UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

EVALUACIÓN DE LA SEGURIDAD PARA LA RED DE DATOS DE UNA DEPENDENCIA UNIVERSITARIA

TESIS

QUE PARA OBTENER EL TÍTULO DE INGENIERO EN COMPUTACIÓN

PRESENTA

JOSUÉ NAMBO RAMÍREZ

DIRECTOR
ING. ORLANDO ZALDÍVAR ZAMORATEGUI

JUNIO 2012

AGRADECIMIENTOS

A Dios.

Por permitirme llegar hasta este punto y hacer realidad un sueño dándome salud para lograr mis objetivos.

A mis padres Margarita y José.

Por haberme apoyado en todo momento, sus valores mostrados para salir adelante, su perseverancia y constancia que los caracterizan, por la motivación y enseñanza constante que me han permitido ser la persona que soy hoy en día, con ese cariño y calor humano necesario, porque han velado por mi salud, mis estudios, mi educación, mi alimentación entre otros, son a ellos a quien les debo todo, horas de consejos, de regaños, de reprimendas, de tristezas y de alegrías, de las cuales estoy muy seguro que las han hecho con todo el amor del mundo.

A los miembros del jurado.

La M. C. María Jaquelina López Barrientos, el Ing. Orlando Zaldívar Zamorategui, el M. C. Alejandro Velázquez Mena, el Dr. Javier Gómez Castellanos y al Ing. Rafael Sandoval Vázquez, por las valiosas contribuciones que hicieron al trabajo final y por el tiempo que dedicaron para revisarlo, aun a pesar de tantas actividades que los ocupan.

A mis maestros.

Gracias por su tiempo, por su apoyo, por entregar parte de su vida para transmitirme su sabiduría durante el desarrollo de mi formación profesional dentro y fuera de las aulas.

A mis Familiares.

Gracias a todos que directamente me impulsaron para llegar hasta este lugar, a todos mis familiares que me resulta muy difícil poder nombrarlos en tan poco espacio, sin embargo ustedes saben quienes son, en especial a mi abuelo Tomas Ramírez que a pesar de no estar entre nosotros el me apoya desde donde está.

A mis amigos.

Que gracias al equipo que formamos logramos llegar hasta el final del camino brindándome todo su apoyo cuando más abatido me sentía, inyectándome fuerza, animo y compañía para continuar lo que había empezado y que hasta el momento, seguimos siendo amigos.

A la ***Universidad Nacional Autónoma de México la máxima casa de estudios*** *y en especial a la* ***Facultad de Ingeniería*** *que me dieron la oportunidad de formar parte de ellas.*

Gracias a todas las personas que han leído este trabajo, porque por ese simple hecho ya forman parte de él.

Son muchas las personas especiales a las que me gustaría seguir agradeciendo su apoyo, animo, el granito de arena que colocaron en las diferentes etapas de mi vida. Algunas están aquí conmigo y otras en mis recuerdos y en mi corazón sin importar donde estén o si alguna vez lleguen a leer estas dedicatorias quiero darles las gracias por formar parte de m, por todo lo que me han brindado y por todas sus bendiciones.

¡Muchas Gracias!

ÍNDICE

INTRODUCCIÓN

La seguridad informática trata de minimizar y gestionar los riesgos, garantizar la adecuada utilización de los recursos y aplicaciones, limita las pérdidas y consigue la recuperación del sistema de una manera más fácil; a su vez, trata de cumplir con el marco legal y con los requisitos impuestos; la integridad, la disponibilidad de los recursos y la confidencialidad de los datos, permitiendo usar dichos recursos y datos en el campo de la investigación y en lo escolar, basándose únicamente en las tareas que desempeña cada uno de los usuarios de la institución.

Es una herramienta muy valiosa para abordar con decisión su detección, causa y consecuencias que puedan acarrear, con la finalidad de eliminar o atenuar los propios riesgos, así como limitar sus consecuencias, en el caso de no poder eliminarlos.

El objetivo de este trabajo consiste en analizar los niveles de seguridad que existen en la dependencia, para que posteriormente, los administradores puedan desarrollar políticas y mecanismos apropiados para minimizar ataques de robo o daño de información relevante y/o confidencial. Asimismo, pretende servir como una herramienta para mantener la integridad y la disponibilidad de los recursos informáticos dependiendo de las necesidades y del presupuesto de dicha institución.

En el Capítulo 1. Marco teórico, se abordarán los conceptos necesarios para comprender la problemática abordada en este documento, así como la metodología que se ocupó para la realización del proyecto, además de encontrar información relacionada con la seguridad informática, tipos de perpetradores, tipos de virus, herramientas o ataques que realizan los perpetradores, mecanismos de seguridad y el principio de defensa profunda, la cual pretende erradicar o minimizar las vulnerabilidades del sistema para evitar dichos ataques de los perpetradores.

En el Capítulo 2. Planteamiento del problema, se hará mención sobre la problemática que aqueja a la dependencia, mostrando reportes que le hicieron llegar a la misma, ejemplificando así los problemas de propagación de virus, robo de bienes, mal uso de red, etcétera.

En el Capítulo 3. Propuesta de solución a la problemática, se mostrará una sugerencia para dar solución al problema abordado en el capítulo 2. Dentro de esta propuesta se encontrarán políticas de seguridad para los diferentes tipos de personal que labora en la dependencia, una bitácora que servirá para organizar las actividades del departamento encargado de los equipos de cómputo de la institución, se desarrollará un sistema para administrar y llevar el control de los equipos de cómputo. Para fortalecer las políticas de seguridad, así como garantizar un uso adecuado de la red, se describirá cómo implementar un firewall con squid sobre el sistema operativo OpenBSD.

En el Capítulo 4. Resultados e impactos, se encontrarán los resultados e impactos que se obtienen al implementar la propuesta mencionada en el capítulo 3.

Dentro del Capítulo llamado Conclusiones, se presentan las conclusiones a las que se llegan después de la realización de este trabajo.

CAPÍTULO 1

MARCO TEÓRICO

La seguridad informática pretende preservar la integridad, la confidencialidad y la disponibilidad de la información, basándose en el principio de la defensa profunda y ayudándose de mecanismos de seguridad, como son: los diferentes tipos de firewalls, la firma digital, la encriptación, la red virtual privada (VPN), las políticas, etcétera, para minimizar los ataques que realizan los perpetradores como el hacker, el lamer, el loser, entre otros; apoyados de virus, gusanos, exploits, malware, etcétera, para explotar las vulnerabilidades de un sistema. En el caso de que vulneren el sistema se establecen planes de contingencia para actuar en los diferentes escenarios que surjan.

1.1 Metodología

Para llevar una organización en la realización de un proyecto se debe seguir una metodología a fin de tener un control sobre lo que se está desarrollando, para no perder de vista los objetivos a los cuales se quieren llegar, asimismo, permite identificar de una forma más rápida algún error que llegase a cometer.

Por tal motivo, para poder analizar y luego decidir cuál es la mejor herramienta o mecanismo que se debe implementar, a fin de proporcionar seguridad a un sistema, un recurso o un bien de la dependencia; es necesario seguir una serie de pasos que permitan identificar ¿qué se quiere proteger?, ¿de qué se quiere proteger? y ¿cómo se va a proteger?

A través de la respuesta a la pregunta ¿qué se quiere proteger?, se encontrarán los servicios o los recursos que nos importa brindarles seguridad, ya sea porque contienen información o son servicios necesarios para la continuidad de las labores de la institución.

Cuando se contesta a la pregunta ¿de qué se quiere proteger?, permite conocer las amenazas y las vulnerabilidades a las que se encuentran expuestos nuestros activos encontrados en la pregunta anterior.

Al responder al cuestionamiento de ¿cómo se va a proteger?, necesariamente ya se debieron haber contestado las dos preguntas anteriores; la respuesta obtenida a esta última pregunta, estará orientada a contrarrestar las amenazas y vulnerabilidades identificadas en los objetos a proteger. [1]

Como ayuda para el análisis de la seguridad se utilizará la metodología de objetivos de control para la información y las tecnologías relacionadas, llamada COBIT por sus siglas en inglés, la cual ha sido desarrollado como un estándar para las buenas prácticas de seguridad y control en la tecnología de la información; ya que pretende mejorar la seguridad, la calidad y la eficiencia; identificar el riesgo, gestionar recursos y medir el desempeño de la entidad, cumpliendo las metas y el nivel de madurez de los procesos de la organización. [2]

La metodología COBIT se utiliza para planear, implementar, controlar y evaluar el gobierno sobre las tecnologías de la información y comunicaciones; incorporando objetivos de control, directivas de auditoría, medidas de rendimiento y resultados, factores críticos de éxito y modelos de madurez. [3] Debido a estas condiciones, COBIT está diseñada para ser utilizada por tres audiencias distintas:

Administración. Permite lograr un balance entre los riesgos y las inversiones en un ambiente de tecnología de información frecuentemente impredecible.

Usuarios. Obtiene una garantía en cuanto a la seguridad y controles de los servicios de tecnología de información proporcionados internamente o por terceras partes.

Auditores de sistemas de información. Dar soporte a las opiniones mostradas a la administración sobre los controles internos.

Con respecto a los aspectos de seguridad, COBIT identifica siete categorías distintas para los criterios de información, tomando como elementos clave a la confidencialidad, la integridad y la disponibilidad, las cuales son:

Efectividad. Habla de que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.

Eficiencia. Se refiere a la provisión de información a través de la utilización óptima de los recursos.

Confidencialidad. Se refiere a la protección de la información sensible contra divulgación no autorizada.

Integridad. Menciona la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.

Disponibilidad. Permite que la información pueda ser utilizada cuando sea requerida por un proceso, en el momento que lo disponga.

Cumplimiento. Sugiere no faltar a las leyes, regulaciones y acuerdos a los que está sujeto el proceso.

Confiabilidad de la información. Alude a la provisión de información apropiada para la administración, con el fin de operar la entidad y para ejercer sus responsabilidades.

COBIT clasifica los recursos de las tecnologías de la información en:

Datos. Son los elementos de la información, ya sea externa o interna, estructurada o no estructurada, gráficos, sonido, etc.

Aplicaciones. Se entiende como sistemas de aplicación a la suma de procedimientos manuales y programas.

Tecnología. Comprende hardware, software, sistemas operativos, redes, multimedia, sistemas de administración de bases de datos, etc.

Instalaciones. Son los recursos para alojar y dar soporte a los sistemas de información.

Personal. Considera la productividad, el conocimiento y la conciencia del personal, sus habilidades para planear, organizar, adquirir, entregar, soportar así como monitorear los servicios y los sistemas de información.

COBIT define cuatro grandes dominios de actuación, los cuales son:

Planeación y organización. Se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio.

Adquisición e implementación. Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

Entrega y soporte. Hace referencia a la entrega de los servicios requeridos, abarcando desde las operaciones tradicionales hasta el entrenamiento, pasando por la seguridad y los aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios.

Monitoreo. Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

En resumen, los recursos de TI necesitan ser administrados por un conjunto de procesos agrupados en forma natural, con la finalidad de proporcionar la información que la empresa necesita para alcanzar sus objetivos. La relación entre las categorías, los recursos y los procesos de los dominios se muestran en la figura 1.1.

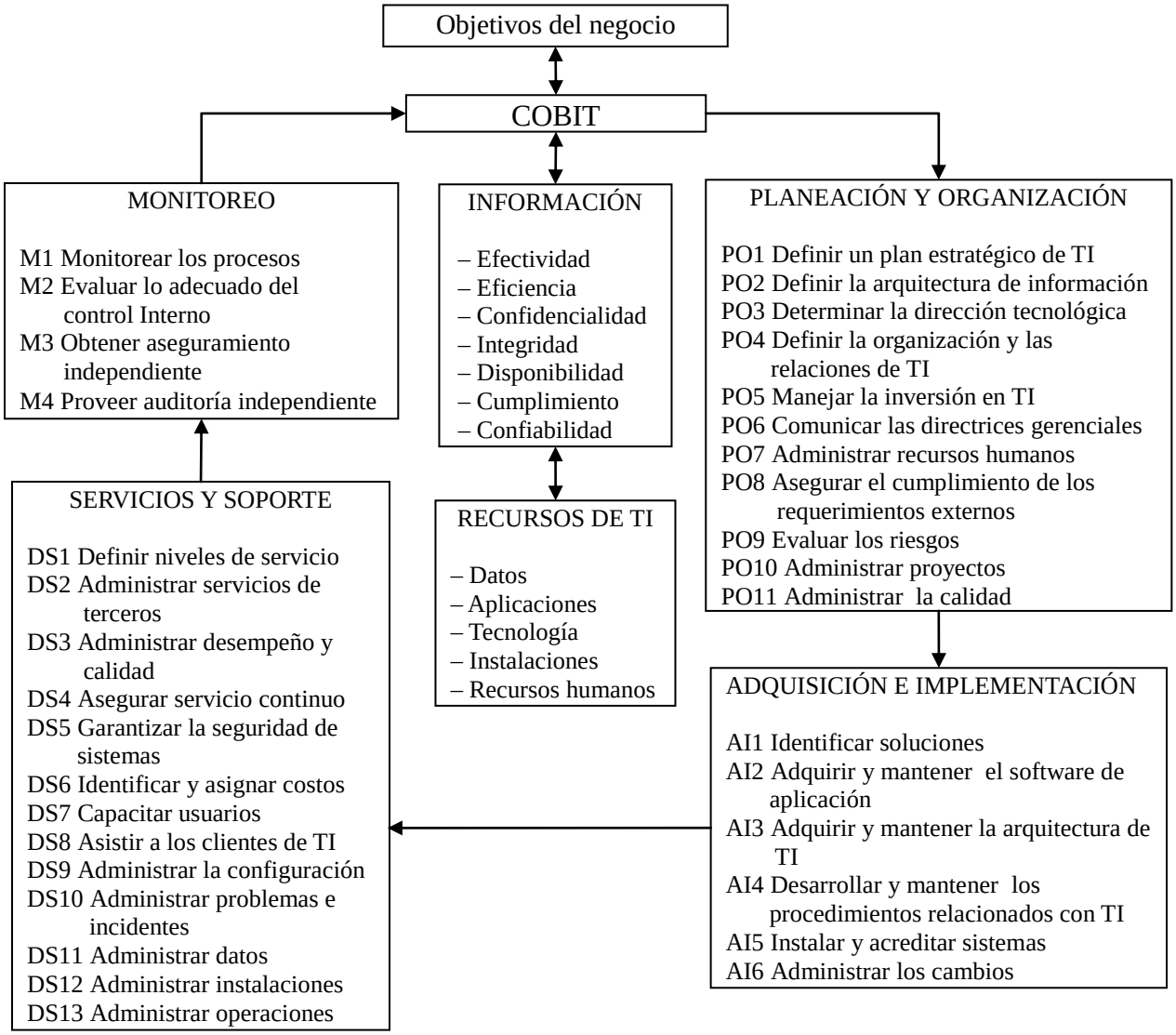


Figura 1. 1. Relación de los dominios de COBIT. [3]

Resulta claro que las medidas de control no satisfarán necesariamente los diferentes requerimientos de información del negocio. Para poder cuantificar los criterios de información existen tres tipos de calificaciones:

Primario. Es el grado al cual el objetivo de control definido impacta directamente el requerimiento de información de interés.

Secundario. Es el grado al cual el objetivo de control definido satisface únicamente de forma indirecta o en menor medida el requerimiento de información de interés.

Blanco (vacío). Podría aplicarse; sin embargo, los requerimientos son satisfechos más apropiadamente por otro criterio en este proceso y/o por otro proceso.

Para seguir con el análisis de la seguridad se utilizará la ISO 17799/27002 la cual se enfocará al análisis de riesgo debido a que utiliza métodos tanto cualitativos, como cuantitativos, los primeros permiten agilidad en el proceso y facilidad en la asignación de valores de impacto o riesgo, y los segundos nos permiten la precisión y exactitud, necesarias a la hora de tomar decisiones de tipo financiero.

Dentro del marco de la norma de seguridad ISO17799/ISO27002 se tratará de identificar los siguientes elementos:

Por medio de entrevistas se busca entender los diferentes aspectos que conforman a la organización, tanto en el aspecto tecnológico, como en los procesos críticos.

Con la evaluación de riesgos se pretende descubrir las amenazas, vulnerabilidades y riesgos de la información, con el propósito de generar un plan de implementación de los controles que promuevan un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad e integridad de la información, para posteriormente definir políticas y mecanismos.

El método o modelo que se empleará para el desarrollo del este escrito será el modelo de cascada, ya que éste ordena rigurosamente las etapas del ciclo de vida del sistema, de tal forma que el inicio de cada etapa debe esperar a la finalización de la inmediatamente anterior.

Las etapas son:

1. Análisis de requisitos. En esta fase se analizan las necesidades de los usuarios finales para determinar qué objetivos debe cubrir el sistema. Es importante señalar que en esta etapa se debe consensuar todo lo que se requiere del sistema y será

aquello lo que seguirá en las siguientes etapas, no pudiéndose requerir nuevos resultados a mitad del proceso de elaboración del sistema.

2. Diseño del sistema. Se divide y organiza el sistema o el problema en elementos que puedan elaborarse por separado, aprovechando las ventajas del desarrollo en equipo.

3. Elaboración del sistema. Se da marcha adelante en la elaboración del sistema contemplando los requisitos establecidos en la primera fase.

4. Pruebas. Los elementos se ensamblan para componer el sistema y se comprueba que funciona correctamente y que cumple con los requisitos, antes de ser implementado.

5. Implementación. El sistema se pone en producción. Durante la explotación del sistema pueden surgir cambios, bien para corregir errores o bien para introducir mejoras. Todo ello se debe documentar.

6. Mantenimiento. Se le realizan actualizaciones al sistema, se modifica conforme lo requiere la dependencia.

1.2 Seguridad informática

La seguridad informática es cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red de información cuyos efectos pueden conllevar daños sobre la información, comprometer su confidencialidad y autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema. Para ello, se han desarrollado protocolos y estándares adecuados para preservar la seguridad.

La norma ISO/IEC 17799 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

La seguridad de la información se define en la norma, como la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (vigilando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (permitiendo que los usuarios autorizados tengan acceso a la información y a sus activos asociados cuando lo requieran).

La Organización Internacional de Estándares (ISO), como parte de su norma 7498, en la que se establece el modelo de referencia para la interconexión de sistemas abiertos, define la seguridad informática como una serie de mecanismos que minimizan la vulnerabilidad de bienes y recursos, donde un bien se define como algo de valor y la vulnerabilidad se define como la debilidad que se puede explotar para violar un sistema o la información que contiene.

En estos momentos, la seguridad informática es un tema de dominio obligado para cualquier persona que haga uso de computadoras e Internet, para no permitir que su información sea comprometida.

"El único sistema seguro es aquél que está apagado en el interior de un bloque de hormigón protegido en una habitación sellada, rodeada por guardias armados" [4]

Y a pesar de lo que dice Gene Spafford no existe un sistema 100% seguro, ya que para la mayoría de los expertos el concepto de seguridad en la informática es utópico; debido a esta circunstancia, para que un sistema se pueda considerar como seguro debe tener las siguientes características, conocidas como pilares de la seguridad:

- Integridad. Se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada o copiada, ya sea, durante el proceso de transmisión o en su propio equipo de origen. Es un riesgo común que el atacante al no poder descifrar

un paquete de información y, sabiendo que es importante, simplemente lo intercepte y lo borre.

- Confidencialidad. Se refiere a que la información sólo puede ser conocida por individuos autorizados. Existe una gran posibilidad de sufrir ataques contra la privacidad, especialmente en la comunicación de los datos, ya que la transmisión a través de un medio presenta múltiples oportunidades para ser interceptada y copiada; las líneas "pinchadas", la intercepción o recepción electromagnética no autorizada o la simple intrusión directa en los equipos donde la información está físicamente almacenada son un ejemplo de la violación a la confidencialidad.

- Disponibilidad. Se refiere a la seguridad de que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

Cuando se habla de seguridad informática, se debe considerar el control en el acceso y registro del uso de los servicios y archivos protegidos, la identificación de autores o mensajes y el cumplimiento legal.

La seguridad informática depende de la sensibilización, de conocimientos y/o capacidades de los responsables, de la formación y asunción de responsabilidades, del correcto diseño, configuración, instalación y mantenimiento, de la limitación en la asignación de servicios, del soporte de los fabricantes, de la consideración del principio de defensa profunda y de la adopción de los objetivos.

1.3 Principio de defensa profunda

El principio de defensa profunda de un sistema de información es una estrategia de protección la cual consiste en el diseño e implementación de introducir múltiples capas de

seguridad que permitan reducir la probabilidad de compromiso en caso de que una de las capas falle y en el peor de los casos minimizar el impacto volviéndose una defensa global y dinámica, al coordinar las diferentes líneas de defensa o capas de seguridad que cubren toda la profundidad del sistema, véase figura 1.2.

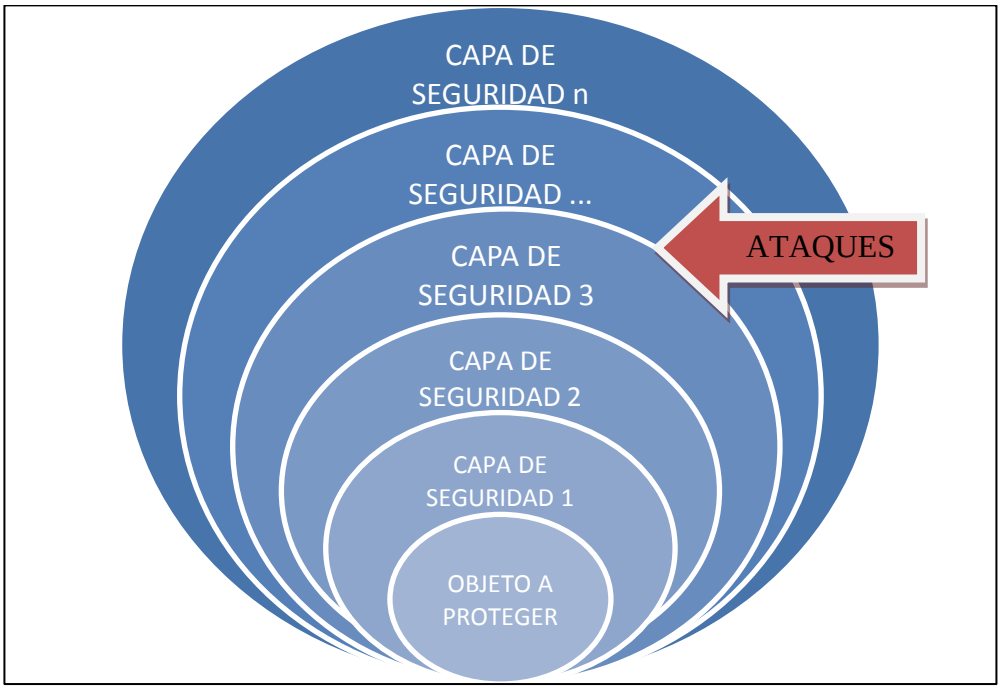


Figura 1. 2. Representación del principio de defensa profunda.

1.4 Objetivos de la seguridad informática

La seguridad informática tiene como objetivo minimizar y gestionar los riesgos, mientras garantiza la adecuada utilización de los recursos y aplicaciones, dando como consecuencia la limitación de las pérdidas y la recuperación del sistema si fuese necesario; cumpliendo con el marco legal y con requisitos impuestos.

Para cumplir estos objetivos se deben contemplar cuatro planos de actuación: el técnico, el humano, el legal y el de la organización.

1.5 Amenazas a un sistema de seguridad

Hay que tomar en cuenta que un activo es un recurso necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Una amenaza es todo aquello que puede, intenta o pretende destruir un activo, es decir, daños latentes que no se han concretado. Las amenazas se clasifican dependiendo de las fuentes que las generan, véase figura 1.3.

a) Naturales. Surgen de las fuerzas naturales tales como las inundaciones, los terremotos, el fuego, el viento, etc. Dichos desastres hacen surgir amenazas directas, pues repercute indiscriminadamente en el funcionamiento físico de las computadoras, redes, instalaciones, líneas de comunicación, etcétera.

b) Hardware. Se da por fallas físicas que presente cualquiera de los dispositivos que conforman a la computadora: desperfecto de los equipo, bajo rendimiento, deterioro, incorrecto funcionamiento, entre otros.

c) Software. Se presenta cuando un diseño bien elaborado de un mecanismo de seguridad se implementa mal, es decir, no cumple con las especificaciones del diseño.

d) Red. Se presenta cuando no se calcula bien el flujo de información que circulará por el canal de comunicación, desconexión del canal de comunicación o varios equipos conectados a la red.

e) Humanas. La amenaza surge por ignorancia en el manejo de la información, por descuido, por negligencia o por inconformidad por parte del personal.

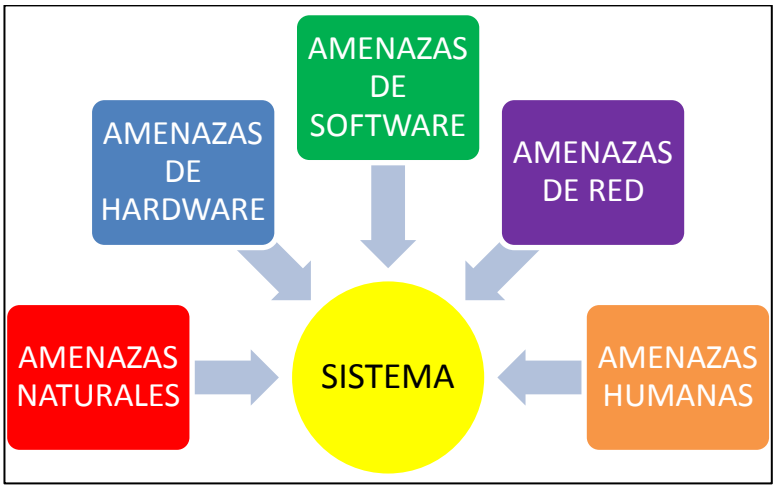


Figura 1. 3. Amenazas de un sistema.

Dependiendo de las fuentes de amenaza, la seguridad puede dividirse en dos partes:

*La seguridad lógica, c*onsiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos aquellas personas autorizadas para hacerlo.

Dicha seguridad tiene como objetivo restringir el acceso a los programas y archivos asegurando que se estén utilizando los datos, así como los procedimientos correctos, para que los operadores trabajen sin una supervisión minuciosa impidiéndoles modificar los programas o los archivos que no correspondan, confiando así en que la información recibida sea la misma que ha sido transmitida a su vez verifica que existan sistemas alternativos, secundarios o de emergencia para la transmisión entre diferentes puntos.

La seguridad física. Consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención ante amenazas a los recursos e información confidencial. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del centro de cómputo, así como los medios de acceso remoto al y desde el mismo; estos mecanismos son implementados para proteger el hardware y medios de almacenamiento de datos. [5]

1.6 Vulnerabilidades de un sistema

Las vulnerabilidades son puntos débiles existentes en el activo o en el entorno, que al ser explotados o aprovechados por una amenaza, ocasionan un ataque.

Las vulnerabilidades se clasifican dependiendo de las fuentes que las generan. Véase figura 1.4:

a) Naturales. Se refiere al grado en que el sistema puede verse afectado por desastres naturales o ambientales.

b) Hardware. El no verificar las características técnicas de los dispositivos junto con sus respectivas especificaciones, la falta de mantenimiento, el adquirir equipo de mala calidad son algunos ejemplos de este tipo de vulnerabilidad.

c) Software. Ciertas fallas o debilidades de los programas de sistema hacen más fácil acceder al mismo por personas no autorizadas y lo hacen menos confiable. Este tipo de vulnerabilidad incluye todos los errores de programación del sistema operativo u otras aplicaciones que permiten aplicar al sistema.

d) Red. La conexión de las computadoras a las redes supone un enorme incremento de la vulnerabilidad del sistema aumentando considerablemente la escala del riesgo al que está sometido, al aumentar la cantidad de gente que puede tener acceso al medio o que intenta tenerlo.

e) Humanas. Ser vulnerable a la ingeniería social, contratar personal sin perfil psicológico y ético, no tener personal para todas las áreas, el descuido, el cansancio, el maltrato al personal, la mala comunicación con el personal, son sólo algunos ejemplos.

f) Física. La podemos encontrar en la estructura del edificio o entorno del sistema. La relacionamos con la posibilidad de poder entrar físicamente al lugar donde se encuentra el sistema para robar, modificar o destruir al mismo.

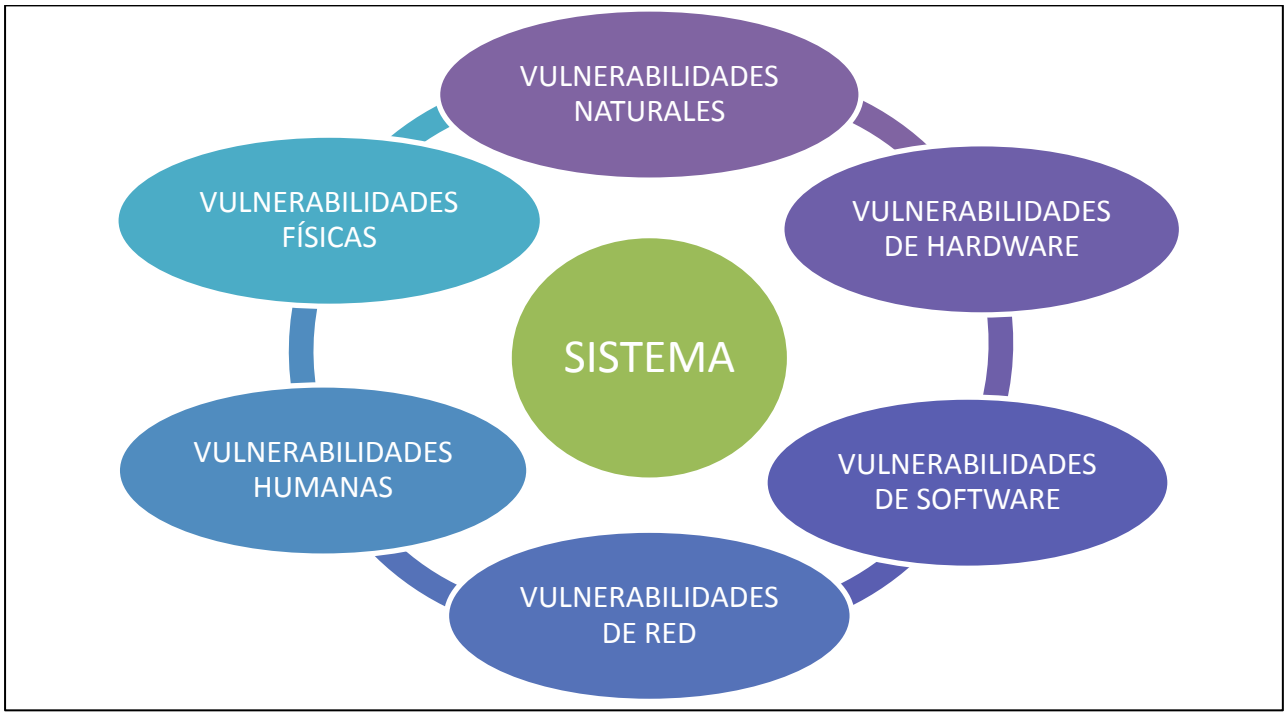


Figura 1. 4. Vulnerabilidades del sistema.

1.7 Identificación de ataques y técnicas de intrusión

Un ataque es una realización o culminación de una amenaza, llega a presentar pérdidas totales o parciales e incluso pueden no existir pérdidas.

Cuando se habla de un flujo normal de la información, no debe de existir ningún tipo de obstáculo para que la información llegue al destinatario; véase figura 1.5.

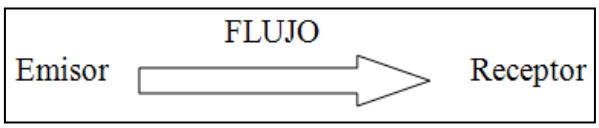


Figura 1. 5. Representación del flujo normal de la información.

Debido a la forma en que los ataques modifican el flujo normal de la información, se clasifican de la siguiente manera:

a) Ataques de suplantación o contra la autenticación. Una entidad no autorizada inserta objetos falsificados en el sistema, véase figura 1.6.

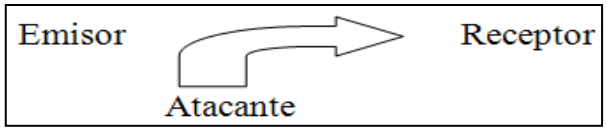


Figura 1. 6. Representación del ataque de suplantación.

b) Ataques de intercepción o contra la confidencialidad. Una entidad no autorizada consigue acceso a un recurso. La entidad no autorizada podría ser una persona o un programa, véase figura 1.7.

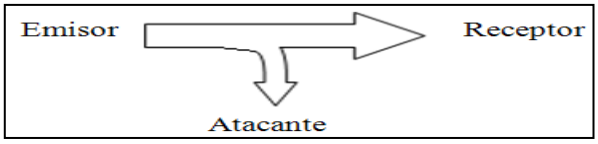


Figura 1. 7. Representación del ataque de intercepción.

c) Ataques de interrupción o contra la disponibilidad. Un recurso del sistema es destruido o se vuelve no disponible, véase figura 1.8.

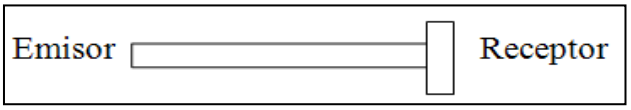


Figura 1. 8. Representación del ataque de interrupción.

d) Ataques de modificación o contra la integridad. Una persona no autorizada no sólo consigue acceder al recurso, sino que es capaz de manipularlo, véase figura 1.9.

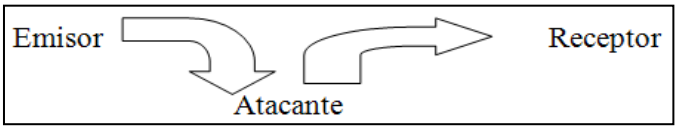


Figura 1. 9. Representación del ataque de modificación.

Un ataque se lleva a cabo por diferentes tipos de perpetradores y éstos se clasifican con base en su objetivo principal o tipo de ataque.

Debido a la división de los perpetradores, los ataques también se dividen en:

a) Pasivos. Recibe su nombre debido a que el atacante no altera en ningún momento la información, es decir, únicamente la observa, escucha, obtiene o monitorea mientras está siendo construida. Es una técnica muy útil para obtener información de la comunicación, que puede consistir en la obtención del origen y destinatario, leyendo las cabeceras de los paquetes monitorizados.

   Se observa el volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales, permitiendo conocer las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

   Los ataques pasivos son muy difíciles de detectar por las personas autorizadas para ver la información, ya que no provocan alteraciones en los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante.

b) Activos. Estos ataques implican algún tipo de modificación del flujo de datos transmitidos o la creación de un falso flujo de datos, pudiendo subdividirse en:

   Suplantación de identidad. Se lleva a cabo al momento en que el perpetrador se hace pasar por una entidad diferente. Normalmente se ayuda de alguna de las otras formas de ataque activo, por ejemplo, las secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

Reactuación. Se efectúa cuando uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo, ingresar dinero repetidas veces en una cuenta dada.

Modificación de mensajes. Sucede cuando una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados para producir un efecto no autorizado. Por ejemplo, el mensaje "Ingresa un millón de pesos en la cuenta A" podría ser modificado para decir "Ingresa un millón de pesos en la cuenta B".

Degradación fraudulenta del servicio. Impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o podría interrumpir el servicio de una red inundándola con mensajes espurios. [6]

Para lograr su objetivo, todos los ataques se componen de 3 fases, véase figura 1.10:

Fase 1: Planteamiento. En esta fase se establecen los objetivos, es decir, es donde los atacantes se preguntan ¿a quién o quiénes voy a atacar?, obtienen la información de la víctima para luego establecer la metodología del ataque.

Algunas de las formas para efectuar esta primera fase se muestran a continuación:

Recolección de información. El atacante puede lograrlo a través de engaños, basándose principalmente en convencer a la gente de hacer algo que en realidad no debería.

Exploración. El atacante necesita conocer las contraseñas, números telefónicos, etcétera, que posteriormente le puedan servir. En esta etapa es cuando se realiza un ataque pasivo.

Fase 2: Activación. Se pone en marcha el ataque. Entra en acción cuando el código de ataque es invocado para que lleve a cabo la misión o una bomba de tiempo estalla a la hora y día determinado

Fase 3: Ejecución. Se observa qué beneficios se obtuvieron del ataque, así como si se cumplió con los objetivos.

Figura 1. 10. Fases de un ataque.

1.8 Perpetradores

Un perpetrador o un atacante es aquella persona que se dedica a llevar a cabo un ataque con éxito o sin él; en el caso de que logre tener éxito puede causar gran o poco impacto.

Tipos de perpetradores.

a) Pasivos: Son aquellos que sólo analizan, observan la información o la estructura. Lo mismo hacen con los bienes de la organización, véase figura 1.11.

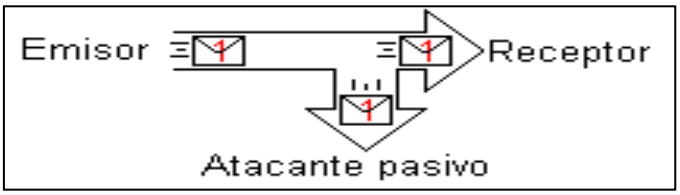


Figura 1. 11. Representación del atacante pasivo.

b) Activos: Son aquellos que alteran, crean, borran cualquier tipo de archivo principalmente la información; actúan de tal manera que los administradores y los dueños de la información se dan cuenta, véase figura 1.12.

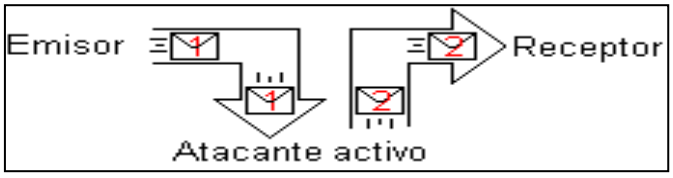


Figura 1. 12. Representación del atacante activo.

Ejemplos de perpetradores: [7, 8, 9, 10, 11]

Cracker. Es la persona que viola la seguridad de un sistema informático con fines de beneficio personal o para hacer daño. Diseña o programa cracks informáticos, que sirven para modificar el comportamiento o ampliar la funcionalidad del software o hardware original al que se aplican. Practica el cracking, acción de modificar el código fuente a un programa.

Hacker. Término para designar a alguien con talento, conocimiento, inteligencia e ingenuidad, especialmente relacionada con las operaciones de computadora, redes, seguridad, etc. Persona que disfruta aprendiendo detalles de los sistemas de programación y cómo extender sus capacidades, no se le considera un delincuente.

Trashing. Obtienen información de la basura, tal como números de tarjetas de crédito, contraseñas, directorios o recibos.

Lamer. Este grupo quizás es el que más número de miembros posee y es el que tiene mayor presencia tienen en la red. Normalmente son individuos con ganas de hacer hacking, pero que carecen de cualquier conocimiento.

Sniffer. Persona que espía y obtiene la información que circula por una red.

Phreaker. Posee conocimientos profundos de los sistemas de telefonía, tanto fijos como móviles. En la actualidad también poseen conocimientos de tarjetas prepago, ya que habitualmente la telefonía celular las emplea.

Samurai. Son lo más parecido a una amenaza pura. Sabe lo que busca, dónde encontrarlo y cómo lograrlo. Hace su trabajo por encargo y a cambio de dinero, no tienen conciencia de comunidad y no forman parte de los clanes reconocidos por los hackers.

Bucanero o pirata. Este personaje dedicado a la copia y distribución de software ilegal, tanto software comercial crackeado, como shareware registrado, etcétera. De una manera consciente o inconsciente todos nos convertimos en un pirata informático descargando programas, juegos, música, etcétera, de forma gratuita, cuando dichas descargas no son de distribución libre.

Newbie. Es un novato o más particularmente es aquel que navega por Internet, tropieza con una página de hacking y descubre que existe un área de descarga de buenos programas de hackeo, después se baja todo lo que puede y empieza a trabajar con los programas. Al contrario que los lamers, los newbies aprenden el hacking siguiendo todos los pasos cautelosos para lograrlo y no se mofa de su logro, sino que aprende.

Loser. Es un término utilizado por hackers para referirse a los usuarios comunes, de manera despectiva y como burla. Generalmente se encuentra en desventaja frente a los usuarios expertos (hackers), quienes pueden controlar todos los aspectos de un sistema.

Coder o virus maker. Creador y desarrollador de virus informáticos.

Wannabe. Desea ser hacker, pero éstos consideran que su coeficiente no da para tal fin. A pesar de su actitud positiva difícilmente consigue avanzar en sus propósitos.

Carders. Persona que hace uso ilegítimo de las tarjetas de crédito (o sus números) pertenecientes a otras personas, genera nuevas tarjetas de crédito para realizar pagos a

sistemas de compra a distancia. En general, cualquier actividad fraudulenta que tenga que ver con las tarjetas de crédito.

1.9 Herramientas y ataques

Algunas de las herramientas que los perpetradores pueden llegar a ocupar, convirtiéndose a su vez en un tipo de ataque son:

Malware. La palabra malware es la conjunción de malicious software. Este programa es sumamente peligroso para la PC, es creado para insertar gusanos, spyware, virus, troyanos o incluso los bots. Su objetivo es causar daño.

Virus. Es un programa o software que se autoejecuta y se propaga insertando copias de sí mismo en otro programa o documento. Necesita interacción con el usuario, modifica o elimina información.

Se pueden clasificar en función de múltiples características y criterios: según su origen, las técnicas que utilizan para infectar, los tipos de ficheros que infectan, los lugares donde se esconden, los daños que causan, el sistema operativo o la plataforma tecnológica que atacan, entre otros.

Todas estas clasificaciones tienen muchos puntos en común, por lo que un mismo virus puede pertenecer a varias categorías al mismo tiempo.

Debido a las características o formas en que funcionan los virus, se pueden subclasificar como:

1. Virus residentes. Su característica principal es ocultarse en la memoria RAM de forma permanente o residente. De este modo, pueden controlar e interceptar todas las operaciones llevadas a cabo por el sistema operativo, infectando todos aquellos ficheros y/o programas que sean ejecutados, abiertos, cerrados, renombrados,

copiados, etc. Estos virus sólo atacan cuando se cumplen ciertas condiciones definidas previamente por su creador (por ejemplo, una fecha y hora determinada). Mientras tanto, permanecen ocultos en una zona de la memoria principal, ocupando un espacio de la misma, hasta que son detectados y eliminados. Algunos ejemplos de este tipo de virus son: Randex, CMJ, Meve, MrKlunky.

2. Virus de acción directa. Éstos no permanecen en memoria. Su objetivo prioritario es reproducirse y actuar en el mismo momento de ser ejecutados. Al cumplirse una determinada condición, se activan y buscan los ficheros ubicados dentro de su mismo directorio para contagiarlos. Además, también realizan sus acciones en los directorios especificados dentro de la línea PATH (camino o ruta de directorios), dentro del fichero autoexec.bat (fichero que siempre se encuentra en el directorio raíz del disco duro). Los virus de acción directa presentan la ventaja de que los ficheros afectados por ellos pueden ser desinfectados y restaurados completamente.

3. Virus de sobreescritura. Se caracterizan por destruir la información contenida en los ficheros que infectan**.** Cuando infectan un fichero, escriben dentro de su contenido, haciendo que queden total o parcialmente inservibles. También se diferencian porque los ficheros infectados no aumentan de tamaño, a no ser que el virus ocupe más espacio que el propio fichero (esto se debe a que se colocan *encima* del fichero infectado, en vez de ocultarse *dentro* del mismo). La única forma de limpiar un fichero infectado por un virus de sobre escritura es borrarlo, perdiéndose su contenido. Algunos ejemplos de este tipo de virus son: Way, Trj.Reboot, Trivial.88.D.

4. Virus de boot o de arranque. Los términos boot o sector de arranque hacen referencia a una sección muy importante de un disco (tanto un disquete como un disco duro respectivamente). En ella se guarda la información esencial sobre las características del disco y un programa que permite arrancar la computadora. Este tipo de virus no infecta ficheros o archivos, sino los discos que los contienen. Actúan infectando en primer lugar el sector de arranque de los discos. Cuando una computadora se pone en marcha con un disco infectado, el virus de boot infectará a su vez el disco duro. No pueden afectar al equipo mientras no se intente poner en marcha a este último con un

disco infectado. Por lo tanto, el mejor modo de defenderse contra ellos es proteger los disquetes contra escritura y no arrancar nunca la computadora con un disquete desconocido en la disquetera, no dejar bootear la USB. Algunos ejemplos de este tipo de virus son: Polyboot.B, AntiEXE.

5. Virus de macro. El objetivo de estos virus es la infección de los ficheros creados usando determinadas aplicaciones que contengan macros: documentos de Word, hojas de cálculo de Excel, bases de datos de Access, presentaciones de PowerPoint, ficheros de Corel Draw, etc. Las macros son microprogramas asociados a un fichero que sirven para automatizar complejos conjuntos de operaciones. Al ser programas, las macros pueden ser infectadas. Cuando se abre un fichero que contenga un virus de este tipo, las macros se cargarán de forma automática, produciéndose la infección. La mayoría de las aplicaciones que utilizan macros cuentan con una protección antivirus y de seguridad específica, pero muchos virus de macro sortean fácilmente dicha protección. Éstos son algunos ejemplos: Relax, Melissa.A, Bablas, O97M/Y2K.

6. Virus de enlace o directorio. Los ficheros se ubican en determinadas direcciones (compuestas básicamente por unidad de disco y directorio), que el sistema operativo conoce para poder localizarlos y trabajar con ellos. Alteran las direcciones que indican dónde se almacenan los ficheros. De este modo, al intentar ejecutar un programa infectado por un virus de enlace, lo que se hace en realidad, es ejecutar el virus, ya que éste habrá modificado la dirección donde se encontraba originalmente el programa, colocándose en su lugar. Una vez producida la infección, resulta imposible localizar y trabajar con los ficheros originales.

7. Virus polimórficos. En cada infección que realizan se cifran o encriptan de una forma distinta. De esta forma, generan una elevada cantidad de copias de sí mismos e impiden que los antivirus los localicen a través de la búsqueda de cadenas o firmas, por lo que suelen ser los virus más difíciles de detectar. Algunos ejemplos de este tipo de virus son: Elkern, Marburg, Satan Bug, Tuareg.

8. Virus multipartitos. Virus muy avanzados, que pueden realizar múltiples infecciones combinando diferentes técnicas para ello. Su objetivo es cualquier elemento que pueda ser infectado: archivos, programas, macros, discos, etc. Se consideran muy peligrosos por su capacidad de combinar muchas técnicas de infección y por los efectos dañinos de sus acciones. Un ejemplo de estos virus es: Ywinz.

9. Virus de fichero. Infectan programas o ficheros ejecutables. Al ejecutarse el programa infectado, el virus se activa, produciendo diferentes efectos. La mayoría de los virus existentes son de este tipo.

10. Virus de compañía. Son virus de fichero que al mismo tiempo pueden ser residentes o de acción directa. Su nombre deriva de que "acompañan" a otros ficheros existentes en el sistema antes de su llegada sin modificarlos, como hacen los virus de sobreescritura o los residentes. Para efectuar las infecciones, los virus de compañía pueden esperar ocultos en la memoria hasta que se lleve a cabo la ejecución de algún programa, o actuar directamente haciendo copias de sí mismos. Algunos ejemplos de este tipo de virus son: Stator, Asimov.1539, Terrax.1069.

11. Virus de FAT. La tabla de asignación de ficheros (FAT) es la sección de un disco utilizada para enlazar la información contenida en éste. Se trata de un elemento fundamental en el sistema. Los virus que atacan a este elemento son especialmente peligrosos, ya que impedirán el acceso a ciertas partes del disco, donde se almacenan los ficheros críticos para el normal funcionamiento del ordenador. Los daños causados a la FAT se traducirán en pérdidas de la información contenida en ficheros individuales y en directorios completos.

Gusano. Son muy parecidos a los virus, pero los gusanos no dependen de archivos portadores para poder infectar a otros sistemas. Éstos pueden modificar el sistema operativo y desconfigurarlo con el fin de autoejecutarse como parte del proceso de inicialización del sistema. Para contaminar otros sistemas, los gusanos explotan vulnerabilidades del objetivo o utilizan algún tipo de ingeniería social para engañar a los usuarios de Internet y poderse ejecutar. Tiene la capacidad de replicarse por la red.

Troyano. Es una pieza de software dañino disfrazado de un software muy limpio. Los troyanos no son capaces de replicarse por sí mismos y pueden ser adjuntados con cualquier tipo de software por un programador o infectan los equipos por medio del engaño; abre puertas traseras que son puertos o servicios que se abren para que el atacante entre.

Exploit. Es un programa o técnica que aprovecha una vulnerabilidad. Dependen de los sistemas operativos y sus configuraciones, de las configuraciones de los programas que se encuentran ejecutándose en la computadora y de la LAN donde están.

Bot. Código que permite el control del equipo dañado (robot) por medio de command and control por medio de canales IRC.

Bombas lógicas. Éste suele ser el procedimiento de sabotaje más comúnmente utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada destruirá, modificará la información o provocará el desborde del sistema.

Rootkit. Son programas que son insertados en una computadora después de que algún atacante ha ganado el control de un sistema. Generalmente incluyen funciones para ocultar los rastros del ataque, como es borrar los log de entradas o encubrir los procesos del atacante; permitiéndole escalar privilegios, puede contener virus, gusanos, etc. Puede ocultar inicio de sesión, procesos, archivos, registros, etc.

Ingeniería social. Es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales o delincuentes computacionales, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos. Es una plática que hace el atacante para ver si puede sacar información.

Keylogger. Es un diagnóstico utilizado en el desarrollo de software que se encarga de registrar las pulsaciones que se realizan sobre el teclado, para memorizarlas en un fichero o enviarlas a través de Internet. El registro de lo que se teclea puede hacerse tanto con medios de hardware como de software.

Sniffer. Es un software que permite capturar tramas de la red. Generalmente es utilizado con fines maliciosos para capturar textos de email, chats, datos personales, contraseñas, etc.

Phising. Es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta.

Fuerza bruta. Esta técnica se basa en reunir información sobre el sistema, información personal del root y cuando tenemos mucha información hacer una lista de passwords.

Pharming. Trata de obtener información personal o privada a través de suplantación de dominio.

Spyware. Es todo aquel programa que se dedica a recolectar y enviar información de los usuarios. Normalmente trabajan y contaminan sistemas como lo hacen los troyanos.

Spam. Se llama spam a la práctica de enviar indiscriminadamente mensajes de correo electrónico no solicitados. Generalmente, se trata de publicidad de productos, servicios o de páginas web.

1.10 Servicio de seguridad

Es aquel servicio que mejora la seguridad de un sistema de información y el flujo de la información de una organización. Los servicios están dirigidos a evitar los ataques de seguridad y utilizan uno o más mecanismos de seguridad.

Los servicios de seguridad se clasifican en 6 tipos:

1. Control de acceso. El acceso a un medio de información puede ser controlado ya sea a través de un dispositivo pasivo tal como una puerta cerrada, o a través de un dispositivo activo como puede ser un monitor.

2. Confidencialidad. La privacidad es la capacidad de asegurar que sólo las personas autorizadas tienen acceso a algo. La forma más común de proteger las cosas en el mundo físico es el uso de candados y cerraduras.

3. Integridad. La integridad provee que los datos no hayan sido modificados y que la secuencia de los datos se mantenga durante la transmisión. Los más utilizados son los sellos. En el mundo físico se hace por medio de lo visual.

4. Autenticación. Con este mecanismo sólo se verifica la identidad. La autenticación es realizada principalmente a través de:

    - Algo que se sabe: una contraseña o un número personal de identificación.

    - Algo que se tiene: como una tarjeta o un pasaporte, el cual es utilizado por el sistema para verificar la identidad.

    - Algo que se es: permite identificar de quién se trata como, por ejemplo: la voz, la retina, etcétera.

5. No repudio. Previene a los emisores o a los receptores de negar un mensaje transmitido, por lo que cuando el mensaje es enviado el receptor puede probar que el mensaje fue enviado por el presunto emisor.

6. Disponibilidad. Se cumple si las personas autorizadas pueden acceder a la información deseada cuando lo requieran y tantas veces como sea necesario.

Tabla 1**.** Relación que se da entre los servicios de seguridad y los ataques. [12]

	ATAQUE					
SERVICIO	Obtención del contenido del mensaje	Análisis del tráfico	Suplantación	Repetición	Modificación del mensaje	Interrupción del servicio
Autenticación de entidades origen/destino	X	X			X	
Autenticación de origen de datos	X	X				
Control de acceso			X			
Confidencialidad	X					
Confidencialidad del flujo del tráfico	X					X
Integridad de datos	X	X		X		
No repudio		X		X		
Disponibilidad				X	X	

1.11 Mecanismos de seguridad

Los mecanismos de seguridad son aquellos que permiten implementar un servicio de seguridad. Son conocidos también como herramientas de seguridad o controles de seguridad.

Puede ser un dispositivo físico o lógico que permite resguardar un activo o disminuir un daño o evitarlo. En términos generales, con base en el objetivo se agrupan en:

1. Controles detectores. Están orientados a detectar la presencia de amenazas o riesgos. Están asociados a los recursos, objetivos o metas. Descubren ataques y disparan controles preventivos y correctivos.

2. Controles preventivos. Protegen vulnerabilidades y hacen que un ataque fracase o reduzca su impacto.

3. Controles correctivos. Actúan luego de ocurrido el hecho y su función es corregir las consecuencias.

4. Controles disuasivos. Son medidas encaminadas a desanimar a las personas, para que lleven a cabo acciones que podrían transformarse en amenazas para la operación. Por ejemplo, mensajes de no utilización de elementos inflamables dentro de las áreas de cómputo. Reducen la probabilidad de un ataque deliberado.

Los mecanismos de seguridad se encuentran relacionados con los servicios, ya que un mecanismo puede proteger uno o más servicios, véase tabla 2.

Tabla 2**.** Basada en X.800, indica la relación que se da entre los servicios de seguridad y los mecanismos de seguridad. [12]

	MECANISMO							
SERVICIO	Cifrado	Firma digital	Control de acceso	Integridad de los datos	Intercambio de auten-ticación	Relleno del tráfico	Control de enruta-miento	Notari-zación
Autenticación de entidades origen/destino	X	X			X			
Autenticación de origen de datos	X	X						
Control de acceso			X					
Confidencialidad	X						X	
Confidencialidad del flujo del tráfico	X					X	X	
Integridad de datos	X	X		X				
No repudio		X		X				X
Disponibilidad				X	X			

Los mecanismos de seguridad necesarios para proteger un activo deben ser analizados previamente para detectar cuáles son los adecuados y qué servicios de seguridad deben proveer.

Es decir, la decisión de qué mecanismos se deben diseñar, desarrollar o implementar se lleva a cabo después de detectar los activos a proteger y de qué se deben proteger.

Un mecanismo puede implementar uno o varios servicios de seguridad y el nivel de protección se basará en la cantidad de servicios implementados o la robustez de éstos.

Como ejemplos de mecanismos de seguridad tenemos:

Encriptación o cifrado de datos. Es el proceso que se sigue para enmascarar los datos, con el objetivo de que sean incomprensibles para cualquier agente no autorizado.

Los datos se enmascaran usando una clave especial y siguiendo una secuencia de pasos preestablecidos, conocida como “algoritmo de cifrado”. El proceso inverso se conoce como descifrado, usa la misma clave y devuelve los datos a su estado original. Fortalece la confidencialidad; véase figura 1.13.

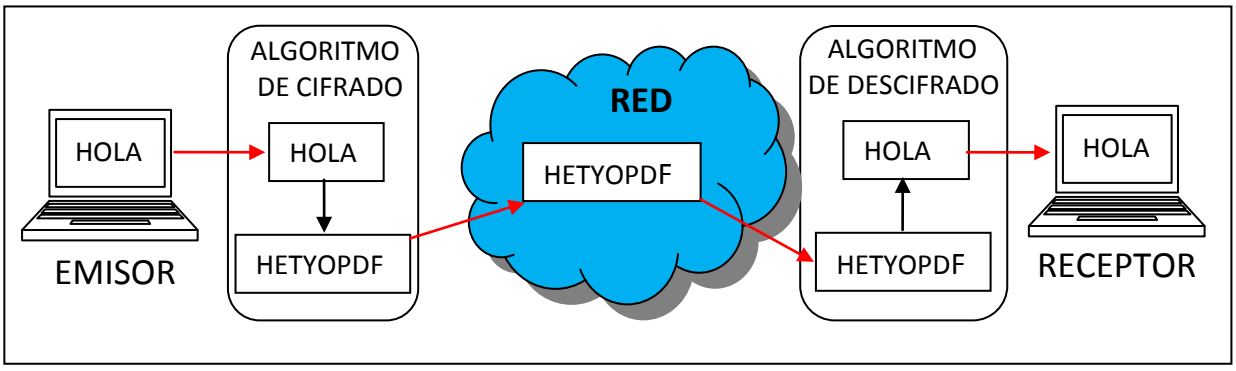


Figura 1. 13. Cifrado y descifrado de mensajes.

Firma digital. Este mecanismo implica el cifrado, por medio de la clave secreta del emisor, de una cadena comprimida de datos que se va a transferir. La firma digital se envía junto con los datos ordinarios.

Software antivirus. Ejercen control preventivo, detectivo y correctivo sobre ataques de virus al sistema. Fortalece la integridad.

Software “firewall”. Es un software que se puede instalar y utilizar libremente, o no, en la computadora. Son también llamados “desktop firewall” o “software firewall”. Son firewalls básicos que monitorean y bloquean, siempre que sea necesario, el tráfico de Internet. Fortalece la integridad. Las características de un firewall por software son:

- Los gratuitos se incluyen con el sistema operativo y normalmente son para uso personal.
- Pueden ser fácilmente integrados con otros productos de seguridad.
- No necesita de hardware para instalarlo en la computadora.
- Es muy simple de instalar, normalmente ya viene activado y el sistema operativo alerta cuando no tenemos ningún tipo de firewall en funcionamiento.
- Un firewall de este tipo es el básico que debe existir en una computadora y no hay razones que justifiquen la no utilización de por lo menos, un desktop firewall.

Firewall por hardware. Un firewall por hardware viene normalmente instalado en los routers que utilizamos para acceder a Internet, lo que significa que todas las computadoras que se encuentren detrás del router estarán protegidas por un firewall que se incluye en el dispositivo.

La diferencia de precio entre un router con firewall y un router sin firewall es muy pequeña, por eso es recomendable comprar un firewall con esta protección.

La configuración de un firewall por hardware es más complicada que una instalación de un firewall por software y es normalmente realizada a través del navegador que se utiliza para acceder a Internet.

Es posible tener un firewall por hardware y un firewall por software activos simultáneamente para lograr una mayor protección.

Los firewalls nos ayudan a fortalecer la política de seguridad de la red de una empresa, por ejemplo: si dentro de nuestra red contamos con un servidor HTTP y colocamos después de este un firewall, que sólo permite conexiones por el puerto 80, cuando un equipo fuera de esta red quiera realizar una conexión FTP o TELNET a nuestro servidor HTTP, el firewall lo va a impedir, debido a que tiene bloqueados los puertos 21 y 23, pero sí va permitir la petición web si se realiza por el puerto 80 declarado para HTTP. Véase figura 1.14.

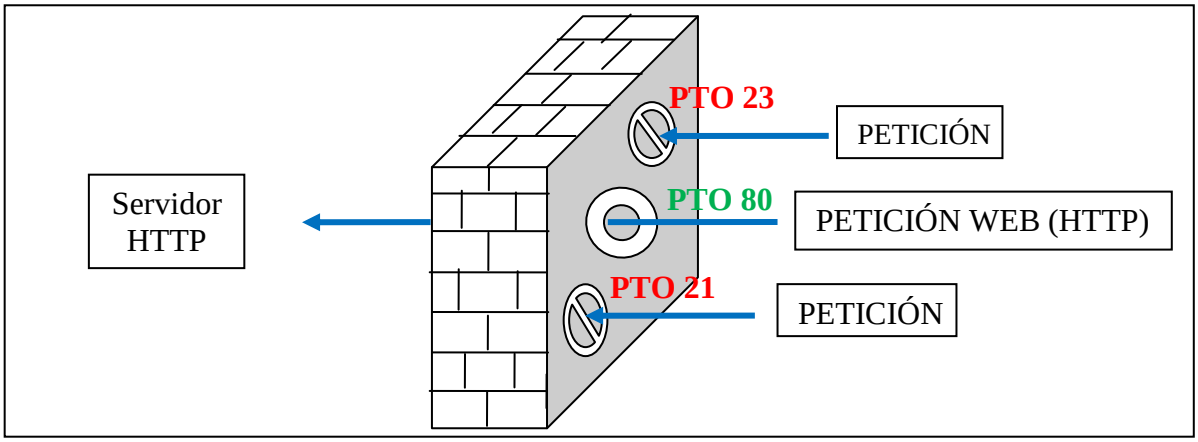


Figura 1. 14. Representación de un firewall.

Tipos de firewalls:

Packet filtering. Consiste en examinar los paquetes entrantes o salientes y permitir o impedir su transmisión o la aceptación sobre la base de un conjunto de reglas configurables, llamadas políticas.

Las políticas de filtrado de paquetes, podrán permitir o denegar los paquetes según la dirección IP de origen, con base en su puerto de destino o de acuerdo al protocolo. Éste es el tipo original y más básico de cortafuegos.

El filtrado de paquetes sólo es eficaz en la información que salen de nuestra red, pero no es la seguridad a toda prueba. Puede bloquear todo el tráfico, que en cierto sentido es la seguridad absoluta, pero para cualquier red de utilidad debe permitir que algunos paquetes se envíen. Una de sus debilidades es que la información sobre la dirección en un paquete puede ser falsificada por el remitente permitiendo que los datos o peticiones contenidas en dichos paquetes logren hacer que las cosas no deseadas sucedan, como cuando un pirata informático explota una vulnerabilidad en un programa del servidor web para hacer cumplir sus órdenes.

Stateful. Es un firewall que mantiene un seguimiento del estado de las conexiones de red (como los paquetes TCP) que pasan a través de él. El firewall está programado para conocer cuáles paquetes legítimos pertenecen a los diferentes tipos de conexiones. Sólo los paquetes que concuerdan con un estado de conexión conocido estarán permitidos para pasar a través del firewall; los otros serán rechazados.

Dynamic packet filtering. Un filtro de paquetes dinámico es un servidor de seguridad que monitorea el estado de las conexiones activas y utiliza esta información para determinar qué paquetes de la red se van a permitir. Estos datos pueden ser: la información, el período de sesiones, la dirección IP y los números de puerto. Un filtro de paquetes dinámico puede aplicar una postura de seguridad mucho más estrecho que un filtro de paquetes estáticos.

Respaldo de los datos. Es el proceso de copiar los elementos de información recibidos, transmitidos, almacenados, procesados y/o generados por el sistema. Existen muchos mecanismos para realizar un respaldo dependiendo de lo que se quiera asegurar. Algunos ejemplos son: copias de la información en dispositivos de almacenamiento secundario, computadoras paralelas ejecutando las mismas transacciones, etcétera, fortalece la disponibilidad.

VPN (Virtual Private Network). Tecnología que permite la conexión virtual segura entre puntos remotos cuya localización geográfica impide que la red local sea física. Es

decir, forma un canal seguro entre dos dispositivos. Los datos se encapsulan dentro de un túnel cifrado usando los protocolos PPTP, IPSec y L2TP; véase figura 1.15.

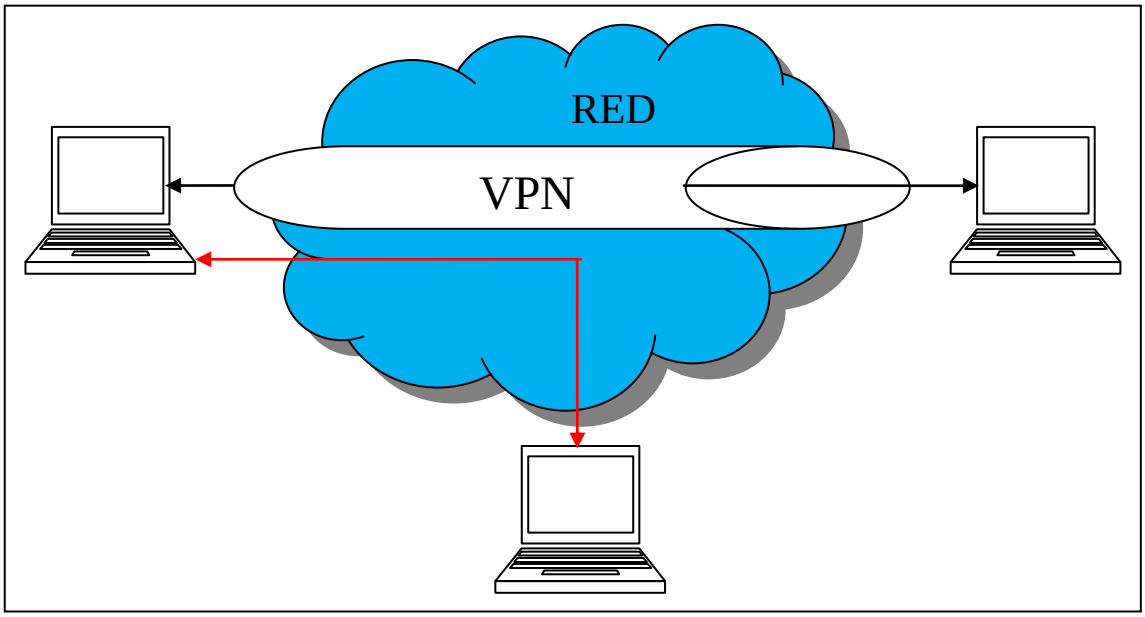


Figura 1. 15. Representación de un VPN.

Tipos de VPN:

Site-to-Site. Los dos sitios a conectarse tienen un lugar e IP fijo requiriendo de negociadores (peer) para comunicarse entre sí.

Client-to-Site. Se puede emplear desde cualquier lugar requiriendo solamente de un software cliente que se encarga de la autenticación y creación del túnel.

1.12 Políticas de seguridad

Una política de seguridad es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos dentro de la misma. En ella se deben de considerar las amenazas contra las computadoras, especificando cuáles son dichas amenazas y cómo contrastarlas, demás,

de ser expresada en un lenguaje en el que todas las personas involucradas puedan entenderlas.

Reglas o consejos para redactar políticas de seguridad.

1. Se debe seleccionar una filosofía, entre:

   a) Permisiva. La cual implica que todo se permite, excepto lo que está explícitamente prohibido.

   b) Prohibitiva. Implica que todo se prohíbe, excepto lo que está explícitamente permitido.

2. Se debe evitar cualquier tipo de ambigüedad.

3. La redacción se debe hacer de manera positiva.

4. Se asignará un dueño.

5. Se debe mencionar una capacitación.

6. Se debe evitar hostigamiento, es decir, se debe considerar que las personas son humanas.

1.13 Características de las políticas de seguridad

La política de seguridad es un documento oficial para las autoridades y la comunidad con vigencia permanente y actualizable periódicamente, que es aprobada por todas las personas afectadas, sirviendo como modelo de referencia para otros esquemas de seguridad debido a que enfocan la problemática particular de cada institución.

Establece obligaciones y derechos, condiciones aceptables y no aceptables de los administradores y usuarios, siendo clara, exacta, precisa y concisa, ya que debe tener una estructura bien definida para ser accesible a toda la comunidad.

Si se desea realizar políticas, se debe tomar en cuenta de declarar el problema, identificando qué se debe proteger y de qué se debe proteger; así como el tipo de usuario a los que se les impondrá.

Dentro del contenido de las políticas debe aparecer el ámbito de aplicación, el análisis de riesgo, los enunciados de políticas, las sanciones que se impondrán al no cumplir los enunciados de las políticas, la sección de uso ético de los recursos y de los procedimientos para el manejo de incidentes, tomando en cuenta los siguientes principios:

1. Responsabilidad individual. Las personas son responsables de sus actos. La gente que está plenamente identificada debe estar consciente de sus actividades, debido a que sus acciones son registradas, guardadas y examinadas.

2. Autorización. Son reglas acerca de quién y de qué manera puede utilizar los recursos.

3. Mínimo privilegio. La gente debe estar autorizada única y exclusivamente para acceder a los recursos que necesita para hacer su trabajo.

4. Separación de obligaciones. Las funciones deben estar divididas entre las diferentes personas relacionadas a la misma actividad o función, con el fin de que ninguna persona cometa un fraude o ataque sin ser detectado.

5. Auditoría. El trabajo y los resultados deben ser monitoreados durante su inicio y hasta después de ser terminados. Una revisión de los registros donde se guardan las actividades ayuda a realizar una reconstrucción de las acciones de cada individuo.

6. Redundancia. Afecta al trabajo y a la información. Múltiples copias son guardadas con importantes registros y dichas copias son frecuentemente almacenadas en diferentes lugares.

7. Reducción de riesgos. Esta estrategia debe reducir el riesgo a un nivel aceptable, haciendo que el costo de la aplicación sea proporcional al riesgo.

Las personas que participan en la elaboración de dichas políticas son:

1. Administrador. Persona que gestionará los recursos a proteger.

2. Personas con autoridad. Persona quien podrá imponer la sanción, tales como jefes de área, supervisores, etcétera.

3. Responsable jurídico. Persona que vigilará que se cumpla los derechos de los individuos.

4. Redactor. Persona que se encargará de escribir con la ortografía debida las políticas.

5. Usuario típico. Persona que hará uso de los recursos proporcionados por el administrador.

En las políticas jamás se establecen los mecanismos empleados sino la necesidad. Se redactan en presente, si se redacta en futuro debe aparecer la fecha en la que entrarán en vigor.

1.14 Procedimiento y planes de contingencia

Un procedimiento es el conjunto de acciones que se implementan para cumplir un objetivo. También es conocido como metodología. Dentro de la seguridad, un procedimiento es en

conjunto de medidas precautorias que se llevan a cabo para recobrarse de un incidente o evitarlo.

En una organización es sumamente importante diseñar, desarrollar e implementar un procedimiento de seguridad. En ocasiones puede plantearse como un esquema de seguridad que llevará a la organización a cumplir sus objetivos.

Los procedimientos se pueden clasificar en:

a) Procedimientos preventivos: Medidas que se implementan para procurar que alguna situación no ocurra.

b) Procedimientos correctivos: Medidas que se implementan cuando alguna situación no esperada ha ocurrido.

Plan de contingencias

Programa de tipo predictivo, preventivo y reactivo con una estructura extra lógica, operativa e informativa, desarrollado por la empresa para el control de alguna o varias emergencias que se produzcan durante la actividad de la empresa.

Estrategia construida por un conjunto de recursos ideados con el propósito de servir de respaldo, contando con la organización de emergencia y con procedimientos de actuación encaminados a conseguir una restauración progresiva y ágil de los servicios del negocio afectados por una paralización total o parcial de la capacidad operativa de la empresa.

El plan de contingencias debe ser diseñado, desarrollado, probado y modificado (Plan, do, check, act).

1.15 Análisis de riesgo

El análisis de riesgo es un procedimiento para estimar el riesgo que tienen los activos para sufrir una pérdida debido a la explotación de las vulnerabilidades de un sistema por medio de las amenazas.

> *"Ya que no existe una seguridad total y las medidas de seguridad no pueden asegurar al 100% la protección en contra de las vulnerabilidades, es imprescindible realizar periódicamente en una organización, un análisis de riesgo para identificar las consecuencias probables o los riesgos con las vulnerabilidades, y así, lograr un manejo de riesgo tras la implementación y el mantenimiento de controles que reduzcan los efectos de éste a un nivel aceptable."[1]*

1.15.1 Consideraciones del análisis de riesgo

En un proceso de análisis de riesgo debe considerarse la siguiente terminología:

a) La amenaza es algo que está latente y pretende hacer uso de una vulnerabilidad.

b) El riesgo es la probabilidad de que exista un daño o pérdida en el sistema.

c) La vulnerabilidad es un punto débil dentro del sistema.

d) Un ataque es la culminación de una amenaza al momento de explotar la vulnerabilidad.

e) La aceptación de un riesgo es cuando, a pesar de saber las consecuencias de los actos, se realiza la acción.

f) El manejo del riesgo sucede al momento en que si hay riesgos, el administrador decide cómo se va a manejar dicho riesgo.

g) En el análisis del riesgo, se toma la información para ver qué va a suceder y en caso de que suceda poder evitarlo.

h) En la evaluación de riesgo, se comprueba lo que se obtuvo con la información, con algún parámetro obtenido con anterioridad, catalogándolo si es mejor o no.

i) Impacto. Se evalúa cuál fue la cantidad de activos, se hace la cuantificación del daño, catalogándolo en denegación de servicio, destrucción, revelación, modificación.

j) La pérdida esperada es imaginar lo que se puede perder.

k) El riesgo residual es el riesgo que queda a pesar de las acciones implementadas.

l) En el control, un análisis de riesgo de seguridad es un procedimiento para estimar el riesgo de los activos de cómputo relacionados y la pérdida debido a la manifestación de las amenazas. El procedimiento primero determina el nivel de vulnerabilidad del activo tras identificar y evaluar el efecto de los controles colocados en el lugar.

Las relaciones de algunos de estos elementos son ilustradas en un modelo relacional simple como se aprecia en la figura 1.16. [1]

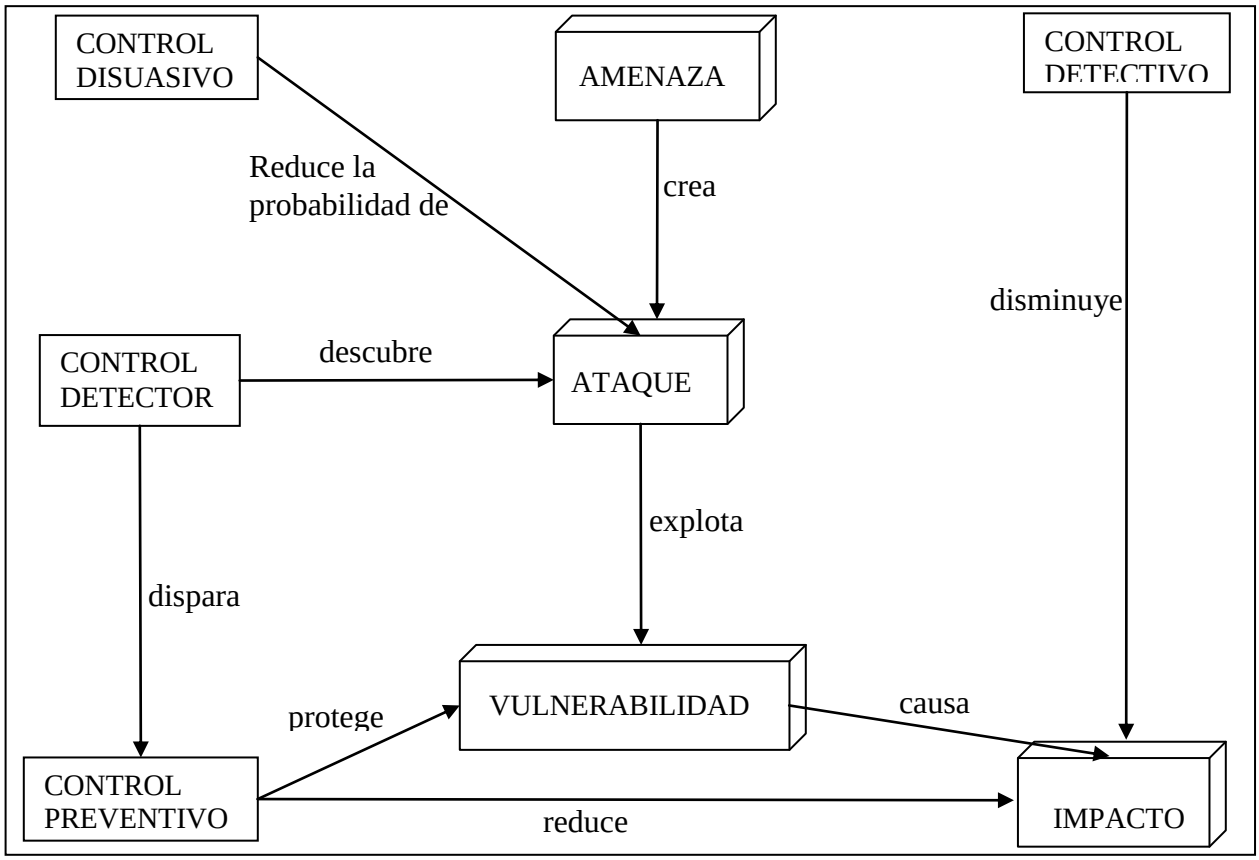


Figura 1. 16. Modelo relacional simple.

1.15.2 Objetivos del análisis de riesgo

Los objetivos que pretende el análisis de riesgo son identificar, evaluar y manejar los riesgos de seguridad, estimando la exposición de un recurso a una amenaza determinada para tomar decisiones en seguridad de la información, como determinar qué combinación de medidas de seguridad proporcionará un nivel de seguridad razonable a un costo aceptable o cómo enfocar recursos y esfuerzos en la protección de los activos.

1.15.3 Valoración en el análisis de riesgo

Existen dos tipos de criterio para darle valor a los recursos dentro del análisis de riesgo, los cuales se presentan a continuación:

a) Análisis cualitativo. En lugar de establecer valores exactos se dan notificaciones que representan la frecuencia de ocurrencia y el valor de los activos.

b) Análisis cuantitativo. Todos los activos y los controles se identifican y se evalúan en términos monetarios. Todas las amenazas potenciales se identifican y se estima la frecuencia de su ocurrencia. Estas amenazas se comparan con las vulnerabilidades potenciales del sistema, de tal forma que se identifican las áreas que son sensibles.

   El análisis cuantitativo hace uso de la expectativa de pérdida anual (ALE) o costo anual estimado (EAC), el cual se calcula para un cierto acontecimiento, multiplicando la frecuencia de la ocurrencia de la amenaza por el valor del activo o clasificación del daño. Para esto se utilizan técnicas matemáticas y estadísticas.

Existen tres puntos que deben tomarse en cuenta para que una organización identifique sus requerimientos de seguridad.

a) Riesgos de seguridad.
b) Requerimientos legales, regulatorios, y contráctiles.
c) Principios, objetivos y recursos para procesar la información.

Además de los puntos antes mencionados, la organización debe balancear el costo de sus controles con el nivel de seguridad requerido, pues no es conveniente que el costo sea excesivo y la seguridad brindada deficiente o nula.

1.15.4 Pasos del análisis de riesgo

Para realizar un análisis de riegos primero se deben identificar los activos, después evaluarlos y posteriormente, identificar las amenazas, vulnerabilidades y el impacto en el momento de la ocurrencia de las amenazas, las cuales se deben catalogar por áreas, como puede ser de revelación, de modificación, de destrucción o de denegación de

servicio; a su vez se debe tener en claro el lugar o sitio de los controles requeridos o discrecionales. Véase figura 1.17. [1]

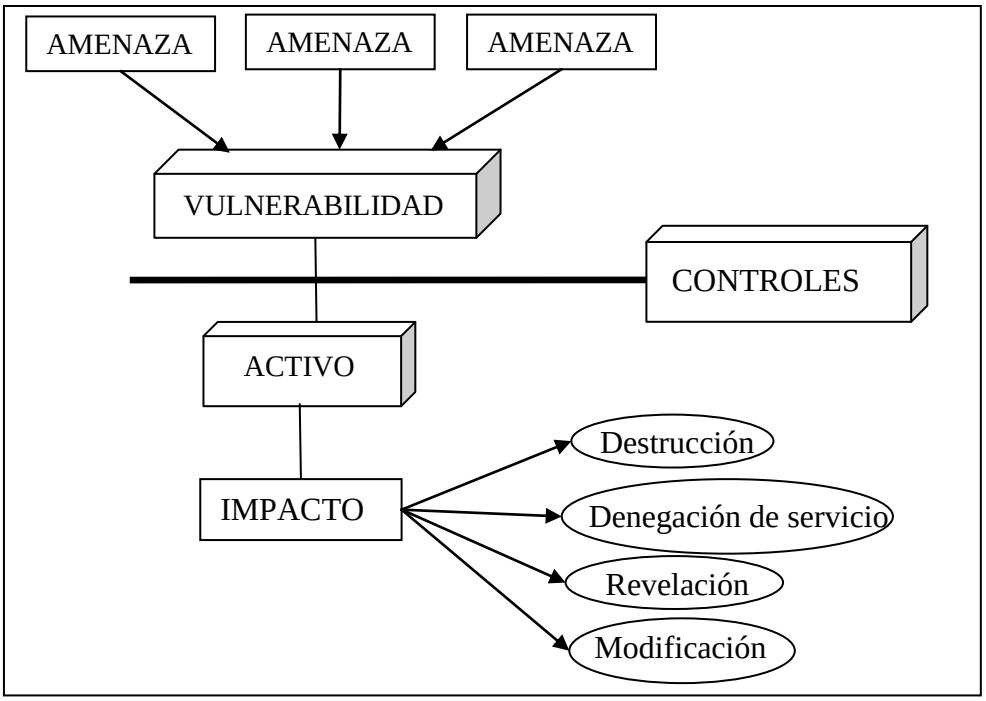


Figura 1. 17. Relaciones entre elementos de un análisis del riesgo.

Una vez realizado lo anterior, se deben determinar los riesgos residuales que pudieran existir para identificar los controles adicionales. Todos los pasos mencionados servirán para preparar un informe del análisis de riesgo, ayudando a saber qué se puede perder en caso de que el sistema sea vulnerado.

CAPÍTULO 2

PLANTEAMIENTO DEL PROBLEMA

2.1 Análisis de requisitos

Basándose en la metodología de cascada, antes descrito en este documento en el punto 1.1 Metodología, podemos observar que, como parte de la fase de análisis de requisitos, se necesita un estudio de la red debido a que la dependencia tiene un número creciente de usuarios de Internet y el servicio de acceso es limitado. Se presentan conflictos como la duplicidad de direcciones IP, ancho de banda sobresaturado e ineficiente. Además, los usuarios se quejan de la lentitud y de que en ocasiones se pierde la conexión a la red.

Los servicios ofrecidos por la dependencia, como el correo y la página web, han sufrido percances de disponibilidad, lo que ha dado a los usuarios la sensación de inseguridad en el envío y recepción de sus correos, así como, que la información presentada en el sitios web no está actualizada ni disponible durante el tiempo que se requiere, además, se extienden rumores de los mismos usuarios sobre la proliferación de virus.

2.1.1 Situación actual de la dependencia

Siguiendo la metodología de cascada antes descrita en este documento y con ayuda del modelo relacional simple, la metodología COBIT y la ISO 17799, explicados en el capítulo 1, se procedió con el análisis de la situación de la dependencia.

Utilizando el método COBIT se examinó la seguridad del gobierno de la dependencia analizando que los recursos de tecnologías de información cumplan con los siete criterios de información en los diferentes procesos en los dominios de: planeación y organización, adquisición e implementación, servicios y soporte, y monitoreo. En la tabla 3 se muestra un resumen de los resultados, se debe considerar que para la valoración de los criterios se ocupó la letra P para abreviar el grado de primario y S para secundario. [13]

Tabla 3. Resumen de los resultados de COBIT.

		Criterios de información								Recursos de TI				
Dominio	**Proceso**	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad		Recursos Humanos	Aplicaciones	Tecnología	Instalaciones	Datos
Planeación y organización														
PO1	Definir un plan estratégico de TI	P	S											
PO2	Definir la arquitectura de información	P	S	S	S					✓			✓	
PO3	Determinar la dirección tecnológica	P	S											
PO4	Definir la organización y relaciones de TI	P	S							✓				
PO5	Manejar la inversión en TI	P	P					S		✓				
PO6	Comunicar las directrices gerenciales	P					S			✓				
PO7	Administrar recursos humanos	P	P							✓				
PO8	Asegurar el cumplir requerimientos externos	P					P	S		✓			✓	
PO9	Evaluar riesgos	S	S	P	P	P	S	S		✓				
PO10	Administrar proyectos	P	P	S	S			S		✓				
PO11	Administrar calidad	P	P		P			S		✓				
Adquisición e implementación														
AI1	Identificar soluciones	P	P					S						
AI2	Adquirir y mantener el software de aplicación	P	P		S	S	S	S						
AI3	Adquirir y mantener arquitectura de TI	P	P		S							✓		
AI4	Desarrollar y mantener procedimientos relacionados con TI	P	P		S		S	S						
AI5	Instalar y acreditar sistemas	P			S	S								
AI6	Administrar cambios	P	P		P	P		S		✓			✓	
Servicios y soporte														
DS1	Definir niveles de servicio	P	P	S	S	S	S	S						
DS2	Administrar servicios de terceros	P	P	S	S	S	S	S						
DS3	Administrar desempeño y capacidad	P	P			S								
DS4	Asegurar servicio continuo	P	S			P				✓				
DS5	Garantizar la seguridad de sistemas			P	P	S	S	S						
DS6	Identificar y asignar costos		P					P		✓				
DS7	Capacitar usuarios	P	S											
DS8	Asistir a los clientes de TI	P								✓				
DS9	Administrar la configuración	P				S		S						
DS10	Administrar problemas e incidentes	P	P			S				✓				
DS11	Administrar datos				P			P						
DS12	Administrar instalaciones				P	P							✓	
DS13	Administrar operaciones	P	P		S	S				✓				
Monitoreo														
M1	Monitorear los procesos	P	S	S	S	S	S	S						
M2	Evaluar lo adecuado del control interno	P	P	S	S	S	S	S		✓				
M3	Obtener aseguramiento independiente	P	P	S	S	S	S	S		✓				
M4	Proveer auditoría independiente	P	P	S	S	S	S	S						

Como se puede observar en la tabla 3, en el caso del dominio de planeación y organización, al no calificase dos de los once procesos a evaluar, los cuales fueron los procesos: PO1 y PO3; en el dominio de adquisición e implementación no se cumplió en cuatro de seis procesos: AI1, AI2, AI4 y AI5; en el dominio de servicios y soporte no se calificó en siete de trece: DS1, DS2, DS3, DS5, DS7, DS9 y DS11; finalmente para el dominio de monitoreo no se verificó dos de cuatro: M1 y M4, debido a lo anterior se puede concluir que la seguridad de la dependencia es mala, ya que existen procesos de los dominios que no se cubrieron.

En la tabla 4 se puede observar un resumen con los porcentajes que se obtienen a partir de la situación antes mencionada.

Tabla 4. Porcentajes obtenidos de la tabla 3.

Dominio	Procesos a evaluar	Procesos no evaluados	Porcentaje de procesos evaluados	Porcentaje de procesos no evaluados
Planeación y organización	11	2	81.82 %	18.18%
Adquisición e implementación	6	4	33.34 %	66.66%
Servicios y soporte	13	7	46.16 %	53.84%
Monitoreo	4	2	50.00 %	50.00%
TOTAL	34	15	55.89 %	44.11%

En conclusión, como se puede observar en la tabla 4, el porcentaje de procesos no evaluados el muy alto, lo que hace pensar que la seguridad de la dependencia es muy baja, para ello en el siguiente capítulo se tratará de minimizar este porcentaje.

Después de revisar el estado del gobierno de la dependencia, se procede a hacer un análisis más orientado a la operatividad de la institución con ayuda de entrevistas al personal de la misma basándose en la norma ISO 17799. [14] Por lo que se obtiene lo siguiente:

- Descripción de la organización y sus objetivos. La dependencia posee un giro educativo y de investigación, su objetivo es instruir a los próximos profesionistas para que se puedan desenvolver en el campo laboral, con los conocimientos básicos y la experiencia necesaria, ayudando así a abrir una oportunidad de progreso al país.

- Levantamiento del detalle topológico de la infraestructura de tecnología existente. Se encontró que la dependencia comparte la red con otras instituciones, aparte de brindar servicios a sus usuarios, como lo es el correo, la plataforma educativa, pagina web, servicio de internet a dispositivos fijos e inalámbricos. Véase figura 2.1.

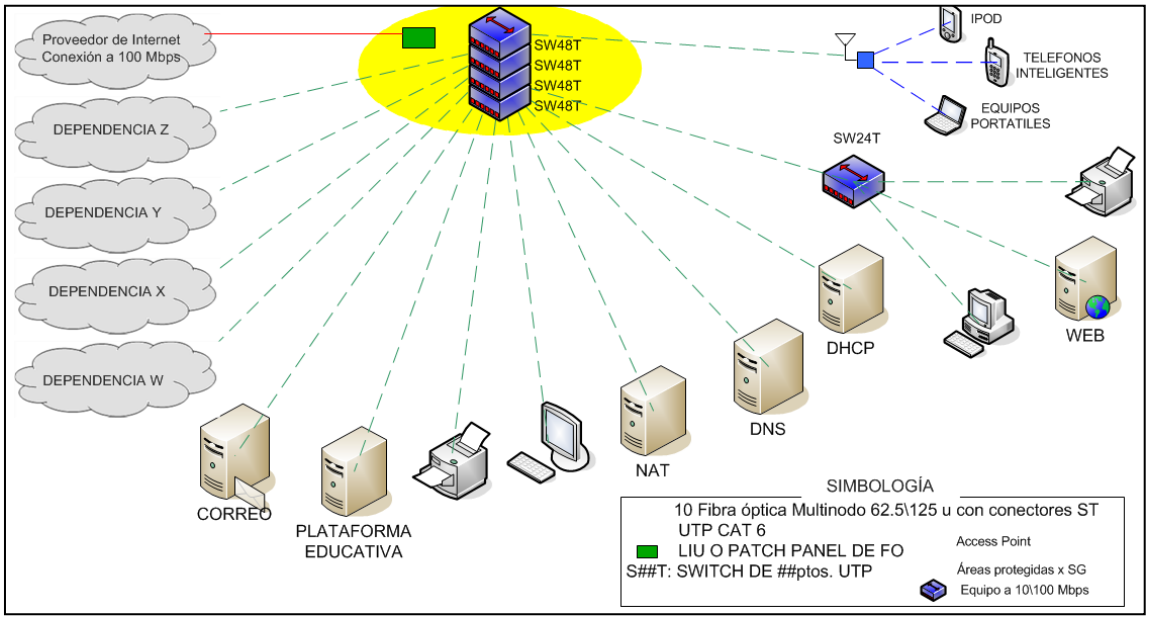


Figura 2. 1. Detalle topológico de la dependencia

En los servidores de correo y DNS se utiliza el sistema operativo Windows Server. La plataforma educativa está hecha en Moodle con una base de datos en MySQL y montada sobre Windows Server. El DHCP y el NAT se encuentran desarrollados en OpenBSD. El servidor web se compone de Joomla, una DB en MySQL trabajando en Ubuntu 9.10.

- Lista de verificación de la infraestructura tecnológica. Esta lista se realizó con el objetivo de identificar las vulnerabilidades, las amenazas y los riesgos que aquejan a la dependencia, así como mostrar un panorama general de su situación. En dicha lista de verificación se podrá ver una paloma (✓) en el campo llamado "EXISTE" cuando la dependencia responde favorablemente a las preguntas de auditoría de los diez diferentes campos de actuación de la seguridad. Véase tabla 5.[15]

Tabla 5. Lista de verificación.

		PREGUNTA DE AUDITORÍA	EXISTE
1 POLÍTICA DE SEGURIDAD	*INFORMACIÓN DE LA POLÍTICA DE SEGURIDAD*		
	SEGURIDAD DE LA INFORMACIÓN POLÍTICA DE DOCUMENTO	¿Existe una política de seguridad de la información, aprobada por la dirección, publicada y comunicada en su caso a todos los empleados?	
		¿Se establece el compromiso de la dirección y el enfoque de la organización para la gestión de seguridad de la información?	
	REVISIÓN Y EVALUACIÓN	¿La política de seguridad tiene un propietario, el cual es responsable de su mantenimiento y revisión con apeglo a un proceso de revisión definido?	
		¿El proceso garantiza que la revisión se lleva a cabo en respuesta a los cambios que afectan a la base de la evaluación inicial?, por ejemplo: los incidentes de seguridad significativos, nuevas vulnerabilidades o cambios en la infraestructura técnica o de organización.	
2 ORGANIZACIÓN DE SEGURIDAD	*INFORMACIÓN DE LA INFRAESTRUCTURA DE SEGURIDAD*		
	INFORMACIÓN DE GESTIÓN DE SEGURIDAD EN EL FORO	¿Existe un foro de gestión para asegurarse de que existe una dirección clara y apoyo a la gestión visible para las iniciativas de seguridad dentro de la organización?	
	COORDINACIÓN DE INFORMACIÓN DE LA SEGURIDAD	¿Existe un foro funcional con representantes de la dirección y partes pertinentes de la organización para coordinar la aplicación de los controles de seguridad de la información?	
	ASIGNACIÓN DE LAS RESPONSABILIDADES DE SEGURIDAD DE INFORMACIÓN	¿Se definieron con claridad las responsabilidades para la protección de los activos individuales y para llevar a cabo los procesos de seguridad específicos?	

	PROCESO PARA LA AUTORIZACIÓN DE INSTALACIONES DE PROCESAMIENTO DE LA INFORMACIÓN	¿Existe un proceso de autorización de gestión en vigor para cualquier instalación de tratamiento de la información nueva? Esto debería incluir todas las instalaciones nuevas, tanto hardware y software.	
	ESPECIALISTA EN SEGURIDAD DE LA INFORMACIÓN ACONSEJA	¿Se obtienen consejos en la seguridad información especializada?	✓
		¿Se puede identificar un individuo con experiencia y conocimientos para coordinar, garantizar la coherencia, y proporcionar ayuda en la toma de decisiones de seguridad?	✓
	COOPERACIÓN ENTRE LAS ORGANIZACIONES	¿La cooperación adecuada con las autoridades, los organismos reguladores, proveedores de servicios de información y los operadores de telecomunicaciones se mantuvieron para garantizar que las medidas adecuadas y los dictámenes pueden ser rápidamente adoptadas, en el caso de un incidente de seguridad?	✓
	REVISIÓN INDEPENDIENTE DE SEGURIDAD DE LA INFORMACIÓN	¿La política de seguridad se revisa de forma independiente de manera regular, para garantizar que las prácticas de la organización reflejan adecuadamente la política, y que es factible y eficaz?	
	SEGURIDAD DE ACCESO DE TERCEROS		
	IDENTIFICACIÓN DE LOS RIESGOS DE ACCESO DE TERCEROS	¿Los riesgos de acceso de terceros se identifican y se ponen en práctica los controles de seguridad apropiados?	
		¿Los tipos de accesos se identifican, clasifican y las razones para el acceso se justifican?	
		¿Los riesgos de seguridad con los contratistas de terceros en el sitio de trabajo fueron identificados y se aplicaron los controles adecuados?	
	REQUISITOS DE SEGURIDAD EN LOS CONTRATOS DE TERCEROS	¿Existe un contrato laboral que contengan, o se refiera a todos los requisitos de seguridad para garantizar el cumplimiento de las políticas de seguridad de la organización y normas?	
	OUTSOURCING		
	REQUISITOS DE SEGURIDAD EN LOS CONTRATOS DE OUTSOURCING	¿Los requisitos de seguridad se abordan en el contrato con el tercero? Cuando la organización ha subcontratado la gestión y control de todos o algunos de sus sistemas de información, redes y / o entornos de escritorio.	
		¿El contrato incluye los requisitos legales que deben cumplir?, como la seguridad de la organización y de los activos son mantenidos y probados, el derecho de la auditoría, las cuestiones de seguridad física y la forma en que se mantendrá en caso de desastre la disponibilidad de los servicios.	
3 CLASIFICACIÓN	*RENDICIÓN DE CUENTAS DE LOS ACTIVOS*		

DE LOS ACTIVOS Y EL CONTROL	INVENTARIO DE LOS BIENES	¿Se mantiene un inventario o registro con los activos importantes asociados a cada sistema de información?	
	CLASIFICACIÓN DE LA INFORMACIÓN	¿Cada uno de los activos identificados tiene un propietario, una clasificación de seguridad definida y acordada y un lugar indicado?	
	DIRECTRICES DE CLASIFICACIÓN	¿Existe un sistema de clasificación de información o guía en su lugar, lo que ayudará a determinar cómo la información debe ser manejada y protegida?	
	INFORMACIÓN DE ETIQUETADO Y MANIPULACIÓN	¿Existe un conjunto adecuado de los procedimientos definidos para la información de etiquetado y manipulación, de acuerdo con el esquema de clasificación, adoptada por la organización?	
4 SEGURIDAD DEL PERSONAL	*SEGURIDAD EN LA DEFINICIÓN DE PUESTOS DE TRABAJO Y RECURSOS*		
	SEGURIDAD EN LAS RESPONSABILIDADES DEL TRABAJO	¿Las funciones y responsabilidades de seguridad según lo establecido en la política seguridad de la información de la organización se documentan?	
		¿Se incluyen las responsabilidades generales de aplicación o el mantenimiento de la política de seguridad, así como las responsabilidades específicas para la protección de determinados bienes o para la ampliación de los procesos de seguridad o actividades?	
	PERSONAL DE INSPECCIÓN Y LA POLÍTICA	¿Los controles de verificación del personal permanente se llevaron a cabo en el momento de las solicitudes de empleo?	✓
		¿Incluye títulos académicos del profesional la referencia del carácter, la confirmación del reclamado y la identidad de los controles independientes?	✓
	ACUERDOS DE CONFIDENCIALIDAD	¿Los empleados firman un acuerdo de confidencialidad, como parte de los términos y condiciones iníciales del empleo?	
		¿Este acuerdo se refiere a la seguridad de la planta de procesamiento de la información y los activos de la organización?	
	TÉRMINOS Y CONDICIONES DE EMPLEO	¿Los términos y condiciones del empleo abarcan la responsabilidad del empleado en cuanto a la seguridad de la información?	
	FORMACIÓN DE USUARIOS		
	INFORMACIÓN, EDUCACIÓN Y FORMACIÓN DE SEGURIDAD	¿Todos los empleados de la organización y usuarios terceros reciben información adecuada de formación de seguridad y actualizaciones regulares en las políticas y procedimientos de organización?	
	EN RESPUESTA A INCIDENTES DE SEGURIDAD Y MAL FUNCIONAMIENTO		
	PRESENTACIÓN DE INFORMES DE INCIDENTES DE SEGURIDAD	¿Existe un procedimiento de notificación formal, para reportar los incidentes de seguridad a través de canales de gestión adecuadas tan pronto como sea posible?	

	INFORMES DE DEBILIDADES DE SEGURIDAD	¿Existe un procedimiento de notificación formal dirigido a los usuarios, para informar la debilidad en la seguridad, o las amenazas a los sistemas o servicios?	
	INFORMES DE MAL FUNCIONAMIENTO DEL SOFTWARE	¿Se establecen procedimientos para reportar cualquier mal funcionamiento del software?	
	APRENDIENDO DE LOS INCIDENTES	¿Se dispone de mecanismos que permitan cuantificar y monitorear los tipos de averías, volúmenes y costos de los incidentes?	
	PROCESO DISCIPLINARIO	¿Existe un proceso disciplinario formal para empleados que han violado las políticas de seguridad y los procedimientos de la organización?	
5 SEGURIDAD FÍSICA Y AMBIENTAL	*ÁREA SEGURA*		
	PERÍMETRO DE SEGURIDAD FÍSICA	¿Qué frontera de protección de la instalación física se ha implementado para proteger el servicio de procesamiento de la información? Algunos ejemplos son el control de tarjeta de puerta de entrada, paredes, recepción, etc.,	Puertas con llave
	CONTROLES DE ENTRADA FÍSICA	¿Qué controles de entrada permiten que sólo el personal autorizado entre en distintas áreas de la organización?	Puertas con llave, personal del área
	OFICINAS DE PROTECCIÓN, HABITACIONES E INSTALACIONES	¿Las habitaciones, que tienen el servicio de procesamiento de la información, se han bloqueado?, ejemplo armarios con llave o caja fuerte.	Puertas con llave
		¿El servicio de procesamiento de la información es protegida por el hombre de desastres naturales?	
		No existe cualquier amenaza potencial de los establecimientos vecinos.	✓
	TRABAJO EN ÁREAS SEGURAS	¿Existe algún control de seguridad para terceros o para el personal que trabaja en un área segura?	✓
	ENTREGA AISLADOS Y ZONAS DE CARGA	¿El área de prestación y el área de procesamiento de la información están aisladas unos de otras para evitar cualquier acceso no autorizado?	
		¿Se llevó a cabo, una evaluación de riesgos para determinar la seguridad en esas zonas?	✓
	EQUIPO DE SEGURIDAD		
	EQUIPOS DE PROTECCIÓN	¿El equipo se encuentra en el lugar adecuado para minimizar el acceso innecesario a las áreas de trabajo?	✓
		¿Los elementos que requieren una protección especial fueron aislados para reducir el nivel general de protección requerido?	✓
		¿Los controles fueron adoptados para minimizar el riesgo de las amenazas potenciales?, tales como incendios, explosivos, humo, agua, vibraciones, efectos químicos, el suministro de interfaces eléctricas, radiación electromagnética,	✓

		las inundaciones.	
		¿Existe una política hacia el comer, beber y fumar en las proximidades de los servicios de procesamiento de la información?	
		¿Las condiciones ambientales que pueden afectar las instalaciones de procesamiento de la información son monitoreadas?	✓
	FUENTES DE ALIMENTACIÓN	¿El equipo está protegido contra fallas de energía mediante el uso de la permanencia de fuentes de alimentación, tales como múltiples fuentes, sistema de alimentación ininterrumpida (UPS), generador de respaldo, etc?	
	CABLEADO	¿El cable de alimentación y de telecomunicaciones que llevan los datos o el apoyo a los servicios de información están protegidos de la intercepción o daño?	✓
		¿Hay controles de seguridad adicionales en un lugar crítico o información confidencial.	✓
	MANTENIMIENTO DE EQUIPO	¿El equipo se mantiene por los intervalos de servicio y las especificaciones como lo recomienda el proveedor?	
		¿El mantenimiento se lleva a cabo únicamente por personal autorizado?	✓
		¿Los registros se mantienen con todos los defectos reales o presuntos y todas las medidas preventivas y correctivas?	
		¿Se aplican los controles adecuados durante el envío de equipos fuera de las instalaciones'	
		¿El equipo está cubierto por el seguro?	✓
	PROTEGER LOS EQUIPOS FUERA DE LAS INSTALACIONES	¿Cualquier uso del equipo fuera de la organización tiene que ser autorizada por la dirección?	✓
		¿La garantía de estos equipos, mientras están fuera, están a la par con uno o más de la garantía de los están dentro de las instalaciones?	
	ASEGURE SU ELIMINACIÓN O REUTILIZACIÓN DE LOS EQUIPOS	¿El dispositivo de almacenamiento que contienen información sensible son destruidos físicamente o bien sobrescrito?	✓
	CONTROLES GENERALES		
	INFORMACIÓN CLARA Y LA POLÍTICA DE PANTALLA CLARA	¿La pantalla de bloqueo automático de la computadora está activada?	
		¿A los empleados se les aconseja que cualquier material confidencial en la forma de documentos en papel, medios de comunicación, etc., se encuentren de una manera cerrada mientras esté desatendida?	
	ELIMINACIÓN DE LA PROPIEDAD	¿El equipo, información o software se pueden tomar fuera de las instalaciones sin la debida autorización?	
		¿Se llevaron a cabo auditorías periódicas para detectar la retirada no autorizada de la propiedad?	
		¿Se concientizan a las personas de las auditorías periódicas?	

6 COMUNICA-CIONES Y GESTIÓN DE OPERACIONES	*PROCEDIMIENTO OPERATIVO Y RESPONSABILIDADES*		
	PROCEDIMIENTOS DOCUMENTADOS DE OPERACIÓN	¿La política de seguridad ha identificado los procedimientos operativos como respaldos, mantenimiento, equipos, etc.?	
		¿Los procedimientos son documentados e implementados?	
	OPERACIONAL DE CAMBIO DE CONTROL	¿Todos los programas que se ejecutan en los sistemas de producción están sujetos a cambio?	✓
		¿Los registros de auditoría se mantienen para cualquier cambio realizado en los programas de producción?	
	INCIDENTES DE LOS PROCEDIMIENTOS DE GESTIÓN	¿Existe un procedimiento de Gestión de Incidentes para tratar los incidentes de seguridad?	
		¿El procedimiento se refiere a la responsabilidades de manejo de incidentes, ordenada y rápida respuesta a incidentes de seguridad?	
		¿El procedimiento de direcciones de diferentes tipos de incidentes va desde la denegación de servicio a la violación de la confidencialidad, etc., y las maneras de manejarlos?	
		Independientemente de que los caminos y registros relativos a los incidentes ¿se toman y se mantienen medidas proactivas de manera que el incidente no vuelva a ocurrir?	
	SEPARACIÓN DE LAS FUNCIONES	¿Los derechos y las áreas de responsabilidad se separan con el fin de reducir las posibilidades de modificación no autorizada o mal el uso de la información o de los servicios?	
	SEPARACIÓN DE DESARROLLO E INSTALACIONES OPERATIVAS	¿El desarrollo y las instalaciones de prueba están aislados de las instalaciones operativas?	✓
	EXTERNOS DE GESTIÓN DE INSTALACIONES	¿Alguna de las instalaciones de procesamiento de la información es administrada por una empresa externa o contratista (tercero)?	
		¿Los riesgos asociados a dicha gestión se identifican con antelación, se discuten con el tercero y los controles adecuados se incorporaron en el contrato?	
		¿La aprobación necesaria se obtiene de la aplicación y los dueños de negocios?	
	SISTEMA DE PLANIFICACIÓN Y LA ACEPTACIÓN		
	PLANIFICACIÓN DE LA CAPACIDAD	¿La capacidad de las demandas son monitoreados y se hacen proyecciones de futuros requerimientos de capacidad?, esto es para asegurar que el proceso de alimentación y de almacenamiento estén disponibles. Ejemplo: Control de espacio en disco duro, RAM, CPU en servidores críticos.	✓
	SISTEMA DE ACEPTACIÓN	¿En la aceptación del sistema se establecen criterios para nuevos sistemas de información, actualizaciones y nuevas versiones?	✓

		¿Las pruebas adecuadas se llevaron a cabo antes de la aceptación?	✓
	PROTECCIÓN CONTRA SOFTWARE MALICIOSO		
	CONTROL CONTRA SOFTWARE MALICIOSO	¿Existe algún tipo de control contra el uso de software malicioso?	✓
		¿La política de seguridad se ocupa de cuestiones de licencias de software tales como la prohibición de uso de software no autorizado?	
		¿Existe algún procedimiento para verificar que todos los boletines de alerta son precisos e informativos en relación con el uso de software malicioso?	
		¿El software antivirus se instala en los equipos para verificar y aislar o eliminar cualquier virus de computadora y los medios de comunicación?	✓
		¿Se actualiza la firma de software de forma periódica para comprobar que se cuenta con la base de virus más reciente?	
	LIMPIEZA		
	INFORMACIÓN DE RESERVA	¿Se toma con regularidad el respaldo de información del servidor de producción, componentes de red críticos, backup de la configuración, etc.? Ejemplo: de lunes a jueves: de copia de seguridad incremental y viernes: de copia de seguridad completa.	
		¿Los medios de copia de seguridad junto con el procedimiento para restaurar la copia de seguridad se almacenan de forma segura y lejos del sitio real?	
		¿Los medios de copia de seguridad se examinan regularmente para asegurarse de que pudieran ser restaurados en el marco de tiempo asignado en el procedimiento operativo para la recuperación?	
	OPERADOR DE REGISTROS	¿Tanto el personal operativo mantiene un registro de sus actividades, como el nombre de la persona, errores, medidas correctivas, etc.?	
		¿Se comprueban los registros del operador de manera regular en contra de los procedimientos de operación?	
	FALLO DE REGISTRO	¿Las fallas que se presentan son administradas? Esto incluye las medidas correctivas adoptadas, la revisión de los registros de la falla y verificación de las medidas adoptadas.	
	GESTIÓN DE REDES		
	RED DE CONTROL	¿Los controles operacionales, tales como red independiente y administración de recursos del sistema se establecen efectivamente cuando es necesario?	
		¿Se establecieron responsabilidades y procedimientos de gestión de equipos remotos?	
		¿Existen controles especiales para proteger la confidencialidad e integridad de procesamiento de	

		datos sobre la red pública y así proteger los sistemas conectados? Ejemplo: Redes privadas virtuales, el cifrado y otros mecanismos de hashing, etc.	
	MEDIOS DE MANIPULACIÓN Y DE SEGURIDAD		
	GESTIÓN DE SOPORTES INFORMÁTICOS EXTRAÍBLES	¿Existe un procedimiento para la gestión de los soportes informáticos extraíbles como cintas, discos, casetes de tarjetas de memoria, y los informes?	
	DISPOSICIÓN DE LOS MEDIOS DE COMUNICACIÓN	¿Los medios de comunicación que ya no son necesarios se disponen de forma segura?	✓
		¿La eliminación de los productos sensibles está en el sistema cuando sea necesario a fin de mantener un registro de auditoría?	
	INFORMACIÓN DE LOS PROCEDIMIENTOS DE MANIPULACIÓN	¿Existe un procedimiento para el manejo del almacenamiento de la información?	
	SEGURIDAD DE LA DOCUMENTACIÓN DEL SISTEMA	¿La documentación del sistema está protegida del acceso no autorizado?	
		¿La lista de acceso para la documentación del sistema se mantiene al mínimo y es autorizado por el propietario de la aplicación?	
	INTERCAMBIO DE INFORMACIÓN Y SOFTWARE		
	INFORMACIÓN Y ACUERDO DE INTERCAMBIO DE SOFTWARE	¿Existe algún acuerdo formal o informal entre las organizaciones para el intercambio de información y software?	✓
		¿El acuerdo no aborda las cuestiones de seguridad basado en la sensibilidad de la información de negocios involucrados?	
	SEGURIDAD DE LOS MEDIOS DE COMUNICACIÓN EN EL TRÁNSITO	¿Existe seguridad en los medios de comunicación durante su traslado?	
		¿Los medios de comunicación están bien protegidos del acceso no autorizado, mal uso o de la corrupción.	✓
	COMERCIO ELECTRÓNICO DE SEGURIDAD	No aplica.	
	SEGURIDAD DE CORREO ELECTRÓNICO	¿Existe una política de seguridad para el uso aceptable del correo electrónico o que se ocupa de las cuestiones con respecto a la utilización del correo electrónico?	
		¿Tanto los controles como la comprobación de antivirus, aislando adjuntos potencialmente peligrosos, control de spam, contra la retransmisión, etc. se ponen en marcha para reducir los riesgos creados por correo electrónico?	✓
	SEGURIDAD DE LOS SISTEMAS ELECTRÓNICOS	¿Existe una política de uso aceptable para abordar el uso de sistemas electrónicos?	
		¿Existen directrices para controlar eficazmente la seguridad y los riesgos de negocio asociados a los sistemas electrónicos?	

	SISTEMAS DISPONIBLES	¿Existe algún proceso de autorización formal para la información que se pondrá a disposición del público?	✓
		¿Existe controles para proteger la integridad de dicha información a disposición del público de cualquier acceso no autorizado, como firewalls, sistema operativo endurecido, etc.?	
	OTRAS FORMAS DE INTERCAMBIO DE INFORMACIÓN	¿Existen políticas, procedimientos o controles para proteger el intercambio de información a través del uso de la voz, vídeo y servicios de comunicación por fax?	✓
		¿Se les recuerda mantener la confidencialidad de la información sensible durante el uso de estas formas de intercambio de servicio de información?	
7 CONTROL DE ACCESO	*REQUERIMIENTOS DE NEGOCIO PARA EL CONTROL DE ACCESO*		
	POLÍTICA DE CONTROL DE ACCESO	¿Los requisitos del negocio para el control del acceso se han definido y documentado?	
		¿La política de control de acceso se ocupa de las normas y derechos para cada usuario o grupo de usuarios?	
		¿Los usuarios y proveedores de servicios se les dieron una declaración clara de los requerimientos de negocio que deben cumplir los controles de acceso?	
	GESTIÓN DE USUARIOS DE ACCESO		
	REGISTRO DE USUARIO	¿Existe algún registro de usuario formales y de procedimiento de registro para la concesión de acceso a la información del usuario en sistemas múltiples y servicios?	✓
	GESTIÓN DE PRIVILEGIOS	¿La asignación y el uso de algún privilegio en el entorno del sistema de información es restringido y controlado, es decir, los privilegios se asignan según las necesidades?	✓
	GESTIÓN DE CONTRASEÑAS DE USUARIO	¿La asignación y reasignación de contraseñas se controla a través de un proceso formal de gestión?	
		¿Los usuarios se les pide que firmen una declaración de mantener la confidencialidad de la contraseña?	
	REVISIÓN DE LOS DERECHOS DE ACCESO DE LOS USUARIOS	¿Existe un proceso de revisión de los derechos de acceso del usuario a intervalos regulares? Ejemplo: el privilegio especial de revisión cada tres meses, los privilegios normales cada seis meses.	
	RESPONSABILIDADES DEL USUARIO		
	USO DE CONTRASEÑAS	¿Existen directrices en el lugar para guiar a los usuarios en la selección y el mantenimiento de contraseñas seguras?	
	SIN VIGILANCIA EQUIPOS DE USUARIO	¿Los usuarios y los contratistas son conscientes de los requisitos y procedimientos de seguridad para la protección de equipos desatendidos, así como su responsabilidad de aplicar esa	

		protección?	
	RED DE CONTROL DE ACCESO		
	POLÍTICA SOBRE EL USO DE LOS SERVICIOS DE RED	¿Existen procedimientos para proteger el acceso a conexiones de red y servicios de red?	
	CAMINO FORZADO	¿Existe cualquier control que restringa la ruta entre la terminal del usuario y los servicios informáticos?	
	LA AUTENTICACIÓN DE USUARIOS PARA CONEXIONES EXTERNAS	¿Existen mecanismos de autenticación para impugnar las conexiones externas? Ejemplos: la criptografía basada en la técnica, los tokens de hardware o de software, protocolo de respuesta, etc.	
	PUERTO DE DIAGNÓSTICO A DISTANCIA DE PROTECCIÓN	¿El acceso a los puertos de diagnóstico están bien controlados, es decir, protegidos por un mecanismo de seguridad?	✓
	PROTOCOLOS DE RED DE CONEXIÓN	¿Existe algún control de la conexión de red para redes compartidas que se extienden más allá de los límites de la organización? Ejemplo: correo electrónico, acceso a Internet, transferencia de archivos, etc.	✓
	ENCAMINAMIENTO DE LA RED DE CONTROL	¿Existe alguna red de control para garantizar que las conexiones de computadora y los flujos de información no violen la política de control de acceso de las aplicaciones de negocio?	
		¿Los controles de enrutamiento se basan en la fuente positiva y mecanismo de identificación de destino? Ejemplo: la traducción de direcciones de red (NAT).	✓
	SEGURIDAD DE LOS SERVICIOS DE RED	¿La organización utiliza una red privada de servicios públicos o se asegura de que se proporcione una descripción clara de los atributos de seguridad de todos los servicios utilizados?	✓
	FUNCIONAMIENTO DEL SISTEMA DE CONTROL DE ACCESO		
	IDENTIFICACIÓN AUTOMÁTICA DE TERMINALES	¿Se utiliza un mecanismo terminal de identificación automática para autenticar las conexiones?	✓
	TERMINAL DE INICIO DE SESIÓN SOBRE LOS PROCEDIMIENTOS	¿El acceso al sistema de información es posible sólo a través de una conexión segura en el proceso?	
		¿Existe un procedimiento para iniciar sesión en un sistema de información? Esto es para minimizar la posibilidad de acceso no autorizado.	✓
	IDENTIFICACIÓN DE USUARIO Y AUTORIZACIÓN	¿El identificador único se proporciona a cada usuario, tales como operadores, administradores de sistemas y el resto del personal incluido el técnico?	✓
		¿Las cuentas de usuario genérico sólo deben ser suministradas bajo circunstancias excepcionales en las que hay un beneficio claro?	
		¿Existe un método de autenticación para	

		acreditar la identidad declarada de los usuarios (contraseña)?	
	CONTRASEÑA DEL SISTEMA DE GESTIÓN	¿Existe un sistema de gestión de contraseñas que impone contraseñas a diversos controles, tales como: contraseña individual para la rendición de cuentas, aplicar los cambios de contraseña, almacenar contraseñas de forma cifrada, no mostrar las contraseñas en pantalla, etc.?	
	USO DE UTILIDADES DEL SISTEMA	¿Las utilidades del sistema que viene con instalaciones informáticas, pueden reemplazar el sistema de control de aplicaciones y es sometida a estrictos controles?	
	LIMITACIÓN DE TIEMPO DE CONEXIÓN	¿Existe alguna restricción en el tiempo de conexión para aplicaciones de alto riesgo? Este tipo de stands, deberán ser considerados para aplicaciones sensibles a los que los terminales están instalados en lugares de alto riesgo.	
	APLICACIÓN DE CONTROL DE ACCESO		
	INFORMACIÓN DE RESTRICCIÓN DE ACCESO	¿El acceso a la aplicación personal de la organización está definido en la política de control de acceso según el requisito de aplicaciones de negocios individuales y es coherente con la organización de la información política de acceso al archivo?	
	AISLAMIENTO DE SISTEMAS SENSIBLES	¿Los sistemas sensibles cuentan con entorno informático aislados como compartir recursos sólo con sistemas de aplicaciones de confianza, etc.?	
	CONTROL DEL ACCESO AL SISTEMA Y EL USO		
	REGISTRO DE EVENTOS	¿Los registros de auditoría, excepciones de registro y otros eventos relevantes de seguridad se producen y se mantienen durante un período acordado para ayudar a futuras investigaciones y al seguimiento de control de acceso?	
	VIGILANCIA DE LA UTILIZACIÓN DEL SISTEMA	¿Se establecen procedimientos de control en la utilización de instalaciones de procesamiento de información?	
		¿El procedimiento debe garantizar que los usuarios están realizando solamente las actividades que están expresamente autorizadas?	
		¿Los resultados de las actividades de supervisión se revisan con regularidad?	
	SINCRONIZACIÓN	¿El dispositivo de la computadora o la comunicación tiene la capacidad de operar un reloj de tiempo real, se debe establecer en una norma aceptada como coordinado tiempo universal u hora estándar local?	✓
	INFORMÁTICA MÓVIL Y EL TELETRABAJO		
	INFORMÁTICA MÓVIL	¿Existe una política oficial que se adopte, que tenga en cuenta los riesgos de trabajar con recursos informáticos, como portátiles, computadoras de bolsillo, etc. especialmente en entornos desprotegidos?	

		¿Existe en la organizaron cursos para el personal a utilizar las instalaciones de computación móvil para aumentar su conciencia sobre los riesgos adicionales derivados de esta forma de trabajo y los controles que deben aplicarse para mitigar los riesgos?	
	TELETRABAJO	¿Existe cualquier política, procedimiento y/o estándar para controlar las actividades de teletrabajo, esta debe ser coherente con la política de seguridad de la organización?	
		¿La protección adecuada del sitio de teletrabajo se encuentra en su lugar para actuar contra amenazas tales como el robo de equipos, la divulgación no autorizada de información, etc.?	
8 SISTEMA DE DESARROLLO Y MANTENIMIEN-TO	*REQUISITOS DE SEGURIDAD DE LOS SISTEMAS*		
	DE SEGURIDAD ANÁLISIS DE LOS REQUISITOS Y LAS ESPECIFICACIONES	¿Los requisitos de seguridad se incorporan como parte del requisito de declaración de negocio para sistemas nuevos o para la mejora de los sistemas existentes?	
		¿Los requisitos de seguridad y los controles identificados reflejan el valor comercial de los activos de información involucrados y la consecuencia de la falta de seguridad?	✓
		¿Las evaluaciones de riesgos se han completado antes del comienzo del desarrollo del sistema?	
	SEGURIDAD EN LOS SISTEMAS DE APLICACIÓN		
	ENTRADA DE VALIDACIÓN DE DATOS	¿La entrada de datos al sistema de aplicación está validada para asegurarse de que es correcto y apropiado?	✓
		¿Los controles, tales como: Diferentes tipos de entradas para ver los mensajes de error, procedimientos para responder a los errores de validación, la definición de responsabilidades de todo el personal involucrado en el proceso de los datos de entrada, etc. son considerados?	✓
	CONTROL DE PROCESO INTERNO	¿Las áreas de riesgos se identifican en el ciclo de procesamiento y los controles de validación se incluyeron?	✓
		¿Los controles adecuados se identifican en las aplicaciones para mitigar los riesgos durante el proceso interno?	✓
		¿Los controles dependen de la naturaleza y el impacto sobre la aplicación de cualquier corrupción de datos?	✓
	AUTENTICACIÓN DE MENSAJES	¿Una evaluación de riesgo para la seguridad se llevó a cabo para determinar si se requiere autenticación de mensajes, y para identificar el método más adecuado de la aplicación si es necesario?	
		¿La autenticación de mensajes es una técnica utilizada para detectar cambios no autorizados, o la corrupción de los contenidos del mensaje electrónico de transmisión?	
	LOS DATOS DE	¿La salida de datos del sistema de aplicación	✓

	SALIDA DE VALIDACIÓN	está validado para asegurar que el tratamiento de la información almacenada sea correcto y apropiado a las circunstancias.	
	CONTROLES CRIPTOGRÁFICOS		
	POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS	¿Existe una política en el uso de controles criptográficos para la protección de la información?	
		¿Se llevó a cabo una evaluación de riesgos para identificar el nivel de protección de la información?	
	CIFRADO	¿Se utilizan técnicas de encriptación para proteger los datos?	
		¿Las evaluaciones se llevaron a cabo para analizar la sensibilidad de los datos y el nivel de protección necesario?	
	FIRMAS DIGITALES	¿Las firmas digitales se utilizan para proteger la autenticidad e integridad de los documentos electrónicos?	
	SERVICIOS DE NO REPUDIO	¿Son utilizados servicios de no repudio para disputas acerca de la ocurrencia o no ocurrencia de un evento o acción?	
	GESTIÓN DE CLAVES	¿Existe un sistema de gestión el cual apoya a la organización el uso de las técnicas criptográficas, como técnica clave secreta y la técnica de clave pública?	
		¿El sistema de gestión de claves se basa en conjunto de normas, procedimientos y métodos seguros?	
	SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA		
	CONTROL DE SISTEMA OPERATIVO	¿Existen controles para minimizar el riesgo de corrupción de los sistemas operativos?	
	PROTECCIÓN DE DATOS DE PRUEBA DEL SISTEMA	¿Los datos de prueba del sistema están protegidos y controlados?	✓
	SEGURIDAD EN EL DESARROLLO Y APOYO DEL PROCESO		
	CAMBIAR LOS PROCEDIMIENTOS DE CONTROL	¿Existen procedimientos de control estricto sobre la implementación de cambios en el sistema de información?	✓
	REVISIÓN TÉCNICA DE LOS CAMBIOS DE SISTEMA OPERATIVO	¿Existe un proceso para garantizar que el sistema fue revisado y probado después del cambio en el sistema operativo, para instalar los service packs, parches, etc.?	
	EXTERNALIZADOS DE DESARROLLO DE SOFTWARE	¿Existen y controles sobre la externalización de software? Los puntos a tener en cuenta incluyen: los acuerdos de licencias, acuerdos de custodia, obligación contractual de garantía de calidad, las pruebas antes de la instalación para detectar códigos troyanos, etc.	✓
9 GESTIÓN DE LA CONTINUIDAD	*ASPECTOS DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO*		
	LA CONTINUIDAD DEL NEGOCIO DE GESTIÓN DE	¿Existe un proceso controlado para desarrollar y mantener la continuidad del negocio en toda la organización?	

DE NEGOCIOS	PROCESOS		
	CONTINUIDAD DEL NEGOCIO Y ANÁLISIS DE IMPACTO	¿Los eventos que podrían causar interrupciones de procesos de negocio se identificaron?, ejemplo: falta de equipo, inundaciones e incendios	
		¿Se llevó a cabo una evaluación de riesgos para determinar el impacto de dichas interrupciones?	
		¿Fue desarrollado con base en los resultados de evaluación de riesgos para determinar un enfoque global para la continuidad del negocio?	
	REDACCIÓN Y EJECUCIÓN DEL PLAN DE CONTINUIDAD	¿Los planes fueron desarrollados para restablecer las operaciones comerciales dentro del marco de tiempo requerido después de una interrupción o la falta de procesos de negocio?	
	CONTINUIDAD DEL NEGOCIO MARCO DE PLANIFICACIÓN	¿Existe un marco único de plan de continuidad de negocio?	
		¿Los planes son coherentes y determinar las prioridades para las pruebas y mantenimiento?	
		¿Se identifican las condiciones y los responsables de la ejecución de cada componente del plan?	
	PRUEBAS, MANTENIMIENTO Y REEVALUACIÓN DE PLAN DE CONTINUIDAD	¿Los planes de continuidad de negocio son evaluados con regularidad para asegurarse de que estén al día?	
		¿Los planes de continuidad de negocio mantienen revisiones y actualizaciones periódicas para garantizar su eficacia en todo momento?	
		¿Los procedimientos se incluyen en el programa de gestión de cambios para asegurar que las cuestiones de continuidad del negocio se aborden debidamente?	
10 **CUMPLIMIENTO**	*CUMPLIMIENTO DE LOS REQUISITOS LEGALES*		
	IDENTIFICACIÓN DE LEGISLACIÓN APLICABLE	¿Los requisitos legales, reglamentarios y contractuales se han definido de manera explícita y documentada para cada sistema de información?	
		¿Los controles específicos y las responsabilidades individuales para cumplir con estos requisitos se han definido y documentado?	
	DERECHOS DE PROPIEDAD INTELECTUAL (DPI)	¿Existen procedimientos para garantizar el cumplimiento de las restricciones legales sobre el uso de materiales en los que puede haber derechos de propiedad intelectual, tales como derechos de autor, derechos sobre diseños, marcas, etc.?	
		¿Los productos de software propietario son suministrados en virtud de un acuerdo de licencia que limita el uso de los productos a máquinas especificadas? La única excepción podría ser para hacer copias de seguridad del software.	
	MANTENIMIENTO DE LOS REGISTROS DE LA ORGANIZACIÓN	¿Los registros importantes de la organización están protegidos de la destrucción y pérdida de funcionalidad?	

	PROTECCIÓN DE DATOS Y PRIVACIDAD DE INFORMACIÓN	¿Existe una estructura de gestión y control para proteger datos y privacidad de información personal?	
	PREVENCIÓN DEL USO INDEBIDO DE INFORMACIÓN Y DE LAS INSTALACIONES DE PROCESAMIENTO	¿El uso de las instalaciones de procesamiento de la información para cualquier no profesional o fines no autorizados sin la aprobación de la gestión, se considera como uso indebido de las instalaciones?	✓
	REGLAMENTO DE LOS CONTROLES CRIPTOGRÁFICOS	¿El reglamento de control criptográfico es dictaminado por el sector y el acuerdo nacional?	
	REUNIÓN DE PRUEBAS	¿El proceso involucrado en la recolección de la evidencia está en conformidad con las prácticas jurídicas y la industria?	
	RESEÑAS DE POLÍTICA DE SEGURIDAD Y CUMPLIMIENTO TÉCNICO		
	CUMPLIMIENTO DE LA POLÍTICA DE SEGURIDAD	¿Todas las áreas de la organización que se revisan periódicamente para asegurar el cumplimiento con la política de seguridad, normas y procedimientos?	
	COMPROBACIÓN DE LA CONFORMIDAD	¿Los sistemas de información fueron controlados periódicamente para el cumplimiento de las normas de implementación de seguridad?	
		¿La prueba de conformidad técnica se lleva a cabo por, o bajo la supervisión de personal competente y autorizado?	
	CONSIDERACIONES DEL SISTEMA DE AUDITORÍA		
	DE AUDITORÍA DE CONTROLES DEL SISTEMA	¿Los requisitos de la auditoría y las actividades relacionadas con el control de los sistemas operativos deben ser cuidadosamente planificados y acordados para reducir al mínimo el riesgo de interrupciones de procesos de negocio?	✓
	PROTECCIÓN DE LAS HERRAMIENTAS DE AUDITORÍA DEL SISTEMA	¿El acceso a las herramientas de auditoría del sistema, tales como software o archivos de datos están protegidos para evitar cualquier posible abuso o compromiso?	

Como se puede observar en la tabla 5, la seguridad de la dependencia es mala, ya que varias de las recomendaciones que hace la norma lSO 17799 no se cubrieron. En la tabla 6 se puede observar un resumen cuantificado para hacer una comparación entre los puntos que se cubrieron y los que no se cubrieron de la lista de verificación, en cada una de las secciones o campos de actuación de la seguridad.

Tabla 6. Porcentajes obtenidos de la tabla 5.

Sección	Puntos a	Puntos	Puntos no	Porcentaje	Porcentaje

	evaluar	evaluados	evaluados	no evaluado	evaluado
1. Política de seguridad	4	0	4	100.0 %	00.00 %
2. Organización de seguridad	14	3	11	78.57 %	21.43 %
3. Clasificación de los activos y el control	4	0	4	100.0 %	00.00 %
4. Seguridad del personal	13	2	11	84.61 %	15.39 %
5. Seguridad física y ambiental	29	16	13	44.82 %	55.18 %
6. Comunicaciones y gestión de operaciones	48	13	35	72.91 %	27.09 %
7. Control de acceso	38	10	28	73.68 %	26.32 %
8. Sistema de desarrollo y mantenimiento	24	10	14	58.33 %	41.67 %
9. Gestión de la continuidad del negocio	11	0	11	100.0 %	00.00 %
10. Cumplimiento	14	2	12	85.71 %	14.29 %
TOTAL	199	56	143	71.85 %	28.15 %

Como se puede observar en la tabla 6, la cantidad de puntos no evaluados es alta, alcanzando un 71.85% de los 199 puntos que se evaluaron.

Influido por los valores de las tabla 4 y 6, considerando los puntos abordados en las tablas 3 y 5, y bajo los criterios de disponibilidad, confidencialidad e integridad de la información, se identificaron las vulnerabilidades, las amenazas, los impactos que ocasionan dichas vulnerabilidades y amenazas; así como los controles que posee la dependencia para mitigarlas. Con la identificación realizada y la ayuda del modelo relacional simple se muestra en la figura 2.2 la relación existente entre las vulnerabilidades, las amenazas, los controles y los impactos de una forma gráfica.

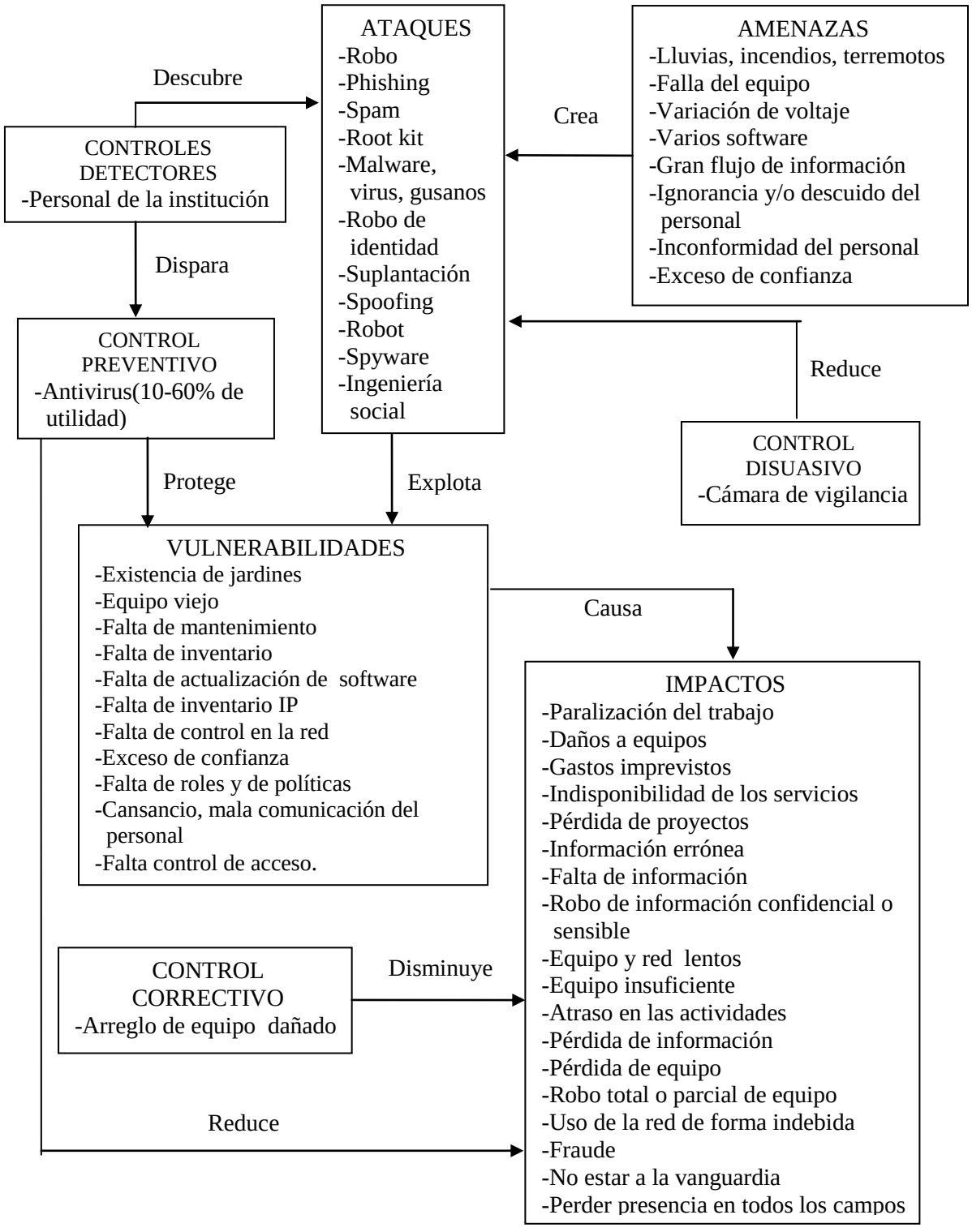


Figura 2. 2. Situación de la dependencia.

Una vez identificados los factores que influyen en la situación de seguridad de la dependencia universitaria, es necesario obtener valores cuantitativos para analizar dicha situación desde un punto inicial a uno final; generar estadísticas, datos históricos, estudiar su comportamiento y así obtener pronósticos concluyendo en una toma de decisiones.

Con el fin de poder determinar la probabilidad de ocurrencia de ciertos eventos (amenazas), se define una escala, en la cual a una probabilidad alta, se asigna el valor P=5, para una probabilidad media le asignamos el valor P=3 y por último para una probabilidad baja le asignamos el valor P=1, esta asignación se define en proporción directa al número de veces que el evento puede ocurrir en un periodo de un año. Para el caso P=5, se considera que ocurre al menos dos veces al año, véase tabla 7.

Tabla 7. Probabilidad de la ocurrencia.

AMENAZA	PROBABILIDAD	AMENAZA	PROBABILIDAD
NATURALES			
Ciclones y huracanes	1	Maremotos	1
Deslaves	1	Polvo	5
Erupciones	1	Temperatura extrema	3
Humedad	2	Terremotos	1
Hundimientos	1	Tormentas eléctricas	1
Incendios	1	Tormentas solares	1
Inundaciones	2	Tornados	1
HARDWARE			
Alto voltaje	3	Distorsión	1
Bajo voltaje	3	Ruido electromagnético	1
Cargas estáticas	1	Sobrecalentamiento	2
SOFTWARE			
Gusanos	5	Troyanos	5
Malware	5	Virus	5
RED			
Corte de cables	2	Flujo de información excesivo	4
Interferencias	1	Sniffers	3
HUMANAS			
Curiosos	5	Exempleado molesto	3
Ingeniería social inversa	4	Fraude	2
Ingeniería social	4	Robo	4
Sabotaje	3	Terroristas	1

Para obtener el porcentaje de la probabilidad de que ocurra una amenaza se utiliza la tabla 7 y la ecuación a); en el caso que se desee obtener el porcentaje de la probabilidad de que no ocurra una amenaza se utiliza la tabla 7 y las ecuaciones a) y b).

a) $$y = \left(\frac{P_A(N)}{\sum_{i=0}^{i=N} V_P}\right)(100[\%])$$

Donde:

y: Probabilidad de ocurrencia de una amenaza.

P_A=5: Valor de la Probabilidad alta.

N: Número total de amenazas.

V_P: Valores de probabilidad de la tabla 7.

b) 100 % = y + z

Donde:

Y: Probabilidad de ocurrencia de una amenaza.

Z: Probabilidad de que no ocurra una amenaza.

Aplicando la fórmula a) cuando N=36, se obtiene que existe un 49% de que una amenaza de cualquier tipo ocurra, véase gráfico 2.1.

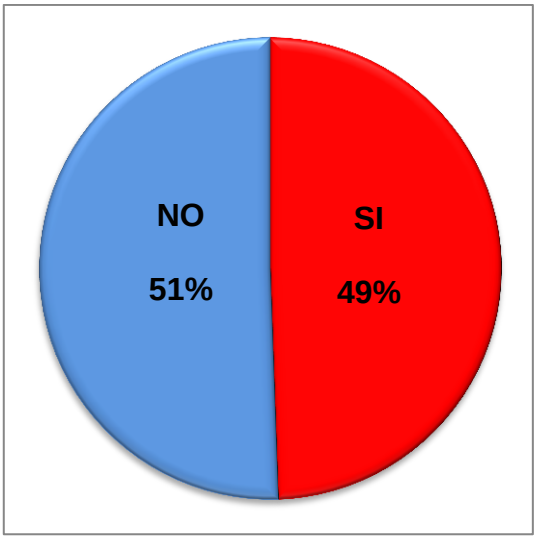


Gráfico 2. 1. Probabilidad de ocurrencia de una amenaza.

Del 49% de que ocurra una amenaza, el 12% corresponde a amenazas naturales, el 6% a amenazas de hardware, el 11% a amenazas de software, el 5% a amenazas de red y el 15% a amenazas humanas, véase gráfico 2.2.

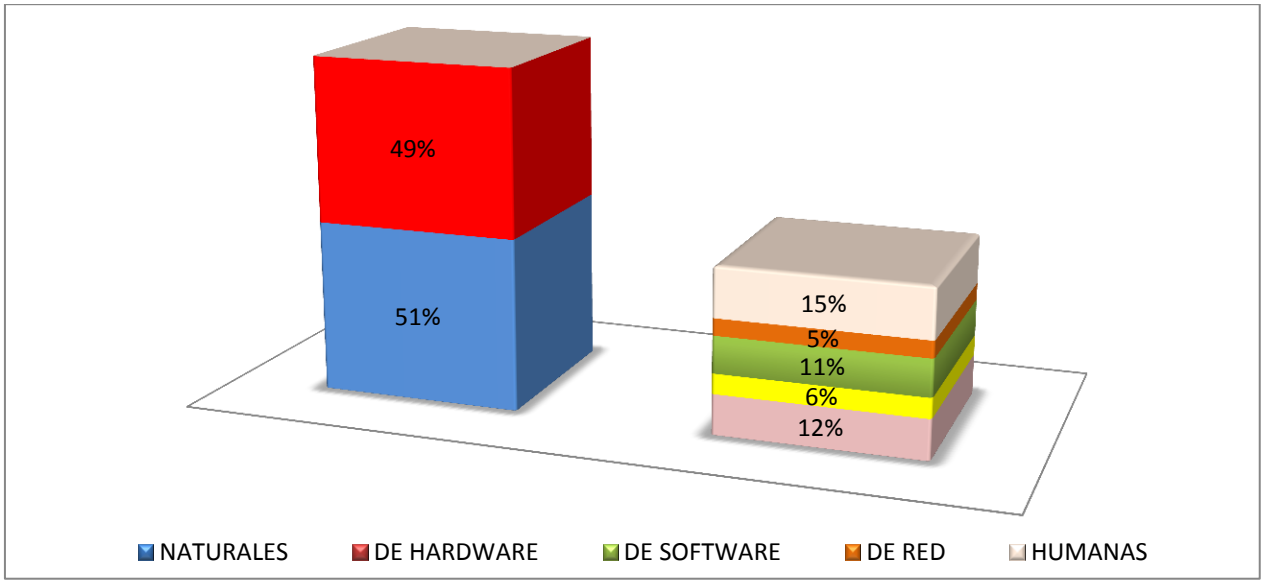


Gráfico 2. 2. Porcentaje de las ocurrencias de las amenazas.

Aplicando la fórmula a) cuando N=14, se obtiene que existe un 31% de que ocurra una amenaza natural, véase gráfico 2.3.

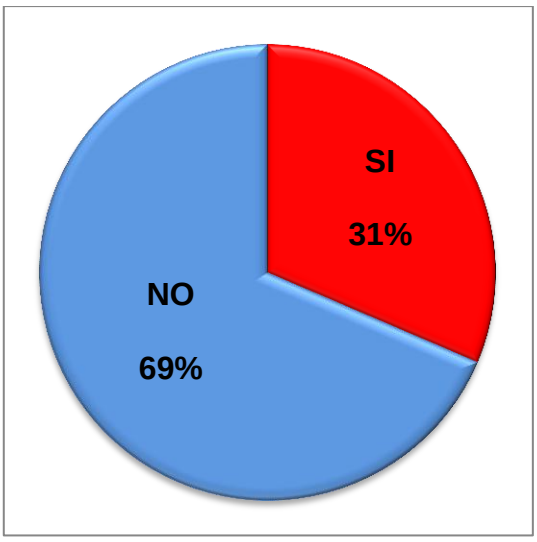


Gráfico 2. 1. Ocurrencia de una amenaza natural.

Aplicando la fórmula a) cuando N=14, se obtiene que existe un 37% de que una amenaza de hardware ocurra, véase gráfico 2.4.

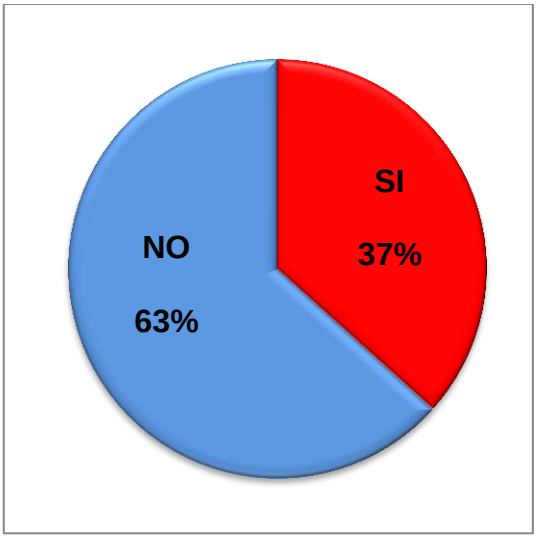


Gráfico 2. 2. Ocurrencia de una amenaza de hardware.

Aplicando la fórmula a) cuando N=4, se obtiene que existe un 100% de que ocurra una amenaza de software, véase gráfico 2.5.

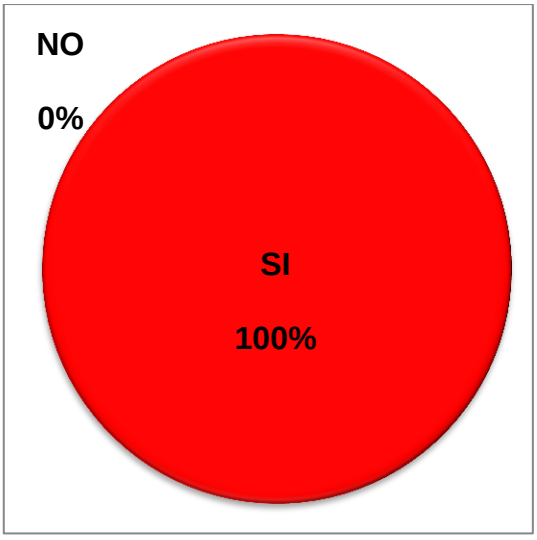


Gráfico 2. 5. Ocurrencia de una amenaza de software.

Aplicando la fórmula a) cuando N=4, se obtiene que existe un 50% de que ocurra una amenaza de red, véase gráfico 2.6.

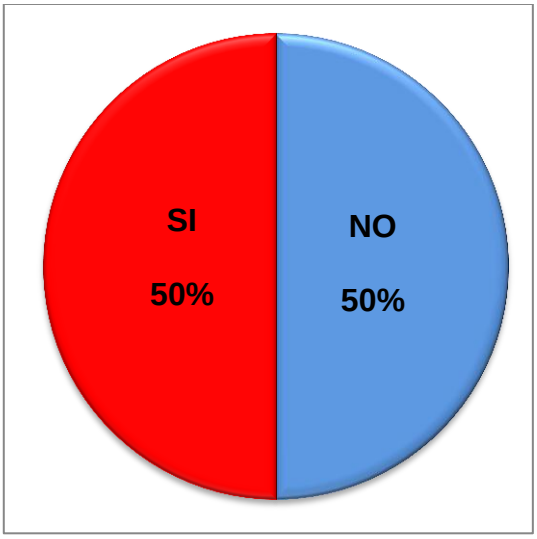


Gráfico 2. 3. Ocurrencia de una amenaza de red.

Aplicando la fórmula a) cuando N=4, se obtiene que existe un 65% de que ocurra una amenaza de humana, véase gráfico 2.7.

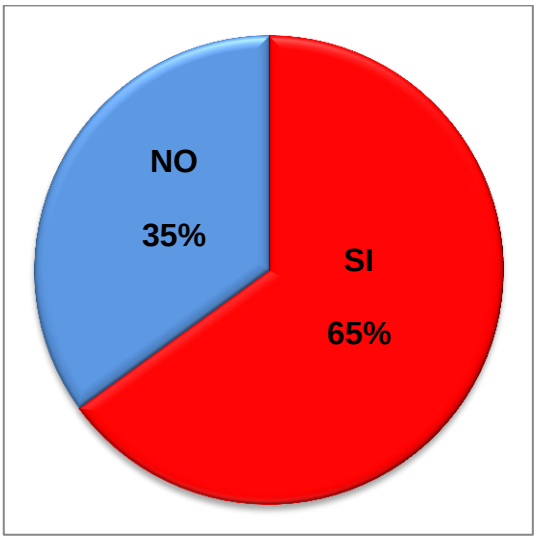


Gráfico 2. 4. Ocurrencia de una amenaza humana.

Con el fin de derivar una probabilidad o una estimación de que una vulnerabilidad potencial pueda ser explotada por una fuente de amenaza se puede clasificar de la siguiente manera:

Tabla 8. Valores para cuantificar la probabilidad de la culminación de una amenaza.

NIVEL	GRADO	DEFINICIÓN
ALTA	5	La amenaza está altamente motivada y es suficientemente capaz de llevarse a cabo
MEDIA-ALTA	4	La amenaza está fundamentada y es posible
MEDIA	3	La amenaza es posible
MEDIA-BAJA	2	La amenaza no posee la suficiente capacidad
BAJA	1	La amenaza no posee la suficiente motivación y capacidad

Asignándole un grado a las amenazas encontradas da como resultado la tabla 9.

Tabla 9. Probabilidad de la culminación de la amenaza.

AMENAZA	PROBABILIDAD	AMENAZA	PROBABILIDAD
NATURALES			
Ciclones y huracanes	1	Maremotos	1
Deslaves	1	Polvo	4
Erupciones	1	Temperatura extrema	2
Humedad	1	Terremotos	2
Hundimientos	1	Tormentas eléctricas	1
Incendios	2	Tormentas solares	1
Inundaciones	2	Tornados	1
HARDWARE			
Alto voltaje	2	Distorsión	1
Bajo voltaje	2	Ruido electromagnético	1
Cargas estáticas	1	Sobrecalentamiento	2
SOFTWARE			
Gusanos	5	Troyanos	5
Malware	5	Virus	5
RED			
Corte de cables	2	Flujo de información excesivo	4
Interferencias	2	Sniffers	5
HUMANAS			
Curiosos	3	Exempleado molesto	3
Ingeniería social inversa	5	Fraude	3
Ingeniería social	5	Robo	4
Sabotaje	4	Terroristas	2

Aplicando la fórmula a) cuando N=36, se obtiene que existe un 52% de posibilidad de que culmine una amenaza, véase gráfico 2.8.

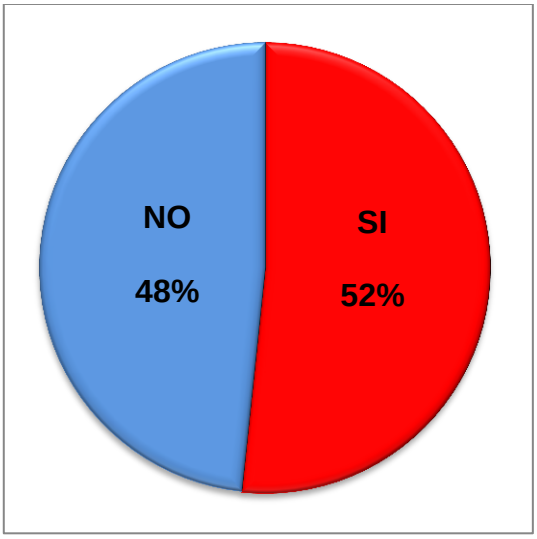


Gráfico 2. 8 Probabilidad de que culmine una amenaza.

Del 52% de posibilidad de que culmine una amenaza, el 12% corresponde a amenazas naturales, el 5% a amenazas de hardware, el 11% a amenazas de software, el 7% a amenazas de red y el 17 % a amenazas humanas, véase gráfico 2.9.

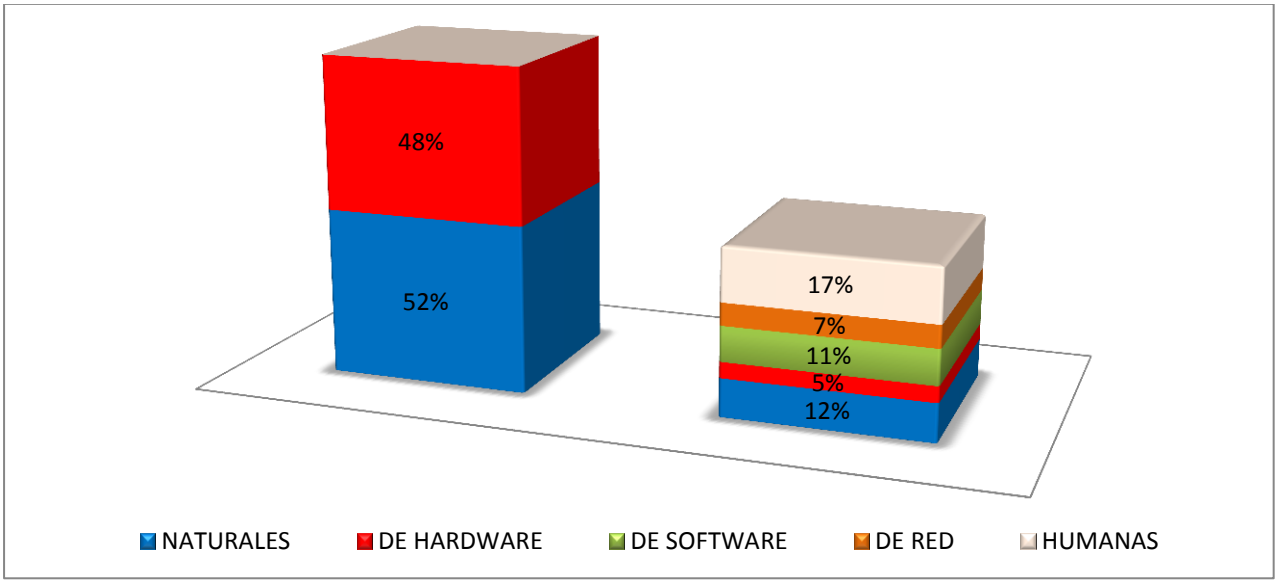


Gráfico 2. 9. Porcentaje de las amenazas.

Aplicando la fórmula a) cuando N=14, se obtiene que existe un 31% de posibilidad que culmine una amenaza natural, véase gráfico 2.10.

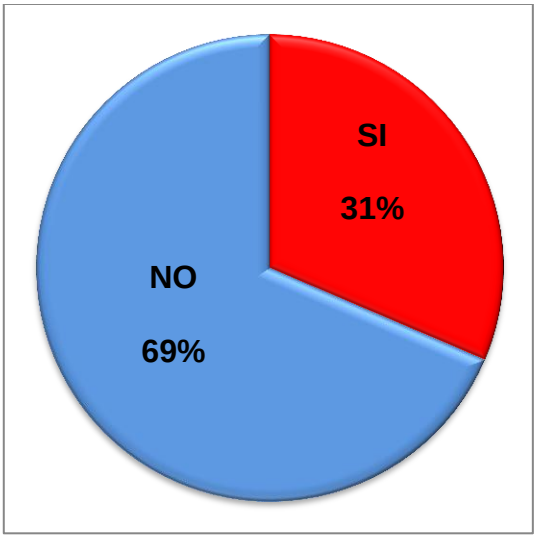


Gráfico 2. 10. Culminación de una amenaza natural.

Usando la fórmula a) cuando N=6, se obtiene que existe un 37% de posibilidad de que culmine una amenaza de hardware, véase gráfico 2.11.

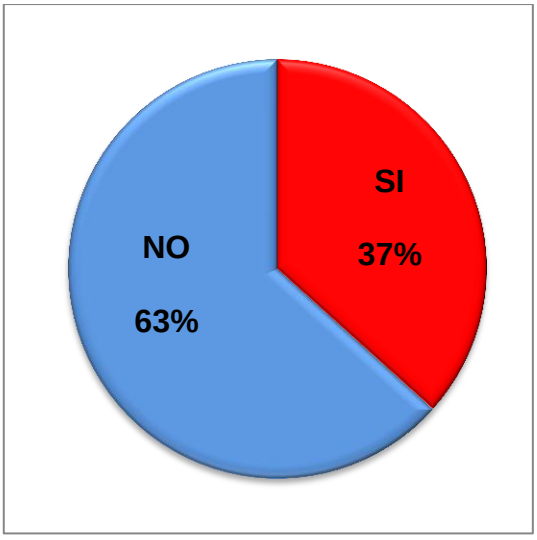


Gráfico 2. 11. Culminación de una amenaza de hardware.

Utilizando la fórmula a) cuando N=4, se obtiene que existe un 100% de posibilidad de que culmine una amenaza de software véase gráfico 2.12.

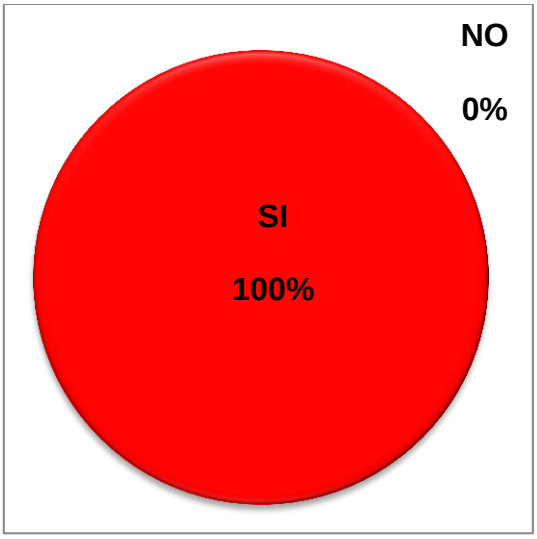


Gráfico 2. 12. Culminación de una amenaza de software.

Sustituyendo en la fórmula a) N=4, se obtiene que existe un 65% de posibilidad de que culmine una amenaza de red, véase gráfico 2.13.

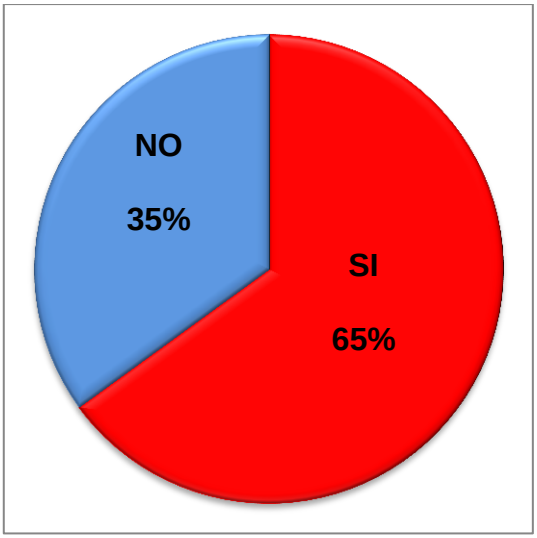


Gráfico 2. 13. Culminación de una amenaza de red.

Aplicando la fórmula a) cuando N=8, se obtiene que existe un 72% de posibilidad de que culmine una amenaza de humana, véase gráfico 2.14.

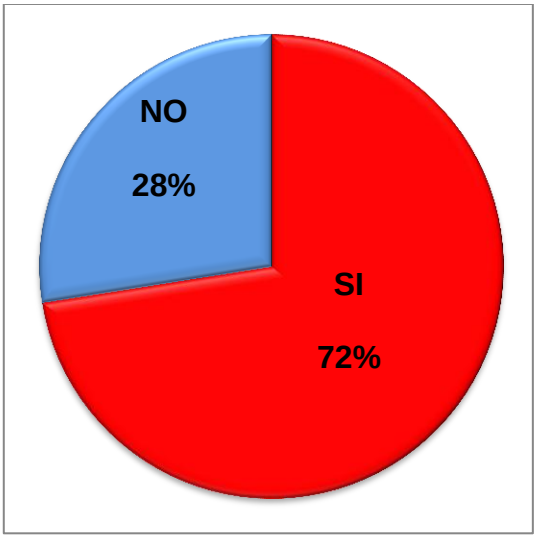


Gráfico 2. 14. Culminación de una amenaza humana.

Después de sustituir los valores de la tabla 9 en la fórmula a) para obtener los porcentajes de las probabilidades de que culminen las amenazas naturales, las humanas, las de hardware, las de software, así como las de red y debido a los porcentajes obtenidos a partir de la tabla 7 para las probabilidades de ocurrencia de las amenazas antes mencionadas, se observa que son demasiados altos, ya que la dependencia cuenta con aproximadamente 30 vulnerabilidades las cuales se muestran en la tabla 10, mismas que podrían ser explotadas por las amenazas expuestas en la tabla 7 y 9, pueden llevar a la dependencia a un nivel no aceptable para sus operaciones.

Tabla 10. Vulnerabilidades de la dependencia.

VULNERABILIDAD
No cuenta con un espejo del sistema
No dispone de no-break
Falta de ventilación
Falta de rociadores
Falta de planes de contingencia
Falta de políticas de seguridad
Equipo viejo
Falta de actualización en antivirus
Falta de actualización en sistemas operativos
Cansancio del personal
Inconformidad del personal
Descuido del personal
Exceso de confianza
Clima variante
Falta de mantenimiento
Falta de inventario de los bienes
Falta de inventario IP
Falta de control en la red
Falta de roles
Falta control de acceso
No contar con credenciales que identifique al personal
No tener control en la entrada y salida de visitantes
Falta de limpieza de las áreas de la organización
No contar con un estricto control en el acceso al site
Falta de capacitación del personal
Falta de personal de vigilancia
Deshonestidad del personal
Irresponsabilidad del personal
Falta de auditorias
Falta de autoridad

Como se puede observar en la figura 2.2 y en las tablas 7, 9 y 10, al momento de realizar un análisis de las amenazas y vulnerabilidades a las que está expuesta la dependencia, se encontró que no está preparada para amenazas naturales, como son las lluvias, incendios, terremotos, entre otros, ya que no se encontró algún plan de contingencia o un documento que dijese cómo actuar durante y después de este tipo de eventos; agregando la inconformidad del personal por el equipo asignado que en ocasiones presenta fallas en el suministro de corriente eléctrica, de incompatibilidad debido a varias versiones de software, volviendo a dicho equipo insuficiente para realizar

sus tareas, sumado al exceso de confianza, la ignorancia y/o descuido del mismo hacia los equipos de cómputo.

Además, se encontró que el departamento encargado de la administración del equipo no cuenta con un inventario de bienes físicos, un inventario de direcciones IP's actualizado, roles y políticas de seguridad, un control de acceso a los recursos y/o servicios, un control sobre la red, una organización para la realización de mantenimiento y actualización de los equipos, tanto de hardware como de software.

Como medidas y/o controles de seguridad para evitar un daño, se observó que se cuenta con software de antivirus con un 10% a 60 % de utilidad por falta de actualización.

Para la vigilancia se cuenta con cámaras y personal que labora en la institución.

2.1.2 Impactos

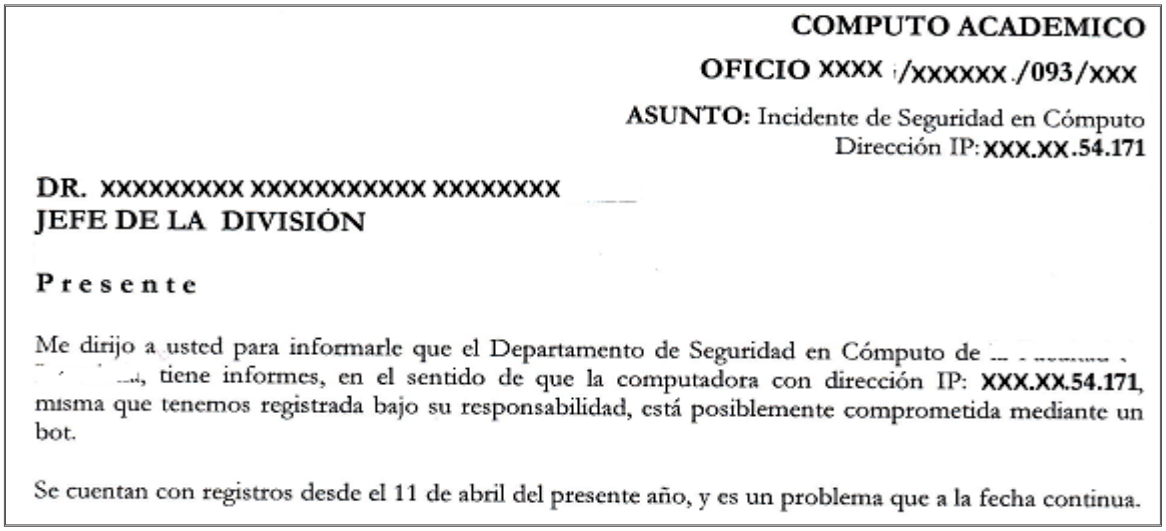
Como se puede observar en la descripción de la figura 2.2, debido a la situación en la que se encuentra la dependencia, provoca que no esté inmune ante ataques como podría ser robo, phishing, spam, root kit, malware, virus, gusanos, robo de identidad, suplantación de equipos, spoofing, robot, spyware, ingeniería social, por mencionar algunos.

Impactando en la paralización del trabajo, daños a equipos, gastos imprevistos, falta de disponibilidad de los servicios como correo y/o web, pérdida de proyectos, fuga de dinero, información errónea, falta de información, revelación de información confidencial o sensible, equipo lento, equipo insuficiente para realizar las actividades deseadas, atraso en las actividades de la dependencia, pérdida de información, pérdida de equipo, red lenta, robo total o parcial de equipo, uso de la red de forma indebida, fraude, no estar a la vanguardia o perder presencia en todos los campos.

2.1.3 Pruebas de la problemática

A continuación se presentan algunos reportes elaborados por terceros. Dichos reportes dan una idea tangible de lo sucedido en la dependencia. Se procedió a borrar algunos datos para brindar confidencialidad a la dependencia y tratar de evitar poner en riesgo a la misma por publicar sus debilidades.

En el primer reporte de seis, se puede observar que la dirección IP xxx.xxx.54.171 se trata de comunicar con el equipo que responde a la dirección IP 86.129.58.232, que escucha por el puerto 6667, pudiendo tratarse de un bot, ver figura 2.3.



COMPUTO ACADEMICO

OFICIO XXXX /XXXXXX./093/XXX

ASUNTO: Incidente de Seguridad en Cómputo
Dirección IP: **XXX.XX.54.171**

DR. XXXXXXXXX XXXXXXXXXXX XXXXXXXX
JEFE DE LA DIVISIÓN

P r e s e n t e

Me dirijo a usted para informarle que el Departamento de Seguridad en Cómputo de ..., tiene informes, en el sentido de que la computadora con dirección IP: **XXX.XX.54.171**, misma que tenemos registrada bajo su responsabilidad, está posiblemente comprometida mediante un bot.

Se cuentan con registros desde el 11 de abril del presente año, y es un problema que a la fecha continua.

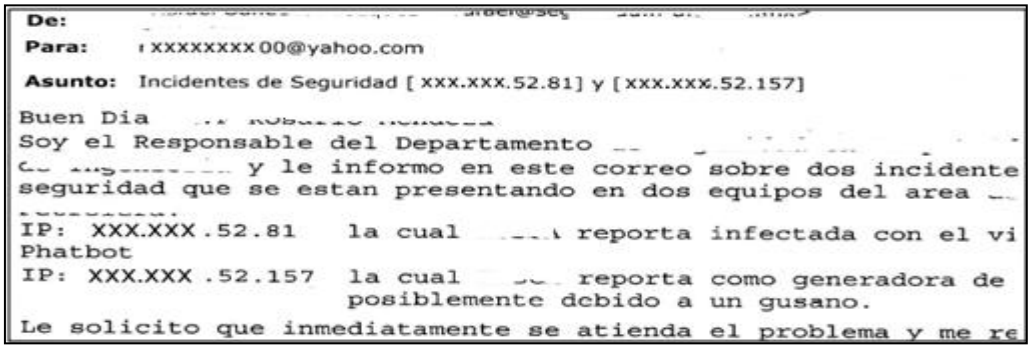
Figura 2. 3. Reporte 1

A continuación, en la figura 2.4 se visualiza un fragmento de la bitácora anexada al reporte mostrado en la figura 2.3, muestra las múltiples peticiones que realiza el equipo con la IP xxx.xxx.54.171 a la 86.129.58.232 utilizando el protocolo tcp.

```
Apr 11 15:00:23.216428  XXX.XXX.54.171.54736 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:00:26.147863  XXX.XXX.54.171.54736 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:00:32.166564  XXX.XXX.54.171.54736 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:00:54.210857  XXX.XXX.54.171.50932 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:00:57.144009  XXX.XXX.54.171.50932 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:01:03.062296  XXX.XXX.54.171.50932 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:01:25.130182  XXX.XXX.54.171.57315 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:01:28.139927  XXX.XXX.54.171.57315 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:01:34.158666  XXX.XXX.54.171.57315 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:01:56.207557  XXX.XXX.54.171.63601 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:01:59.136114  XXX.XXX.54.171.63601 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:02:05.054399  XXX.XXX.54.171.63601 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:02:27.120662  XXX.XXX.54.171.65260 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:02:30.132283  XXX.XXX.54.171.65260 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:02:36.150885  XXX.XXX.54.171.65260 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:02:58.194528  XXX.XXX.54.171.60872 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:03:01.128327  XXX.XXX.54.171.60872 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:03:07.046751  XXX.XXX.54.171.60872 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:03:29.089893  XXX.XXX.54.171.54513 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:03:32.124525  XXX.XXX.54.171.54513 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:03:38.143078  XXX.XXX.54.171.54513 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:04:00.187362  XXX.XXX.54.171.52891 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:04:03.120566  XXX.XXX.54.171.52891 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:04:09.038992  XXX.XXX.54.171.52891 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:04:31.081404  XXX.XXX.54.171.52821 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:04:34.116602  XXX.XXX.54.171.52821 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:04:40.135332  XXX.XXX.54.171.52821 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:05:02.179722  XXX.XXX.54.171.64985 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:05:05.112640  XXX.XXX.54.171.64985 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:05:11.031077  XXX.XXX.54.171.64985 > 86.129.58.232.6667: tcp 0 (DF)
Apr 11 15:05:33.074457  XXX.XXX.54.171.53450 > 86.129.58.232.6667: tcp 0 (DF)
```

Figura 2. 4. Bitácora anexa al reporte 1.

En este segundo reporte se mencionan dos equipos, uno con la IP XXX.XXX. 52.81 que se encuentra infectada con el virus Phatbot y el quipo con la IP XXX.XXX.52.157 infectada con un gusano, nos da una prueba de contagio, véase figura 2.5.


De:

Para: xxxxxxxx00@yahoo.com

Asunto: Incidentes de Seguridad [xxx.xxx.52.81] y [xxx.xxx.52.157]

Buen Dia

Soy el Responsable del Departamento

y le informo en este correo sobre dos incidente
seguridad que se estan presentando en dos equipos del area

IP: XXX.XXX.52.81 la cual reporta infectada con el vi
Phatbot

IP: XXX.XXX.52.157 la cual reporta como generadora de
posiblemente debido a un gusano.

Le solicito que inmediatamente se atienda el problema y me re

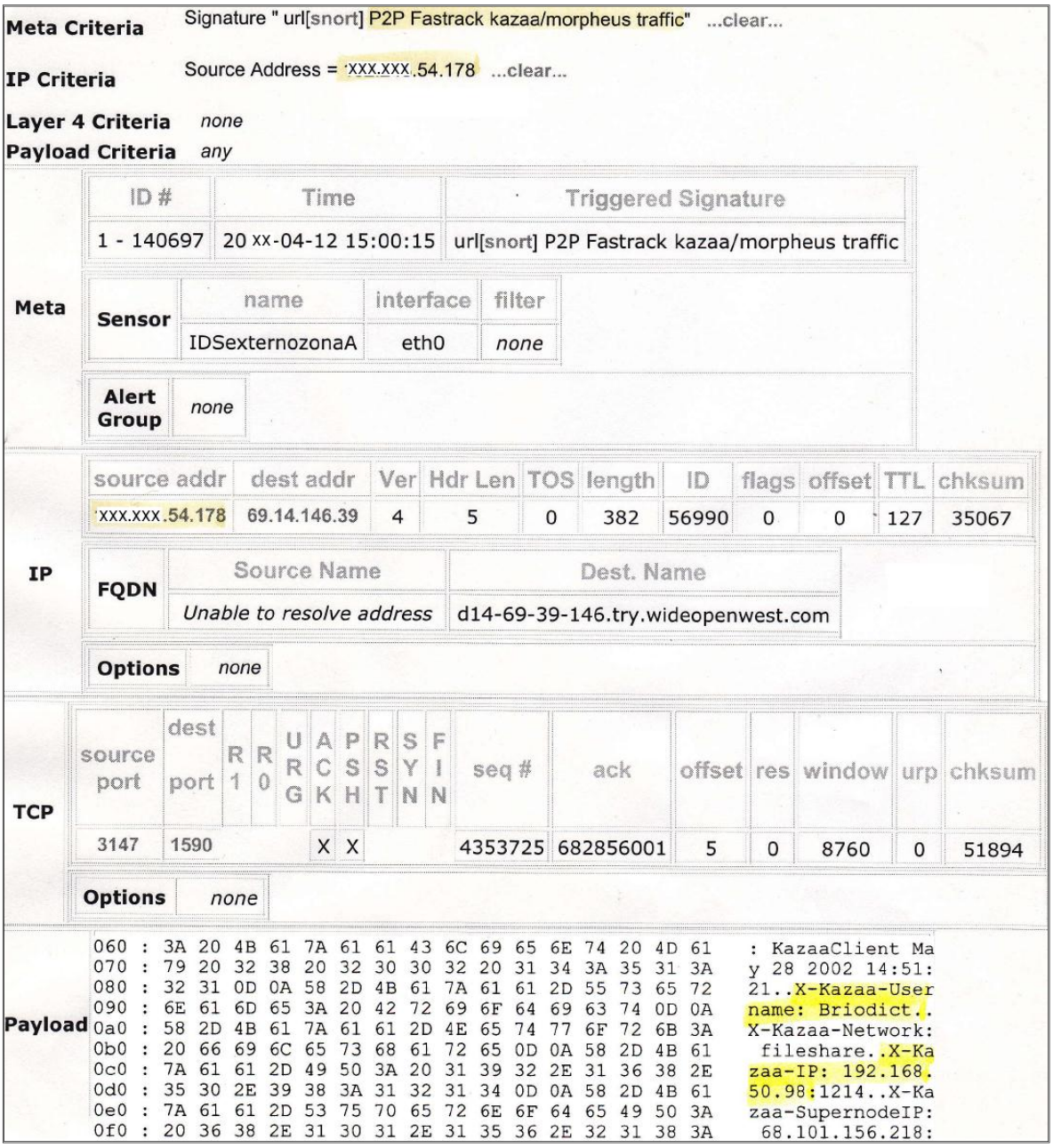
Figura 2. 5. Reporte 2.

Como muestra del mal uso de la red, se presentan los siguientes reportes, en los cuales se hace mención de un equipo que responde a la IP XXX.XXX.54.178, el cual hace uso del P2P Bit Torrent tranfer y el P2P Frastrack kazaa ocupados comúnmente para la descarga de música, sin pago por derechos de autor, consumiendo a su vez ancho de banda que bien podría utilizarse para la transferencia de información útil para las actividades específicas de la dependencia, véase figuras 2.6, 2.7 y 2.8.

Queried DB on : Tue April 26, 20xx 12:28:56
Meta Criteria *any*
IP Criteria Source Address = xxx.xxx.54.178 ...clear...
Layer 4 Criteria *none*
Payload Criteria *any*

< Signature >	< Classification >	< Total # >	Sensor #	< Src. Addr. >	< Dest. Addr. >	< First >	< Last >
[snort] P2P BitTorrent transfer	policy-violation	1256 (7%)	1	1	253	20xx-04-21 15:10:09	20xx-04-26 17:12:36
[snort] CHAT IRC nick change	policy-violation	4074 (24%)	1	1	133	20xx-04-08 20:00:57	20xx-04-21 15:27:37
[snort] POLICY FTP anonymous login attempt	misc-activity	72 (0%)	1	1	4	20xx-04-09 00:37:43	20xx-04-21 16:50:52
arachnids[snort] INFO FTP no password	unknown	47 (0%)	1	1	3	20xx-04-11 14:56:46	20xx-04-21 16:50:52
url[snort] P2P Fastrack kazaa/morpheus traffic	policy-violation	6159 (36%)	1	1	253	20xx-04-08 20:31:07	20xx-04-12 15:00:15
[snort] CHAT IRC dns request	policy-violation	9 (0%)	1	1	2	20xx-04-11 12:36:42	20xx-04-21 15:27:38

Figura 2. 6. Reporte 3.



Meta Criteria Signature " url[snort] P2P Fastrack kazaa/morpheus traffic" ...clear...

IP Criteria Source Address = xxx.xxx.54.178 ...clear...

Layer 4 Criteria *none*

Payload Criteria *any*

Meta

ID #	Time	Triggered Signature
1 - 140697	20xx-04-12 15:00:15	url[snort] P2P Fastrack kazaa/morpheus traffic

Sensor	name	interface	filter
	IDSexternozonaA	eth0	*none*

Alert Group *none*

IP

source addr	dest addr	Ver	Hdr Len	TOS	length	ID	flags	offset	TTL	chksum
xxx.xxx.54.178	69.14.146.39	4	5	0	382	56990	0	0	127	35067

FQDN	Source Name	Dest. Name
	Unable to resolve address	d14-69-39-146.try.wideopenwest.com

Options *none*

TCP

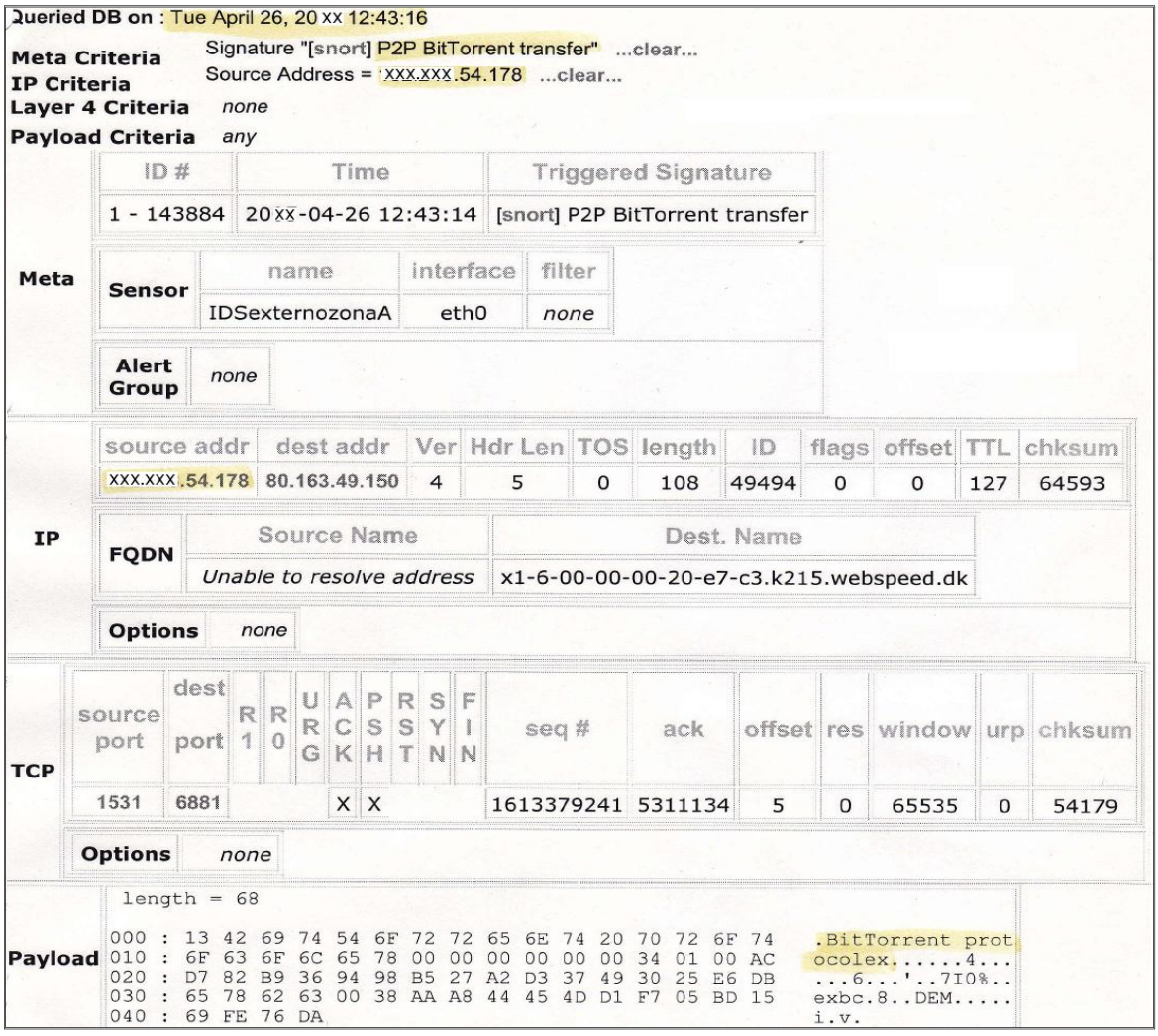
source port	dest port	R 1	R 0	URG	ACK	PSH	RST	SYN	FIN	seq #	ack	offset	res	window	urp	chksum
3147	1590				X	X				4353725	682856001	5	0	8760	0	51894

Options *none*

Payload

```
060 : 3A 20 4B 61 7A 61 61 43 6C 69 65 6E 74 20 4D 61   : KazaaClient Ma
070 : 79 20 32 38 20 32 30 30 32 20 31 34 3A 35 31 3A   y 28 2002 14:51:
080 : 32 31 0D 0A 58 2D 4B 61 7A 61 61 2D 55 73 65 72   21..X-Kazaa-User
090 : 6E 61 6D 65 3A 20 42 72 69 6F 64 69 63 74 0D 0A   name: Briodict..
0a0 : 58 2D 4B 61 7A 61 61 2D 4E 65 74 77 6F 72 6B 3A   X-Kazaa-Network:
0b0 : 20 66 69 6C 65 73 68 61 72 65 0D 0A 58 2D 4B 61    fileshare..X-Ka
0c0 : 7A 61 61 2D 49 50 3A 20 31 39 32 2E 31 36 38 2E   zaa-IP: 192.168.
0d0 : 35 30 2E 39 38 3A 31 32 31 34 0D 0A 58 2D 4B 61   50.98:1214..X-Ka
0e0 : 7A 61 61 2D 53 75 70 65 72 6E 6F 64 65 49 50 3A   zaa-SupernodeIP:
0f0 : 20 36 38 2E 31 30 31 2E 31 35 36 2E 32 31 38 3A    68.101.156.218:
```

Figura 2. 7. Reporte 4.



Queried DB on : Tue April 26, 20 xx 12:43:16

Meta Criteria Signature "[snort] P2P BitTorrent transfer" ...clear...
IP Criteria Source Address = xxx.xxx.54.178 ...clear...
Layer 4 Criteria *none*
Payload Criteria *any*

Meta

ID #	Time	Triggered Signature
1 - 143884	20xx-04-26 12:43:14	[snort] P2P BitTorrent transfer

Sensor	name	interface	filter
	IDSexternozonaA	eth0	*none*

Alert Group *none*

IP

source addr	dest addr	Ver	Hdr Len	TOS	length	ID	flags	offset	TTL	chksum
xxx.xxx.54.178	80.163.49.150	4	5	0	108	49494	0	0	127	64593

FQDN	Source Name	Dest. Name
	Unable to resolve address	x1-6-00-00-00-20-e7-c3.k215.webspeed.dk

Options *none*

TCP

source port	dest port	R 1	R 0	URG	ACK	PSH	RST	SYN	FIN	seq #	ack	offset	res	window	urp	chksum
1531	6881				X	X				1613379241	5311134	5	0	65535	0	54179

Options *none*

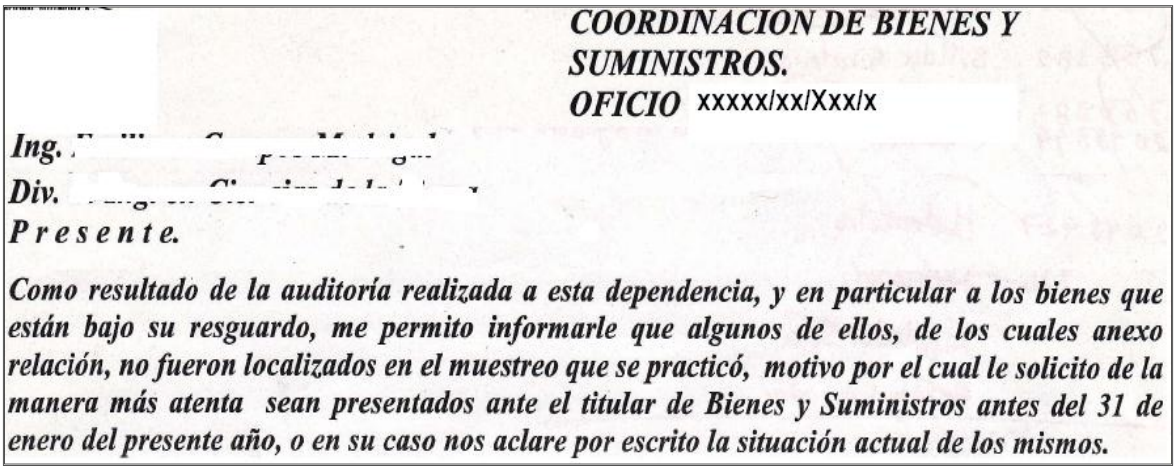
Payload

```
length = 68

000 : 13 42 69 74 54 6F 72 72 65 6E 74 20 70 72 6F 74   .BitTorrent prot
010 : 6F 63 6F 6C 65 78 00 00 00 00 00 00 34 01 00 AC   ocolex......4...
020 : D7 82 B9 36 94 98 B5 27 A2 D3 37 49 30 25 E6 DB   ...6...'..7I0%..
030 : 65 78 62 63 00 38 AA A8 44 45 4D D1 F7 05 BD 15   exbc.8..DEM.....
040 : 69 FE 76 DA                                       i.v.
```

Figura 2. 8. Reporte 5.

Como pruebas de posibles robos, se presenta un oficio, mediante el cual se hace referencia a la falta equipo registrado como parte del inventario de la dependencia, ver figura 2.9.



COORDINACION DE BIENES Y SUMINISTROS.
OFICIO xxxxx/xx/Xxx/x

Ing.
Div.
P r e s e n t e.

Como resultado de la auditoría realizada a esta dependencia, y en particular a los bienes que están bajo su resguardo, me permito informarle que algunos de ellos, de los cuales anexo relación, no fueron localizados en el muestreo que se practicó, motivo por el cual le solicito de la manera más atenta sean presentados ante el titular de Bienes y Suministros antes del 31 de enero del presente año, o en su caso nos aclare por escrito la situación actual de los mismos.

Figura 2. 9. Reporte 6.

Cuando sucede el robo de algún equipo de cómputo, hay que tener en cuenta que puede cometerse a la vez un robo de información, debido a que los usuarios guardan todo tipo de datos en dichos equipos, siempre y cuando, el equipo de cómputo no fuera de reciente adquisición o que haya sufrido un cambio de disco duro, por tanto al momento de habla sobre seguridad en equipos de cómputos hay que tomar en cuenta que no sólo la información que transita por una red es la única que se encuentra susceptible a pérdidas, daños o copias no autorizadas mientras viaja del remitente al emisor, sino que también existe la posibilidad de robo de algún equipo de cómputo; en conclusión cuando queremos proteger la información se debe de considerar los mecanismos que nos permitan salvaguardarla tanto en los medios de almacenamiento físico como el medio de trasmisión.

CAPÍTULO 3

PROPUESTA DE SOLUCIÓN A LA PROBLEMÁTICA

3.1 Diseño del sistema

En la etapa de análisis se descubrió que no se cuenta con mecanismos suficientes para evitar o minimizar los riesgos de ataques ni para tener un mayor control de los residuos que se generen al momento de eliminar las herramientas que los perpetradores utilicen.

La metodología que se usa para la solución del problema, entra así a la etapa de diseño. En esta etapa se pretende solucionar el problema detectado, para ello se subdividirá el problema general en:

- ✓ Políticas de seguridad para la dependencia, para los diferentes tipos de usuarios que existen en la organización.
- ✓ Medidas de seguridad para la dependencia, para controlar o al menos minimizar los problemas que llegarán a presentarse en diferentes escenarios.
- ✓ Plan de contingencias para la dependencia, para saber cómo actuar en el caso de que alguna medida de seguridad haya sido vulnerada, evitando que el problema sea mayor y tenga consecuencias graves.
- ✓ Mecanismos de protección, se desarrollarán e implementarán algunos mecanismos que nos ayudarán a fortalecer las políticas de seguridad apoyadas por las medidas de seguridad para mejorar la situación de la dependencia.

3.2 Elaboración, prueba e implementación del sistema

Debido a que se dividió el problema de la dependencia en casos particulares, la etapa de elaboración, pruebas e implementación se tomó por separado; en cada uno de los casos mencionados en el punto 3.1; sin olvidar, que lo mostrado en este capítulo concerniente a la solución de la problemática de la dependencia, es el resultado de varias pruebas.

3.3 Políticas de seguridad para la dependencia

Durante el análisis de la problemática se pudo constatar que la dependencia carece de políticas de seguridad, en las cuales pueda basarse, haciendo énfasis en que existe un exceso de confianza.

Para combatir el problema de ancho de banda y minimizar el mal uso de la red, respetando los reglamentos establecidos por los superiores de la dependencia, se propone realizar políticas conforme al tipo de usuario y al organigrama que presenta dicha institución, véase figura 3.1.

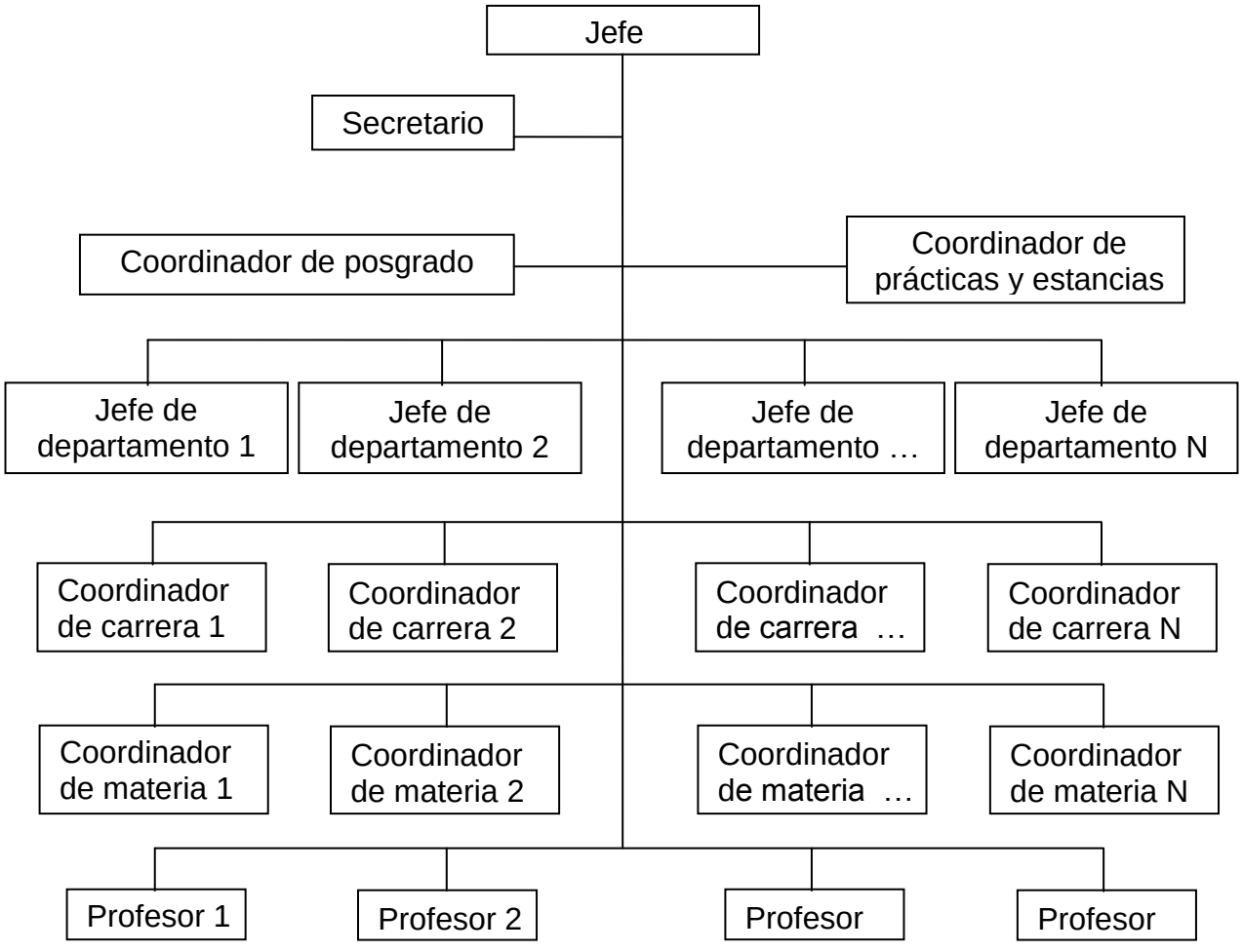


Figura 3. 1. Organigrama de la dependencia.

3.3.1 Políticas para el personal del servicio social y/o ayudante

Filosofía prohibitiva. Todo se prohíbe excepto lo que está explícitamente permitido.

Para todo el personal que realiza actividades del servicio social y/o de ayudante dentro de la dependencia:

1. Se le permite el uso del mobiliario, respetando su integridad.

   Dependiendo de los daños ocasionados se aplicarán las sanciones correspondientes a juicio de las autoridades de la institución.

2. Podrá solicitar una cuenta de usuario para acceder al equipo de cómputo a su superior inmediato, quien lo hará saber al departamento correspondiente; dicha cuenta se dará de baja al término de su estancia como servidor social o como ayudante.

3. Podrá solicitar una cuenta de correo de la institución a su superior inmediato, quien lo hará saber al departamento correspondiente; dicha cuenta se dará de baja al término de su estancia como servidor social o como ayudante.

4. Se le permite la consulta a páginas web que contengan información académica o de investigación.

5. Puede usar el software instalado en el equipo de cómputo.

6. Podrá solicitar la instalación de software específico para realizar sus actividades del servicio social o ayudantía a su superior inmediato, quien lo hará saber al departamento correspondiente.

7. Podrá hacer uso de sus propios dispositivos de almacenamiento previamente desinfectados de malware, tomando en cuenta que la integridad física de dichos dispositivos es responsabilidad del propietario, así como el daño que ocasione a los equipos de la institución.

Dependiendo de los daños ocasionados se aplicarán las sanciones correspondientes a juicio de sus superiores.

8. Podrá traer su propio equipo de cómputo, siempre y cuando cumpla con antivirus y sistema operativo actualizado, tomando en cuenta que la integridad física del equipo es responsabilidad del propietario.

9. Podrá solicitar la conexión a la red de la dependencia a su superior inmediato quien lo hará saber al departamento correspondiente, para uso escolar o de investigación; dicha conexión se dará de baja al término de su estancia como servidor social o ayudante.

10. Podrá realizar llamadas telefónicas dentro de la dependencia con la debida autorización de su superior inmediato.

11. Se le permite el uso de la impresora con la debida autorización de su superior inmediato.

12. Podrá solicitar a su superior inmediato un espacio en la página web, quien lo hará saber al departamento correspondiente, sólo se podrá publicar información de tipo académico o de investigación.

En caso de no cumplir dichas políticas se procederá a desactivar el servicio solicitado por el servidor social o ayudante, durante un mes; en caso de reincidencia, se suspenderá el servicio definitivamente.

3.3.2 Políticas para los administradores de la red

Filosofía permisiva. Todo se permite excepto lo que está explícitamente prohibido.

Para todo el personal que funge la tarea de administrador de red en la dependencia:

1. Se prohíbe sacar equipo de la dependencia sin antes avisar a los demás administradores y a su superior.
2. Se prohíbe usar la información de terceros en beneficio propio.
3. Se prohíbe comercializar con la información.
4. Se prohíbe dañar intencionalmente equipo que tenga a su cargo.
5. Se prohíbe hacer uso indebido de la red.
6. Se prohíbe dejar a cargo a personal ajeno al departamento.
7. Se prohíbe dejar a la dependencia sin claves de acceso o sin parte de ellas cuando se separe de la institución.
8. Se prohíbe dejar a la dependencia sin manuales de uso cuando se separe de la institución.
9. Se prohíbe el cambio indiscriminado de direcciones IP.
10. Se prohíbe el mal uso de los equipos.
11. Se prohíbe divulgar contraseñas.
12. Se prohíbe compartir usuarios.

13. Se prohíbe no aplicar las políticas.

14. Se prohíbe después de la separación con la institución conservar las llaves proporcionadas por su superior.

15. Se prohíbe usar el site con fines diferentes a los establecidos.

16. Se prohíbe comer, fumar o beber en el site.
17. Se prohíbe divulgar información relacionada con la dependencia.

18. Se prohíbe no reconocer a las autoridades de la dependencia.

19. Se prohíbe conservar un usuario y contraseña de personal una vez separado de la institución.

20. Se prohíbe dejar con libre acceso a equipo bajo resguardo.

21. Se prohíbe dejar las luces encendidas innecesariamente.

22. Se prohíbe el uso de sus propios dispositivos de almacenamiento sin desinfección de malware, tomando en cuenta que la integridad física de dichos dispositivos es responsabilidad del propietario, así como el daño que ocasione a los equipos de la institución.

    Dependiendo de los daños ocasionados se aplicarán las sanciones correspondientes a juicio de las autoridades de la institución.

23. Se prohíbe traer su propio equipo de cómputo cuando no cumpla con antivirus y sistema operativo actualizado, tomando en cuenta que la integridad física del equipo es responsabilidad del propietario.

24. En ningún caso podrá dejar sesión abierta en el equipo de cómputo cuando ya no la use.

Deberá reportar a los demás administradores y a su superior alguna anomalía con el equipo a su cargo. En caso de no cumplir dichas políticas será degradado en sus actividades como administrador durante un mes; en caso de residencia se degradará definitivamente.

3.3.3 Políticas para el personal que labora como laboratorista

Filosofía prohibitiva. Todo se prohíbe excepto lo que está explícitamente permitido.

Para todo el personal que realiza actividades en un laboratorio de la dependencia:

1. Se le permite el uso del mobiliario, respetando su integridad.

   Dependiendo de los daños ocasionados, se aplicarán las sanciones correspondientes a juicio de las autoridades de la institución.

2. Podrá solicitar una cuenta de usuario para acceder al equipo de cómputo a su superior inmediato, quien lo hará saber al departamento correspondiente, dicha cuenta se dará de baja al término de su estancia.

3. Podrá solicitar una cuenta de correo de la institución a su superior inmediato, quien lo hará saber al departamento correspondiente; dicha cuenta se dará de baja al término de su estancia.

4. Se le permite la consulta a páginas web que contengan información académica o de investigación.

5. Puede usar el software instalado en el equipo de cómputo.

6. Puede solicitar la instalación de software específico para realizar sus actividades, a su superior inmediato, quien lo hará saber al departamento correspondiente.

7. Podrá hacer uso de sus propios dispositivos de almacenamiento previamente desinfectados de malware, tomando en cuenta que la integridad física de dichos dispositivos es responsabilidad del propietario así como el daño que ocasione a los equipos de la institución.

   Dependiendo de los daños ocasionados, se aplicarán las sanciones correspondientes a juicio de las autoridades de la institución.

8. Podrá traer su propio equipo de cómputo siempre y cuando cumpla con antivirus y sistema operativo actualizado, tomando en cuenta que la integridad física del equipo es responsabilidad del propietario.

9. Podrá solicitar la conexión a la red de la dependencia a su superior inmediato quien lo hará saber al departamento correspondiente, para uso escolar o de investigación; dicha conexión se dará de baja al término de su estancia.

10. Podrá realizar llamadas telefónicas dentro de la dependencia con la debida autorización de su superior inmediato.

11. Podrá solicitar a su superior inmediato un espacio en la página web, quien lo hará saber al departamento correspondiente, sólo se podrá publicar información de tipo académico o de investigación.

Deberá reportar al departamento correspondiente alguna anomalía con el equipo a su cargo. En caso de no cumplir dichas políticas se procederá a reportarlo con su jefe.

3.3.4 Políticas para el personal que labora como técnico académico y académicos

Filosofía prohibitiva. Todo se prohíbe excepto lo que está explícitamente permitido.

Para todo el personal que labore como técnico académico o académico dentro de la dependencia:

1. Se le permite el uso del mobiliario, respetando su integridad.

   Dependiendo de los daños ocasionados, se aplicarán las sanciones correspondientes a juicio de las autoridades de la institución.

2. Podrá solicitar una cuenta de usuario para acceder al equipo de cómputo al departamento correspondiente, dicha cuenta se dará de baja al término de su estancia.

3. Podrá solicitar una cuenta de correo al departamento correspondiente, dicha cuenta se dará de baja al término de su estancia.

4. Se le permite la consulta a páginas web que contengan información académica o de investigación.

5. Puede usar el software instalado en el equipo de cómputo.

6. Puede solicitar la instalación de software especializado para realizar sus actividades al departamento correspondiente siempre y cuando no esté explícitamente prohibido por las reglas de la dependencia.

7. Podrá hacer uso de sus propios dispositivos de almacenamiento previamente desinfectados de malware, tomando en cuenta que la integridad física de dichos dispositivos es responsabilidad del propietario, así como el daño que ocasione a los equipos de la dependencia.

Dependiendo de los daños ocasionados se aplicarán las sanciones correspondientes a juicio de las autoridades de la institución.

8. Podrá traer su propio equipo de cómputo, siempre y cuando cumpla con antivirus y sistema operativo actualizado, tomando en cuenta que la integridad física del equipo es responsabilidad del propietario.

9. Podrá solicitar la conexión a la red de la dependencia al departamento correspondiente, para uso escolar o de investigación; dicha conexión se dará de baja al término de su estancia.

10. Podrá realizar llamadas telefónicas dentro de la institución.

11. Podrá solicitar un espacio en la página web a su superior, quien lo hará saber al departamento correspondiente, sólo se podrá publicar información de tipo académico, de investigación o administrativas.

12. Se le permite el uso de la impresora.

13. Podrá solicitar la apertura de puertos de cómputo que requiera para la realización de sus actividades, salvo las restricciones que imponga el jefe de la institución.

14. Podrá solicitar la actualización de su equipo del que está a cargo, siempre y cuando las autoridades correspondientes lo autoricen.

15. Podrá solicitar la adquisición de equipo adicional al que tiene a cargo, siempre y cuando las autoridades correspondientes lo autoricen.

16. Puede solicitar la adaptación de nueva tecnología, siempre y cuando no altere el equipo de cómputo y de red actual.

17. Puede solicitar el mantenimiento del equipo.

18. Puede solicitar el apoyo para el reubicamiento de su equipo de cómputo cuando cambie de cubículo u oficina.

19. Podrá solicitar la instalación de equipo especializado, siempre y cuando se cuente con los recursos necesarios.

20. Podrá solicitar apoyo para los trámites administrativos de su equipo.

21. Podrá solicitar apoyo para el uso del software que ocupe o que vaya a ocupar, siempre y cuando se cuente con los recursos.

22. Podrá solicitar una cuenta para el uso de la plataforma educativa.

23. Podrá solicitar asesoría para la adquisición de equipo nuevo.

Deberá reportar al departamento correspondiente alguna anomalía con el equipo a su cargo. En caso de no cumplir dichas políticas, se procederá a reportarlo con sus superiores, quienes designarán la sanción correspondiente a su juicio.

3.3.5 Políticas para el personal que labora como funcionario

Filosofía prohibitiva. Todo se prohíbe excepto lo que está explícitamente permitido.

Para todo el personal que labore como funcionario dentro de la dependencia:

1. Se le permite el uso del mobiliario, respetando su integridad.

   Dependiendo de los daños ocasionados, se aplicarán las sanciones correspondientes a juicio de las autoridades de la institución.

2. Podrá solicitar una cuenta de usuario para acceder al equipo de cómputo al departamento correspondiente; dicha cuenta se dará de baja al término de su estancia.

3. Podrá solicitar una cuenta de correo a su superior inmediato, quien lo hará saber al departamento correspondiente, dicha cuenta se dará de baja al término de su estancia.
4. Se le permite la consulta a páginas web que contengan información académica o de investigación.

5. Puede usar el software instalado en el equipo de cómputo.

6. Puede solicitar la instalación de software especializado para realizar sus actividades al departamento correspondiente, siempre y cuando no esté explícitamente prohibido por las reglas de la dependencia.

7. Podrá hacer uso de sus propios dispositivos de almacenamiento previamente desinfectados de malware, tomando en cuenta que la integridad física de dichos dispositivos es responsabilidad del propietario; así como el daño que ocasione a los equipos de la dependencia.

   Dependiendo de los daños ocasionados, se aplicarán las sanciones correspondientes a juicio de las autoridades de la institución.

8. Podrá traer su propio equipo de cómputo, siempre y cuando cumpla con antivirus y sistema operativo actualizado, tomando en cuenta que la integridad física del equipo es responsabilidad del propietario.

9. Podrá solicitar la conexión a la red de la dependencia al departamento correspondiente, para uso escolar o de investigación; dicha conexión se dará de baja al término de su estancia.

10. Podrá realizar llamadas telefónicas dentro de la institución.

11. Podrá solicitar un espacio en la página web a su superior inmediato, quien lo hará saber al departamento correspondiente, sólo se podrá publicar información de tipo académico, de investigación o administrativas.

12. Se le permite el uso de la impresora.
13. Podrá solicitar la apertura de puertos de cómputo que requiera para la realización de sus actividades, salvo las restricciones que imponga el jefe de la institución.

14. Podrá solicitar la actualización de su equipo del que está a su cargo, siempre y cuando las autoridades correspondientes lo autoricen.

15. Podrá solicitar la adquisición de equipo adicional al que tiene a cargo, siempre y cuando las autoridades correspondientes lo autoricen.

16. Puede solicitar la adaptación de nueva tecnología, siempre y cuando no altere el equipo de cómputo y de red actual.

17. Puede solicitar el mantenimiento del equipo.

18. Puede solicitar el apoyo para el reubicamiento de su equipo de cómputo cuando cambie de cubículo u oficina.

19. Podrá solicitar la instalación de equipo especializado, siempre y cuando se cuente con los recursos necesarios.

20. Podrá solicitar apoyo para los trámites administrativos de su equipo.

21. Podrá solicitar apoyo para el uso del software que ocupe o que vaya a ocupar, siempre y cuando se cuente con los recursos.

22. Podrá solicitar una cuenta para el uso de la plataforma educativa.

23. Podrá solicitar asesoría para la adquisición de equipo nuevo.

En caso de contar con personal propio de soporte técnico, este personal podrá realizar las peticiones pertinentes y dar solución a los problemas que se le presenten como administrador, sujetándose a las normas establecidas por la institución.

Deberá reportar al departamento correspondiente alguna anomalía con el equipo a su cargo. En caso de no cumplir dichas políticas, se procederá a reportarlo con sus superiores, quienes designarán la sanción correspondiente a su juicio.

3.3.6 Políticas para todo el personal que labora dentro de la dependencia y cuenta con un equipo de cómputo

Establecen el cuidado de los equipos de cómputo.

Políticas respecto a la seguridad física

1. Mantener las computadoras alejadas del fuego, humo, polvo y temperaturas extremas.

2. Colocar las computadoras fuera del alcance de rayos solares, vibraciones, insectos, ruido eléctrico (balastros, equipo industrial, etc.), agua, etcétera.

3. Todos los servidores deberán ubicarse en lugares de acceso físico restringido; para acceder a ellos deberán contar con puertas con chapas.

4. El lugar donde se instalen los servidores contarán con una instalación eléctrica adecuada, entre sus características, con tierra física; y dichos equipos deberán contar con no-breaks.

5. En los lugares donde se encuentre el equipo de cómputo, queda prohibido el consumo de bebidas y alimentos.

6. El lugar donde se encuentren los servidores, se mantendrá condiciones de higiene.

3.3.7 Políticas de cuentas

Establecen qué es una cuenta de usuario de un sistema de cómputo, cómo está conformada, a quién puede ser otorgada, quién es el encargado de asignarlas, cómo deben ser creadas y comunicadas.

1. Las cuentas deben ser otorgadas exclusivamente a usuarios legítimos. Se consideran usuarios legítimos aquellos usuarios quienes hayan realizado su trámite de registro de cuenta y que:

   a) Sean miembros vigentes de la comunidad de la dependencia.

   b) Participen en proyectos especiales y tengan la autorización del jefe del área.

2. Una cuenta deberá estar conformada por: un nombre de usuario y su respectiva contraseña.

3. La asignación de cuentas las hará el administrador del servidor del área en cuestión y al usuario sólo le dará derecho de acceder a los recursos del servidor donde se realiza el registro.

4. El administrador podrá deshabilitar las cuentas que no sean vigentes.

5. Las cuentas y contraseñas personales son intransferibles.

3.3.8 Políticas de contraseñas

Las políticas de contraseñas son una de las políticas más importantes, ya que por lo general, las contraseñas constituyen la primera y tal vez la única manera de autenticación y, por tanto, la única línea de defensa contra ataques. Estas políticas establecen quién asignará la contraseña, qué longitud deberá tener, a qué formato deberá apegarse y cómo será comunicada.

Políticas

1. El administrador del servidor será el responsable de asignar las contraseñas.

2. El administrador deberá contar con herramientas de detección de contraseñas débiles.

3. La longitud de una contraseña deberá siempre ser verificada de manera automática al ser construida por el administrador/usuario. Todas las contraseñas deberán contar con al menos ocho caracteres que contengan números, mayúsculas, minúsculas y caracteres especiales.

4. Todas las contraseñas elegidas por los usuarios deben ser difíciles de adivinar. No deben ser utilizadas palabras que aparezcan en el diccionario, secuencias conocidas de caracteres, datos personales ni acrónimos.

5. Está prohibido que los usuarios construyan contraseñas compuestas de algunos caracteres constantes y otros que cambien de manera predecible y sean fáciles de adivinar.

6. Los usuarios no deben construir contraseñas idénticas o muy parecidas a contraseñas anteriores.

7. La comunicación de la contraseña se realizará de manera personal y no se podrá informar a otra persona que no sea el interesado.

8. Está prohibido informar contraseñas por vía telefónica.

9. Las contraseñas deberán cambiarse máximo cada seis meses.

10. Está prohibido dejar a la vista las contraseñas.

3.3.9 Políticas de control de acceso para el equipo de cómputo

Especifican cómo deben acceder los usuarios al sistema, desde dónde y de qué manera deben autenticarse.

Filosofía prohibitiva. Todo se prohíbe excepto lo que está explícitamente permitido.

Para todo el personal que labore dentro de la dependencia:

1. Todos los usuarios deberán acceder al sistema con su cuenta y no podrán hacer uso de sesiones activas de otros usuarios.

2. Está prohibido acceder al sistema con una cuenta diferente de la propia, aún con la autorización del dueño de dicha cuenta.

3. El usuario tendrá el derecho a cambiar su contraseña.

4. El usuario podrá utilizar los servicios de sesiones remotas si se brinda.

3.3.10 Políticas de respaldos

Para el usuario

1. Será responsabilidad del usuario mantener una copia de la información de su cuenta.

Para el administrador del sistema

1. El administrador del sistema es el responsable de realizar respaldos de la información crítica, siempre que tenga los medios físicos para realizarla. Cada treinta días deberá efectuarse un respaldo completo del sistema y deberá verificar que se haya realizado correctamente.

2. El administrador del sistema es el responsable de restaurar la información.

3. La información respaldada deberá ser almacenada en un lugar seguro.

4. Deberá mantenerse una versión reciente de los archivos más importantes del sistema.

5. En el momento de que la información respaldada deje de ser útil a la organización, dicha información deberá ser borrada antes de deshacerse del medio.

3.3.11 Políticas de correo electrónico

Establecen tanto el uso adecuado como inadecuado del servicio de correo electrónico, los derechos y obligaciones que el usuario debe hacer valer y cumplir al respecto.

Filosofía prohibitiva. Todo se prohíbe excepto lo que está explícitamente permitido.

Para todo el personal que labore dentro de la dependencia:

1. El usuario es la única persona autorizada para leer su propio correo, a menos que él mismo autorice explícitamente a otra persona para hacerlo, o bien, que su cuenta esté involucrada en un incidente de seguridad de cómputo, donde el administrador del sistema podrá auditar dicha cuenta.

2. Está estrictamente prohibido usar la cuenta de correo electrónico proporcionada por la organización para propósitos ajenos a sus actividades académicos o laborales, según sea el caso.
3. Está prohibido enviar correos conteniendo injurias y falsedades.

4. Está prohibido enviar correos sin remitente.

5. Está prohibido enviar por correo virus, archivos o información que ponga en peligro la seguridad del sistema.

6. Está prohibido enviar correos spam.

7. Está prohibido enviar correos de publicidad personal o con intereses personales.

8. Está prohibido enviar correos haciéndose pasar por otra persona.

3.4 Medidas de seguridad para la dependencia

Además de las políticas de seguridad para mitigar el riesgo de un ataque, podrían aplicarse las siguientes medidas, cuyo objetivo es anular o reducir los riesgos existentes o sus consecuencias para el sistema. Frente a las amenazas, algunas de las medidas que se podrían implementar en diferentes escenarios son:

3.4.1 Errores humanos

> *"Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los ordenadores." [16]*

Para evitar errores humanos se puede invertir en:

La formación o educación del personal. Como dice Confucio *"El auténtico conocimiento es conocer la extensión de la propia ignorancia",* ya que en numerosas ocasiones los errores humanos se producen por desconocimiento, pudiéndose evitar con la formación o educación impartida al personal. Tomando como consejo que:

En otras ocasiones se deben por distracciones del mismo personal.

La asignación adecuada de los permisos de acceso a los objetos. Podemos minimizar las consecuencias de los efectos de un posible error ocasionados por los errores humanos limitando el acceso a los objetos (ficheros y directorios) mediante la asignación adecuada de permisos, según las necesidades del usuario para la realización de sus labores dentro de la dependencia.

3.4.2 Robo y alteración de la información contenida en un sistema

Como una medida hacía la atenuación en contra del robo y/o alteración de la información contenida en un sistema se puede implementar:

La autenticación de usuarios. En ésta sólo pueden acceder al sistema los usuarios autorizados y para poder hacerlo deben de introducir una clave secreta o identificarse de alguna otra forma: huellas dactilares, tarjetas inteligentes, etc.

La elección de claves seguras y mantenimiento en secreto. Las claves para acceder a los sistemas deben adaptarse a ciertas recomendaciones para evitar que sean descubiertas fácilmente y deben de mantenerse en secreto.

La asignación adecuada de los permisos de acceso a los objetos. Cada usuario debe tener acceso de lectura y/o escritura únicamente a la información que necesite consultar.

El establecimiento de alarmas sobre eventos. Los sistemas operativos multidisciplinarios permiten establecer alarmas sobre determinados eventos de forma que, cuando se producen, envía un aviso al administrador de la red.

Programas de bloqueo cuando haya que dejar el sistema desatendido. Para que los posibles intrusos no entren en el sistema aprovechando la ausencia.

El cifrado. El cifrado de la información evitará que el ladrón pueda leer de forma clara la información y luego utilizarla como más le convenga a sus intereses.

Registros de auditoría. En un sistema multiusuario la auditoría permite establecer un control sobre quién usa el sistema, qué hace cada usuario o quién utiliza cada recurso, facilitando así la detección de intentos de violación de la seguridad. No es una medida que evite el robo directamente aunque puede disuadir al ladrón, sabiendo que las huellas que deje pueden conducir a su identificación.

3.4.3 Robo y alteración de información durante la transmisión

Una medida contra la intercepción de la información que se transmite por la red es la utilización de canales seguros. Lo habitual es que circule por redes públicas sobre las que no se tiene control directo, por lo que puede ser capturada; por lo tanto, en estos medios debe de recurrirse al cifrado de la información.

3.4.4 Robo de equipos

Como medida precautoria ante el robo de equipos se puede:

Implementar un acceso restringido a la sala donde se encuentra el sistema.

Diseñar un soporte de fijación para el equipo. Existen diferentes artículos disponibles en el mercado para fijar los equipos a un soporte, como puede ser la mesa sobre la que se encuentra.

Realizar copias de seguridad. Más valiosa que el propio equipo, en la gran mayoría de los casos es la información que contiene; por ello las copias de seguridad evitarán que el robo se convierta en una verdadera catástrofe.

Tener equipos de reserva. Disponiendo de equipo, con la configuración básica y las copias de seguridad, se podrá tener operatividad en pocas horas para que no afecte gravemente el trabajo normal.

Marcar los equipos. Hacer una pequeña marca en los equipos facilitará su posterior localización e incluso puede contribuir que el ladrón desista.

Apuntar modelos y números de serie. Llevar un control del inventario para posibilitar su localización, nos permite conocer cuánto un equipo falta.

3.4.5 Recepción de información falsa

Autenticación de la información mediante firmas digitales. Las firmas digitales aseguran que la información que se recibe proviene de quien realmente dice ser.

3.4.6 Sabotaje de los equipos

Para evitar el sabotaje de equipos debería de existir un acceso restringido a la sala donde se encuentra el sistema y en caso de que sea saboteado se debe tener disponibles equipos de reserva para hacer el cambio y continuar con el sistema.

3.4.7 Sabotaje de la información

Para evitar este problema se debe restringir el acceso a la sala, así como al sistema, dar una asignación adecuada de los permisos de acceso a los objetos y cuando no se encuentre en uso el sistema, se utilizarán programas de bloqueo.

3.4.8 Virus, malware, etcétera

Ante los problemas de virus, malware, entre otros; se debe tener control sobre los programas introducidos. La mejor medida para evitar que los virus lleguen al sistema, es no introducir programas ilegales ni ejecutar programas que provengan de otro equipo o usuario sin pasarles antes un detector de virus. Para ello se puede instalar un antivirus residente actualizado; éste podrá detectar la presencia de virus en el sistema e impedirá su activación y propagación.

A su vez, se debe evitar arrancar desde unidades lectoras. Los virus de arranque se activan cuando se inicia la computadora con el dispositivo infectado. En caso de tener que hacerlo, hay que escanearlos antes por el detector de antivirus.

En caso de ser vulnerada esta medida, se deben tener copias de seguridad actualizadas para no perder la información y para no tener detenido el sistema por un tiempo prolongado mientras se reúne de nuevo la información.

3.4.9 Desastres naturales

Ante desastres naturales se pueden almacenar las copias de seguridad en un armario ignifugo. En ellos las copias de seguridad no sólo estarán protegidas frente al fuego sino también a terremotos e inundaciones. Si no se dispone de un armario ignifugo es recomendable mantener una copia de seguridad almacenada en otro edificio.

3.4.10 Contraseñas

Cuando se hace uso de contraseñas debe de tomarse en cuenta que:

> *"Las contraseñas son como la ropa interior. No puedes dejar que nadie la vea, debes cambiarla regularmente y no debes compartirla con extraños." (Chris Pirillo. Fundador y mantenedor de Lockergnome, una red de blogs, foros web, listas de correo y las comunidades en línea)*

Para verificar el nivel de seguridad de las contraseñas se puede utilizar páginas como: *https://www.microsoft.com/protect/fraud/passwords/checker.aspx*

En la figura 3.2 se muestra un ejemplo de cuando se introduce una contraseña débil en la página web *https://www.microsoft.com/protect/fraud/passwords/checker.aspx. N*os damos cuenta que es débil debido a que sólo se colorea un cuarto de la barra, indicándonos que es 25% segura.

Figura 3. 2. Ejemplo de una prueba de contraseña débil.

En la figura 3.3 se muestra un ejemplo cuando se introduce una contraseña más fuerte que la introducida en la figura 3.2. Nos damos cuenta que es más fuerte debido a que se colorea tres cuartos de la barra, indicándonos que es aproximadamente 75% segura.

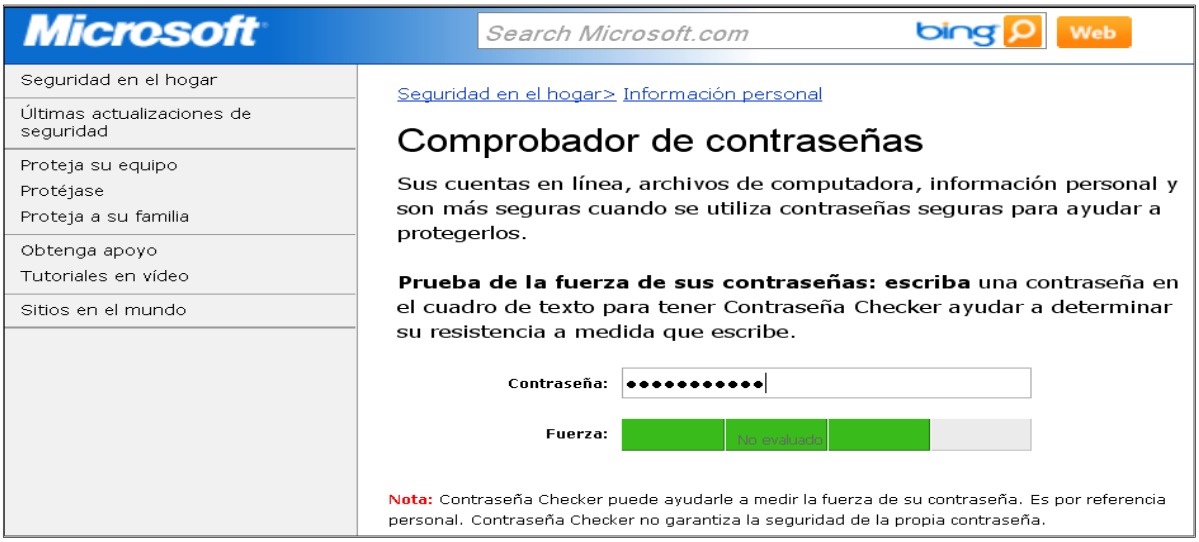


Figura 3. 3. Ejemplo de una prueba de contraseña fuerte.

También, podemos descargar programas como el “password meter”, que nos permitirán conocer el nivel de complejidad de nuestra contraseña. Este pequeño programa da más detalles sobre la contraseña, ya que cuenta el número de caracteres que componen dicha contraseña, haciendo a su vez un conteo de letras mayúsculas, minúsculas, números o símbolos existentes, así como la distribución de las mismas. La puntuación se muestra en unidades de porcentaje y nos da una calificación de la complejidad de forma cualitativa.

En la figura 3.4 se hace el estudio de la contraseña hola1234 tiene una puntación del 51% quedando en un rango de buena.

Test Your Password		Minimum Requirements
Password:	hola12345	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	51%	
Complexity:	Good	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	9	+ 36
Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
Lowercase Letters	Cond/Incr	+((len-n)*2)	4	+ 10
Numbers	Cond	+(n*4)	5	+ 20
Symbols	Flat	+(n*6)	0	0
Middle Numbers or Symbols	Flat	+(n*2)	4	+ 8
Requirements	Flat	+(n*2)	3	0
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Incr	-(n(n-1))	0	0
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	3	- 6
Consecutive Numbers	Flat	-(n*2)	4	- 8
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	3	- 9

Figura 3. 4. Ejemplo de un análisis con password meter.

3.5 Plan de contingencias para la dependencia

Ante cualquier problema o incidente que afecte a la seguridad del sistema, lo prioritario es intentar neutralizarlo para poder continuar el trabajo habitual, en la medida de lo posible. La recuperación de los equipos o la información que hayan sido afectados y que por el momento, no sean necesarios o no interrumpan el trabajo, puede esperar.

Una vez que todo vuelve a la normalidad, será el momento de replantearse si las medidas de seguridad que se adoptaron eran suficientes o si es necesario aumentarlas.

Para la recuperación, después de un incidente es muy útil hacer una lista con los posibles percances y las acciones a seguir; es decir en estas listas se responde a la pregunta ¿qué ser debe hacer en caso de…?

Dicha lista podría tener el siguiente aspecto:

3.5.1 En caso de robo de equipos

En caso de algún robo de un equipo se debe:

1. Utilizar equipo de reserva. Restaurando los datos de las copias de seguridad e instalando los programas que no estaban en el equipo de reserva.

2. Dar parte del delito. Se deberá hacer un reporte a las autoridades competentes; habrá que facilitarles los números de serie e identificación de marcas que se habían efectuado.

3. Mantener un seguimiento del hecho.

4. Hacer anotaciones en la bitácora de sucesos.

3.5.2 En caso de desastre natural

En caso de algún desastre natural se debe:

1. Verificar los daños ocasionados y cuantificar pérdidas.

2. Utilizar equipo de reserva. Restaurando los datos de las copias de seguridad e instalando los programas que no estaban en el equipo de reserva.

3. Primero se deberán restaurar equipos que brinden servicios como servidores web, servidores DNS, servidores de correo. Posteriormente los equipos de los usuarios según su jerarquía y su importancia dentro de la institución.

4. Hacer anotaciones en la bitácora.

3.5.3 En caso de fallos de equipo

En caso de algún fallo de equipo se debe:

1. Verificar la causa del fallo.

2. Revisar si aún se tiene garantía y qué daños cubre dicha garantía.

3. Si dicha garantía ya no es vigente, ver cuánto tiempo se puede llevar en reparar el desperfecto.

4. Si la reparación excede en tiempo, se deberá utilizar el equipo de reserva, restaurando los datos con ayuda de las copias de seguridad e instalando los programas que no estaban en el equipo de reserva. En el caso de que no sea demasiado el tiempo que tarde en realizarse la reparación, se efectuará en ese momento.

5. Hacer anotaciones en la bitácora de sucesos.

3.5.4 En caso de virus

En caso de algún contagio por virus, gusanos o malware en general se debe:

1. Descargar las actualizaciones más recientes del antivirus.
2. Eliminar el virus, ya sea con antivirus o manualmente de los ficheros o partes infectadas del sistema.

3. Restaurar los programas y datos perdidos con ayuda de las copias de seguridad.

4. Hacer un estudio del tipo de contagio para averiguar la fuente de contaminación y saber si el virus tuvo contacto con cualquier otro equipo.

5. En el caso de que si hubiera contacto, se deberá darle el mismo mantenimiento a la posible máquina contagiada.

6. Si se encuentra la fuente de propagación, ésta deberá ser desinfectada, en el caso de dispositivos; si la fuente de propagación es consecuencia de una consulta a una página web, convendrá bloquear esa página con ayuda de un firewall.

7. Hacer anotaciones en la bitácora.

3.5.5 Bitácora

En todos los casos se hace mención de una bitácora, la cual es un registro escrito de las acciones, tareas o actividades que se deben llevar a cabo en una determinada actividad, empresa o trabajo. En este caso, la bitácora permitirá registrar los hechos o percances en la dependencia para posteriormente, saber cómo se resolvió el problema si llegase a

ocurrir, minimizando el tiempo de respuesta; a su vez nos permitirá tener un control y una organización en las actividades de los administradores. Para ello podemos hacer uso de software que existe en la red, como es iDailyDiary; véase figura 3.5 y 3.6.

Figura 3. 5. Software iDailyDiary.

Figura 3. 6. Ejemplo del uso del Software iDailyDiary.

O se puede realizar una pequeña base de datos, por ejemplo, en Acces de Microsoft, ver figura 3.7.

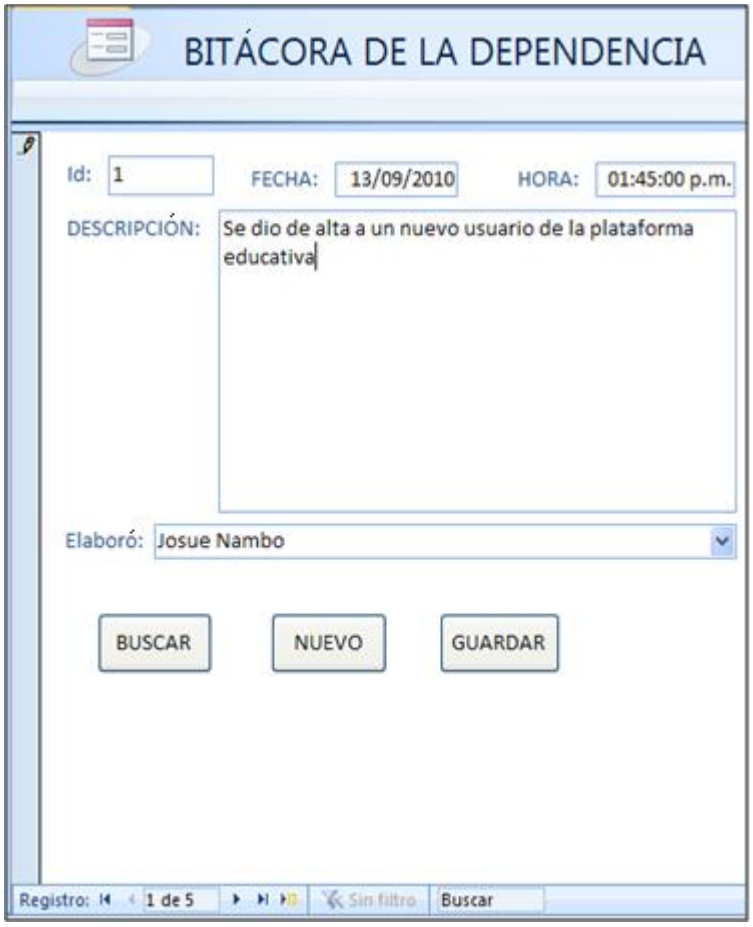


Figura 3. 7. Ejemplo de una base de datos usada como bitácora.

El diagrama físico de la base de datos sería muy sencillo, tal como se muestra en la figura 3.8.

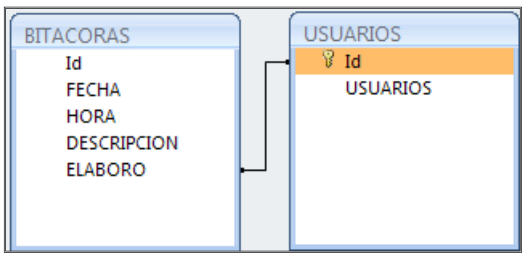


Figura 3. 8. Diagrama físico.

3.6 Mecanismos de seguridad para la dependencia

Después de analizar los activos a proteger y saber de qué se deben proteger, se propone implementar un control preventivo que nos permitirá reducir el riesgo de un ataque, el cual sería un firewall; a su vez se propone construir un sistema de inventario, que además de darnos organización, nos podría servir como control disuasivo, ya que nos permitirá desanimar a las personas de realizar un robo o modificación del equipo.

3.6.1 NAT con firewall

Al implementar este mecanismo nos ayudará a reforzar las políticas de seguridad antes mencionadas. Se propone desarrollar el firewall de software sobre el sistema operativo OpenBSD, debido a que es un sistema operativo libre, multiplataforma y muy seguro; en éste se utilizará el Squid que es un proxy cache web para el filtrado de HTTP, HTTPS, FTP y mucho más. Se decidió emplearlo debido a que reduce los tiempos de respuesta y mejora el ancho de banda, mediante el almacenamiento en caché, además de que nos permite hacer un filtrado por palabras para bloquear ciertas páginas de internet.

3.6.1.1 Instalación de OpenBSD

Para su instalación necesitamos un equipo que al menos cuente con 8 gigas en disco duro 256 en RAM y dos tarjetas de red.

Obtendremos la distribución de openBSD desde la página *http://www.openbsd.org/,* la descarga se grabará en un CD, dicho CD se utilizará para reiniciar el equipo.

Al iniciar el equipo con el disco en la unidad lectora, se muestra una pantalla como la que se observa en la figura 3.9:

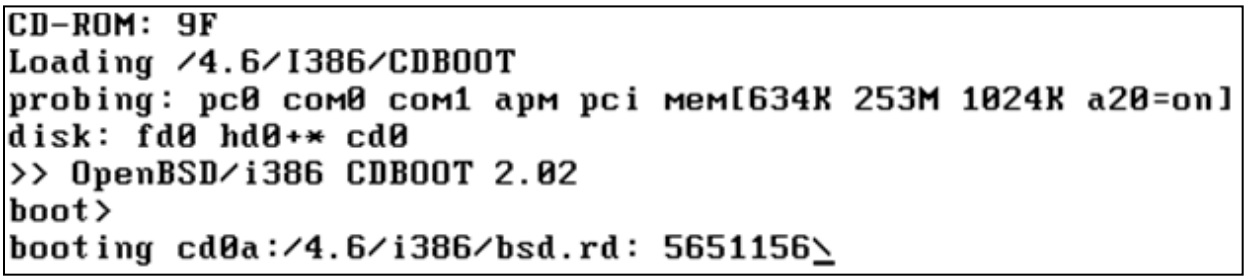


Figura 3. 9. Carga del Sistema Operativo OpenBSD.

Una vez que el equipo termina la carga del sistema, pregunta si se requiere instalar, actualizar o si el usuario necesita una shell, en este caso se oprime la tecla “I” para instalar el nuevo sistema operativo, ver figura 3.10.

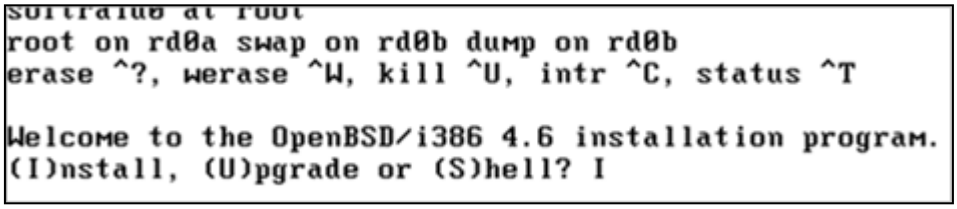


Figura 3. 10. Instalación de OpenBSD.

Posteriormente pide la configuración del teclado, por estar localizado en México al momento de desarrollar este mecanismo, como dicha configuración del teclado es latinoamericana, en consecuencia se teclea “la”; ver figura 3.11.

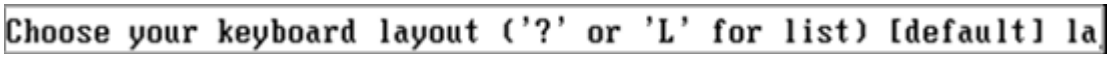


Figura 3. 11. Configuración del teclado.

Ahora pregunta por el hostname; en este caso, se escribe el nombre por el cual se identificará el equipo en el que se realiza la instalación, para ejemplificar se usa el nombre de “fire”; ver figura 3.12.

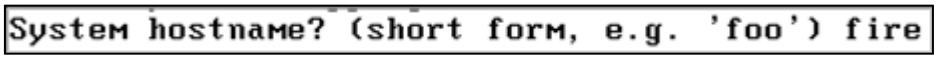


Figura 3. 12. Configuración del hostname.

Después de escribir el hostame, pregunta qué tarjeta se desea configurar; en este caso la tarjeta de red se llama vic0; ver figura 3.13.

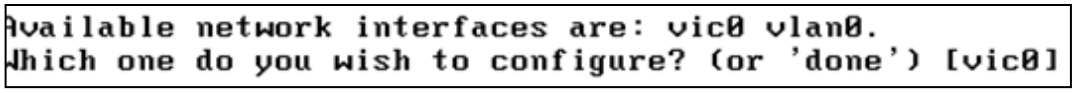


Figura 3. 13. Selección de la tarjeta de red.

Al decidir qué tarjeta de red se quiere configurar, pide la asignación de un dirección IP a la cual responderá esta tarjeta, dentro de esta opción puede asignarse la dirección IP de forma automática, al momento de seleccionar la opción de DHCP, o bien, se puede asignar de forma manual, no se debe olvidar, que la IP asignada debe encontrarse dentro del segmento de la IP que se maneja en la institución; para el ejemplo se decidió asignar la IP 10.0.180.1; ver figura 3.14.

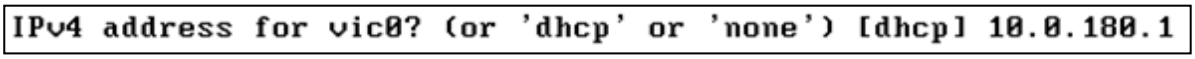


Figura 3. 14. Asignación de la IPv4.

Es momento de elegir el tipo de la máscara de red que se usará, para conseguir un rango de 254 IP's disponibles, se deja la máscara que aparece por defecto, si se desea se puede cambiar; ver figura 3.15.

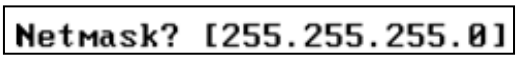


Figura 3. 15. Asignación de la máscara de red.

Una vez configurada la máscara de red, pregunta si desea el uso de IPv6, si no se cuenta con el soporte para esa versión se escribe none; ver figura 3.16.

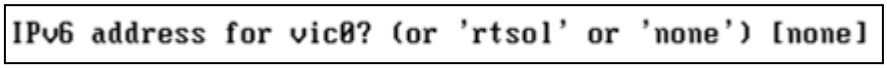


Figura 3. 16. Asignación de la IPV6.

Como siguiente paso, se introduce la dirección IP que corresponde a la puerta de enlace, por ejemplo la 10.0.180.254; ver figura 3.17.

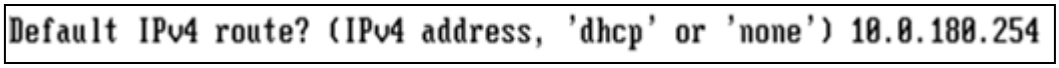


Figura 3. 17. Asignación de la puerta de enlace.

En la siguiente pregunta, hay que contestar con el nombre de nuestro dominio, posteriormente se introduce la dirección IP correspondiente a dicho servidor; ver figura 3.18.

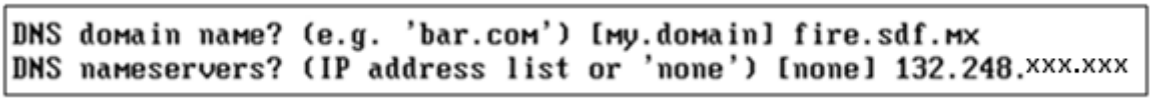


Figura 3. 18. Asignación del Dominio.

Para finalizar la configuración de las direcciones en la tarjeta pregunta, si se necesita algún manual de configuración, en este punto, se deja seleccionado la opción por defecto; ver figura 3.19.

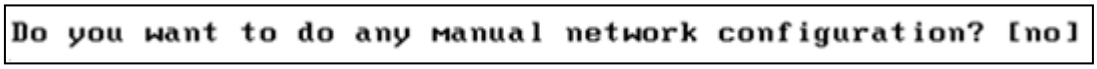


Figura 3. 19. Instalación del manual de red.

En el siguiente punto hay que introducir la contraseña a emplearse para el inicio de sesión, debe escribirse dos veces: una para indicar cuál es y en la segunda pregunta sólo para la verificación; hay que tomar en cuenta que mientras introducimos la contraseña no se muestra lo que se está tecleando, cuestión por la cual conviene poner atención a lo que se introduce; ver figura 3.20.

Figura 3. 20. Asignación de contraseña.

Se inicia el demonio de SSH, pero no el demonio de ntpd; ver figura 3.21.

```
Start sshd(8) by default? [yes]
Start ntpd(8) by default? [no]
```

Figura 3. 21. Inicialización de demonios.

No se recomienda iniciar el ambiente gráfico para obtener un poco más de seguridad; ver figura 3.22.

```
Do you expect to run the X Window System? [yes] no_
```

Figura 3. 22. Inicialización de gráficos.

Ha llegado el momento de elegir en qué disco se quiere hacer la instalación del sistema operativo, enseguida nos muestra cómo quedarían las particiones si elegimos que las realice automáticamente. En caso de esta instalación, se hacen las particiones de forma personalizada, para ello se teclea “C”; ver figura 3.23.

```
Available disks are: sd0.
Which one is the root disk? (or 'done') [sd0]
MBR has invalid signature; not showing it.
Use (W)hole disk or (E)dit the MBR? [whole]
Setting OpenBSD MBR partition to whole sd0...done.
The auto-allocated layout for sd0 is:
#                size           offset  fstype [fsize bsize  cpg]
  a:           159.9M               63  4.2BSD   2048 16384    1 # /
  b:           159.9M           327468    swap
  c:          8192.0M                0  unused
  d:           247.8M           654873  4.2BSD   2048 16384    1 # /tmp
  e:           287.7M          1162337  4.2BSD   2048 16384    1 # /var
  f:           631.9M          1751446  4.2BSD   2048 16384    1 # /usr
  g:           559.9M          3045672  4.2BSD   2048 16384    1 # /usr/X11R6
  h:          2127.9M          4192387  4.2BSD   2048 16384    1 # /usr/local
  i:          1071.9M          8550256  4.2BSD   2048 16384    1 # /usr/src
  j:          1071.9M         10745547  4.2BSD   2048 16384    1 # /usr/obj
  k:          1870.6M         12940838  4.2BSD   2048 16384    1 # /home
Use (A)uto layout, (E)dit auto layout, or create (C)ustom layout? [a] _
```

Figura 3. 23. Particiones del DD.

Se empiezan a crear las particiones considerando el tamaño de nuestro disco duro, a su vez no se debe olvidar que, por recomendación, el tamaño de espacio para el directorio /swap, debe de ser el doble del espacio con el que se cuenta en la memoria RAM. Por ejemplo, si la memoria RAM del equipo en el cual se está montando dicho sistema es de 256 megas entonces el tamaño de /swap será de 512 megas. Al momento de configurar estas particiones hay que tomar en cuenta que la letra G significa gigas, M = megas; ver figura 3.24 y 3.25.

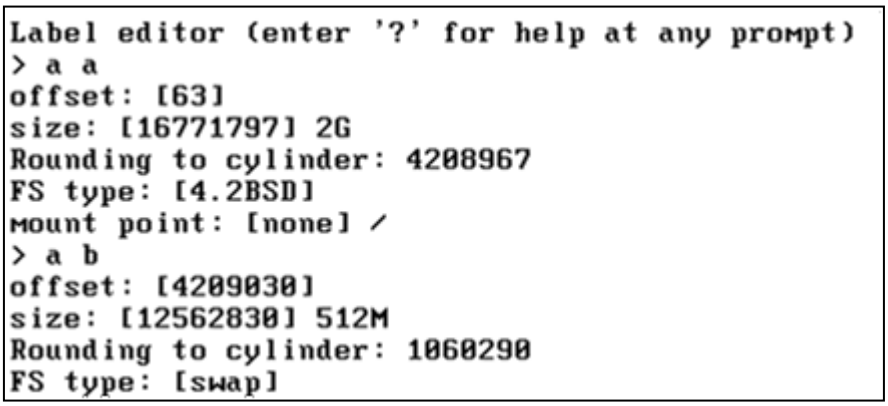


Figura 3. 24. Configuración de particiones.

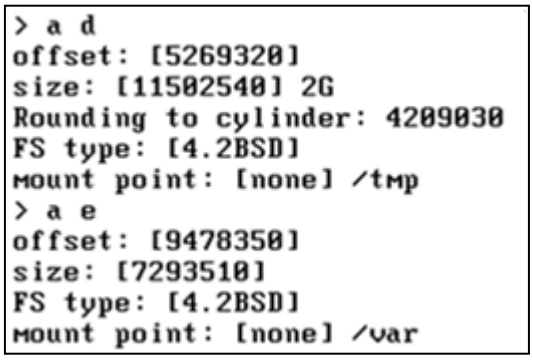


Figura 3. 25. Configuración de particiones.

Para poder visualizar cómo queda la configuración de las particiones, se oprime la tecla con la letra p. Si las particiones se hicieron correctamente es momento de escribir w para guardar la configuración y la letra q para salir; una vez afuera del administrador de particiones empieza la asignación de los sectores, hay que permitir que termine la asignación; ver figura 3.26.

```
> p
OpenBSD area: 63-16771860; size: 16771797; free: 0
#                size           offset  fstype [fsize bsize  cpg]
  a:            4208967               63  4.2BSD   2048 16384    1 # /
  b:            1060290          4209030    swap
  c:           16777216                0  unused
  d:            4209030          5269320  4.2BSD   2048 16384    1 # /tmp
  e:            7293510          9478350  4.2BSD   2048 16384    1 # /var
>
> w
> q
No label changes.
/dev/rsd0a: 2055.2MB in 4208964 sectors of 512 bytes
11 cylinder groups of 202.47MB, 12958 blocks, 25984 inodes each
/dev/rsd0d: 2055.2MB in 4209028 sectors of 512 bytes
11 cylinder groups of 202.47MB, 12958 blocks, 25984 inodes each
```

Figura 3. 26. Termino de configuración de particiones.

Cuando finaliza pregunta de dónde obtiene la información y qué nombre tendrá el path, a estas preguntas se contesta que el origen de la información es el cd y el pathname es el que trae por defecto; ver figura 3.27.

```
/dev/sd0e on /mnt/var type ffs (rw, asynchronous, local, nodev, nosuid)

Let's install the sets!
Location of sets? (cd disk ftp http or 'done') [cd]
Available CD-ROMs are: cd0.
Which one contains the install media? (or 'done') [cd0]
Pathname to the sets? (or 'done') [4.6/i386]
```

Figura 3. 27. Configuración del pathname.

Nos pide qué paquetería se desea instalar, como en pasos anteriores, no se pidió el ambiente gráfico, debemos quitar los paquetes para ello, los cuales serán los que empiezan con “x” como por ejemplo **x**base46.tgz, así mismo quitaremos los juegos; ver figura 3.28.

```
Select sets by entering a set name, a file name pattern or 'all'. De-select
sets by prepending a '-' to the set name, file name pattern or 'all'. Selected
sets are labelled '[X]'.
    [X] bsd           [X] etc46.tgz     [X] game46.tgz    [X] xfont46.tgz
    [X] bsd.rd        [X] misc46.tgz    [X] xbase46.tgz   [X] xserv46.tgz
    [ ] bsd.mp        [X] comp46.tgz    [X] xetc46.tgz
    [X] base46.tgz    [X] man46.tgz     [X] xshare46.tgz
```

Figura 3. 28. Paquetería del OpenBSD.

Para quitar los paquetes, lo haremos escribiendo el nombre del archivo a desmarcar; al terminar de desmarcar los archivos que no queremos le decimos done y empezará la instalación de los que dejamos marcados; ver figuras 3.29.

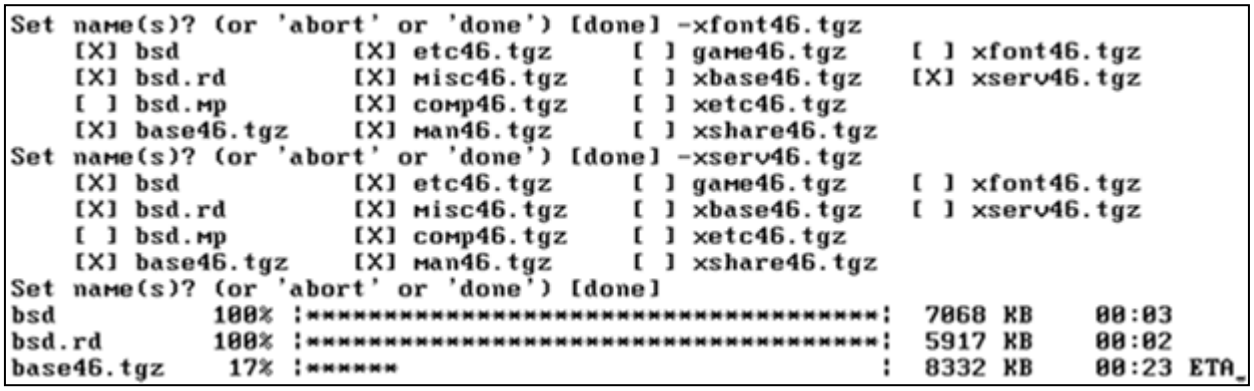


Figura 3. 29. Instalación de la paquetería del OpenBSD.

Si todo se hizo bien y conforme al manual habrá terminado de instalar el sistema operativo, sólo hay que configurar la zona horaria. Para el caso de la Ciudad de México es Mexico/General. Reiniciamos al equipo con la instrucción reboot; ver figura 3.30.

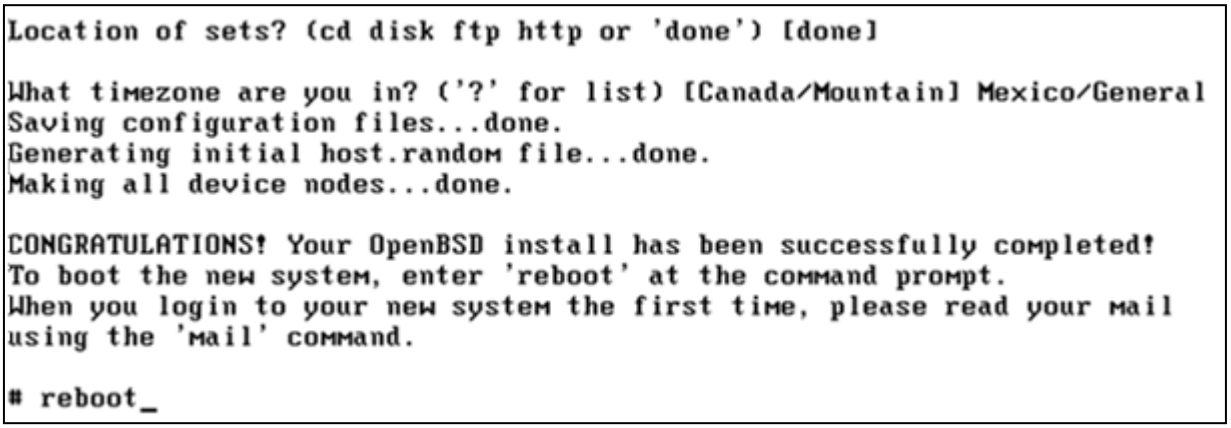


Figura 3. 30. Finalización de la instalación del OpenBSD.

Para navegar por los archivos necesitamos autenticarnos; para ello en el login escribimos root y en password ponemos el que configuramos en esta instalación; ver figura 3.31.

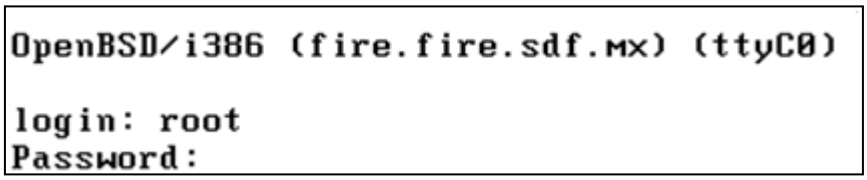


Figura 3. 31. Inicio de sesión.

Si la contraseña fue correcta nos mostrará una pantalla como la de la figura 3.32.

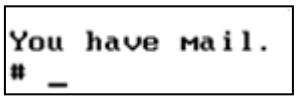


Figura 3. 32. Sesión iniciada.

3.6.1.2 Configuración

Después de la instalación entramos al directorio /etc/, en este directorio creamos el archivo hostname.vic0, ver figura 3.33 y agregamos la línea, inet “IP” “máscara de red” en el archivo creado, donde IP se cambia por una IP correspondiente al segmento de red y máscara de red se sustituye por la máscara a utilizar; ver figura 3.34.

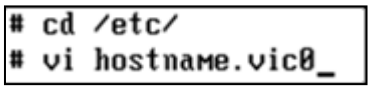


Figura 3. 33. Creación archivo hostname.vic0.

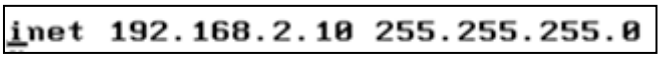


Figura 3. 34. Ejemplo del contenido de hostname.vic0.

Creamos un archivo llamado hostname.vic1, correspondiente a la tarjeta interna; ver figura 3.35. Escribe la IP del Gateway de nuestra red interna, por ejemplo 192.168.187.254, entonces quedaría, inet 192.168.187.254 255.255.255.0; ver figura 3.36.

```
# vi hostname.vic1_
```

Figura 3. 35. Creación archivo hostname.vic1.

```
inet 192.168.187.254 255.255.255.0
```

Figura 3. 36. Ejemplo del contenido de hostname.vic1.

En el archivo sysctl.conf hay que quitar el comentario (#) a la línea "net.inet.ip.forwarding=1"; ver figura 3.37.

```
#       $OpenBSD: sysctl.conf,v 1.47 2009/06/09 11:52:54 sthen Exp $
#
# This file contains a list of sysctl options the user wants set at
# boot time.  See sysctl(3) and sysctl(8) for more information on
# the many available variables.
#
net.inet.ip.forwarding=1        # 1=Permit forwarding (routing) of IPv4 packets
#net.inet.ip.mforwarding=1      # 1=Permit forwarding (routing) of IPv4 multicas
t packets
#net.inet.ip.multipath=1        # 1=Enable IP multipath routing
#net.inet.icmp.rediraccept=1    # 1=Accept ICMP redirects
#net.inet6.icmp6.rediraccept=0  # 0=Don't accept IPv6 ICMP redirects
#net.inet6.ip6.forwarding=1     # 1=Permit forwarding (routing) of IPv6 packets
#net.inet6.ip6.mforwarding=1    # 1=Permit forwarding (routing) of IPv6 multicas
t packets
#net.inet6.ip6.multipath=1      # 1=Enable IPv6 multipath routing
#net.inet6.ip6.accept_rtadv=1   # 1=Permit IPv6 autoconf (forwarding must be 0)
#net.inet.tcp.rfc1323=0         # 0=Disable TCP RFC1323 extensions (for if tcp i
s slow)
#net.inet.tcp.rfc3390=0         # 0=Disable RFC3390 for TCP window increasing
#net.inet.esp.enable=0          # 0=Disable the ESP IPsec protocol
#net.inet.ah.enable=0           # 0=Disable the AH IPsec protocol
#net.inet.esp.udpencap=0        # 0=Disable ESP-in-UDP encapsulation
#net.inet.ipcomp.enable=1       # 1=Enable the IPCOMP protocol
sysctl.conf: unmodified: line 1
```

Figura 3. 37. Contenido de sysctl.conf.

En el archivo rc.conf, en la línea que dice pf, asegurarse que diga pf=YES, ver figura 3.38.

```
#!/bin/sh -
#
#       $OpenBSD: rc.conf,v 1.133 2009/05/31 19:16:16 henning Exp $

# set these to "NO" to turn them off.  otherwise, they're used as flags
ripd_flags=NO           # for normal use: ""
mrouted_flags=NO        # for normal use: "", if activated
                        # be sure to enable multicast_router below.
dvmrpd_flags=NO         # for normal use: ""
ospfd_flags=NO          # for normal use: ""
ospf6d_flags=NO         # for normal use: ""
bgpd_flags=NO           # for normal use: ""
rarpd_flags=NO          # for normal use: "-a"
bootparamd_flags=NO     # for normal use: ""
rbootd_flags=NO         # for normal use: ""
sshd_flags=""           # for normal use: ""
named_flags=NO          # for normal use: ""
rdate_flags=NO          # for normal use: [RFC868-host] or [-n RFC2030-host]
timed_flags=NO          # for normal use: ""
ldattach_flags=NO       # for normal use: "[options] linedisc cua-device"
ntpd_flags=NO           # for normal use: ""
isakmpd_flags=NO        # for normal use: ""
sasyncd_flags=NO        # for normal use: ""
mopd_flags=NO           # for normal use: "-a"
```

Figura 3. 38. Contenido de rc.conf.

En el archivo pf.conf, agregamos las líneas:

****

ext_if="vic0"

int_if="vic1"

set skip on lo

nat on $ext_if from $int_if:network to any -> $ext_if

****

Dichas líneas van a permitir la comunicación entre las dos tarjetas; ver figura 3.39:

```
#       $OpenBSD: pf.conf,v 1.44 2009/06/10 15:29:34 sobrado Exp $
#
# See pf.conf(5) for syntax and examples; this sample ruleset uses
# require-order to permit mixing of NAT/RDR and filter rules.
# Remember to set net.inet.ip.forwarding=1 and/or net.inet6.ip6.forwarding=1
# in /etc/sysctl.conf if packets are to be forwarded between interfaces.

ext_if="vic0"
int_if="vic1"


set skip on lo
#scrub in

nat on $ext_if from $int_if:network to any -> $ext_if
```

Figura 3. 39. Contenido de pf.conf.

Hasta aquí un cliente o un equipo que se conecte con la configuración TCP/IP correspondiente a nuestra red; en este caso la IP 192.168.18.X, debería de ser capaz de conectarse a la red externa, como la Internet, sólo que sin ningún tipo de restricción.

Lo que sigue es instalar el proxy-cache SQUID, que nos ayudará a filtrar el tránsito de la red y modificar el PATH; ver figura 3.40.

```
# export PKG_PATH=ftp://ftp.openbsd.org/pub/OpenBSD/4.6/packages/i386/
# pkg add -i squid
```

Figura 3. 40. Instalación del SQUID.

SQUID se instala, dejando los archivos de configuración bajo /etc/squid

Antes de configurarlos, debemos editar el archivo /etc/pf.conf; el archivo completo quedaría de la siguiente forma:

****

$OpenBSD: pf.conf,v 1.44 2010/09/11 15:29:34 sobrado Exp $

ext_if="em0"

int_if="rl0"

set skip on lo

nat on $ext_if from $int_if:network to any -> $ext_if

rdr on $int_ifinet proto { tcp, udp } from any to any port www -> 127.0.0.1 port 3128

block out on $ext_if proto { tcp, udp } from any to any port = 1863

****

Donde con la línea “rdr on $int_ifinet …”, redirecciona el tránsito de la conexión hacia el SQUID para que lo analice y decida si lo permite o lo restringe; ver figura 3.41.

```
#       $OpenBSD: pf.conf,v 1.44 2009/06/10 15:29:34 sobrado Exp $
#
# See pf.conf(5) for syntax and examples; this sample ruleset uses
# require-order to permit mixing of NAT/RDR and filter rules.
# Remember to set net.inet.ip.forwarding=1 and/or net.inet6.ip6.forwarding=1
# in /etc/sysctl.conf if packets are to be forwarded between interfaces.

ext_if="vic0"
int_if="vic1"


set skip on lo
#scrub in

nat on $ext_if from $int_if:network to any -> $ext_if

rdr on $int_if inet proto { tcp, udp } from any to any port www -> 127.0.0.1 por
t 3128

block out on $ext_if proto { tcp, udp } from any to any port = 1863


# NAT/filter rules and anchors for ftp-proxy(8)
#nat-anchor "ftp-proxy/*"
pf.conf: unmodified: line 1
```

Figura 3. 41. Contenido del pf.conf.

Ya en el directorio /etc/squid debemos configurar squid.conf; ver figura 3.42.

```
#        WELCOME TO SQUID 2.7.STABLE6
#        ----------------------------


# OPTIONS FOR AUTHENTICATION
# -----------------------------------------------------------------------------

#  TAG: auth_param
#
#       auth_param negotiate keep_alive on
#
#Recommended minimum configuration per scheme:
#auth_param negotiate program <uncomment and complete this line to activate>
#auth_param negotiate children 5
#auth_param negotiate keep_alive on
#auth_param ntlm program <uncomment and complete this line to activate>
#auth_param ntlm children 5
#auth_param ntlm keep_alive on
#auth_param digest program <uncomment and complete this line>
#auth_param digest children 5
#auth_param digest realm Squid proxy-caching web server
#auth_param digest nonce_garbage_interval 5 minutes
#auth_param digest nonce_max_duration 30 minutes
squid.conf: unmodified: line 1
```

Figura 3. 42. Archivo squid.conf.

Como este archivo es muy extenso, la parte que interesa es donde pondremos las reglas de filtrado; para ello nos ayudaremos de ACLs.

Algunos puntos importantes:

****

INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

aclmiredlocalsrc “segmento”/”mascara de red”

aclpag_prohibidasurl_regex "/etc/squid/pag_prohibidas"

aclpag_pornourl_regex "/etc/squid/pag_porno"

aclpag_descargasurl_regex "/etc/squid/pag_descargas_directas"

aclusuarios_vipsrc "/etc/squid/usuarios_vip"

aclpag_messengerurl_regex "/etc/squid/pag_web_messenger"

aclusuarios_msnsrc "/etc/squid/usuarios_messenger"

aclpalabras_filtradasurl_regex "/etc/squid/palabras_filtradas"

http_access allow usuarios_vip
http_access deny palabras_filtradas
http_access deny pag_porno
http_access deny pag_descargas
http_access allow usuarios_msn
http_access deny pag_messenger
http_access deny pag_prohibidas
http_access allow miredlocal
****

Aquí por ejemplo, hay que revisar que aclmiredlocalsrc tenga el segmento de red adecuado, por ejemplo: 192.168.1.0.

“cache_mem 100MB”; en esta línea configuramos cuánto espacio va a tener nuestra memoria caché.

“cache_dirufs /var/squid/cache 9216 16 256”; en esta línea definimos el espacio del directorio cache donde se almacenarán las páginas, para un mayor acceso, cuando éstas no son tan dinámicas y otras características, el valor de 9216, se puede cambiar por uno más pequeño, como la partición de /var es de 5, con 1024 está bien.

En el archivo ya editado, hay muchas líneas comentadas, para otras funcionalidades de SQUID, al parecer ya sólo hay que verificar los directorios de donde se guardan los logs, los cuales son llamados con las líneas que contiene la siguiente estructura: http_access allow “nombre del archivo”

Ejemplo del archivo que llama la línea http_access deny pag_prohibidas; ver figura 3.43:

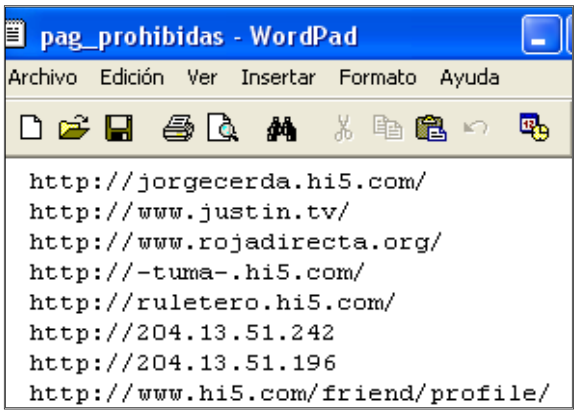


Figura 3. 43. Archivo que contiene paginas prohibidas.

Una vez configurado, se debe crear el swap directory con el comando squid –z; ver figura 3.44.

```
# squid -z
2010/09/11 17:52:26| Creating Swap Directories
```

Figura 3. 44. Creación del swap directory.

Luego corremos el demonio con squid; ver figura 3.45.

```
# squid -z
2010/09/11 17:52:26| Creating Swap Directories
# squid
```

Figura 3. 45. Demonio.

Y si modificamos las listas de acceso o algo de la configuración, debemos aplicar el comando squid –k reconfigure después de haber hecho las modificaciones.

3.6.1.3 Pruebas

Siguiendo con la metodología mencionada con anterioridad, se realizan las pruebas para verificar el funcionamiento correcto de nuestro mecanismo. Para ello una vez terminado de

instalar y configurar nuestro proxy, sólo hay que asignar una IP a la máquina que queremos que quede bajo el régimen de dicho dispositivo.

Por ejemplo, asignamos a un equipo con Windows la IP 192.168.187.5, la cual va a estar dentro de las IP restringidas; ver figura 3.46.

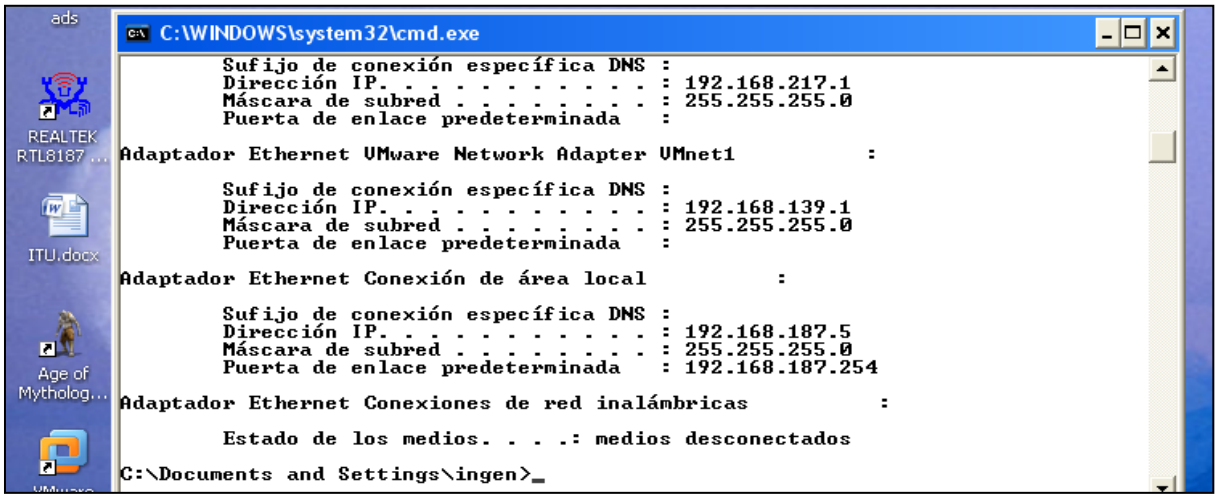


Figura 3. 46. Configuración de IP.

La IP 192.168.187.5 tendrá acceso a Internet, pero si escribimos en un explorador como Google una palabra que se encuentre dentro del archivo de palabras filtradas, no nos permite el acceso a la página condicha palabra. Por ejemplo, vamos a filtrar las páginas que contengan la palabra sexo; ver figura 3.47.

Figura 3. 47. Prueba de palabras filtradas

Si la configuración del proxy fue la correcta deberá mostrar un aviso como el que sigue:

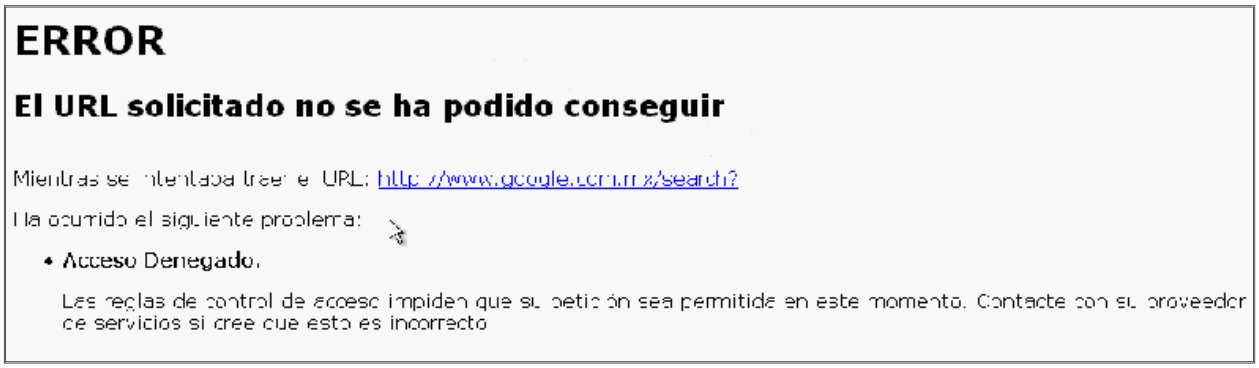


Figura 3. 48. Palabra filtrada.

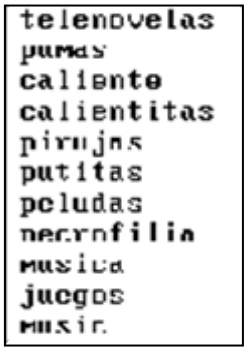


Figura 3. 49. Lista de palabras filtradas.

Si no está dentro de las palabras filtradas, si se podrá hacer la búsqueda; figura 3.50.

Figura 3. 50. Palabra no filtrada.

Lo mismo pasa con las páginas, sólo hay que editar el archivo que contenga las páginas que se desea filtrar; ver figuras 3.51 y 3.52.

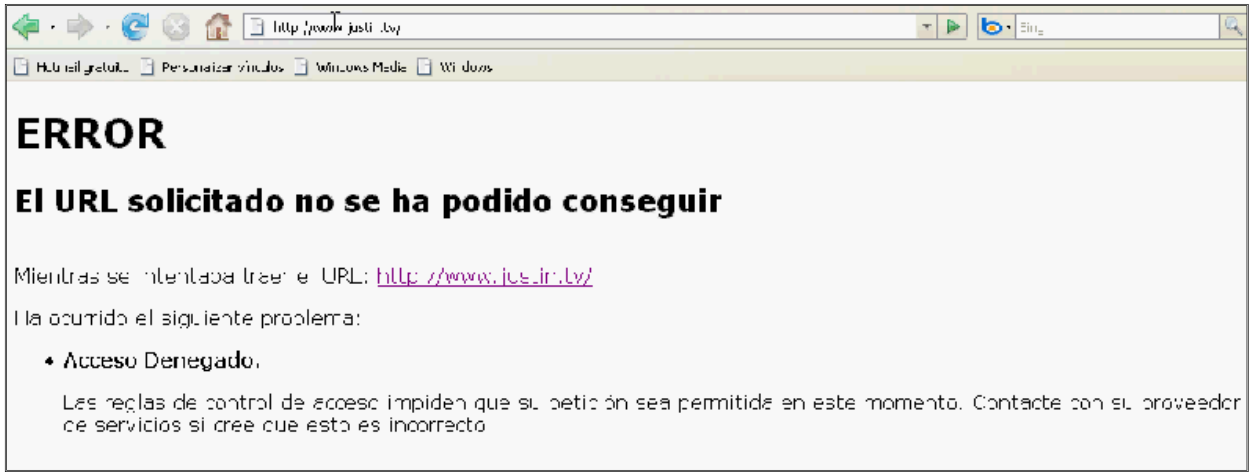


Figura 3. 51. Páginas filtradas.

Figura 3. 52. Archivo con las páginas filtradas.

Si queremos que la IP tenga acceso completo sólo hay que darla de alta en el archivo que contenga las IP's con acceso; ver figura 3.53 y 3.54.

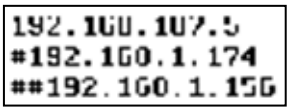


Figura 3. 53. Lista de IP´s con acceso ilimitado.

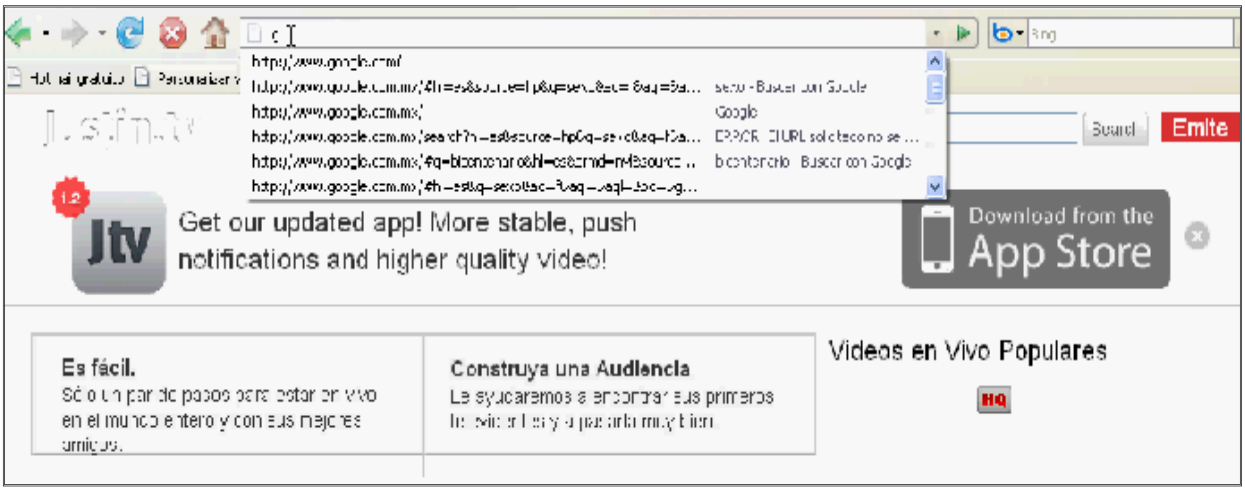


Figura 3. 54. IP con acceso ilimitado.

3.6.2 Desarrollo de aplicación para la administración del equipo

Para evitar el problema de pérdida de equipo, así como para tener una mejor administración de los equipos de la institución al momento de realizar un cambio, una actualización o mantenimiento, se propone realizar un sistema de inventario, el cual permita acceder desde la red, consiguiendo así la portabilidad del sistema, Para ello se presenta una base de datos tomando en cuenta que se pueden quitar o aumentar campos de las tablas, al igual que el diseño de la presentación del sistema puede ser modificada como lo requiera la dependencia.

En la figura 3.55 se presenta el diagrama entidad-relación de la base de datos para el sistema mencionado y en la figura 3.56 se muestra el diagrama lógico obtenido a partir del diagrama entidad-relación.

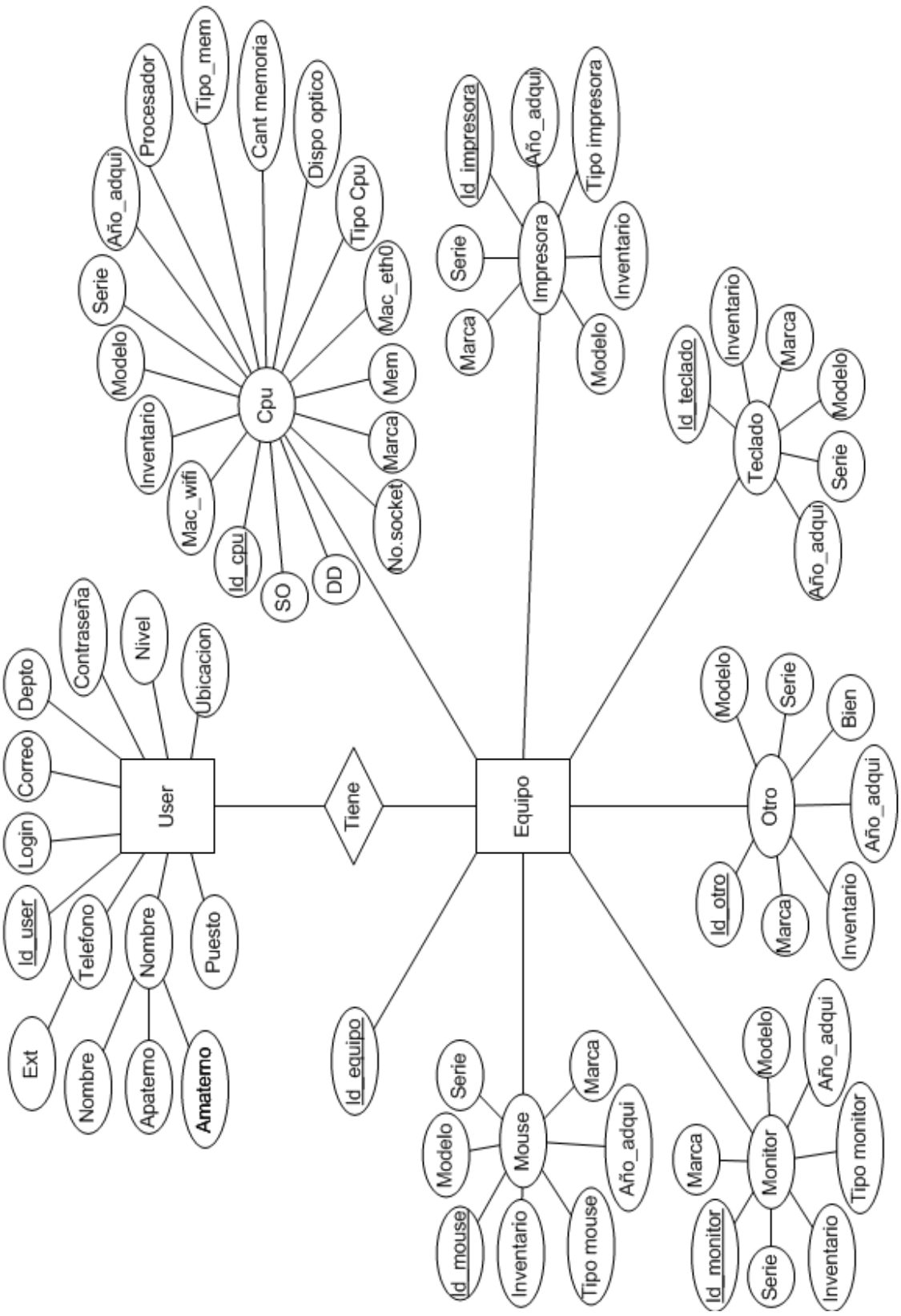


Figura 3. 55. Diagrama entidad relación de la base de datos.

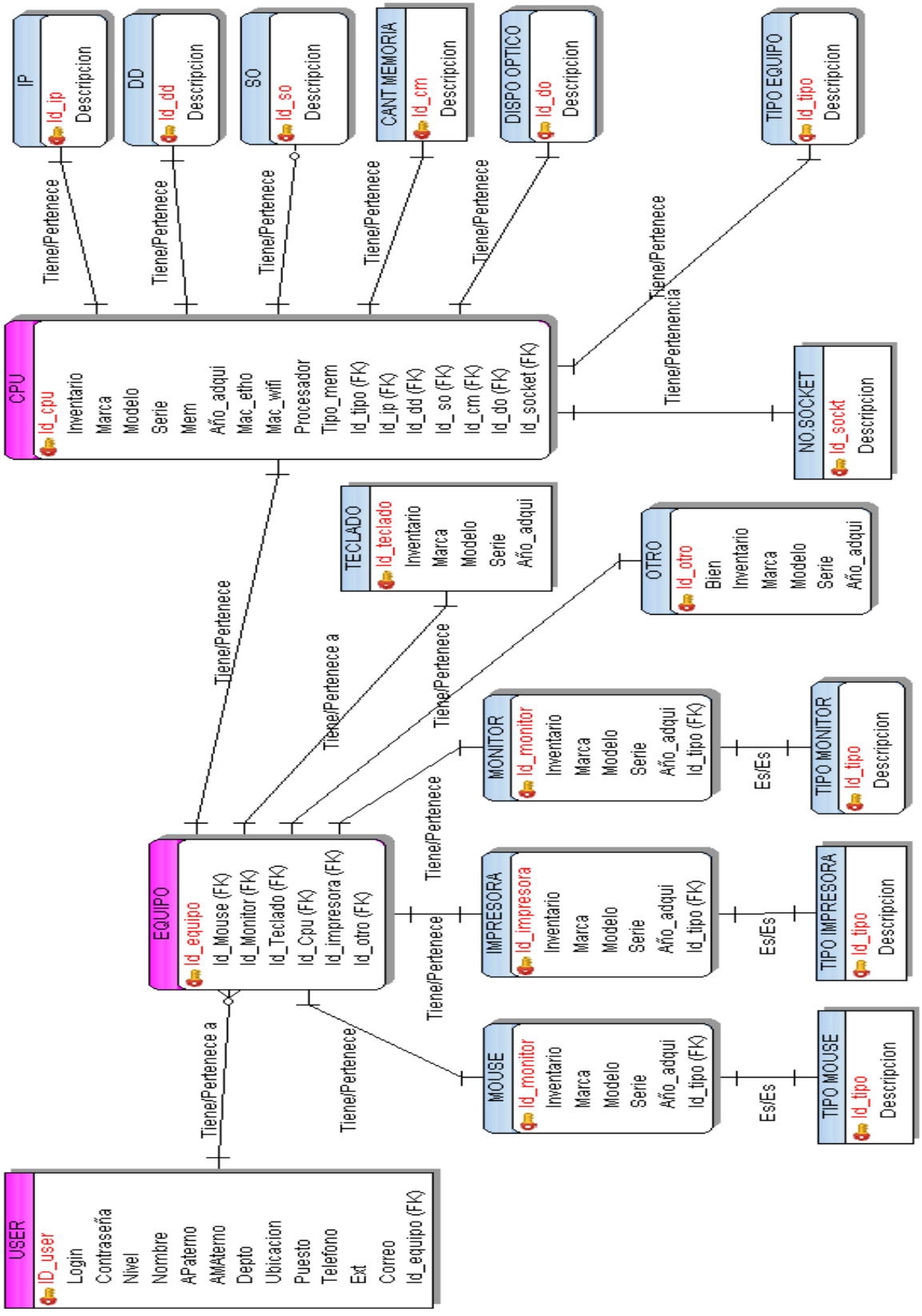


Figura 3. 56. Diagrama lógico de la base de datos.

La aplicación elaborada a partir de la base de datos anterior puede tener lo siguiente:

Una ventana de bienvenida controlando el acceso con un usuario y contraseña; ver figura 3.57.

Figura 3. 57. Ventana de acceso.

Una vez logrado el acceso, se muestra una siguiente página, que contiene un menú, en el cual da la opción de ingresar nuevo equipo, hacer una consulta, ya sea por bien o por dispositivo, por ejemplo, por monitores, teclados, etcétera; del mismo modo nos permite hacer una impresión en archivo .pdf de la misma vista, dicha impresión sirve como un reporte de los bienes de la dependencia; ver figura 3.58.

Figura 3. 58. Menú.

Si se da click en el botón que dice “pdf directorio” muestra un listado con el directorio del personal de la institución como un archivo pdf, ver figura 3.59.

Figura 3. 59. Archivo pdf.

Ahora bien, si requiere ver la relación de los teclados que hay en la dependencia, sólo basta dar click en el botón que dice “teclados” del menú que aparece en la figura 3.58, para que lo muestre. De una forma parecida sucede para el caso de los demás botones que dicen monitores, cpu, mouse, otros bienes, muestran la relación en una ventana, donde aparecen los datos correspondientes a cada bien, como se muestra en la figura 3.60.

Figura 3. 60. Relación de teclados.

Para el caso de si se deseara ingresar un nuevo equipo al sistema, se diseña un formulario donde pida los datos como nombre del usuario del bien, datos del cpu, monitor, mouse, teclado, impresora, y otros bienes que no todos los usuarios tienen en común, como se muestra en las figuras 3.61, 3.62 y 3.63.

Figura 3. 61. Formulario para el ingreso de nuevo equipo.

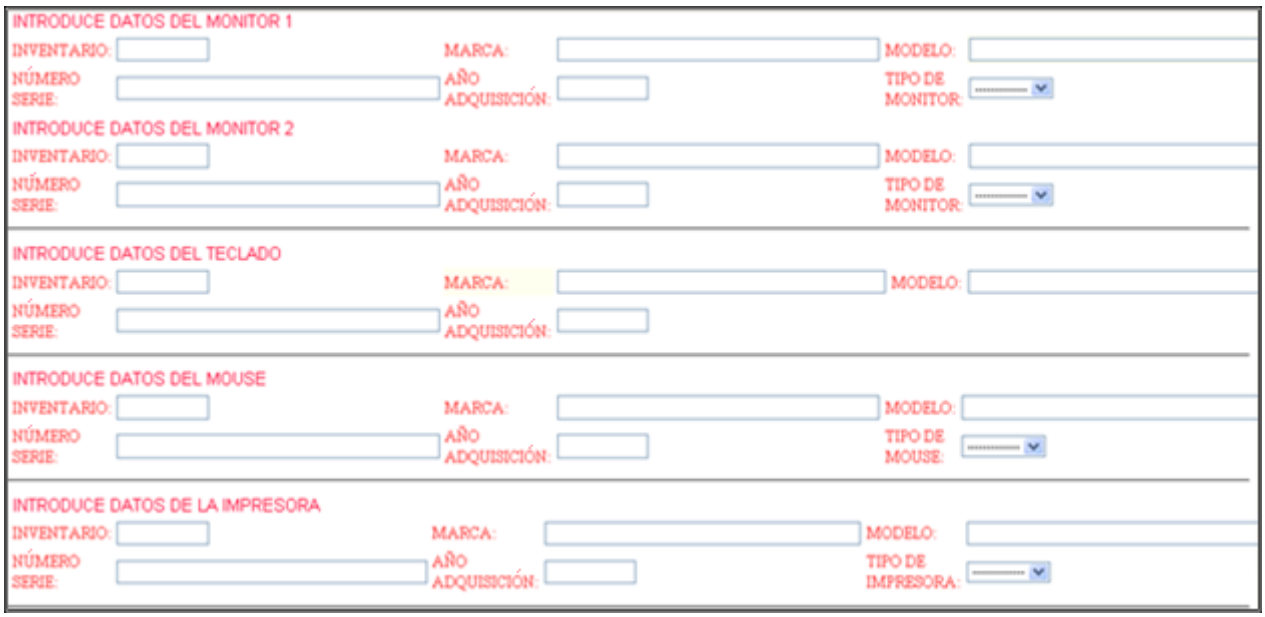


Figura 3. 62. Formulario para el ingreso de nuevo equipo.

Figura 3. 63. Formulario para el ingreso de nuevo equipo.

Se tiene en el menú de la figura 3.58 un botón que dice usuario, este botón permite visualizar la relación de los usuarios a cargo de un equipo de cómputo en la dependencia en una nueva página; además de que esta página cuenta con una búsqueda, da la opción de generar un reporte; ver figuras 3.64 y 3.65.

Figura 3. 64. Relación de los usuarios.

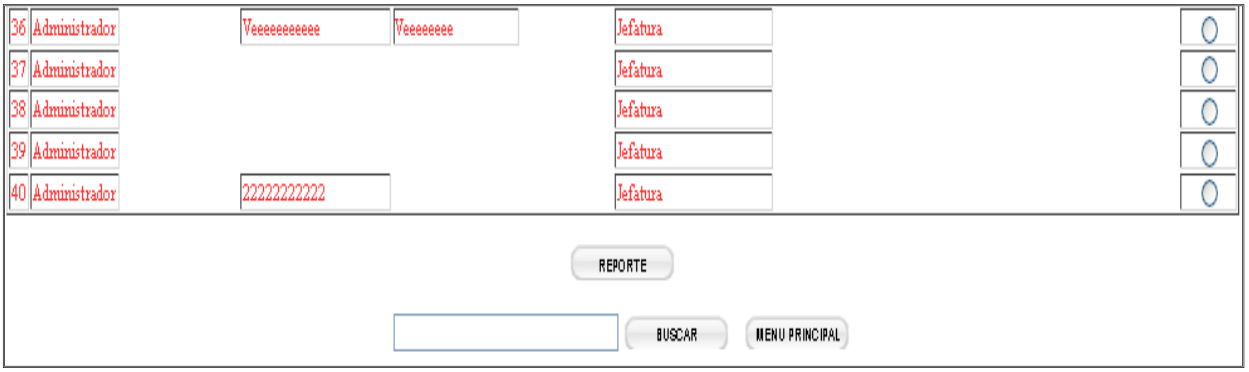


Figura 3. 65. Relación de los usuarios.

Al pedir el reporte del usuario, nos muestra una ventana con todos los datos del usuario seleccionado, además de la información sobre todos los bienes a su cargo, esta misma página permite actualizar la información presentada, así como da la oportunidad de crear un archivo PDF al seleccionar el botón de resguardo con el resumen del equipo; ver figuras 3.66 y 3.67.

Figura 3. 66. Reporte de los usuarios.

Figura 3. 67. Reporte de los usuarios.

Al momento de pedir el resguardo, se despliega un archivo .pdf con la información de los bienes, a cargo del usuario seleccionado con anterioridad; ver figuras 3.68 y 3.69.

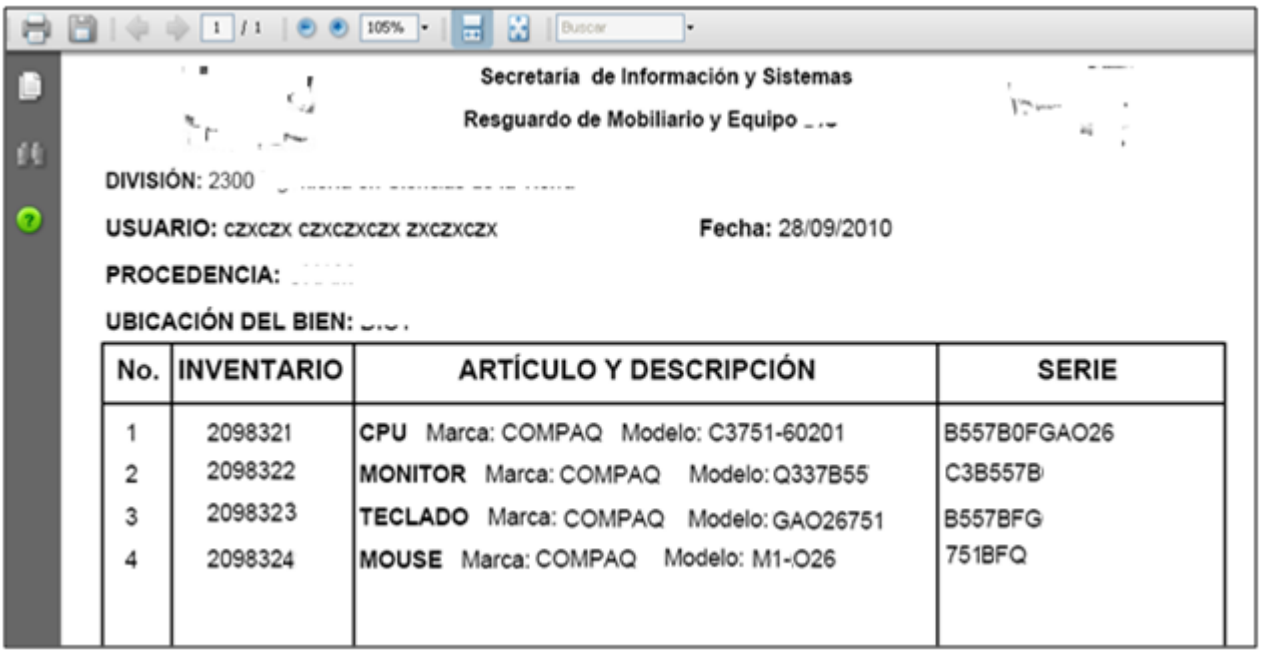


Figura 3. 68. Resguardo de los usuarios.

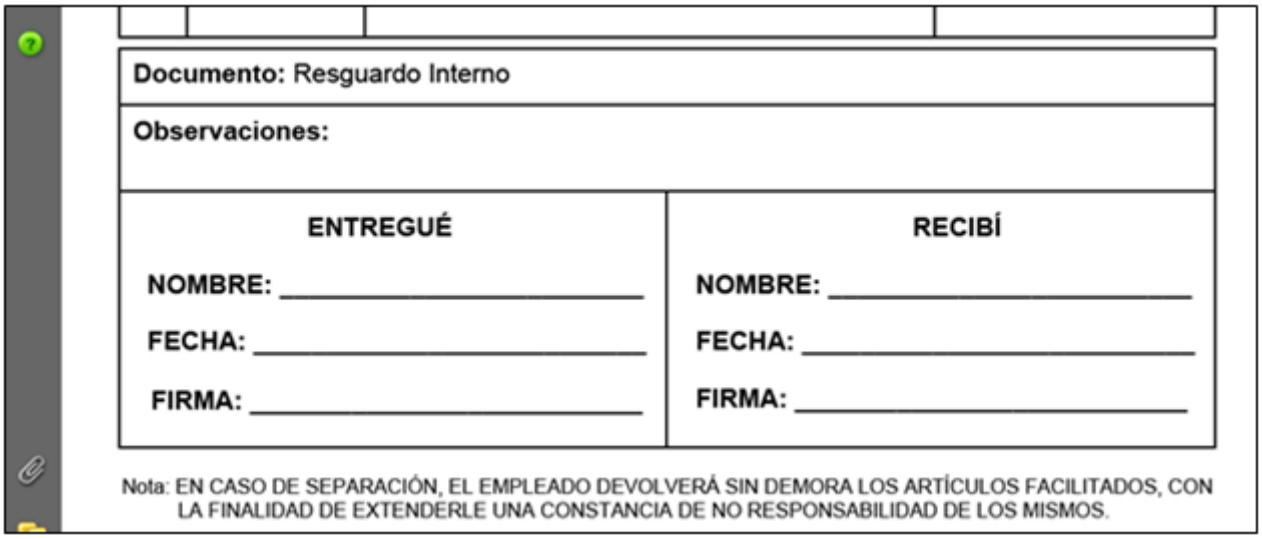


Figura 3. 69. Resguardo de los usuarios.

El archivo PDF mostrado en las figuras 3.68 y 3.69 recibe el nombre de resguardo interno. Este archivo se imprime para ser firmado por el administrador de los equipos y el usuario que ocupará el equipo, se firma este documento como un instrumento que avala las condiciones, al tiempo en que se describe el equipo entregado al empleado para realizar sus tareas laborales; el empleado debe tomar en cuenta que al firmar se compromete a cuidar los bienes entregados y reportar si llegasen a sufrir algún daño o pérdida.

3.7 Mantenimiento

Para la etapa de mantenimiento de la metodología ocupada durante este proyecto se recomienda a los administradores actualizar la base de datos con la información que se vaya generando por movimiento, adquisición o baja de equipos, realizar los cambios al sistema si se requieren, dar continuidad a las políticas desarrolladas, no dejar de hacer las anotaciones debidas en la bitácora, mantener actualizados los antivirus y, sobre todo, nunca bajar la guardia en el aspecto que involucre la seguridad.

CAPÍTULO 4

RESULTADOS E IMPACTOS

4.1 Resultados

Los resultados obtenidos durante la realización de este trabajo fueron ampliamente satisfactorios, debido entre otras cosas a que se contó con el apoyo del equipo del departamento de cómputo de la institución, permitiendo alcanzar el objetivo planteado en el capítulo llamado Introducción, el cual consiste en analizar los niveles de seguridad de la dependencia

Al final, este trabajo no sólo quedó en el ámbito de lo teórico ni en el análisis de los niveles de seguridad, ya que, tras apreciarse en su utilidad, se vio coronada con la implementación de un sistema de inventario para el control de la administración de los recursos informáticos de la dependencia, que incluye un directorio de las direcciones IP al conocer a quién pertenece un dirección determinada.

La consecuencia de la implementación de este sistema es la reducción en la pérdida del equipo. Antes del desarrollo del sistema, la información sobre la ubicación y el estado de los equipos era almacenada de los recuerdos de los administradores, quedando susceptible a olvidos; ahora con el desarrollo propuesto del sistema de inventario se obtiene una mayor confianza y exactitud con respecto a la localización correcta de la información en dispositivos de almacenamiento.

Al mismo tiempo, las usurpaciones en el servicio de red se ven minimizadas, ya que, antes no se tenía control sobre las direcciones IP, lo cual generaba duplicidad. La asignación de la IP se hacía a discreción de acuerdo al criterio de cada administrador, dando como consecuencia una información incompleta, este problema se corrige al momento de tener un directorio de direcciones IP que es el mismo para todos los administradores de los recursos informáticos de la dependencia, disminuyendo así los reportes, que eran aproximadamente de tres por mes, a uno cada seis meses.

Estas consecuencias se constatan porque hasta la fecha no se han recibido nuevas notificaciones por parte de usuarios afectados o por supervisores del tráfico de la red.

Con el desarrollo del firewall se mejoró el uso de la red reduciendo en gran medida la carga sobre ella, debido a que el personal de la dependencia en general ya no la utiliza para tareas que no tiene asignadas y que generalmente caían en el ámbito del ocio o de lo lúdico. Cuando esto no era controlado provocaba que los usuarios realizaran sus labores con distracciones, tales como los juegos en internet, descarga de música y más.

Con la realización de un plan de contingencias y una bitácora, podemos obtener una mejor respuesta a los problemas que se presentan de una forma rápida y precisa. En el ánimo del personal de la dependencia, saberse usuarios de servicios modernos, atendidos por personal calificado y profesional.

Al hacer un plan de contingencias, se obtuvo un manual sobre cómo actuar en diferentes situaciones, en las cuales pudiera verse involucrado el equipo de cómputo y el servicio de red de la dependencia. Se destacó la importancia de hacer respaldos en los servicios críticos, así como la actualización de los equipos en los que reside la página web, el servicio de correo electrónico, servidores de información, NAT, firewall, DNS, DHCP, entre otros.

Con la implementación de la bitácora se puede llevar un seguimiento más claro de las actividades del departamento de cómputo de la dependencia. Lo que es de suma importancia y ayuda para los responsables del departamento, ayudándolos en la organización y planeación de sus actividades, entre las cuales destacan las actualizaciones del software instalado en los equipos. Como ejemplo, está la actualización del software de antivirus que ha aumentado de un 40% a un 90% en su funcionalidad. La bitácora provee un medio eficaz para minimizar el tiempo de reacción, sobre todo ante los casos que se presentaban de forma recurrente.

Con las políticas de seguridad se logró establecer límites a los usuarios al controlar lo que tienen permitido hacer y lo que no en la red. Las políticas se fortalecieron con el firewall desarrollado. De esta manera se implementó una medida para cuidar los bienes y servicios de la dependencia.

Con las herramientas que permiten analizar la complejidad de las contraseñas, se aumentó la seguridad en el acceso a la información, en proporción al incremento de la dificultad para poder descifrarlas.

Todas las implementaciones antes mencionadas contribuyen a mejorar la situación de la dependencia al aumentar su seguridad y al calificar positivamente varios procesos de los diferentes dominios analizados. Lo anterior queda sustentado al aplicar nuevamente la metodología COBIT e ISO 17799 para ver una comparativa del antes y después de haber implementado la propuesta de solución a la problemática de la dependencia.

Así, al implementar COBIT con el mismo criterio con que se obtuvo la tabla 3 se consigue la siguiente tabla:

Tabla 11. Resumen de los resultados de COBIT.

Dominio	Proceso	Criterios de Información								Recursos de TI				
		Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad		Recursos Humanos	Aplicaciones	Tecnología	Instalaciones	Datos
Planeación y organización														
PO1	Definir un plan estratégico de TI	P	S							✓				
PO2	Definir la arquitectura de información	P	S	S	S					✓			✓	
PO3	Determinar la dirección tecnológica	P	S							✓				
PO4	Definir la organización y relaciones de TI	P	S							✓				
PO5	Manejar la inversión en TI	P	P					S		✓				
PO6	Comunicar las directrices gerenciales	P					S			✓				
PO7	Administrar recursos humanos	P	P							✓				
PO8	Asegurar el cumplir requerimientos externos	P					P	S		✓			✓	
PO9	Evaluar riesgos	S	S	P	P	P	S	S		✓				
PO10	Administrar proyectos	P	P	S	S			S		✓				
PO11	Administrar calidad	P	P		P			S		✓				
Adquisición e implementación														
AI1	Identificar soluciones	P	P					S		✓	✓	✓	✓	✓
AI2	Adquisición y mantener software de aplicación	P	P		S	S	S	S			✓			✓
AI3	Adquirir y mantener arquitectura de TI	P	P		S							✓		
AI4	Desarrollar y mantener procedimientos relacionados con TI	P	P		S		S	S			✓			✓
AI5	Instalar y acreditar sistemas	P			S	S					✓			✓
AI6	Administrar cambios	P	P		P	P		S		✓	✓	✓	✓	✓
Servicios y soporte														
DS1	Definir niveles de servicio	P	P	S	S	S	S	S		✓	✓	✓	✓	✓
DS2	Administrar servicios de terceros	P	P	S	S	S	S	S		✓	✓	✓	✓	✓
DS3	Administrar desempeño y capacidad	P	P			S				✓	✓	✓	✓	✓
DS4	Asegurar servicio continuo	P	S			P				✓	✓	✓	✓	✓
DS5	Garantizar la seguridad de sistemas			P	P	S	S	S		✓	✓	✓	✓	✓
DS6	Identificar y asignar costos		P					P		✓				
DS7	Capacitar usuarios	P	S							✓				
DS8	Asistir a los clientes de TI	P								✓				
DS9	Administrar la configuración	P				S		S			✓		✓	✓
DS10	Administrar problemas e incidentes	P	P			S				✓	✓	✓	✓	✓
DS11	Administrar datos				P			P						✓
DS12	Administrar instalaciones				P	P							✓	
DS13	Administrar operaciones	P	P		S	S				✓				
Monitoreo														
M1	Monitorear los procesos	P	S	S	S	S	S	S		✓	✓	✓	✓	✓
M2	Evaluar lo adecuado del control interno	P	P	S	S	S	S	S		✓	✓	✓	✓	✓
M3	Obtener aseguramiento independiente	P	P	S	S	S	S	S		✓	✓	✓	✓	✓
M4	Proveer auditoría independiente	P	P	S	S	S	S	S		✓	✓	✓	✓	✓

Como se puede observar en la tabla 11, la seguridad de la dependencia aumentó, ya que, se logró cubrir procesos PO1, PO3, AI1, AI2, AI4, AI5, DS1, DS2, DS3, DS5, DS7, DS9, DS11, M1 y M4 que no se cubrieron en el primer análisis.

En la tabla 12 se puede observar un resumen de los porcentajes que se obtienen a partir del análisis mostrado en la tabla 11.

Tabla 12. Porcentajes obtenidos de la tabla 11.

Dominio	Procesos a evaluar	Procesos no evaluados	Porcentaje de procesos evaluados	Porcentaje de procesos no evaluados
Planeación y organización	11	0	100 %	0 %
Adquisición e implementación	6	0	100 %	0 %
Servicios y soporte	13	0	100 %	0 %
Monitoreo	4	0	100 %	0 %
TOTAL	34	0	100 %	0 %

Si se aplica nuevamente el cuestionario del ISO 17799 y tomando las consideraciones con las que se generó la lista de verificación que conforma a la tabla 5 se obtiene la tabla 13, que la muestra la situación de la dependencia al implementar las propuestas abordadas en el capítulo anterior.

Tabla 13. Resumen del análisis.

		PREGUNTA DE AUDITORÍA	EXISTE
1 POLÍTICA DE SEGURIDAD	*INFORMACIÓN DE LA POLÍTICA DE SEGURIDAD*		
	SEGURIDAD DE LA INFORMACIÓN POLÍTICA DE DOCUMENTO	¿Existe una política de seguridad de la información, aprobada por la dirección, publicada y comunicada en su caso a todos los empleados?	✓
		¿Se establece el compromiso de la dirección y el enfoque de la organización para la gestión de seguridad de la información?	✓
	REVISIÓN Y EVALUACIÓN	¿La política de seguridad tiene un propietario, el cual es responsable de su mantenimiento y revisión con apego a un proceso de revisión	✓

		definido?	
		¿El proceso garantiza que la revisión se lleva a cabo en respuesta a los cambios que afectan a la base de la evaluación inicial?, por ejemplo: los incidentes de seguridad significativos, nuevas vulnerabilidades o cambios en la infraestructura técnica o de organización.	✓
2 ORGANIZACIÓN DE SEGURIDAD	*INFORMACIÓN DE LA INFRAESTRUCTURA DE SEGURIDAD*		
	INFORMACIÓN DE GESTIÓN DE SEGURIDAD EN EL FORO	¿Existe un foro de gestión para asegurarse de que existe una dirección clara y apoyo a la gestión visible para las iniciativas de seguridad dentro de la organización?	✓
	COORDINACIÓN DE INFORMACIÓN DE LA SEGURIDAD	¿Existe un foro funcional con representantes de la dirección y partes pertinentes de la organización para coordinar la aplicación de los controles de seguridad de la información?	✓
	ASIGNACIÓN DE LAS RESPONSABILIDADES DE SEGURIDAD DE INFORMACIÓN	¿Se definieron con claridad las responsabilidades para la protección de los activos individuales y para llevar a cabo los procesos de seguridad específicos?	✓
	PROCESO PARA LA AUTORIZACIÓN DE INSTALACIONES DE PROCESAMIENTO DE LA INFORMACIÓN	¿Existe un proceso de autorización de gestión en vigor para cualquier instalación de tratamiento de la información nueva? Esto debería incluir todas las instalaciones nuevas, tanto hardware y software.	✓
	ESPECIALISTA EN SEGURIDAD DE LA INFORMACIÓN ACONSEJA	¿Se obtienen consejos en la seguridad información especializada?	✓
		¿Se puede identificar un individuo con experiencia y conocimientos para coordinar, garantizar la coherencia, y proporcionar ayuda en la toma de decisiones de seguridad?	✓
	COOPERACIÓN ENTRE LAS ORGANIZACIONES	¿La cooperación adecuada con las autoridades, los organismos reguladores, proveedores de servicios de información y los operadores de telecomunicaciones se mantuvieron para garantizar que las medidas adecuadas y los dictámenes pueden ser rápidamente adoptadas, en el caso de un incidente de seguridad?	✓
	REVISIÓN INDEPENDIENTE DE SEGURIDAD DE LA INFORMACIÓN	¿La política de seguridad se revisa de forma independiente de manera regular, para garantizar que las prácticas de la organización reflejan adecuadamente la política, y que es factible y eficaz?	✓
	SEGURIDAD DE ACCESO DE TERCEROS		
	IDENTIFICACIÓN DE LOS RIESGOS DE ACCESO DE TERCEROS	¿Los riesgos de acceso de terceros se identifican y se ponen en práctica los controles de seguridad apropiados?	✓
		¿Los tipos de accesos se identifican, clasifican y las razones para el acceso se justifican?	
		¿Los riesgos de seguridad con los contratistas de terceros en el sitio de trabajo fueron identificados y se aplicaron los controles adecuados?	
	REQUISITOS DE SEGURIDAD EN	¿Existe un contrato laboral que contiene o se refiera a todos los requisitos de seguridad para	

	LOS CONTRATOS DE TERCEROS	garantizar el cumplimiento de las políticas de seguridad de la organización y normas?	
	OUTSOURCING		
	REQUISITOS DE SEGURIDAD EN LOS CONTRATOS DE OUTSOURCING	¿Los requisitos de seguridad se abordan en el contrato con el tercero, cuando la organización ha subcontratado la gestión y control de todos o algunos de sus sistemas de información, redes y / o entornos de escritorio?	
		¿El contrato incluye los requisitos legales que deben cumplir, como la seguridad de la organización y de los activos son mantenidos y probados, el derecho de la auditoría, las cuestiones de seguridad física y la forma en que se mantendrá en caso de desastre la disponibilidad de los servicios?	
3 CLASIFICACIÓN DE LOS ACTIVOS Y EL CONTROL	*RENDICIÓN DE CUENTAS DE LOS ACTIVOS*		
	INVENTARIO DE LOS BIENES	¿Se mantiene un inventario o registro con los activos importantes asociados a cada sistema de información?	✓
	CLASIFICACIÓN DE LA INFORMACIÓN	¿Cada uno de los activos identificados tiene un propietario, una clasificación de seguridad definida y acordada y un lugar indicado?	✓
	DIRECTRICES DE CLASIFICACIÓN	¿Existe un sistema de clasificación de información o guía en su lugar, lo que ayudará a determinar cómo la información debe ser manejada y protegida?	
	INFORMACIÓN DE ETIQUETADO Y MANIPULACIÓN	¿Existe un conjunto adecuado de los procedimientos definidos para la información de etiquetado y manipulación, de acuerdo con el esquema de clasificación, adoptada por la organización?	✓
4 SEGURIDAD DEL PERSONAL	*SEGURIDAD EN LA DEFINICIÓN DE PUESTOS DE TRABAJO Y RECURSOS*		
	SEGURIDAD EN LAS RESPONSABILIDADES DEL TRABAJO	¿Las funciones y responsabilidades de seguridad según lo establecido en la política seguridad de la información de la organización se documentan?	✓
		¿Se incluyen las responsabilidades generales de aplicación o el mantenimiento de la política de seguridad así como las responsabilidades específicas para la protección de determinados bienes o para la ampliación de los procesos de seguridad o actividades?	✓
	PERSONAL DE INSPECCIÓN Y LA POLÍTICA	¿Los controles de verificación del personal permanente se llevaron a cabo en el momento de las solicitudes de empleo?	✓
		¿Incluye títulos académicos del profesional la referencia del carácter, la confirmación del reclamado y la identidad de los controles independientes?	✓
	ACUERDOS DE CONFIDENCIALIDAD	¿Los empleados firman un acuerdo de confidencialidad, como parte de los términos y condiciones iníciales del empleo?	
		¿Este acuerdo se refiere a la seguridad de la planta de procesamiento de la información y los	

		activos de la organización?	
	TÉRMINOS Y CONDICIONES DE EMPLEO	¿Los términos y condiciones del empleo abarcan la responsabilidad del empleado en cuanto a la seguridad de la información?	
	FORMACIÓN DE USUARIOS		
	INFORMACIÓN, EDUCACIÓN Y FORMACIÓN DE SEGURIDAD	¿Todos los empleados de la organización y usuarios terceros reciben información adecuada de formación de seguridad y actualizaciones regulares en las políticas y procedimientos de organización?	✓
	EN RESPUESTA A INCIDENTES DE SEGURIDAD Y MAL FUNCIONAMIENTO		
	PRESENTACIÓN DE INFORMES DE INCIDENTES DE SEGURIDAD	¿Existe un procedimiento de notificación formal, para reportar los incidentes de seguridad a través de canales de gestión adecuadas tan pronto como sea posible?	✓
	INFORMES DE DEBILIDADES DE SEGURIDAD	¿Existe un procedimiento de notificación formal dirigido a los usuarios, para informar la debilidad en la seguridad, o las amenazas a los sistemas o servicios?	✓
	INFORMES DE MAL FUNCIONAMIENTO DEL SOFTWARE	¿Se establecen procedimientos para reportar cualquier mal funcionamiento del software?	✓
	APRENDIENDO DE LOS INCIDENTES	¿Se dispone de mecanismos que permitan cuantificar y monitorear los tipos de averías, volúmenes y costos de los incidentes?	
	PROCESO DISCIPLINARIO	¿Existe un proceso disciplinario formal para empleados que han violado las políticas de seguridad y los procedimientos de la organización?	✓
5 SEGURIDAD FÍSICA Y AMBIENTAL	*ÁREA SEGURA*		
	PERÍMETRO DE SEGURIDAD FÍSICA	¿Qué frontera de protección de la instalación física se ha implementado para proteger el servicio de procesamiento de la información? Algunos ejemplos son el control de tarjeta de puerta de entrada, paredes, recepción, etc.,	Puertas con llave
	CONTROLES DE ENTRADA FÍSICA	¿Qué controles de entrada permiten que sólo el personal autorizado entre en distintas áreas de la organización?	Puertas con llave, personal del área
	OFICINAS DE PROTECCIÓN, HABITACIONES E INSTALACIONES	¿Las habitaciones, que tienen el servicio de procesamiento de la información, se han bloqueado?, ejemplo armarios con llave o caja fuerte.	Puertas con llave
		¿El servicio de procesamiento de la información es protegida por el hombre de desastres naturales?	
		No existe cualquier amenaza potencial de los establecimientos vecinos.	✓
	TRABAJO EN ÁREAS SEGURAS	¿Existe algún control de seguridad para terceros o para el personal que trabaja en un área segura?	✓

	ENTREGA AISLADOS Y ZONAS DE CARGA	¿El área de prestación y el área de procesamiento de la información están aisladas unos de otras para evitar cualquier acceso no autorizado?	
		¿Se llevó a cabo, una evaluación de riesgos para determinar la seguridad en esas zonas?	✓
	EQUIPO DE SEGURIDAD		
	EQUIPOS DE PROTECCIÓN	¿El equipo se encuentra en el lugar adecuado para minimizar el acceso innecesario a las áreas de trabajo?	✓
		¿Los elementos que requieren una protección especial fueron aislados para reducir el nivel general de protección requerido?	✓
		¿Los controles fueron adoptados para minimizar el riesgo de las amenazas potenciales?, tales como incendios, explosivos, humo, agua, vibraciones, efectos químicos, el suministro de interfaces eléctricas, radiación electromagnética, las inundaciones.	✓
		¿Existe una política hacia el comer, beber y fumar en las proximidades de los servicios de procesamiento de la información?	✓
		¿Las condiciones ambientales que pueden afectar las instalaciones de procesamiento de la información son monitoreadas?	✓
	FUENTES DE ALIMENTACIÓN	¿El equipo está protegido contra fallas de energía mediante el uso de la permanencia de fuentes de alimentación, tales como múltiples fuentes, sistema de alimentación ininterrumpida (UPS), generador de respaldo, etc?	
	CABLEADO	¿El cable de alimentación y de telecomunicaciones que llevan los datos o el apoyo a los servicios de información están protegidos de la intercepción o daño?	✓
		¿Hay controles de seguridad adicionales en un lugar crítico o información confidencial.	✓
	MANTENIMIENTO DE EQUIPO	¿El equipo se mantiene por los intervalos de servicio y las especificaciones como lo recomienda el proveedor?	
		¿El mantenimiento se lleva a cabo únicamente por personal autorizado?	✓
		¿Los registros se mantienen con todos los defectos reales o presuntos y todas las medidas preventivas y correctivas?	✓
		¿Se aplican los controles adecuados durante el envío de equipos fuera de las instalaciones'	
		¿El equipo está cubierto por el seguro?	✓
	PROTEGER LOS EQUIPOS FUERA DE LAS INSTALACIONES	¿Cualquier uso del equipo fuera de la organización tiene que ser autorizada por la dirección?	✓
		¿La garantía de estos equipos, mientras están fuera, están a la par con uno o más de la garantía de los están dentro de las instalaciones?	

	ASEGURE SU ELIMINACIÓN O REUTILIZACIÓN DE LOS EQUIPOS	¿El dispositivo de almacenamiento que contienen información sensible son destruidos físicamente o bien sobrescrito?	✓
	CONTROLES GENERALES		
	INFORMACIÓN CLARA Y LA POLÍTICA DE PANTALLA CLARA	¿La pantalla de bloqueo automático de la computadora está activada?	✓
		¿A los empleados se les aconseja que cualquier material confidencial en la forma de documentos en papel, medios de comunicación, etc., se encuentren de una manera cerrada mientras esté desatendida?	✓
	ELIMINACIÓN DE LA PROPIEDAD	¿El equipo, información o software se pueden tomar fuera de las instalaciones sin la debida autorización?	
		¿Se llevaron a cabo auditorías periódicas para detectar la retirada no autorizada de la propiedad?	
		¿Se concientizan a las personas de las auditorías periódicas?	✓
6 COMUNICA-CIONES Y GESTIÓN DE OPERACIONES	*PROCEDIMIENTO OPERATIVO Y RESPONSABILIDADES*		
	PROCEDIMIENTOS DOCUMENTADOS DE OPERACIÓN	¿La política de seguridad ha identificado los procedimientos operativos como respaldos, mantenimiento, equipos, etc.?	✓
		¿Los procedimientos son documentados e implementados?	✓
	OPERACIONAL DE CAMBIO DE CONTROL	¿Todos los programas que se ejecutan en los sistemas de producción están sujetos a cambio?	✓
		¿Los registros de auditoría se mantienen para cualquier cambio realizado en los programas de producción?	✓
	INCIDENTES DE LOS PROCEDIMIENTOS DE GESTIÓN	¿Existe un procedimiento de Gestión de Incidentes para tratar los incidentes de seguridad?	✓
		¿El procedimiento se refiere a la responsabilidades de manejo de incidentes, ordenada y rápida respuesta a incidentes de seguridad?	✓
		¿El procedimiento de direcciones de diferentes tipos de incidentes va desde la denegación de servicio a la violación de la confidencialidad, etc., y las maneras de manejarlos?	✓
		Independientemente de que los caminos y registros relativos a los incidentes ¿se toman y se mantienen medidas proactivas de manera que el incidente no vuelva a ocurrir?	✓
	SEPARACIÓN DE LAS FUNCIONES	¿Los derechos y las áreas de responsabilidad se separan con el fin de reducir las posibilidades de modificación no autorizada o mal el uso de la información o de los servicios?	✓

	LA SEPARACIÓN DE DESARROLLO E INSTALACIONES OPERATIVAS	¿El desarrollo y las instalaciones de prueba están aislados de las instalaciones operativas?	✓
	EXTERNOS DE GESTIÓN DE INSTALACIONES	¿Alguna de las instalaciones de procesamiento de la información es administrada por una empresa externa o contratista (tercero)?	
		¿Los riesgos asociados a dicha gestión se identifican con antelación, se discuten con el tercero y los controles adecuados se incorporaron en el contrato?	
		¿La aprobación necesaria se obtiene de la aplicación y los dueños de negocios?	
	SISTEMA DE PLANIFICACIÓN Y LA ACEPTACIÓN		
	PLANIFICACIÓN DE LA CAPACIDAD	¿La capacidad de las demandas son monitoreados y se hacen proyecciones de futuros requerimientos de capacidad?, esto es para asegurar que el proceso de alimentación y de almacenamiento estén disponibles. Ejemplo: Control de espacio en disco duro, RAM, CPU en servidores críticos.	✓
	SISTEMA DE ACEPTACIÓN	¿En la aceptación del sistema se establecen criterios para nuevos sistemas de información, actualizaciones y nuevas versiones?	✓
		¿Las pruebas adecuadas se llevaron a cabo antes de la aceptación?	✓
	PROTECCIÓN CONTRA SOFTWARE MALICIOSO		
	CONTROL CONTRA SOFTWARE MALICIOSO	¿Existe algún tipo de control contra el uso de software malicioso?	✓
		¿La política de seguridad se ocupa de cuestiones de licencias de software tales como la prohibición de uso de software no autorizado?	✓
		¿Existe algún procedimiento para verificar que todos los boletines de alerta son precisos e informativos en relación con el uso de software malicioso?	✓
		¿El software antivirus se instala en los equipos para verificar y aislar o eliminar cualquier virus de computadora y los medios de comunicación?	✓
		¿Se actualiza la firma de software de forma periódica para comprobar que se cuenta con la base de virus más reciente?	✓
	LIMPIEZA		
	INFORMACIÓN DE RESERVA	¿Se toma con regularidad el respaldo de información del servidor de producción, componentes de red críticos, backup de la configuración, etc.? Ejemplo: de lunes a jueves: de copia de seguridad incremental y viernes: de copia de seguridad completa.	✓

		¿Los medios de copia de seguridad junto con el procedimiento para restaurar la copia de seguridad se almacenan de forma segura y lejos del sitio real?	
		¿Los medios de copia de seguridad se examinan regularmente para asegurarse de que pudieran ser restaurados en el marco de tiempo asignado en el procedimiento operativo para la recuperación?	✓
	OPERADOR DE REGISTROS	¿Tanto el personal operativo mantiene un registro de sus actividades, como el nombre de la persona, errores, medidas correctivas, etc.?	✓
		¿Se comprueban los registros del operador de manera regular en contra de los procedimientos de operación?	✓
	FALLO DE REGISTRO	¿Las fallas que se presentan son administradas? Esto incluye las medidas correctivas adoptadas, la revisión de los registros de la falla y verificación de las medidas adoptadas.	✓
	GESTIÓN DE REDES		
	RED DE CONTROL	¿Los controles operacionales, tales como red independiente y administración de recursos del sistema se establecen efectivamente cuando es necesario?	
		¿Se establecieron responsabilidades y procedimientos de gestión de equipos remotos?	
		¿Existen controles especiales para proteger la confidencialidad e integridad de procesamiento de datos sobre la red pública y así proteger los sistemas conectados? Ejemplo: Redes privadas virtuales, el cifrado y otros mecanismos de hashing, etc.	
	MEDIOS DE MANIPULACIÓN Y DE SEGURIDAD		
	GESTIÓN DE SOPORTES INFORMÁTICOS EXTRAÍBLES	¿Existe un procedimiento para la gestión de los soportes informáticos extraíbles como cintas, discos, casetes de tarjetas de memoria, y los informes?	
	DISPOSICIÓN DE LOS MEDIOS DE COMUNICACIÓN	¿Los medios de comunicación que ya no son necesarios se disponen de forma segura?	✓
		¿La eliminación de los productos sensibles está en el sistema cuando sea necesario a fin de mantener un registro de auditoría?	✓
	INFORMACIÓN DE LOS PROCEDIMIENTOS DE MANIPULACIÓN	¿Existe un procedimiento para el manejo del almacenamiento de la información?	✓
	SEGURIDAD DE LA DOCUMENTACIÓN DEL SISTEMA	¿La documentación del sistema está protegida del acceso no autorizado?	
		¿La lista de acceso para la documentación del sistema se mantiene al mínimo y es autorizado por el propietario de la aplicación?	
	INTERCAMBIO DE INFORMACIÓN Y SOFTWARE		

	INFORMACIÓN Y ACUERDO DE INTERCAMBIO DE SOFTWARE	¿Existe algún acuerdo formal o informal entre las organizaciones para el intercambio de información y software?	✓
		¿El acuerdo no aborda las cuestiones de seguridad basado en la sensibilidad de la información de negocios involucrados?	
	SEGURIDAD DE LOS MEDIOS DE COMUNICACIÓN EN EL TRÁNSITO	¿Existe seguridad en los medios de comunicación durante su traslado?	
		¿Los medios de comunicación están bien protegidos del acceso no autorizado, mal uso o de la corrupción.	✓
	COMERCIO ELECTRÓNICO DE SEGURIDAD	No aplica.	
	SEGURIDAD DE CORREO ELECTRÓNICO	¿Existe una política de seguridad para el uso aceptable del correo electrónico o que se ocupa de las cuestiones con respecto a la utilización del correo electrónico?	✓
		¿Tanto los controles como la comprobación de antivirus, aislando adjuntos potencialmente peligrosos, control de spam, contra la retransmisión, etc. se ponen en marcha para reducir los riesgos creados por correo electrónico?	✓
	SEGURIDAD DE LOS SISTEMAS ELECTRÓNICOS	¿Existe una política de uso aceptable para abordar el uso de sistemas electrónicos?	✓
		¿Existen directrices para controlar eficazmente la seguridad y los riesgos de negocio asociados a los sistemas electrónicos?	
	SISTEMAS DISPONIBLES	¿Existe algún proceso de autorización formal para la información que se pondrá a disposición del público?	✓
		¿Existe controles para proteger la integridad de dicha información a disposición del público de cualquier acceso no autorizado, como firewalls, sistema operativo endurecido, etc.?	✓
	OTRAS FORMAS DE INTERCAMBIO DE INFORMACIÓN	¿Existen políticas, procedimientos o controles para proteger el intercambio de información a través del uso de la voz, vídeo y servicios de comunicación por fax?	✓
		¿Se les recuerda mantener la confidencialidad de la información sensible durante el uso de estas formas de intercambio de servicio de información?	✓
7 CONTROL DE ACCESO	*REQUERIMIENTOS DE NEGOCIO PARA EL CONTROL DE ACCESO*		
	POLÍTICA DE CONTROL DE ACCESO	¿Los requisitos del negocio para el control del acceso se han definido y documentado?	
		¿La política de control de acceso se ocupa de las normas y derechos para cada usuario o grupo de usuarios?	✓
		¿Los usuarios y proveedores de servicios se les dieron una declaración clara de los requerimientos de negocio que deben cumplir los controles de acceso?	

	GESTIÓN DE USUARIOS DE ACCESO		
	REGISTRO DE USUARIO	¿Existe algún registro de usuario formales y de procedimiento de registro para la concesión de acceso a la información del usuario en sistemas múltiples y servicios?	✓
	GESTIÓN DE PRIVILEGIOS	¿La asignación y el uso de algún privilegio en el entorno del sistema de información es restringido y controlado, es decir, los privilegios se asignan según las necesidades?	✓
	GESTIÓN DE CONTRASEÑAS DE USUARIO	¿La asignación y reasignación de contraseñas se controla a través de un proceso formal de gestión?	✓
		¿Los usuarios se les pide que firmen una declaración de mantener la confidencialidad de la contraseña?	
	REVISIÓN DE LOS DERECHOS DE ACCESO DE LOS USUARIOS	¿Existe un proceso de revisión de los derechos de acceso del usuario a intervalos regulares? Ejemplo: el privilegio especial de revisión cada tres meses, los privilegios normales cada seis meses.	✓
	RESPONSABILIDADES DEL USUARIO		
	USO DE CONTRASEÑAS	¿Existen directrices en el lugar para guiar a los usuarios en la selección y el mantenimiento de contraseñas seguras?	
	SIN VIGILANCIA EQUIPOS DE USUARIO	¿Los usuarios y los contratistas son conscientes de los requisitos y procedimientos de seguridad para la protección de equipos desatendidos, así como su responsabilidad de aplicar esa protección?	
	RED DE CONTROL DE ACCESO		
	POLÍTICA SOBRE EL USO DE LOS SERVICIOS DE RED	¿Existen procedimientos para proteger el acceso a conexiones de red y servicios de red?	✓
	CAMINO FORZADO	¿Existe cualquier control que restringa la ruta entre la terminal del usuario y los servicios informáticos?	
	LA AUTENTICACIÓN DE USUARIOS PARA CONEXIONES EXTERNAS	¿Existen mecanismos de autenticación para impugnar las conexiones externas? Ejemplos: la criptografía basada en la técnica, los tokens de hardware o de software, protocolo de respuesta, etc.	
	PUERTO DE DIAGNÓSTICO A DISTANCIA DE PROTECCIÓN	¿El acceso a los puertos de diagnóstico están bien controlados, es decir, protegidos por un mecanismo de seguridad?	✓
	PROTOCOLOS DE RED DE CONEXIÓN	¿Existe algún control de la conexión de red para redes compartidas que se extienden más allá de los límites de la organización? Ejemplo: correo electrónico, acceso a Internet, transferencia de archivos, etc.	✓
	ENCAMINAMIENTO DE LA RED DE CONTROL	¿Existe alguna red de control para garantizar que las conexiones de computadora y los flujos de información no violen la política de control de	

		acceso de las aplicaciones de negocio?	
		¿Los controles de enrutamiento se basan en la fuente positiva y mecanismo de identificación de destino? Ejemplo: la traducción de direcciones de red (NAT).	✓
	SEGURIDAD DE LOS SERVICIOS DE RED	¿La organización utiliza una red privada de servicios públicos o se asegura de que se proporcione una descripción clara de los atributos de seguridad de todos los servicios utilizados?	✓
	FUNCIONAMIENTO DEL SISTEMA DE CONTROL DE ACCESO		
	IDENTIFICACIÓN AUTOMÁTICA DE TERMINALES	¿Se utiliza un mecanismo terminal de identificación automática para autenticar las conexiones?	✓
	TERMINAL DE INICIO DE SESIÓN SOBRE LOS PROCEDIMIENTOS	¿El acceso al sistema de información es posible sólo a través de una conexión segura en el proceso?	
		¿Existe un procedimiento para iniciar sesión en un sistema de información? Esto es para minimizar la posibilidad de acceso no autorizado.	✓
	IDENTIFICACIÓN DE USUARIO Y AUTORIZACIÓN	¿El identificador único se proporciona a cada usuario, tales como operadores, administradores de sistemas y el resto del personal incluido el técnico?	✓
		¿Las cuentas de usuario genérico sólo deben ser suministradas bajo circunstancias excepcionales en las que hay un beneficio claro?	✓
		¿Existe un método de autenticación para acreditar la identidad declarada de los usuarios (contraseña)?	✓
	CONTRASEÑA DEL SISTEMA DE GESTIÓN	¿Existe un sistema de gestión de contraseñas que impone contraseñas a diversos controles, tales como: contraseña individual para la rendición de cuentas, aplicar los cambios de contraseña, almacenar contraseñas de forma cifrada, no mostrar las contraseñas en pantalla, etc.?	✓
	EL USO DE UTILIDADES DEL SISTEMA	¿Las utilidades del sistema que viene con instalaciones informáticas, pueden reemplazar el sistema de control de aplicaciones y es sometida a estrictos controles?	
	LIMITACIÓN DE TIEMPO DE CONEXIÓN	¿Existe alguna restricción en el tiempo de conexión para aplicaciones de alto riesgo? Este tipo de stands, deberán ser considerados para aplicaciones sensibles a los que los terminales están instalados en lugares de alto riesgo.	
	APLICACIÓN DE CONTROL DE ACCESO		
	INFORMACIÓN DE RESTRICCIÓN DE ACCESO	¿El acceso a la aplicación personal de la organización está definido en la política de control de acceso según el requisito de aplicaciones de negocios individuales y es coherente con la organización de la información política de acceso al archivo?	
	AISLAMIENTO DE SISTEMAS	¿Los sistemas sensibles cuentan con entorno informático aislados como compartir recursos sólo	

	SENSIBLES	con sistemas de aplicaciones de confianza, etc.?	
	CONTROL DEL ACCESO AL SISTEMA Y EL USO		
	REGISTRO DE EVENTOS	¿Los registros de auditoría, excepciones de registro y otros eventos relevantes de seguridad se producen y se mantienen durante un período acordado para ayudar a futuras investigaciones y al seguimiento de control de acceso?	✓
	VIGILANCIA DE LA UTILIZACIÓN DEL SISTEMA	¿Se establecen procedimientos de control en la utilización de instalaciones de procesamiento de información?	✓
		¿El procedimiento debe garantizar que los usuarios están realizando solamente las actividades que están expresamente autorizadas?	✓
		¿Los resultados de las actividades de supervisión se revisan con regularidad?	✓
	SINCRONIZACIÓN	¿El dispositivo de la computadora o la comunicación tiene la capacidad de operar un reloj de tiempo real, se debe establecer en una norma aceptada como coordinado tiempo universal u hora estándar local?	✓
	INFORMÁTICA MÓVIL Y EL TELETRABAJO		
	INFORMÁTICA MÓVIL	¿Existe una política oficial que se adopte, que tenga en cuenta los riesgos de trabajar con recursos informáticos, como portátiles, computadoras de bolsillo, etc. especialmente en entornos desprotegidos?	✓
		¿Existe en la organizaron cursos para el personal a utilizar las instalaciones de computación móvil para aumentar su conciencia sobre los riesgos adicionales derivados de esta forma de trabajo y los controles que deben aplicarse para mitigar los riesgos?	✓
	TELETRABAJO	¿Existe cualquier política, procedimiento y/o estándar para controlar las actividades de teletrabajo, esta debe ser coherente con la política de seguridad de la organización?	✓
		¿La protección adecuada del sitio de teletrabajo se encuentra en su lugar para actuar contra amenazas tales como el robo de equipos, la divulgación no autorizada de información, etc.?	✓
	REQUISITOS DE SEGURIDAD DE LOS SISTEMAS		
	DE SEGURIDAD ANÁLISIS DE LOS REQUISITOS Y LAS ESPECIFICACIONES	¿Los requisitos de seguridad se incorporan como parte del requisito de declaración de negocio para sistemas nuevos o para la mejora de los sistemas existentes?	✓
		¿Los requisitos de seguridad y los controles identificados reflejan el valor comercial de los activos de información involucrados y la consecuencia de la falta de seguridad?	✓
		¿Las evaluaciones de riesgos se han completado antes del comienzo del desarrollo del sistema?	✓
	SEGURIDAD EN LOS SISTEMAS DE APLICACIÓN		

8 SISTEMA DE DESARROLLO Y MANTENIMIENTO	ENTRADA DE VALIDACIÓN DE DATOS	¿La entrada de datos al sistema de aplicación está validada para asegurarse de que es correcto y apropiado?	✓
		¿Los controles, tales como: Diferentes tipos de entradas para ver los mensajes de error, procedimientos para responder a los errores de validación, la definición de responsabilidades de todo el personal involucrado en el proceso de los datos de entrada, etc. son considerados?	✓
	CONTROL DE PROCESO INTERNO	¿Las áreas de riesgos se identifican en el ciclo de procesamiento y los controles de validación se incluyeron?	✓
		¿Los controles adecuados se identifican en las aplicaciones para mitigar los riesgos durante el proceso interno?	✓
		¿Los controles dependen de la naturaleza y el impacto sobre la aplicación de cualquier corrupción de datos?	✓
	AUTENTICACIÓN DE MENSAJES	¿Una evaluación de riesgo para la seguridad se llevó a cabo para determinar si se requiere autenticación de mensajes, y para identificar el método más adecuado de la aplicación si es necesario?	
		¿La autenticación de mensajes es una técnica utilizada para detectar cambios no autorizados, o la corrupción de los contenidos del mensaje electrónico de transmisión?	
	LOS DATOS DE SALIDA DE VALIDACIÓN	¿La salida de datos del sistema de aplicación está validado para asegurar que el tratamiento de la información almacenada sea correcto y apropiado a las circunstancias.	✓
	CONTROLES CRIPTOGRÁFICOS		
	POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS	¿Existe una política en el uso de controles criptográficos para la protección de la información?	
		¿Se llevó a cabo una evaluación de riesgos para identificar el nivel de protección de la información?	
	CIFRADO	¿Se utilizan técnicas de encriptación para proteger los datos?	
		¿Las evaluaciones se llevaron a cabo para analizar la sensibilidad de los datos y el nivel de protección necesario?	
	FIRMAS DIGITALES	¿Las firmas digitales se utilizan para proteger la autenticidad e integridad de los documentos electrónicos?	
	SERVICIOS DE NO REPUDIO	¿Son utilizados servicios de no repudio para disputas acerca de la ocurrencia o no ocurrencia de un evento o acción?	
	GESTIÓN DE CLAVES	¿Existe un sistema de gestión el cual apoya a la organización el uso de las técnicas criptográficas, como técnica clave secreta y la técnica de clave pública?	
		¿El sistema de gestión de claves se basa en conjunto de normas, procedimientos y métodos	✓

		seguros?	
	SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA		
	CONTROL DE SISTEMA OPERATIVO	¿Existen controles para minimizar el riesgo de corrupción de los sistemas operativos?	✓
	PROTECCIÓN DE DATOS DE PRUEBA DEL SISTEMA	¿Los datos de prueba del sistema están protegidos y controlados?	✓
	SEGURIDAD EN EL DESARROLLO Y APOYAR EL PROCESO		
	CAMBIAR LOS PROCEDIMIENTOS DE CONTROL	¿Existen procedimientos de control estricto sobre la implementación de cambios en el sistema de información?	✓
	REVISIÓN TÉCNICA DE LOS CAMBIOS DE SISTEMA OPERATIVO	¿Existe un proceso para garantizar que el sistema fue revisado y probado después del cambio en el sistema operativo, para instalar los service packs, parches, etc.?	✓
	EXTERNALIZADOS DE DESARROLLO DE SOFTWARE	¿Existen y controles sobre la externalización de software? Los puntos a tener en cuenta incluyen: los acuerdos de licencias, acuerdos de custodia, obligación contractual de garantía de calidad, las pruebas antes de la instalación para detectar códigos troyanos, etc.	✓
9 GESTIÓN DE LA CONTINUIDAD DE NEGOCIOS	*ASPECTOS DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO*		
	LA CONTINUIDAD DEL NEGOCIO DE GESTIÓN DE PROCESOS	¿Existe un proceso controlado para desarrollar y mantener la continuidad del negocio en toda la organización?	✓
	CONTINUIDAD DEL NEGOCIO Y ANÁLISIS DE IMPACTO	¿Los eventos que podrían causar interrupciones de procesos de negocio se identificaron?, ejemplo: falta de equipo, inundaciones e incendios	✓
		¿Se llevó a cabo una evaluación de riesgos para determinar el impacto de dichas interrupciones?	✓
		¿Fue desarrollado con base en los resultados de evaluación de riesgos para determinar un enfoque global para la continuidad del negocio?	✓
	REDACCIÓN Y EJECUCIÓN DEL PLAN DE CONTINUIDAD	¿Los planes fueron desarrollados para restablecer las operaciones comerciales dentro del marco de tiempo requerido después de una interrupción o la falta de procesos de negocio?	✓
	CONTINUIDAD DEL NEGOCIO MARCO DE PLANIFICACIÓN	¿Existe un marco único de plan de continuidad de negocio?	
		¿Los planes son coherentes y determinar las prioridades para las pruebas y mantenimiento?	
		¿Se identifican las condiciones y los responsables de la ejecución de cada componente del plan?	✓
	PRUEBAS, MANTENIMIENTO Y REEVALUACIÓN DE PLAN DE CONTINUIDAD	¿Los planes de continuidad de negocio son evaluados con regularidad para asegurarse de que estén al día?	✓
		¿Los planes de continuidad de negocio mantienen revisiones y actualizaciones periódicas para garantizar su eficacia en todo momento?	
		¿Los procedimientos se incluyen en el programa de gestión de cambios para asegurar que las	

		cuestiones de continuidad del negocio se aborden debidamente?	
10 **CUMPLIMIENTO**	*CUMPLIMIENTO DE LOS REQUISITOS LEGALES*		
	IDENTIFICACIÓN DE LEGISLACIÓN APLICABLE	¿Los requisitos legales, reglamentarios y contractuales se han definido de manera explícita y documentada para cada sistema de información?	
		¿Los controles específicos y las responsabilidades individuales para cumplir con estos requisitos se han definido y documentado?	
	DERECHOS DE PROPIEDAD INTELECTUAL (DPI)	¿Existen procedimientos para garantizar el cumplimiento de las restricciones legales sobre el uso de materiales en los que puede haber derechos de propiedad intelectual, tales como derechos de autor, derechos sobre diseños, marcas, etc.?	✓
		¿Los productos de software propietario son suministrados en virtud de un acuerdo de licencia que limita el uso de los productos a máquinas especificadas? La única excepción podría ser para hacer copias de seguridad del software.	
	MANTENIMIENTO DE LOS REGISTROS DE LA ORGANIZACIÓN	¿Los registros importantes de la organización están protegidos de la destrucción y pérdida de funcionalidad?	✓
	PROTECCIÓN DE DATOS Y PRIVACIDAD DE INFORMACIÓN	¿Existe una estructura de gestión y control para proteger datos y privacidad de información personal?	✓
	PREVENCIÓN DEL USO INDEBIDO DE INFORMACIÓN Y DE LAS INSTALACIONES DE PROCESAMIENTO	¿El uso de las instalaciones de procesamiento de la información para cualquier no profesional o fines no autorizados sin la aprobación de la gestión, se considera como uso indebido de las instalaciones?	✓
	REGLAMENTO DE LOS CONTROLES CRIPTOGRÁFICOS	¿El reglamento de control criptográfico es dictaminado por el sector y el acuerdo nacional?	
	REUNIÓN DE PRUEBAS	¿El proceso involucrado en la recolección de la evidencia está en conformidad con las prácticas jurídicas y la industria?	
	RESEÑAS DE POLÍTICA DE SEGURIDAD Y CUMPLIMIENTO TÉCNICO		
	CUMPLIMIENTO DE LA POLÍTICA DE SEGURIDAD	¿Todas las áreas de la organización que se revisan periódicamente para asegurar el cumplimiento con la política de seguridad, normas y procedimientos?	✓
	COMPROBACIÓN DE A CONFORMIDAD	¿Los sistemas de información fueron controlados periódicamente para el cumplimiento de las normas de implementación de seguridad?	✓
		¿La prueba de conformidad técnica se lleva a cabo por, o bajo la supervisión de personal competente y autorizado?	✓
	CONSIDERACIONES DEL SISTEMA DE AUDITORÍA		
	DE AUDITORÍA DE	¿Los requisitos de la auditoría y las actividades	✓

	CONTROLES DEL SISTEMA	relacionadas con el control de los sistemas operativos deben ser cuidadosamente planificados y acordados para reducir al mínimo el riesgo de interrupciones de procesos de negocio?	
	PROTECCIÓN DE LAS HERRAMIENTAS DE AUDITORÍA DEL SISTEMA	¿El acceso a las herramientas de auditoría del sistema, tales como software o archivos de datos están protegidos para evitar cualquier posible abuso o compromiso?	✓

Como se puede observar en la tabla 13, la seguridad de la dependencia mejoró, ya que consigue cubrir varias de las recomendaciones que no se lograron alcanzar en el primer análisis. En la tabla 14 se puede observar un resumen de los puntos de las secciones que no se cubrieron, así como los porcentajes que se obtienen a partir de esta situación.

Tabla 14. Porcentajes obtenidos de la Tabla 13.

Sección	Puntos a evaluar	Puntos evaluados	Puntos no evaluados	Porcentaje no evaluado	Porcentaje evaluado
1. Política de seguridad	4	4	0	0.00%	100.00%
2. Organización de seguridad	14	9	5	35.71%	64.29%
3. Clasificación de los activos y el control	4	3	1	25.00%	75.00%
4. Seguridad del personal	13	9	4	30.76%	69.24%
5. Seguridad física y ambiental	29	21	8	27.58%	72.42%
6. Comunicaciones y gestión de operaciones	48	35	13	27.03%	72.97%
7. Control de acceso	38	25	13	34.21%	65.79%
8. Sistema de desarrollo y mantenimiento	24	15	9	37.50%	62.50%
9. Gestión de la continuidad del negocio	11	7	4	36.36%	63.64%
10. Cumplimiento	14	9	5	35.71%	64.29%
TOTAL	199	137	62	31.16%	68.84%

Como se puede observar en la tabla 14, el porcentaje de puntos no evaluados bajo de 71.85% a un 31%. Haciendo un nuevo análisis con el mismo criterio con el que se obtuvo la tabla 9, se obtiene la tabla 15, la cual contiene la probabilidad de culminación de una amenaza después de implementar las propuestas abordadas en el capítulo 3.

Tabla 15. Probabilidad de culminación de una amenaza.

AMENAZA	PROBABILIDAD	AMENAZA	PROBABILIDAD
NATURALES			
Ciclones y huracanes	1	Maremotos	1
Deslaves	1	Polvo	2
Erupciones	1	Temperatura extrema	3
Humedad	2	Terremotos	1
Hundimientos	1	Tormentas eléctricas	1
Incendios	1	Tormentas solares	1
Inundaciones	2	Tornados	1
HARDWARE			
Alto voltaje	3	Distorsión	1
Bajo voltaje	3	Ruido electromagnético	1
Cargas estáticas	1	Sobrecalentamiento	2
SOFTWARE			
Gusanos	2	Troyanos	2
Malware	3	Virus	2
RED			
Corte de cables	1	Flujo de información excesivo	2
Interferencias	1	Sniffers	2
HUMANO			
Curiosos	2	Exempleado molesto	2
Ingeniería social inversa	2	Fraude	1
Ingeniería social	2	Robo	2
Sabotaje	2	Terroristas	1

Para obtener el porcentaje de la probabilidad de que ocurra una culminación de una amenaza, se utiliza la tabla 15 y la ecuación a); en el caso que querer obtener el porcentaje de la probabilidad de que no ocurra una amenaza se utiliza la tabla 15 y las ecuaciones a) y b).

a) $y = \left(\frac{P_A(N)}{\sum_{i=0}^{i=N} V_P}\right)(100[\%])$

Donde:

y: Probabilidad de ocurrencia de una amenaza.

P_A=5: Valor de la Probabilidad alta.

N: Número total de amenazas.

V_P: Valores de probabilidad de la tabla 7.

b) 100% = y + z

Donde:

Y: Probabilidad de ocurrencia de una amenaza.

Z: Probabilidad de que no ocurra una amenaza.

Aplicando la fórmula a) cuando N=36, se obtiene que existe un 32% de que culmine una amenaza, véase gráfico 4.1.

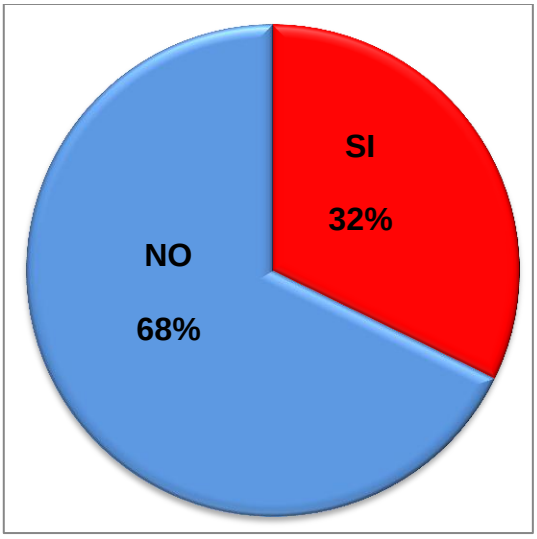


Gráfico 4. 1. Probabilidad de ocurrencia de una amenaza.

Del 32% de que ocurra una amenaza, el 11% corresponde a amenazas naturales, el 6% a amenazas de hardware, el 4% a amenazas de software, el 3% a amenazas de red y el 8% a amenazas humanas, véase gráfico 4.2.

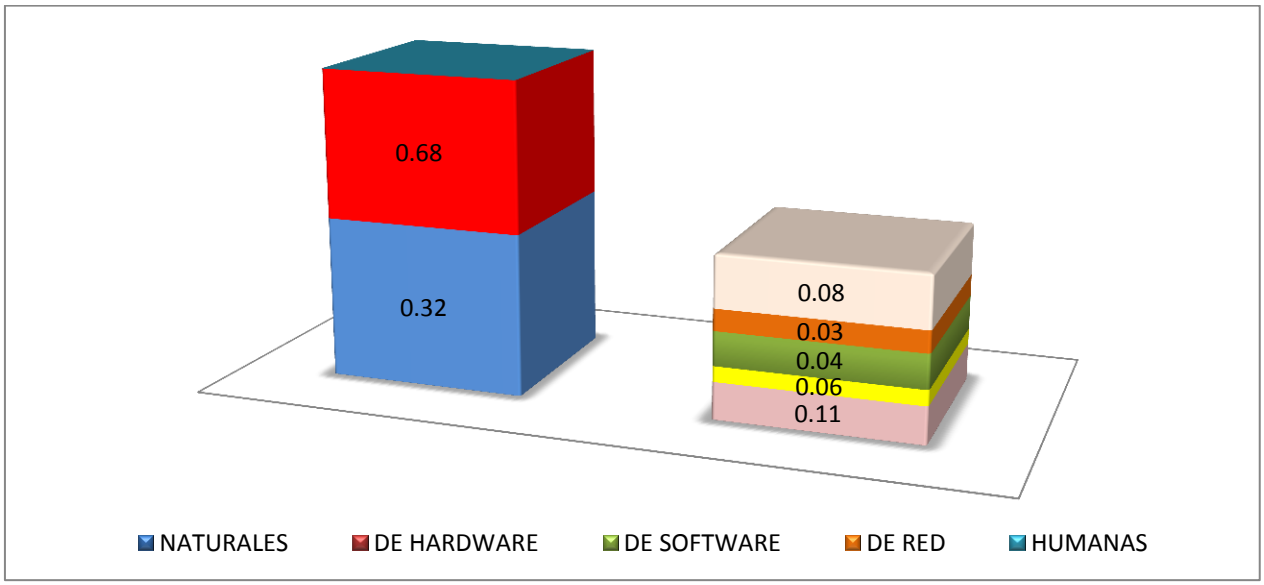


Gráfico 4. 2. Porcentaje de las ocurrencias de las amenazas.

Sustituyendo en la fórmula a) N=14, se obtiene que existe un 27% de que culmine una amenaza natural, véase gráfico 4.3.

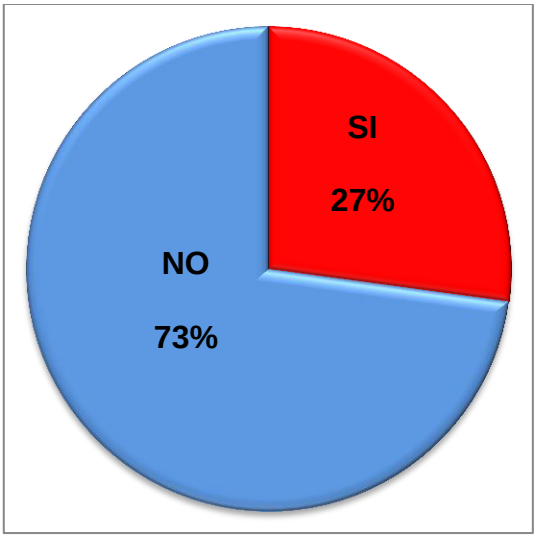


Gráfico 4. 3. Ocurrencia de una amenaza natural.

Aplicando la fórmula a) cuando N=6, se obtiene que existe un 30% de que culmine una amenaza de hardware, véase gráfico 4.4.

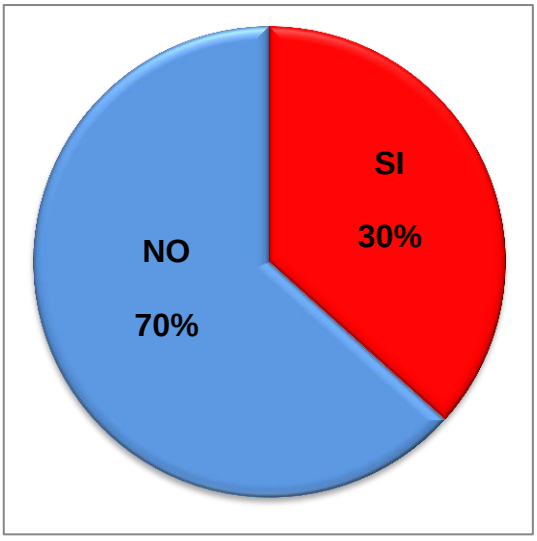


Gráfico 4. 4. Ocurrencia de una amenaza de hardware.

Utilizando la fórmula a) cuando N=4, se obtiene que existe un 40% de que culmine una amenaza de software, véase gráfico 4.5.

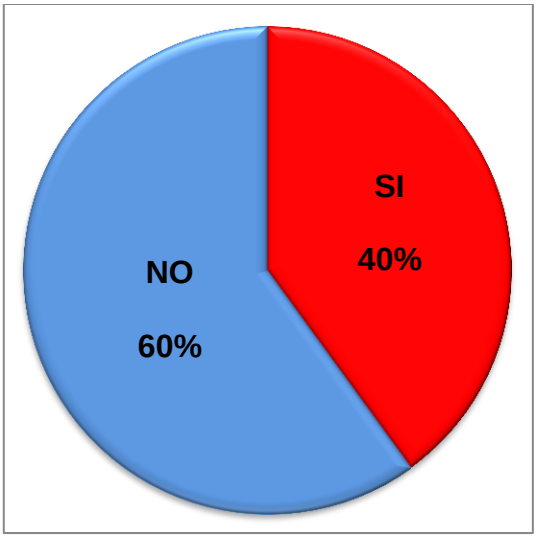


Gráfico 4. 5. Ocurrencia de una amenaza de software.

Usando la fórmula a) cuando N=4, se obtiene que existe un 30% de que culmine una amenaza de red, véase gráfico 4.6.

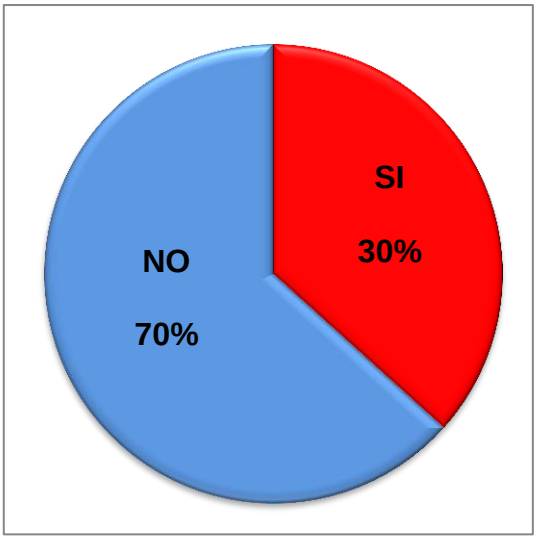


Gráfico 4. 6. Ocurrencia de una amenaza de red.

Utilizando la fórmula a) cuando N=8, se obtiene que existe un 35% de que culmine una amenaza humana, véase gráfico 4.7.

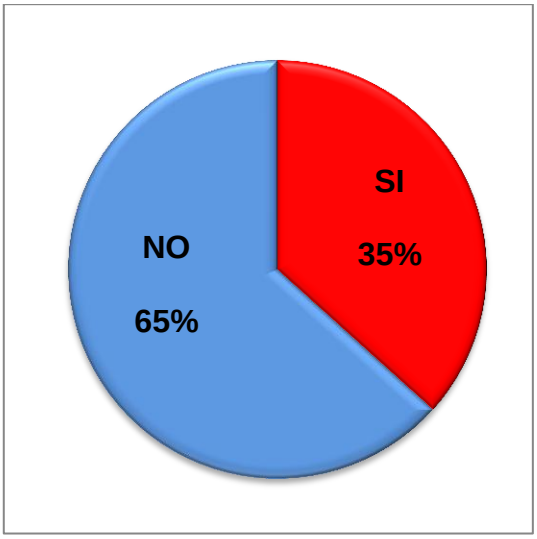


Gráfico 4. 7. Ocurrencia de una amenaza humana.

Los porcentajes obtenidos a partir de la tabla 16 para las probabilidades de las culminaciones de las amenazas naturales, humanas, de hardware, de software, y de red, han disminuido después de implementar la propuesta mencionada en el capítulo 3; la dependencia cuenta con aproximadamente 11 vulnerabilidades, las cuales se muestran en la tabla 17.

Tabla 17. Vulnerabilidades de la dependencia.

VULNERABILIDAD
No dispone de no-breaks
Falta de ventilación
Falta de rociadores
Cansancio del personal
Inconformidad del personal
Exceso de confianza
Clima variante
No contar con credenciales que identifique al personal
No tener control en la entrada y salida de visitantes
Falta de limpieza de las áreas de la organización
Deshonestidad del personal

Haciendo un comparativo entre el antes y el después de implementar “la propuesta solución”, elaborada en este trabajo, se puede observar que esta propuesta ayuda a mejorar la situación de la dependencia al disminuir sus vulnerabilidades y el nivel o probabilidad de ocurrencia como se muestra en la tabla 18.

Tabla 18. Comparativa de la situación de la dependencia.

AMENAZA	ANTES DE IMPLEMENTAR LA PROPUESTA	DESPUÉS DE IMPLEMENTAR LA PROPUESTA
GENERAL	52 %	32 %
NATURALES	31 %	27 %
DE HARDWARE	37 %	30 %
DE SOFTWARE	100 %	40 %
DE RED	65 %	30 %
HUMANAS	72 %	35 %

En la tabla 18, se puede observar la probabilidad de culminación de una amenaza bajó de un 52% a un 32%, las amenazas naturales no tuvieron una disminución considerable debido a que son sucesos que no podemos controlar a diferencia de las amenazas de software las cuales disminuyeron de un 100% a un 40%.

4.2 Impacto

El desarrollo e implementación de este trabajo fue de suma importancia debido a que se constató la crítica situación de la dependencia al no contar con medidas de seguridad en la información, ni una organización adecuada. Con la realización de esta tesis, se encaminó a la dependencia a un nivel aceptable para que pueda brindar un mejor servicio con calidad al contar con la disponibilidad, integridad, confiabilidad y confidencialidad en la información o servicios que brindan, además, se exhorta a la dependencia a prepararse para alcanzar certificaciones en estándares como la ISO 15408, ISO 17795, ISO 17799 y la ISO 9000.

Al proponer e implementar las soluciones abordadas en el capítulo 3. Propuesta de solución de la problemática; se causó un impacto positivo, ya que se minimizó la

proliferación de virus disminuyendo los ataques de phishing, spam, rootkit, malware, virus, gusanos, etcétera y al tomar en cuenta que, los atacantes siempre siguen innovando y que no se puede erradicar en su totalidad el riesgo latente de sufrir ataques por parte de los nuevos virus a los que estamos expuestos como usuarios de los equipos de computo, en gran manera, a los atacantes se llegan a disuadirlos al poner obstáculos en sus intentos de afectar a los usuarios, al limitar el uso de pequeños ataques como herramientas para alcanzar su objetivo.

La pérdida de equipos se neutralizó al tener mayor control sobre ellos; a su vez, se obtuvo una mejor administración de los equipos de cómputo al contar con información actualizada de los mismos, como por ejemplo: el nombre y ubicación del usuario, uso de los equipos, condiciones, características, limitaciones de los equipos, etcétera. Antes se tenía por año un reporte de pérdida con al menos cinco equipos, ahora este reporte contiene un equipo por año como máximo.

La información sobre las características de los equipos al almacenarse en una base de datos, se otorga el beneficio de que el personal del departamento de cómputo de la dependencia puede realizar reportes y estadísticas veraces de los equipos que tiene a su cargo en un lapso corto de tiempo, así como una buena administración de sus recursos informáticos.

Con ayuda de programas que posibilita el análisis de passwords como passwordmeter, se fortalecen las contraseñas de los usuarios minimizando la probabilidad de ser descubiertas, protegiendo contra robo de identidad, robo y sabotaje de la información del personal y de la institución. Esto causa molestias a los usuarios, pero las ventajas son evidentes cuando se trata de proteger un proyecto, como por ejemplo se brinda mayor confidencialidad a la información que se maneja, asimismo se minimiza la probabilidad de sufrir un robo o una modificación por personas no autorizadas, tomándose en cuenta que en muchas ocasiones la investigación para el desarrollo de un proyecto requiere de una gran inversión financiera.

Con la implementación de políticas de seguridad y el firewall, se logró obtener herramientas que posibilitasen el control sobre la red para que, posteriormente, se pudiesen administrar adecuadamente los recursos de la misma, lo que les permite a los administradores brindar un servicio a nuevos usuarios y conservar o cambiar los privilegios de los usuarios incorporados tiempo atrás.

Aunado a lo anterior, se posibilita la continuidad del trabajo, debido a la disponibilidad de los servicios, lo cual evita gastos imprevistos cuando tardíamente se descubre la necesidad de modificar una infraestructura rígida por el aumento de usuarios o del número de proyectos. Con esto se logra algo vital, como lo es la confiabilidad de los servicios y de la información. El resultado palpable es la obtención de más ingresos monetarios al utilizar los servicios proporcionados por la dependencia para desarrollar proyectos de forma individual o junto con otras empresas, que indudablemente impactará en terceros. Los nuevos recursos se podrán destinar para seguir brindando apoyo al sector educativo, al actualizar, dar mantenimiento o remodelar los salones y laboratorios de los alumnos para los cuales trabaja la dependencia.

Con la actualización del personal se logra minimizar los daños a los equipos, disminuyendo la carga de trabajo de los administradores en cuanto a asesorías, lo que les permite liberarse para invertir más tiempo en otras actividades que requieran una atención más cuidadosa, como por ejemplo, la realización de sistemas para facilitar las actividades del personal y reducir el tiempo que les lleva realizarlas.

CONCLUSIONES

Durante el análisis de la situación de la dependencia, se observó que la protección de la información es necesaria, debido al giro que mantiene y a la existencia de personas que no son propietarias o no tienen autorización para el uso de ésta, que buscan tener acceso para modificar o sustraer los datos para posteriormente ocuparlos en provecho propio, como podría ser con el robo de un importante proyecto.

No es necesario que estos personajes sean ajenos a la institución ya que en varios casos los individuos forman parte del personal que labora al interior de la dependencia Debido a que conoce los procesos, metodologías y tiene acceso a la información sensible o de suma importancia, incluso el golpe que puede dar sería catastrófico.

Después de analizar la situación de la dependencia con ayuda de la norma ISO 17799 y COBIT se llegó a la hipótesis de que la dependencia no contaba con una seguridad adecuada, por lo se concluyó que debe de existir alguna medida o mecanismo que la proteja o que minimice el daño que pudiera tener la información. Sin embargo, se debe tomar en cuenta que, para alcanzar la máxima seguridad, conviene mantener a la institución en un ciclo de revisiones, gracias a que la tecnología avanza de forma acelerada sin olvidar que nunca se va a conseguir la seguridad a un 100%.

A pesar de esta situación, se debe tratar de lograr que la información de los usuarios y en general de cualquier organización, sea utilizada de la manera en la que el autor lo decidió; así como el acceso y modificación a dicha información sólo sea permitido a las personas autorizadas.

Una de estas medidas es tomar en cuenta la actualización del personal con respecto al uso de estos procedimientos, ya que ellos son los últimos usuarios de los sistemas. El mal uso y desconocimiento en muchas ocasiones puede ser la mayor amenaza o potencial de las vulnerabilidades.

Debido a lo anterior, sin lugar a duda se observa la importancia de este trabajo, al tratar de llevar a la dependencia a alcanzar niveles de seguridad nunca antes conocidos y apreciados por parte de sus usuarios.

De igual forma se pueden beneficiar otras organizaciones o instituciones al consultar este documento en sus respectivas instalaciones, no como la estrategia más importante, sino como una guía para tener un mayor cuidado en sus sistemas de interconexión digital en este mundo cada vez más dependiente de la tecnología.

En la realización de este escrito no sólo me vi beneficiado al aplicar los conocimientos que adquirí durante mi estadía en la Facultad de Ingeniería como estudiante de la carrera de Ingeniería en Computación, también se benefició la dependencia en la cual se implementó el proyecto, al minimizarse la probabilidad de sufrir una propagación masiva de virus, lo que la pondría en la antesala de una pérdida masiva de información y una disminución sustancialmente perjudicial en la calidad de los servicios que presta.

REFERENCIAS

Referencias

1. López Barrientos, María Jaquelina y Quezada Reyes, Cintia. *Fundamentos de seguridad informática.* Facultad de Ingeniería; UNAM, México, 2006.

2. www.comip.mendoza.gov.ar/cobit.doc, abril 2011.

3. http://tutoriales.conalepqro.edu.mx/APLICASION%20DE%20LA%20SEGURIDAD%20INFORMATICA/Templates/COBIT.htm, abril 2011.

4. Gene Spafford, profesor de universidad de Purdue, experto en seguridad.

5. Huerta Villalón Antonio. *Seguridad en Unix y Redes*. Open Publication License v.10.2, versión 1.2 Digital.2 de Octubre de 2000.

6. http://www.iec.csic.es/criptonomicon/seguridad/amenazas.html Amenazas a sistemas de información, abril 2010.

7. http://www.seguridadpc.net/hackers.htm Concepto de hacker, marzo 2010.

8. http://psicopsi.com/Presentacion-y-analisis-de-resultados Amenazas a sistemas de información, marzo 2010.

9. http://www.segu-info.com.ar/amenazashumanas/otros.htm Amenazas a sistemas de información, marzo 2010.

10. http://www.elforux.org/index.php?topic=572.0;wap2 Tipos de atacantes, marzo 2010.

11. http://foro.el-hacker.com/f60/definicion-hacker-cracker-lamer-etc-k1llers-primera-parte-144864/ Atacantes, marzo 2010.

12. Stallings, William. *Fundamentos de seguridad en redes, Aplicaciones y Estándares*. Pearson Educación, Madrid 2004.

13. http://www.tgti.es/?q=node/151, mayo.2010

14. http://www.sisteseg.com/files/Microsoft_Word_-_METODOLOGIA_DE_ANALISIS_DE_RIESGO.pdf, mayo 2010.

15. http://www.sans.org/score/checklists/ISO_17799_checklist.pdf, mayo 2010.

16. Nombela, Juan José. *Seguridad informática*. Paraninfo; Madrid, 1996.

17. Quezada, Reyes Cintia. *Apuntes de seguridad informática*. Facultad de Ingeniería, UNAM, México, 2009.

18. Ramírez Pichardo, José de Jesús. *Apuntes de seguridad informática II.* Facultad de Ingeniería, UNAM, México, 2010.

19. http://www.eurologic.es/conceptos/conbasics.htmConceptos básicos de seguridad informática, marzo 2010.

20. informatica.uv.es/it3guia/ARS/apuntes/seguridad1.ppt Seguridad distribuida en la red y centralizada en los sistemas, marzo 2010.

21. http://seguinfo.wordpress.com/2006/09/29/defensa-en-profundidad-de-sistemas-de--informacion-3/ Blog sobre defensa profunda de sistemas de información, marzo 2010.

22. http://www.pergaminovirtual.com.ar/definicion/Cracker.html Diccionario de computación, marzo 2010.

23. http://www.seguridadpc.net/hackers.htm Concepto de hacker, abril 2010.

24. http://foro.el-hacker.com/f60/definicion-hacker-cracker-lamer-etc-k1llers-primera--parte-144864/ Foro sobre tipos de atacantes, marzo 2010.

25. http://mafe0821.galeon.com/aficiones1892052.htmlTipos de atacantes, marzo 2010.

22. http://www.elhacker.net/exploits/ Foro sobre exploits, abril 2010.

23. http://www.masadelante.com/faqs/virus Conceptos de virus, abril 2010.

24. http://www.pergaminovirtual.com.ar/definicion/Sniffer.html Diccionario de computación, marzo 2010.

25. searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1244889,00.html Manejo de pharming, marzo2010.

26. http://www.virusportal.com/es/formacion/train_dat3.shtml Virus, marzo 2010.

27. http://www.delitosinformaticos.com/seguridad/clasificacion.shtml Clasificación y tipos de ataques contra sistemas de información, abril 2010.

28. http://www.segu-info.com.ar/logica/seguridadlogica.htm Seguridad lógica, abril 2010.

29. http://www.segu-info.com.ar/fisica/seguridadfisica.htm Seguridad física, agosto 2010.

30. http://www.rompecadenas.com.ar/spam.htm Concepto de spam, agosto 2010.

31. http://seguridadinformatica.foroes.net/criptologia-otra-forma-de-protejerse-en-la-red-f49/definiciones-amenazas-y-mecanismos-de-seguridad-t299.htm Foro de seguridad informática, octubre 2010.

32. http://www.informatica-hoy.com.ar/seguridad-informatica/Tipos-de-firewall.php Tipos de firewall, marzo 2010.

33. http://www.pc-help.org/www.nwinternet.com/pchelp/security/firewalls.htm ¿Qué es un firewall?, octubre 2010.

34. http://www.rediamerica.net/index.php?option=com_content&task=view&id=41&Itemid=52 Statefull firewall, abril 2010.

35. http://searchnetworking.techtarget.com/sDefinition/0,sid7_gci212023,00.html Definición de seguridad, mayo 2010.

36. http://promexico.wordpress/2010/03/14/seguridad de datos-i/Blog sobre seguridad de datos, marzo 2010.

37. http://www.thedragoncorp.com/seguridad/seguridad01.html Conceptos básicos de seguridad, mazo 2011.

38. http://www.teleinformatica.gob.ve/?p=127mazo 2011.

39. http://www.une.com.co/hogares/index.php?option=com_content&view=article&id=26 Conceptos generales de seguridad, mazo 2011.

40. http://www.segu-info.com.ar/logica/seguridadlogica.htmSeguridad lógica, mazo 2011.

41. http://www.univalle.edu/publicaciones/journal/journal18/pagina17.htmSeguridad informática: un enfoque desde la auditoria informática, mazo 2011.

42. http://www.iec.csic.es/criptonomicon/seguridad/amenazas.html Amenazas deliberadas a la seguridad de la información, mazo 2011.

43. http://www.pergaminovirtual.com/definicion/Cracker.html?PHPSESSID=6ca66c36adfd500ec95c3aa18b82e9d6Diccionario de computación, mazo 2011.

44. http://psicopsi.com/Presentacion-y-analisis-de-resultadosPsicología del hacker, mazo 2011.

45. http://www.segu-info.com.ar/amenazashumanas/otros.htmlTipos de atacantes, mazo 2011.

46. http://www.elforux.org/index.php?topic=572.0;wap2Concepto de hacker y herramientas, mazo 2011.

47. http://sideshare.net/julizel/tecnologias-biometricas. Kevin Mitnick. Craker y pheaker estadounidense, marzo 2010.

48. Lizarraga Ramírez, Gabriela Betzabe. *Apuntes de bases de datos.* Facultad de Ingeniería, UNAM, México, 2009.

49. Pérez, Cesar. *Oracle 10g. Administración y análisis de bases de datos*. Alfaomega Grupo Editor, México D.F. 2008.