicos	Recursos humanos
del WebFiltering en el UTM existe	Creación de políticas de navegación según las necesidades de la empresa			
	Pruebas de políticas de navegación			
Implementación de módulo de Auditoria del SIAFP	Análisis de requerimientos	U$3,500.00	*Servidor de SIAFP *Códigos fuentes	*Directora Administrativa *Personal de Informática *Contador *Personal outsourcing
	Contratación del outsourcing			*Especialista en Oracle *Personal de Informática *Personal de adquisiciones
	Programación del módulo y pruebas			*Personal de Informática *Usuarios del SIAFP *Personal outsourcing

Dentro de las soluciones no se contempla realizar cableado, pues se reutilizará y aprovechará el existente, al igual que los demás dispositivos como servidores, Router y Access Point.

Los controles de la propuesta (ver tabla 16) que tienen relacionado la adquisición o contratación de servicios, tendrán que respectarse y cumplirse los tiempos que lleva el proceso de contratación de bienes de acuerdo a la ley 801.

8.2. Estimación de tiempos y costos

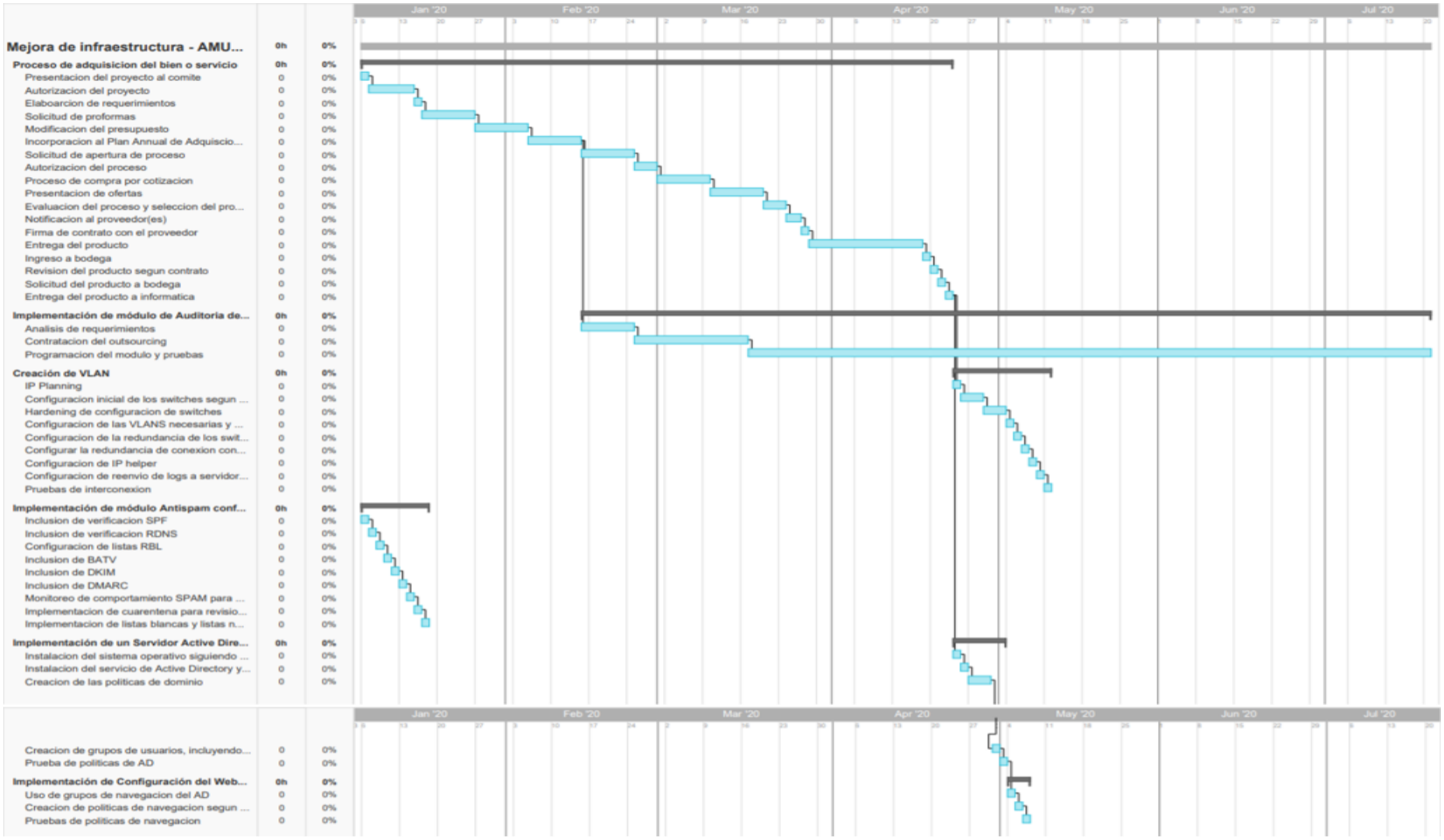
La siguiente tabla muestra la estimación de tiempo y costos para el desarrollo de cada uno de las soluciones propuestos en este plan. Ver tabla 17 y Figura 14

Fuentes de Financiación: La fuente principal de financiación es el disponible con que cuenta AMUNIC, dado que la relación costo beneficio es de 100/100, por todos los argumentos expuestos a lo largo de este trabajo de investigación.

Proyecto	Inversión US Dólares	Tiempo	Responsable
Creación de VLAN	**91,850.00**	**4 meses**	**Responsable de Informática**
Implementación de un Servidor Active Directory	**5,600.00**	**4 meses**	**Responsable de Informática**
Implementación de Configuración del WebFiltering en el UTM existe	**200.00**	**2 días**	**Responsable de Informática**
Implementación de módulo de Auditoria del SIAFP	**3,500.00**	**8 meses**	**Responsable de Informática/Outsourcing**
Implementación de módulo Antispam conforme a las necesidades de AMUNIC	**200.00**	**2 días**	**Responsable de Informática/ Outsourcing**
Totales	**100,850.00**		

Tabla 17: Estimación de Costos de los Controles de la Propuesta de Optimización de la Infraestructura Tecnológica

Figura 14: Cronograma de la Implementación de la propuesta de Optimización de AMUNIC



9. CONCLUSIONES

Producto del diagnóstico realizado a la infraestructura tecnológica de AMUNIC, se encontró un sin número de riesgos que amenazan la triada de la seguridad informática entre estos:

- Recursos compartidos
- Explotación de vulnerabilidades de los software y equipos
- Acceso no autorizado a otros equipos
- No tener implementado políticas de seguridad a través de GPO
- Información comprometida del SIAFP
- Incorrecta implementación de políticas del Firewall.

La Propuesta de Optimización de la Infraestructura Tecnológica permite pasar los riesgos críticos de un estado de tratamiento correctivo a un nivel aceptable proactivo y de esta manera, se fortalece la infraestructura tecnológica a través de la adquisición y actualización de dispositivos de seguridad y red, dando las siguientes soluciones:

- Control de acceso a usuarios y equipos
- Control de equipos de red por medio de monitoreo y Agilización en el tráfico de la red.
- Control en la navegación de los usuarios en dependencia de los perfiles
- Reducir el ingreso de correos maliciosos
- Control de las transacciones realizadas en SIAFP por roles y cuentas de usuarios para auditorias

La Propuesta de Optimización de la Infraestructura Tecnológica, propone un plan de implementación de la infraestructura de seguridad que incluye estimaciones de costos, actividades, recursos tecnológicos y humanos, entendiendo esto último como la aprobación de la propuesta y la adquisición de infraestructura necesaria.

10. RECOMENDACIONES

Para continuar con una evaluación posterior de riesgos que actualmente no son considerados críticos, pero podrían cambiar su estado por las vulnerabilidades que se presenten en la infraestructura tecnológica; es necesario que la presente investigación se tome como referencia porque facilitará el análisis y tratamiento de los riesgos.

Las soluciones que contempla la propuesta de optimización de la infraestructura tecnológica de seguridad de AMUNIC deben implementarse para mitigar los riesgos críticos a los que están expuestos los servicios, priorizado en una primera fase la implementación del módulo de auditoria del Sistema Integral Administrativo Financiero y Planificación (SIAFP) ya que este control es independiente del resto de controles.

Una vez implementado el módulo de auditoria del SIAFP, debe seguirse el orden planeado en la propuesta de optimización de la infraestructura tecnológica de seguridad de AMUNIC, es decir la Creación de VLANs, Implementación del módulo Antispam, Implementación de servidor Active Directory e implementación de WebFiltering.

Los usuarios de la institución deben recibir un ciclo de capacitación y socialización de las propuestas a ser implementadas para conocer y adoptar la política de cambio de seguridad informática en pro de las mejores prácticas.

11. GLOSARIO

AMUNIC: Asociación de Municipios de Nicaragua

SIAFP: Sistema Integral Administrativo Financiero

BD: Base de Datos

Firewall: Un firewall o cortafuegos es un dispositivo de hardware o un software que nos permite gestionar y filtrar la totalidad de tráfico entrante y saliente que hay entre 2 redes o computadoras de una misma red.

Switch: es un dispositivo que sirve para conectar varios elementos dentro de una red

ISP: Sistema de Prevención de Intrusos

IDS: Sistema de Detección de Intrusos

PC: Computadora Personal

TI: Tecnología de la Información

Outsourcing: 'subcontratación', 'externalización' o 'tercerización, proceso en el cual una organización contrata a otras empresas externas para que se hagan cargo de parte de su actividad o producción.

DNS: Sistema de Nombres de Dominio

VPN: Red Privada Virtual

NAC: Control de Acceso a la Red

LAN: Red de área Local

VLAN: Red de área local virtual

AD: Servidor de Directorio Activo

UTM: Gestión Unificada de amenazas, básicamente es un cortafuego de red que engloban múltiples funcionalidades (servicios) en una misma máquina de protección perimetral.

SIEM: Gestión de Eventos e Información de Seguridad

IDE: Entorno de desarrollo integrado**,** editor de código fuente

Antispam: Es un método para prevenir correos basura.

Wireless: Red sin cable, inalámbrico

Backbone: principales conexiones troncales de Internet.

TCP: Protocolo de control de transmisión

IP: Protocolo de Internet

Hacker: es alguien que descubre las debilidades de un computador o de una red informática

UDP: Protocolo de datagrama de usuarios

DHCP: Protocolo de configuración dinámica de host

LDAP: Protocolo Ligero/Simplificado de Acceso a Directorios

12. REFERENCIAS BIBLIOGRAFICAS

1. Areitio, J. (2008). *Seguridad de la información. Paraninfo*.
2. Blaustein, Leon. (2014). *¿Cómo ayuda la segmentación de la red a proteger la red empresarial?* Recuperado de https://searchdatacenter.techtarget.com/es/consejo/Como-ayuda-la-segmentacion-de-la-red-a-proteger-la-red-empresarial

3. Como configurar VLAN en Cisco Switch. Recuperado de http://blog.capacityacademy.com/2014/06/06/cisco-ccna-como-configurar-vlan-en-switch-cisco/

4. Como configurar Port Security en Cisco Switch. Recuperado de http://blog.capacityacademy.com/2014/08/21/ccna-security-como-configurar-port-security-en-cisco-switch/

5. Consejo Superior de Administración Electrónica del Gobierno de España. (2012). *Metodología de Análisis y Gestión de Riesgo de los Sistemas de Información MAGERIT versión 3.0.* Madrid, España. Recuperado de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?comentarioContenido=0#.XcxfR9VKgdU

6. Fernández Collado, Carlos Baptista, Lucio María del Pilar, Hernández Sampieri, Roberto. (6ta Edición). 2014. *Metodología de la Investigación.* Recuperado de http://observatorio.epacartagena.gov.co/wp-content/uploads/2017/08/metodologia-de-la-investigacion-sexta-edicion.compressed.pdf

7. Giraldo, J. (2006). *Manual para seminarios de investigación en psicología profundización conceptual y textual.* Introducción a Active Directory. Recuperado de https://support.microsoft.com/es-es/help/196464

8. Instituto Nacional de Ciberseguridad. (s.f). Desarrollando *Cultura en Seguridad*. Recuperado de https://www.incibe.es/protege-tu-empresa/que-te-interesa/desarrollar-cultura-en-seguridad

9. Instituto Nacional de Ciberseguridad. (s.f). Protección *de la Información*. Recuperado de https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

10. International Organization for Standardization. Estándar ISO/IEC 27001. Recuperado de https://www.iso.org/isoiec-27001-information-security.html

11. Lista de control de Acceso. (s.f). En Wikipedia. Recuperado de https://es.wikipedia.org/wiki/Lista_de_control_de_acceso

12. Lowe, D. (10th Ed). (2013). *Networking for dummies*. Recuperado de http://www.nortonaudio.com/Ficheiros/1118474082.Netwo.pdf

13. Simon Errol. (1996). *Interactive Distributed Multimedia System and Telecomunication Services.*

14. Soriano Miguel. (s.f). Seguridad en redes y seguridad de la información. Recuperado de http://improvet.cvut.cz/project/download/C2ES/Seguridad_de_Red_e_Informacion.pdf

15. Stalling, W. (s.f). *Cryptography and Network Security Principles and Practices.* Recuperado de http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/material-cripto-seg/2014-/Stallings/Stallings_Cryptography_and_Network_Security.pdf

16. Villalobos, J. (s.f). Principios básicos de seguridad en bases de datos. Recuperado de https://revista.seguridad.unam.mx/numero-12/principios-basicos-de-seguridad-en-bases-de-datos

13. ANEXOS

Anexo 1: Entrevista dirigida a usuarios SIAFP y directores de Áreas

Entrevistados:

- 5 usuarios del SIAFP
- 7 directores

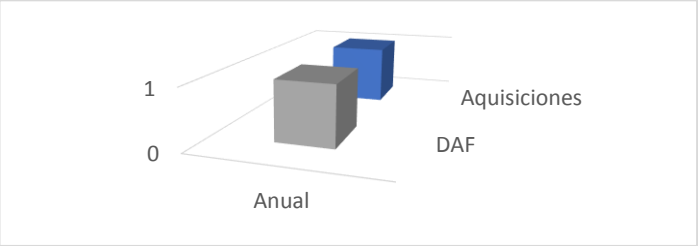
1. ¿Existen procedimientos e instructivos establecidos en el área?

Si (continuar con la pregunta 2)

No (continuar con la pregunta 3)

2. ¿Cada cuánto tiempo se actualizan los Procedimientos?

Mensual	
Trimestral	
Semestral	
Otros	Anual



3. ¿Se tiene identificado y categorizado los activos de información del área?

Si

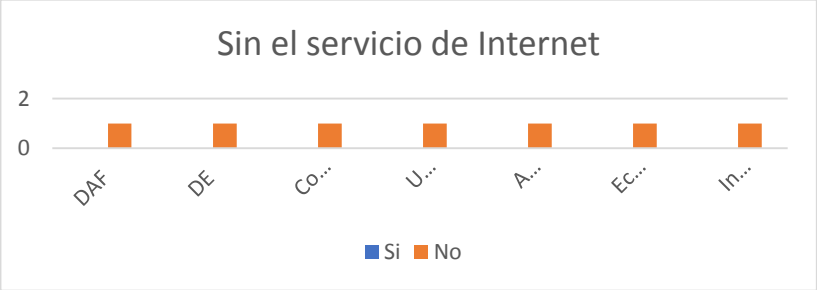
Nombre del activo	Categoría (Confidencial, pública, de uso interno)

No:

Todas las áreas y unidades manifiestan no tener identificado y categorizado los activos

4. ¿Ha ocurrido algún evento que ha afectado a la continuidad de sus actividades?

Suceso	Tiempo de interrupción
Sin el servicio de Internet	1 día



Todas las áreas expresan que el evento más reciente es no tener el servicio de Internet con la interrupción de 1 día

5. ¿Los usuarios poseen tarjetas de acceso para ingresar al área?

Si (continuar con la pregunta 7)

No (continuar con la pregunta 6)

R: No, solo los jefes de áreas tienen llaves para ingresar a las oficinas

6. ¿Por qué razón los usuarios no poseen tarjetas o llave de acceso al área?

No las provee la Institución	Por políticas solo los jefes de las áreas
No son necesarias	
No hay sistemas de control de acceso	
Otras	

7. ¿Se han presentados retrasos o problemas por falta de controles de seguridad (antivirus no actualizado, la no existencia de restricciones a internet, entre otros) en los equipos utilizados por los usuarios del área?

Problema	Criticidad (Alta, media, baja)
Ingreso de Virus por memoria de	Media

8. ¿Quién es la persona responsable de definir los accesos que debe tener cada usuario del área?

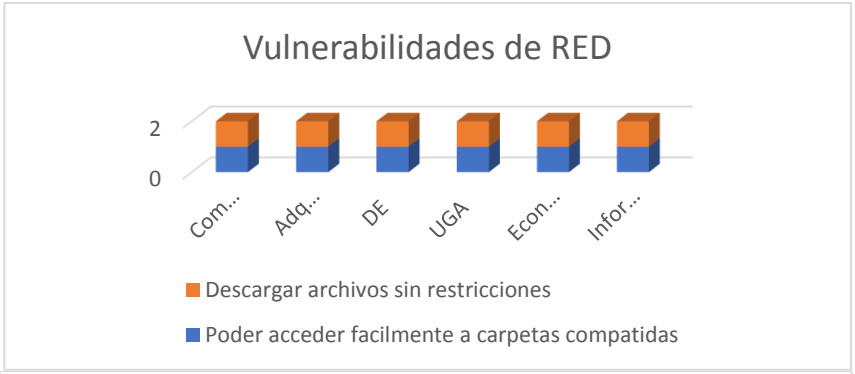
Los jefes de áreas son los responsables de definir los accesos que debe tener cada usuario

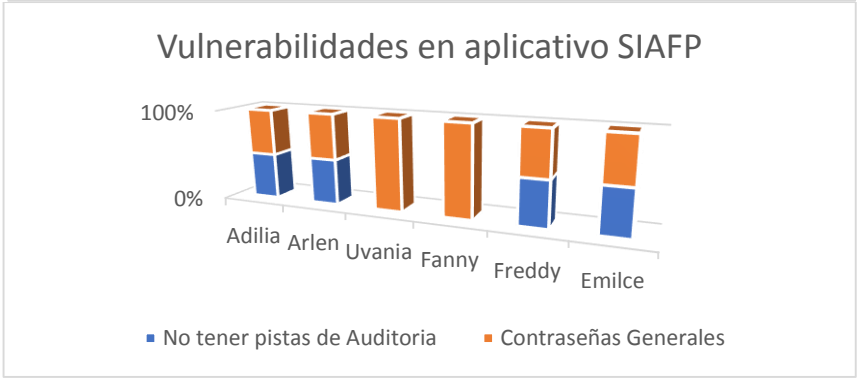
9. ¿Cuándo se le bloquea el acceso a la estación de trabajo, correo electrónico o sistema utilizado en el área, a quien solicita ayuda?

El 100% de los usuarios solicitan ayuda a Unidad de Informática

10. ¿Ha detectado alguna vez una vulnerabilidad en los aplicativos de la institución?

Si (continuar con la pregunta 11)





El otro 50% de la muestra señalo vulnerabilidades referidas al acceso a la red

No (continuar con la pregunta 12)

11. ¿A quién notificó la vulnerabilidad encontrada?

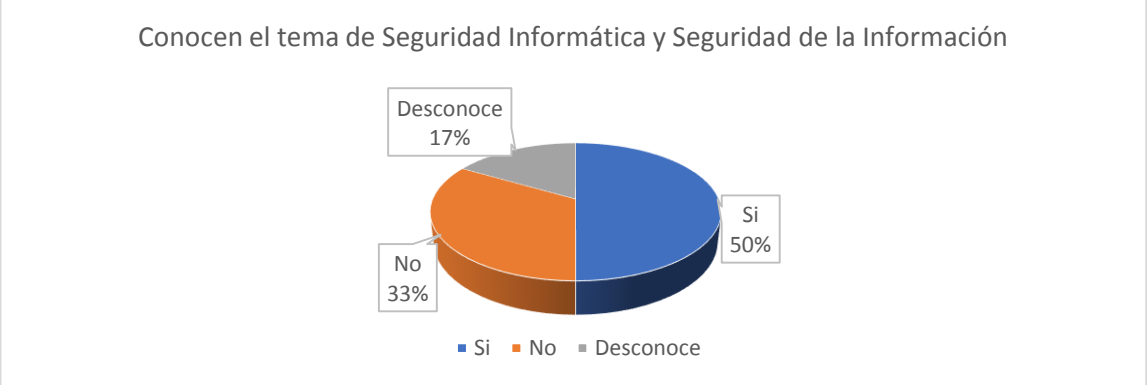
El 100% notifica a su jefe inmediato y luego a Informática

12. ¿El Departamento de Sistema los capacita para el correcto uso de los nuevos aplicativos o cuando realiza modificaciones en los aplicativos existentes?

100% manifiesta que Si, la Unidad de Informática capacita en el correcto uso de nuevo o modificaciones de aplicativos

13. ¿Conoce de qué se trata el tema de Seguridad Informática y Seguridad de la Información?

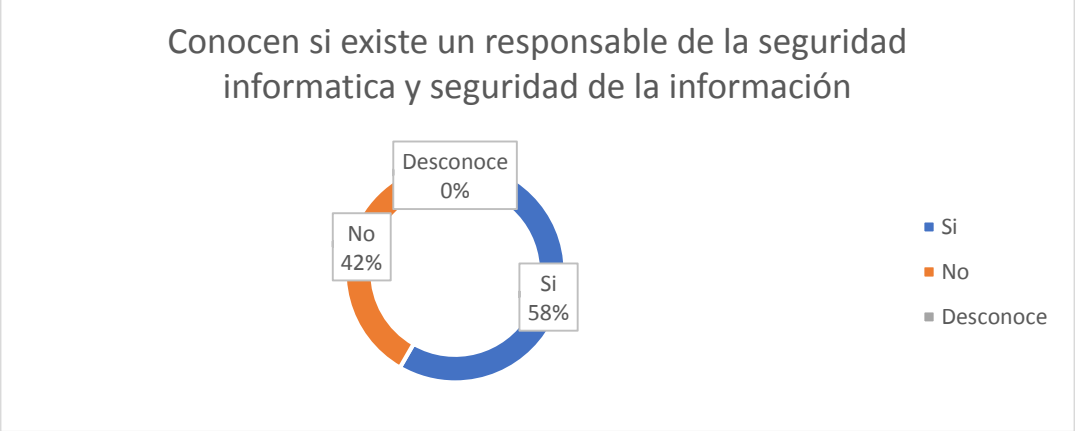
Sí ○ No ○ Desconoce ○



14. ¿Conoce si en la Institución existe un responsable o área encargada de la seguridad informática y seguridad de la información?

Del 100% de la muestra, el 58% manifiesta que si existe.

Sí ○ No ○ Desconoce ○



15. ¿Qué área considera que debe ser responsable de la seguridad de la informática y de la información? (se puede seleccionar varias alternativas)

Informática ☐

Administrativo ☐

Todas las áreas ☐

Otra, ¿cuál? ☐

El 100% de muestra dice: informática

16. ¿Cuántas capacitaciones ha recibido acerca de temas seguridad de la información en el último año?

Más de 5 ○ Menos de 5 ○ Nunca ha recibido ○

En este año el 100% de la muestra dicen menos de 5 capacitaciones en temas de seguridad.

17. ¿Las contraseñas que utiliza tiene combinación de números, letras y es de más de 10 caracteres?

Solo Números y más de 10 caracteres

Solo letras y más de 10 caracteres

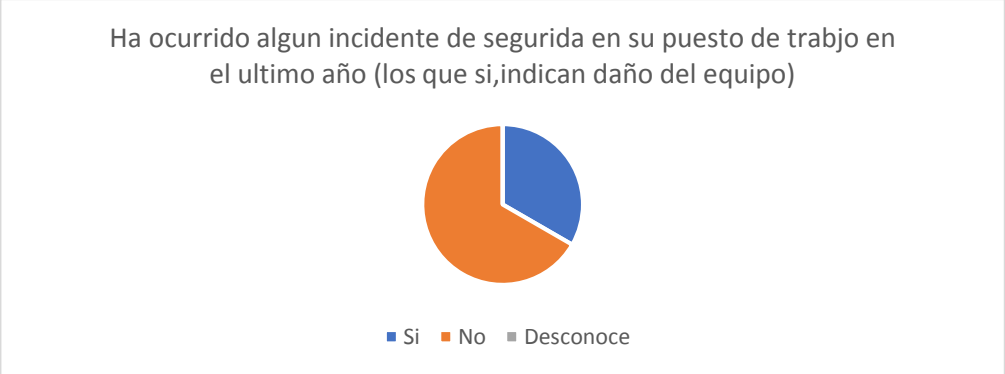
Números y letras, más de 10 caracteres

¿Otras, describa?

El 100% de la muestra dice utilizar combinación de letras y menos de 10 caracteres.

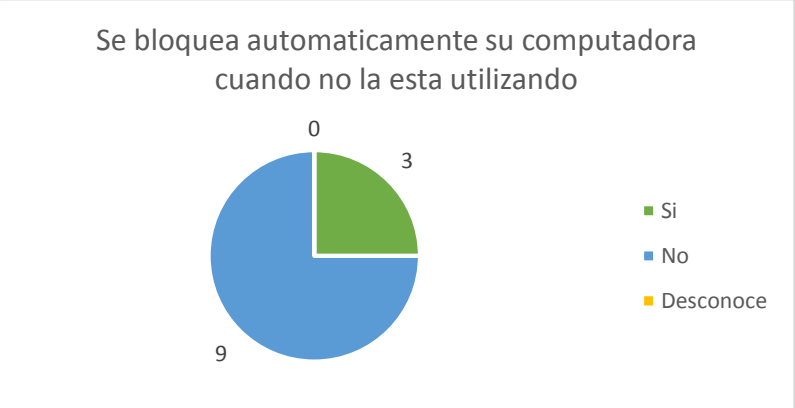
18. ¿Ha ocurrido algún incidente de seguridad en su puesto de trabajo en el último año? (bloqueo de la computadora, pérdida de documentos, daño de computadora, entre otros)

Sí ○ No ○ Desconoce ○



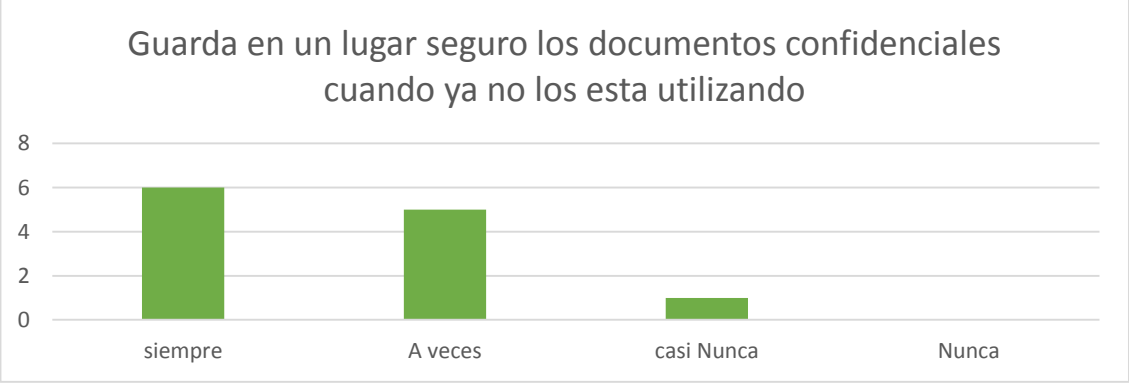
19. ¿Se le bloquea automáticamente su computadora cuando no la está utilizando?

Sí ○ No ○ Desconoce ○



20. ¿Guarda en un lugar seguro (caja fuerte, gabinetes con llave) los documentos confidenciales cuando ya no los está utilizando?

Siempre ○ A veces ○ Casi Nunca ○ Nunca ○



21. ¿Cuándo tiene algún incidente de seguridad (falla de equipo, bloqueo de contraseña, pérdida de información) a quién lo notifica? (se puede seleccionar varias alternativas)

Responsable de Informática ☐

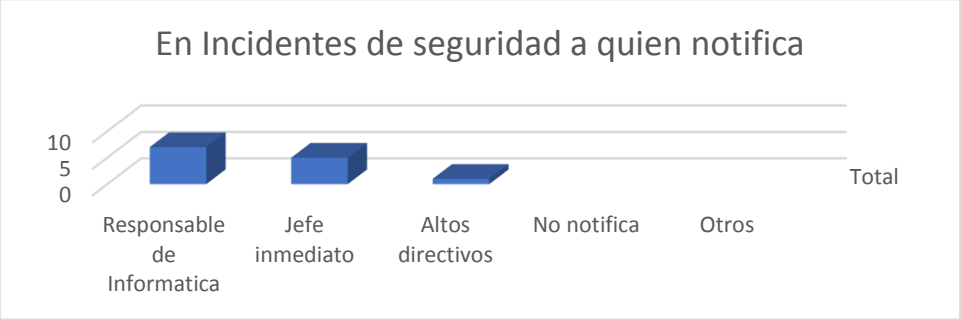
Jefe Inmediato ☐

Altos Directivos ☐

No notifica ☐

Otros,

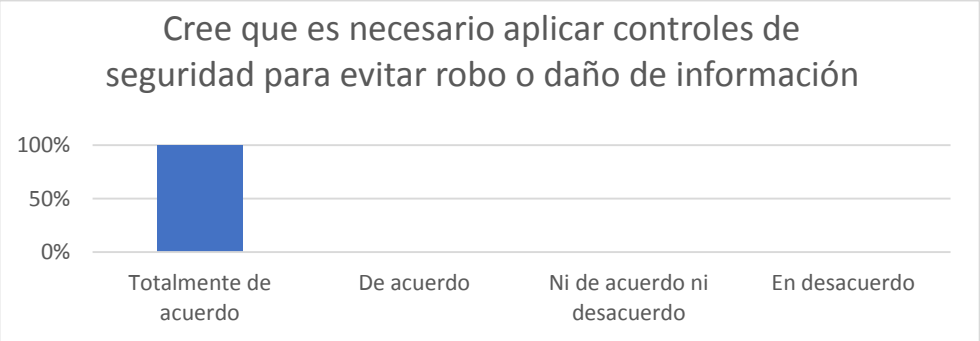
¿Cuál? ☐



22. ¿Cree que es necesario aplicar controles de seguridad para evitar robo o daño de información importante para la Institución?

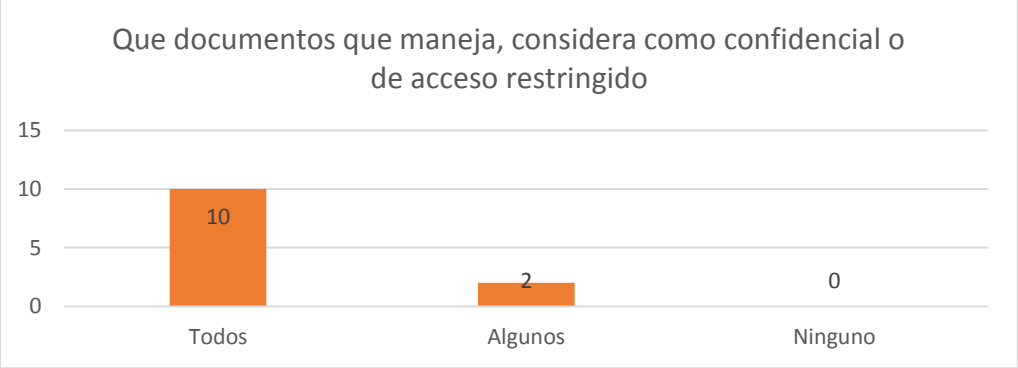
Totalmente de acuerdo ☐ De acuerdo ☐

Ni de acuerdo ni en desacuerdo ☐ ¿En desacuerdo, por qué? ☐



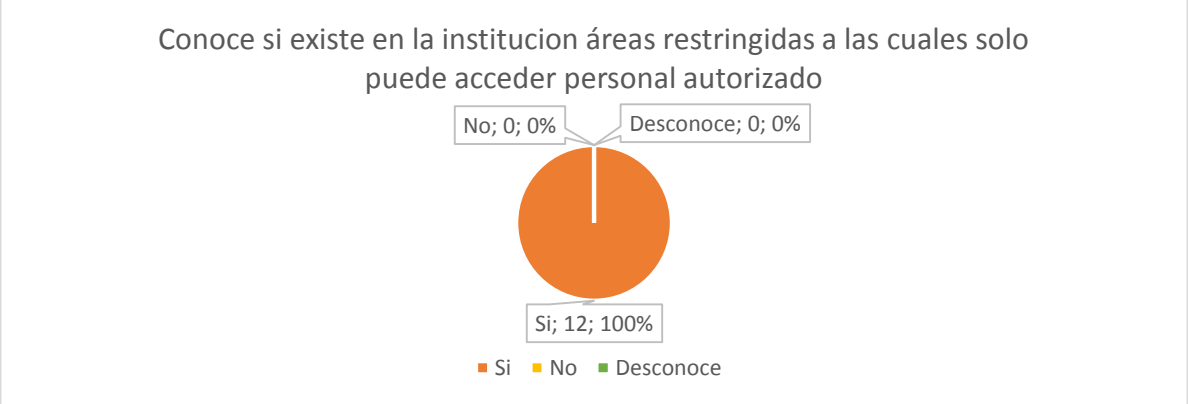
23. ¿Qué documentos que maneja, considera usted que son catalogados como confidencial o de acceso restringido?

Todos ○ Algunos ○ Ninguno ○



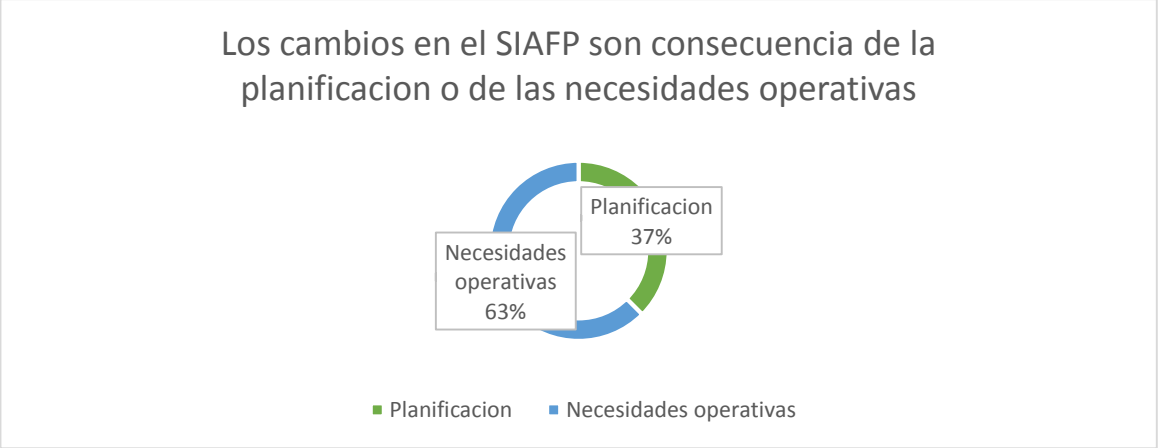
24. ¿Conoce si existe en la Institución áreas restringidas a las cuales solo pueden acceder personal autorizado?

Sí ○ No ○ Desconoce ○



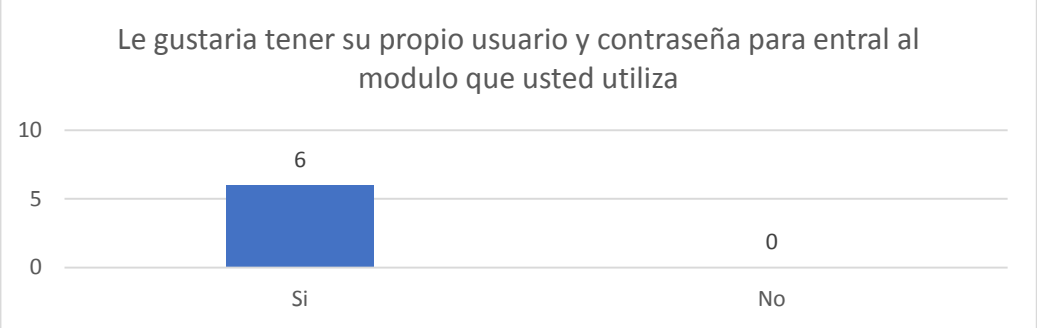
25. ¿Los cambios en los sistemas son consecuencia de la planificación o de las necesidades operativas?

Sí ○ No ○



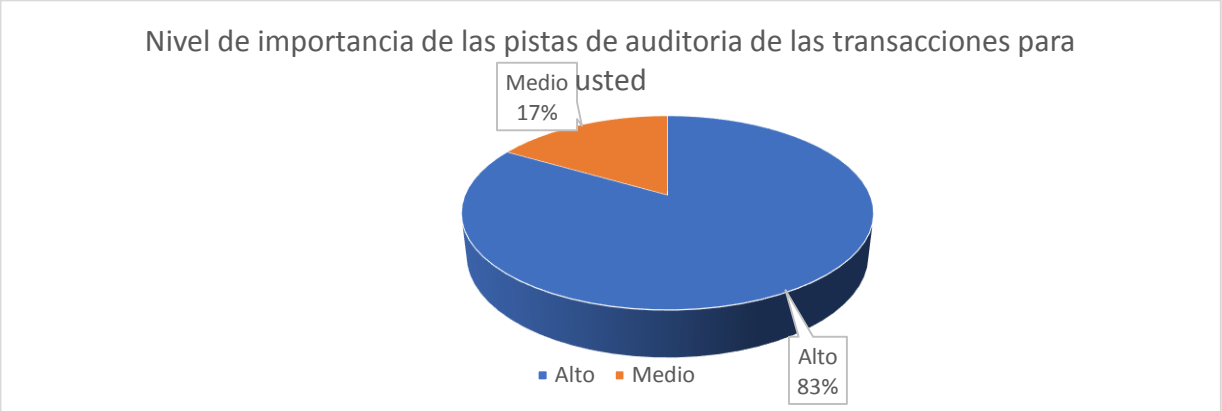
26. ¿Le gustaría tener su propio usuario y contraseña para entrar al módulo que usted utiliza?

Si ____ No _



27 ¿cuál es el nivel de importancia de las pistas de auditorías de las transacciones para usted?

Alto___ medio ____ bajo___



28 ¿Qué opina usted de una mejora del sistema SIAFP para llevar un mejor control de las transacciones realizadas en él?

_____
_____
_____

Anexo 2: Modelo de Política de seguridad para control de acceso

Antecedentes

Controlar quien accede a la información de nuestra empresa es un primer paso para protegerla. Es esencial que podamos decidir quién tiene permisos para acceder a nuestra información, como, cuando y con qué finalidad.

A la hora de gestionar el control de acceso a nuestros datos debemos tener en cuenta que la información, los servicios y las aplicaciones utilizadas no tienen por qué ubicarse de manera centralizada en nuestras instalaciones, sino que pueden estar diseminadas en equipos y redes remotas propias o de terceros. También tenemos que considerar que cada vez es más habitual el uso de dispositivos móviles en los centros de trabajo. En ocasiones estos dispositivos son propiedad del propio empleado lo que dificulta esta tarea.

Por otra parte, el registro de los accesos en logs de los sistemas va a ser determinante para analizar los incidentes de seguridad.

Objetivos

- Establecer quien, como y cuando puede acceder a los activos de información de la empresa y registrar convenientemente dichos accesos.

Se usará un Checklist que incluyen una serie de controles para revisar el cumplimiento en lo relativo al control de acceso.

Checklist:

Los controles se clasificarán en dos niveles de complejidad:

Básico (B): el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.

Avanzado (A): el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente alcance:

- Procesos (PRO): aplica a la dirección o al personal de gestión.
- Tecnología (TEC): aplica al personal técnico especializado.
- Personas (PER): aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
B	PRO	Política de usuarios y grupos Defines los roles de usuarios y de grupos en función del tipo de información al que podrán acceder.	☐
B	PRO	Asignación de permisos Asignas los permisos necesarios para que cada usuario o grupo de usuarios solo puedan realizar las acciones oportunas sobre la información a la que tienen acceso.	☐
B	TEC	Creación/modificación/borrado de cuentas de usuario con permisos Defines y aplicas un procedimiento para dar de alta/baja o modificar las cuentas de usuario.	☐
B	TEC	Cuentas de administración Gestionas las cuentas de administración de sistemas y aplicaciones teniendo en cuenta su criticidad.	☐
A	TEC	Mecanismos de autenticación Determinas e implantas las técnicas de autenticación más apropiados para permitir el acceso a la información de tu empresa.	☐
A	TEC	Registro de eventos Estableces los mecanismos necesarios para registrar todos los eventos relevantes en el manejo de la información de tu empresa.	☐
B	TEC	Revisión de permisos Revisas cada cierto tiempo que los permisos concedidos a los usuarios son los adecuados.	☐
B	TEC	Revocación de permisos y eliminación de cuentas Desactivas los permisos de acceso y eliminas las cuentas de usuario una vez finalizada la relación contractual.	☐

Revisado por: _____ Fecha: _____

Puntos clave

Los puntos clave de esta política son:

- Política de usuarios y grupos. Definiremos una serie de grupos que tendrán determinados accesos para cada tipo de información establecido. Esta clasificación se puede hacer teniendo en cuenta los siguientes aspectos:
    - en función del área o departamento al que pertenezca el empleado;
    - en función del tipo de información a la qué accederá;
    - en función de las operaciones permitidas sobre la información a la que se tiene acceso.

En función de los criterios anteriores podemos establecer diversos perfiles de usuarios.

- Asignación de permisos. Una vez establecidos los tipos de información, los perfiles de usuarios y los grupos existentes, podremos concretar los tipos de acceso a la información a los que tienen derecho. Los permisos concretarán que acciones pueden realizar sobre la información (creación, lectura, borrado, modificación, copia, ejecución, etc.). Como norma general siempre se otorgará el mínimo privilegio en el establecimiento de los permisos.
- Creación/modificación/borrado de cuentas de usuario. Para permitir el acceso real a los sistemas de información de la empresa debemos tener un procedimiento que permita gestionar la creación/modificación/borrado de las cuentas de acceso de los usuarios (por ejemplo: cuenta de correo, acceso al CRM, etc.) indicando quién debe autorizarlo. Detallaremos los datos identificativos de las mismas, las acciones que se permiten y las dotaremos de las credenciales de acceso correspondientes que deberán ser entregadas de forma confidencial a sus dueños. Se incluirán asimismo parámetros tales como la caducidad de las contraseñas y los procedimientos de bloqueo oportunos. Se debe informar al usuario de estos requisitos al entregarle las credenciales, así como de la Política de contraseñas.
- Cuentas de administración. Las cuentas de administración permiten realizar cualquier acción sobre los sistemas que administran, por lo que deben ser gestionadas con la máxima precaución. Tendremos en cuenta los siguientes aspectos:
    - utilizar este tipo de cuentas únicamente para realizar labores que requieran permisos de administración;
    - implantar un control de acceso basado en un doble factor de autenticación;
    - registrar convenientemente todas sus acciones (registro de logs);

    - cuando accedemos a un sistema en modo administrador, este debe indicarnos claramente tal situación a través de su contexto;
    - el acceso como administrador debería ser notificado convenientemente;
    - evitar que los privilegios de las cuentas de administrador puedan ser heredados;
    - las claves de acceso deben ser lo más robustas posibles y ser cambiadas con frecuencia;
    - pueden ser sometidas a auditorías periódicas;
- Mecanismos de autenticación. Definiremos e implantaremos los mecanismos de autenticación más adecuados para permitir el acceso a la información de nuestra empresa. Tendremos en cuenta aspectos tales como:
    - utilizar mecanismos de autenticación internos o basados en servicios de autenticación de terceros (como la federación de identidades o el social-login)
    - las tecnologías que utilizaremos:
        - autenticación vía web
        - servicios de directorio
        - LDAP
    - factores de los mecanismos de autenticación (uno o varios):
        - algo que somos (a través de técnicas biométricas)
        - algo que sabemos (a través de contraseñas)
        - algo que tenemos (a través de dispositivos personales, tokens criptográficos)
- Registro de eventos. Estableceremos los mecanismos necesarios para registrar todos los eventos relevantes en el manejo de la información de la empresa. Registraremos convenientemente quién accede a nuestra información, cuando, cómo y con qué finalidad.
- Revisión de permisos. Revisaremos periódicamente que los permisos concedidos a los usuarios son los adecuados.
- Revocación de permisos y eliminación de cuentas. Al finalizar la relación contractual con el empleado es necesario revocar sus permisos de accesos a nuestros sistemas e instalaciones. Eliminaremos sus cuentas de correo, sus cuentas de acceso a los repositorios, servicios y aplicaciones. Además, exigiremos la devolución de cualquier activo de información que se le hubiese asignado (tarjetas de acceso o de crédito, equipos, dispositivos de almacenamiento, tokens criptográficos, etc.).

Anexo 3: Dirigida a la Unidad de Informática

CheckList ISO 27001-2013 – Cumplimiento de Dominios y Controles

¿Se cumple el control?		Si	No	Calculo
5	Políticas de seguridad de la información			0.00%
5.1	Directrices de gestión de la seguridad de la información			0
5.1.1	Políticas para la seguridad de la información		x	
5.1.2	Revisión de las políticas para la seguridad de la información		x	
6	Organización de la seguridad de la información			42.86%
6.1	Organización interna			3
6.1.1	Roles y responsabilidades en seguridad de la información	x		
6.1.2	Segregación de tareas	x		
6.1.3	Contacto con las autoridades	x		
6.1.4	Contacto con grupos de interés especial		x	
6.1.5	Seguridad de la información en la gestión de proyectos		x	
6.2	Los dispositivos móviles y el teletrabajo			0
6.2.1	Política de dispositivos móviles		x	
6.2.2	Teletrabajo		x	
7	Seguridad relativa a los recursos humanos			28.57%
7.1	Antes del empleo			2

7.1.1	Investigación de antecedentes	x		
7.1.2	Términos y condiciones del empleo	x		
7.2	Durante el empleo			3
7.2.1	Responsabilidades de gestión	x		
7.2.2	Concienciación, educación y capacitación en seguridad de la información	x		
7.2.3	Proceso disciplinario	x		
7.3	Finalización del empleo o cambio en el puesto de trabajo			1
7.3.1	Responsabilidades ante la finalización o cambio	x		
8	Gestión de activos			40.00%
8.1	Responsabilidad sobre los activos			4
8.1.1	Inventario de activos	x		
8.1.2	Propiedad de los activos	x		
8.1.3	Uso aceptable de los activos	x		
8.1.4	Devolución de activos	x		
8.2	Clasificación de la información			0
8.2.1	Clasificación de la información		x	
8.2.2	Etiquetado de la información		x	
8.2.3	Manipulado de la información		x	

8.3	Manipulación de los soportes			
8.3.1	Gestión de soportes extraíbles		x	1
8.3.2	Eliminación de Medios	x		
8.3.3	Transferencia física de medios		x	
9	Control de acceso			14.29%
9.1	Requisitos de negocio para el control de acceso			2
9.1.1	Política de control de acceso	x		
9.1.2	Acceso a las redes y a los servicios de red	x		
9.2	Gestión de acceso de usuario			0
9.2.1	Registro y baja de usuario		x	
9.2.2	Provisionamiento de acceso de usuario		x	
9.2.3	Gestión de privilegios de acceso		x	
9.2.4	Gestión de la información secreta de autenticación de los usuarios		x	
9.2.5	Revisión de los derechos de acceso de usuario		x	
9.2.6	Retirada o reasignación de los derechos de acceso		x	
9.3	Responsabilidades del usuario			0
9.3.1	Uso de la información secreta de autenticación		x	
9.4	Control de acceso a sistemas y aplicaciones			2
9.4.1	Restricción del acceso a la información	x		
9.4.2	Procedimientos seguros de inicio de sesión		x	

9.4.3	Sistema de gestión de contraseñas		x	
9.4.4	Uso de utilidades con privilegios del sistema		x	
9.4.5	Control de acceso al código fuente de los programas	x		
10	Criptografía			0.00%
10.1	Controles criptográficos			0
10.1.1	Política de uso de los controles criptográficos		x	
10.1.2	Gestión de claves		x	
11	Seguridad física y del entorno			40.00%
11.1	Áreas seguras			6
11.1.1	Perímetro de seguridad física	x		
11.1.2	Controles físicos de entrada	x		
11.1.3	Seguridad de oficinas, despachos y recursos	x		
11.1.4	Protección contra las amenazas externas y ambientales	x		
11.1.5	El trabajo en áreas seguras	x		
11.1.6	Áreas de carga y descarga	x		
11.2	Seguridad de los equipos			7
11.2.1	Emplazamiento y protección de equipos	x		
11.2.2	Instalaciones de suministro		x	
11.2.3	Seguridad del cableado	x		
11.2.4	Mantenimiento de los equipos	x		

11.2.5	Retirada de materiales propiedad de la empresa	x		
11.2.6	Seguridad de los equipos fuera de las instalaciones	x		
11.2.7	Reutilización o eliminación segura de equipos	x		
11.2.8	Equipo de usuario desatendido	x		
11.2.9	Política de puesto de trabajo despejado y pantalla limpia		x	
12	Seguridad de las operaciones			21.43%
12.1	Procedimientos y responsabilidades operacionales			3
12.1.1	Documentación de procedimientos operacionales	x		
12.1.2	Gestión de cambios		x	
12.1.3	Gestión de capacidades	x		
12.1.4	Separación de los recursos de desarrollo, prueba y operación	x		
12.2	Protección contra el software malicioso (malware)			1
12.2.1	Controles contra el código malicioso	x		
12.3	Copias de seguridad			1
12.3.1	Copias de seguridad de la información	x		
12.4	Registros y supervisión			2
12.4.1	Registro de eventos	x		
12.4.2	Protección de la información del registro	x		
12.4.3	Registros de administración y operación		x	
12.4.4	Sincronización del reloj		x	

12.5	Control del software en explotación			0
12.5.1	Instalación del software en explotación		x	
12.6	Gestión de la vulnerabilidad técnica			0
12.6.1	Gestión de las vulnerabilidades técnicas		x	
12.6.2	Restricción en la instalación de software		x	
12.7	Consideraciones sobre la auditoria de sistemas de información			0
12.7.1	Controles de auditoría de sistemas de información		x	
13	Seguridad de las comunicaciones			0.00%
13.1	Gestión de la seguridad de las redes			0
13.1.1	Controles de red		x	
13.1.2	Seguridad de los servicios de red		x	
13.1.3	Segregación en redes		x	
13.2	Intercambio de información			2
13.2.1	Políticas y procedimientos de intercambio de información		x	
13.2.2	Acuerdos de intercambio de información		x	
13.2.3	Mensajería electrónica	x		
13.2.4	Acuerdos de confidencialidad o no revelación	x		
14	Adquisición, desarrollo y mantenimiento de los sistemas de información			0.00%
14.1	Requisitos de seguridad en los sistemas de información			0
14.1.1	Análisis de requisitos y especificaciones de seguridad de la información		x	
14.1.2	Asegurar los servicios de aplicaciones en redes públicas		x	

14.1.3	Protección de las transacciones de servicios de aplicaciones		x	
14.2	Seguridad en el desarrollo y en los procesos de soporte			
14.2.1	Política de desarrollo seguro		x	
14.2.2	Procedimiento de control de cambios en sistemas	x		
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo		x	
14.2.4	Restricciones a los cambios en los paquetes de software	x		4
14.2.5	Principios de ingeniería de sistemas seguros		x	
14.2.6	Entorno de desarrollo seguro		x	
14.2.7	Externalización del desarrollo de software	x		
14.2.8	Pruebas funcionales de seguridad de sistemas		x	
14.2.9	Pruebas de aceptación de sistemas	x		
14.3	Datos de prueba			1
14.3.1	Protección de los datos de prueba	x		
15	Relación con proveedores			20.00%
15.1	Seguridad en las relaciones con proveedores			
15.1.1	Política de seguridad de la información en las relaciones con los proveedores		x	
15.1.2	Requisitos de seguridad en contratos con terceros	x		1
15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones		x	
15.2	Gestión de la provisión de servicios del proveedor			2

15.2.1	Control y revisión de la provisión de servicios del proveedor	x		
15.2.2	Gestión de cambios en la provisión del servicio del proveedor	x		
16	Gestión de incidentes de seguridad de la información			85.71%
16.1	Gestión de incidentes de seguridad de la información y mejoras			6
16.1.1	Responsabilidades y procedimientos	x		
16.1.2	Notificación de los eventos de seguridad de la información	x		
16.1.3	Notificación de puntos débiles de la seguridad		x	
16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	x		
16.1.5	Respuesta a incidentes de seguridad de la información	x		
16.1.6	Aprendizaje de los incidentes de seguridad de la información	x		
16.1.7	Recopilación de evidencias	x		
17	Aspectos de seguridad de la información para la gestión de la continuidad de negocio			0.00%
17.1	Continuidad de la seguridad de la información			0
17.1.1	Planificación de la continuidad de la seguridad de la información		x	
17.1.2	Implementar la continuidad de la seguridad de la información		x	
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información		x	
17.2	Redundancias			0
17.2.1	Disponibilidad de los recursos de tratamiento de la información		x	

18	Cumplimiento			57.14%
18.1	Cumplimiento de los requisitos legales y contractuales			4
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	x		
18.1.2	Derechos de Propiedad Intelectual (DPI)	x		
18.1.3	Protección de los registros de la organización	x		
18.1.4	Protección y privacidad de la información de carácter personal	x		
18.1.5	Regulación de los controles criptográficos		x	
18.2	Revisiones de la seguridad de la información			0
18.2.1	Revisión independiente de la seguridad de la información		x	
18.2.2	Cumplimiento de las políticas y normas de seguridad		x	

Anexo 4: Entrevista acerca de Seguridad Informática dirigida a la Unidad de Informática

Nota: Marcar con una X sus respuestas

1. ¿Existe un área o persona responsable de seguridad informática y seguridad de la información en la institución?

Sí ○ No ○

2. ¿Qué tipo de herramientas de seguridad tiene implementado en la institución? (se puede seleccionar varias alternativas)

- Software ☐
- Hardware ☐
- No tiene ☐
- Otros, indique cuáles ☐

3. ¿Tiene instalado antivirus en los equipos (PC, Laptop, Servidores)?

Sí ○ No (continuar con la pregunta 5) ○

4. ¿Qué software utiliza en la Institución para controlar software malicioso? (se puede seleccionar varias alternativas)

- Antivirus ☐
- Anti-Spam ☐
- Antispyware ☐
- Cortafuegos/firewall ☐
- Otros, indique cuáles ☐

5. ¿Cuáles de los siguientes mecanismos de autenticación utiliza en la Institución? (se puede seleccionar varias alternativas)

Firma electrónica digital ☐

Clave de Acceso ☐

No tiene ☐

Otros, indique cuáles ☐

6. ¿Se realiza un mantenimiento periódico en los sistemas de procesamiento de información y equipos informáticos?

Sí ○ No (continuar con la pregunta 8) ○

7. ¿Cada cuánto tiempo realizan mantenimientos en los sistemas de procesamiento de información? (se puede seleccionar varias alternativas)

Trimestral ☐

Semestral ☐

Mensual ☐

Otros, Indique el período ☐

8. ¿De cuántas computadoras dispone su Institución?

20 – 40 ○ 40 – 60 ○ 60 o más ○

9. ¿Disponen de servidores centrales de datos en la Institución?

Sí ○ No ○

10. Si su Institución tiene conexión WIFI, ¿existen restricciones de seguridad para el acceso de dichas conexiones?

Sí ○ No ○

11. ¿Se realizan respaldo de la información en la Institución?

Sí ○ No (continuar en 13) ○

12. ¿En caso de que se realice respaldo de información, con qué frecuencia lo realizan? (se puede seleccionar varias alternativas)

Diaria ☐

Semanal ☐

Mensual ☐

Otros, indique el período ☐

13. ¿Se utilizan mecanismos de bloqueo automático de los equipos de trabajo para cuando se encuentran desatendidos?

Sí ○ No ○

14. ¿Existen equipos que provean de energía ininterrumpida a los servidores y computadores de los usuarios?

Sí ○ No ○

15. ¿Qué servicios y sistemas considera más críticos en términos de disponibilidad? (se puede seleccionar varias alternativas)

De almacenamiento de datos ☐

Servicios de comunicación ☐

Sistemas de procesamiento de datos ☐

Otros, indique cuáles ☐

16. ¿Dónde se encuentran almacenados los medios de respaldos? (se puede seleccionar varias alternativas)

Dentro del área de sistemas ☐

Dentro de la empresa, pero fuera de la Unidad de Informática ☐

Fuera de la Institución ☐

No se realizan almacenamientos. ☐

Otros, indique cuáles ☐

17. ¿Durante el último año tuvieron algún incidente de seguridad grave de la información?

Sí ○ No ○ Desconoce ○

18. ¿Se mantiene un registro de fallas cuando ocurre algún evento en los sistemas de procesamiento de información (servidores, computadores, redes, etc.)?

Sí ○ No ○

19. ¿El acceso a internet en la Institución es limitado por? (se puede seleccionar varias alternativas)

Cargo ☐

Usuario ☐

Indique el mecanismo ☐

Ninguna ☐

20. ¿Posee un plan de contingencia vigente en caso de desastres naturales?

Sí ○ No ○ Desconoce ○

ANEXO 5: Entrevistas dirigidas a la Unidad de Informática de la ISO 27001-2013

1. ¿La Institución cuenta con un Manual de Política de Seguridad de la Información?

Si (continuar con la pregunta 2)

No (continuar con la pregunta 4)

2. ¿Cada que tiempo actualiza el Manual de Política Seguridad de la Información?

3. ¿El Manual de Política de Seguridad de la Información se encuentran socializadas a todo el personal de la Institución?

4. ¿Se actualizan periódicamente los procedimientos e instructivos establecidos en la Unidad de Informática?

Si (continuar con la pregunta 6)

No (continuar con la pregunta 5)

5. ¿Por qué no se actualizan los procedimientos e instructivos de la Unidad de Informática?

No es necesario modificarla	
No se dispone de suficiente personal	
No lo considera importante	
Otra	

6. ¿Existe el apoyo necesario de las máximas autoridades en temas de tecnología?

Si No

7. ¿Se realizan capacitaciones periódicamente para dar a conocer temas relacionados con seguridad de la información?

Si (continuar con la pregunta 9) No (continuar con la pregunta 8)

8. Describa la razón del porqué no se realizan capacitaciones referentes a seguridad de la información

9. ¿Se tiene establecido perfiles de usuarios de acuerdo a los roles, responsabilidades para otorgar acceso a los usuarios?

Si No

10. ¿Existen criterios para la clasificación de la información?

Si No

11. ¿Existen controles de seguridad implementados en los aplicativos utilizados en la Institución?

Nombre de Control	Si/ No	Forma de Implementación	Se encuentra documentado	Intervalo de actualización
Medios extraíbles de datos				
Control de Accesos: Creación y Eliminación de privilegios de usuarios				
Clasificación de la información				
Gestión de cambio				
Control contra software malicioso				
Gestión en la entrega de servicios de terceros				
Respaldo de información				

Control de Acceso a Internet				
Control de Acceso a correo				
Control de Acceso/Seguridad de redes alámbricas e inalámbricas				
Aceptación del sistema				
Gestión de Incidentes				
Derecho de Propiedad Intelectual				

12. ¿Cuántos USER-ID y contraseñas manejan cada usuario de la Institución?

13. ¿Cada cuánto tiempo obliga el sistema a cambiar la contraseña del correo institucional, estación de trabajo y aplicativos manejados por los usuarios?

14. ¿Existe una infraestructura adecuada donde se disponen equipos como ups, rack?

15. ¿Poseen inventarios de tecnología?

Si

	Inventario	Intervalo de actualización
Software	Licencias	
	Suite ofimática	
	Sistemas Operativos	
	Aplicativos del negocio	
Hardware	Equipos móviles	

	Equipos de computación	
	Equipos de red	
	Dispositivos de almacenamiento	
Otros		

16. ¿Cuál es el motivo de no realizar un inventario de los activos de software y hardware?

17. En caso de haber ocurrido un incidente de seguridad en el último año, describa lo ocurrido

18. Describa el plan de contingencia en casos de incidentes graves o desastres naturales

Anexo 6: Resultado de la implementación de la Propuesta de Optimización de la Infraestructura Tecnológica (Mitigación de Riesgos)

Situación Actual de Riesgos						Riesgos con la implementación de la Propuesta de Optimización de la Infraestructura Tecnológica					
Riesgo	**Probabilidad**	**Impacto**	**Magnitud del Riesgo**	**Porcentaje de magnitud de riesgo**	Comparación de Pre y Post Propuesta de Optimización de la Infraestructura Tecnológica	**No**	**Riesgo**	**Probabilidad**	**Impacto**	**Magnitud del Riesgo**	**Porcentaje de magnitud de riesgo**
Incorrecta implementación de políticas de Firewall	5	4	20	80		R1	Incorrecta implementación de políticas de Firewall	1	4	4	16
Instalación de software no licenciado y autorizado	4	3	12	48		R2	Instalación de software no licenciado y autorizado	1	3	3	12
Recursos Compartidos por defecto	5	4	20	80		R3	Recursos Compartidos por defecto	1	4	4	16

No tener implementada Políticas de seguridad a través de GPO (Global Policy Object)	5	4	20	80		R4	No tener implementada Políticas de seguridad a través de GPO (Global Policy Object)	1	4	4	16
Información comprometida del SIAFP	5	5	25	100		R5	Información comprometida del SIAFP	3	5	15	60
Aplicaciones clientes por defecto y desactualizadas	2	3	6	24		R6	Aplicaciones clientes por defecto y desactualizadas	2	3	6	24
Acceso no autorizado a los sistemas	4	5	20	80		R7	Acceso no autorizado a los sistemas	2	5	10	40
Ingreso de correos masivos al servidor de correo	1	4	4	16		R8	Ingreso de correos masivos al servidor de correo	1	4	4	16

Ingreso de phishing causando identidades robadas de los usuarios	2	5	10	40	R9	Ingreso de phishing causando identidades robadas de los usuarios	1	5	10	40
Pérdida masiva de Datos	2	5	10	40	R10	Pérdida masiva de Datos	2	5	10	40
Filtración de información	5	5	20	80	R11	Filtración de información	1	4	4	16
Infección de Malware	3	5	15	60	R12	Infección de Malware	1	5	5	20
Interrupción de Servicio	1	4	4	16	R13	Interrupción de Servicio	1	4	4	16
Daño de equipos	3	2	6	24	R14	Daño de equipos	3	2	6	24
Daño, Pérdida o Robo de Equipos	2	5	10	40	R15	Daño, Pérdida o Robo de Equipos	2	5	10	40
Explotación de Vulnerabilidades de los software y equipos	5	5	25	100	R16	Explotación de Vulnerabilidades de los software y equipos	1	5	5	20

Perdida de reputación por Hacking	5	5	25	100
Acceso no autorizado a los servicios	5	4	20	80
Manipulación de la información	3	3	9	36
Robo de información	3	5	15	60
Lentitud en la red	5	3	15	60
Acceso no autorizado a otros equipos de usuario	4	5	20	80

R17	Perdida de reputación por Hacking	1	5	5	20
R18	Acceso no autorizado a los servicios	1	4	4	16
R19	Manipulación de la información	3	3	9	36
R20	Robo de información	1	5	5	20
R21	Lentitud en la red	1	3	3	12
R22	Acceso no autorizado a otros equipos de usuario	2	5	10	40