UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

METODOLOGÍA DE SEGURIDAD INFORMÁTICA CON BASE EN LA NORMA ISO 27002 Y EN HERRAMIENTAS DE PREVENCIÓN DE INTRUSOS PARA LA RED ADMINISTRATIVA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA.

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

AUTOR: MARIO ANDRÉS CEVALLOS MICHILENA

DIRECTOR: ING. EDGAR MAYA

Ibarra – Ecuador

2013

DECLARACIÓN

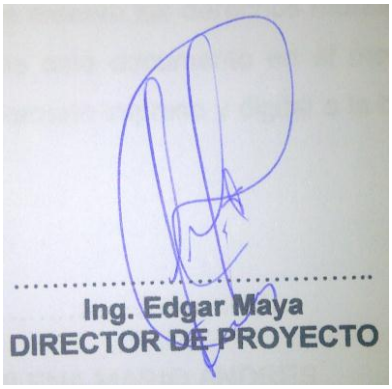
Yo, Mario Andrés Cevallos Michilena con cédula de identidad nro. 1002872289, estudiante de la carrera de Ingeniería en Electrónica y Redes de Comunicación, libre y voluntariamente declaro que el presente trabajo de investigación, es de mi autoría y no ha sido realizado, ni calificado por otro profesional, para efectos académicos y legales será de mi responsabilidad.

CEVALLOS M. Andrés

CI: 100287228-9

CERTIFICACIÓN

Certifico, que el presente trabajo de titulación “METODOLOGÍA DE SEGURIDAD INFORMÁTICA CON BASE EN LA NORMA ISO 27002 Y EN HERRAMIENTAS DE PREVENCIÓN DE INTRUSOS PARA LA RED ADMINISTRATIVA DEL GAD-IBARRA.” fue desarrollado en su totalidad por el Sr. Mario Andrés Cevallos Michilena, bajo mi supervisión.



UNIVERSIDAD TÉCNICA DEL NORTE

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE INVESTIGACIÓN A FAVOR DE LA UNIVERSIDAD

Cesión de derechos de Autor del Trabajo de Grado a favor de la Universidad Técnica del Norte.

Yo, Mario Andrés Cevallos Michilena con cedula nro. 1002872289, manifiesto que es mi voluntad de ceder a la Universidad Técnica del Norte, los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador Art.4,5 y 6 en calidad de autor del Trabajo de Grado denominado: **"METODOLOGÍA DE SEGURIDAD INFORMÁTICA CON BASE EN LA NORMA ISO 27002 Y EN HERRAMIENTAS DE PREVENCIÓN DE INTRUSOS PARA LA RED ADMINISTRATIVA DEL GAD-IBARRA",** que ha sido desarrollado para obtener el título de INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN en la Universidad Técnica del Norte, quedando facultada la Universidad para ejercer plenamente los derechos cedidos anteriormente.

En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia se suscribe este documento en el momento en que se hace la entrega del trabajo final en formato impreso y digital a la biblioteca de la Universidad Técnica del Norte.

(Firma): 

Nombre: CEVALLOS MICHILENA MARIO ANDRES

Cédula: 1002872289

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

La Universidad Técnica del Norte dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos en forma digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo por sentada mi voluntad de participar en este proyecto, para lo cual ponemos a disposición la siguiente información.

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1002872289		
APELLIDOS Y NOMBRES:	Cevallos Michilena Mario Andrés		
DIRECCIÓN:	Barrio San Cristóbal, Azcasubi y Eloy Alfaro, San Pablo		
EMAIL:	m.andrescevallos@gmail.com		
TELÉFONO FIJO:	062919-418	**TELÉFONO MOVIL:**	0979026028

DATOS DE LA OBRA	
TÍTULO:	"METODOLOGÍA DE SEGURIDAD INFORMÁTICA CON BASE EN LA NORMA ISO 27002 Y EN HERRAMIENTAS DE PREVENCIÓN DE INTRUSOS PARA LA RED ADMINISTRATIVA DEL GAD-IBARRA"

AUTOR:	Cevallos Michilena Mario Andrés
FECHA:	2013/09/04
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	■ PREGRADO ▭ POSGRADO
TÍTULO POR EL QUE OPTA:	Ingeniería en Electrónica y Redes de Comunicación
ASESOR/DIRECTOR:	Ing. Edgar Maya

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Mario Andrés Cevallos Michilena con cédula de ciudadanía Nro. 1002872289, en calidad de autor y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago la entrega del ejemplar respectivo en formato digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión; en concordancia con la Ley de Educación Superior Artículo 143.

3. CONSTANCIAS

El (La) autor (a) (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 4 días del mes de octubre del 2013.

EL AUTOR:

(Firma):

Nombre: CEVALLOS MICHILENA MARIO ANDRES

Cédula: 100287228-9

ACEPTACIÓN:

(Firma): …….

Nombre: MSc. Ximena Vallejos

Cargo: JEFA DE BIBLIOTECA

Facultado por la resolución de Consejo Universitario

_____

AGRADECIMIENTO

A mis padres y abuelitos por su amor infinito y apoyo incondicional, porque siempre creyeron en mí e inculcaron el valor de la responsabilidad y la constancia para salir adelante pese a las adversidades y obstáculos del camino.

A mis compañeros de aula con los que viví muchas experiencias inolvidables, de los cuales me llevo su amistad sincera para toda la vida.

Para los distinguidos maestros de la facultad, por su guía y apoyo desinteresado a lo largo de mis años de estudio.

Al personal del GAD Ibarra por abrirme las puertas de tan noble institución y participar activamente en el desarrollo de este proyecto.

A mi novia y amigos por su compañía, por ser ese aliciente necesario para soportar las jornadas más difíciles.

A todos ellos mi más profundo cariño y agradecimiento.

Andrés C.

DEDICATORIA

Este proyecto de titulación lo dedico a mis padres, por ser ese ejemplo de lucha y superación, por su sacrificio y compromiso con nuestro hogar, por todo el amor que nos entregan día a día. También a mi hermana por llenar cada vacío con su alegría y sonrisa y a mi abuelita por esa misión que tomó desinteresadamente para intentar hacer de mí, un hombre de bien y sentimientos nobles.

Andrés C.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

CAPÍTULO I

CAPÍTULO IV

CAPÍTULO V

ÍNDICE DE TABLAS

CAPÍTULO I

CAPÍTULO II

CAPÍTULO IV

RESUMEN

El objetivo del presente proyecto es el de crear una Metodología de Seguridad Informática para la red administrativa del GAD Ibarra, con el fin de resguardar sus activos informáticos frente a potenciales amenazas de origen interno o externo.

Consiste en una estrategia de protección integral, que propone primeramente orientar al usuario hacia el uso adecuado y responsable de los recursos mediante un manual de Políticas y Procedimientos de Seguridad de la información, para posteriormente enfocarse en mitigar aquellas amenazas netamente informáticas, mediante herramientas técnicas de seguridad como las tecnologías IDS e IPS, vigentes en la actualidad.

Para este propósito, se usó la Norma ISO 27002 como referencia para la elaboración de las políticas de seguridad propuestas. Además se requirieron los motores de detección Snort y Snort Inline para montar el servidor IDS/IPS basado en software libre (CentOS).

ABSTRACT

The objective of the present project is to create a Computing Security Methodology for GAD Ibarra´s administrative network, in order to protect their information assets against potential threats from internal or external sources.

It consists of an integral protection strategy, first proposed to guide the user to the appropriate and responsible use of resources through of a Policies and Procedures Manual for the Security Information, later to mitigate those informatics type threats, using technical security tools as IDS and IPS technologies, actives today.

For this purpose, the ISO 27002 standard has been used as a reference for the development of security policies proposed. Besides, the detection engines as Snort and Snort Inline have been requested to mount IDS / IPS server based on free software (CentOS).

PRESENTACIÓN

El presente proyecto consiste en el desarrollo de una METODOLOGÍA DE SEGURIDAD INFORMÁTICA CON BASE EN LA NORMA ISO 27002 Y EN HERRAMIENTAS DE PREVENCIÓN DE INTRUSOS PARA LA RED ADMINISTRATIVA DEL GAD-IBARRA**,** cuyo informe final se encuentra estructurado en seis capítulos con orden lógico, los cuales se detallan a continuación:

En el Capítulo I, se expone una breve reseña respecto a la importancia de la seguridad informática en escenarios corporativos, los diversos tipos de amenazas y los mecanismos de protección más importantes. Además se describen las normas y estándares de Seguridad Informática existentes, priorizando la norma ISO 27002.

En el capítulo II, se realiza el Análisis de Riesgos en los activos de la red administrativa del GAD Ibarra mediante la metodología MAGERIT v3. Se identifica una lista de activos y amenazas con índices de riesgo alto o muy alto, los cuales deben captar mayor atención por parte del gestor de seguridad, para la ejecución de medidas de mitigación.

En el capítulo III, se elabora el manual de Políticas y Procedimientos de seguridad de la información, destinada a usuarios y administradores de la red.

En el capítulo IV, se detallan las herramientas que fueron utilizadas para la ejecución del servidor IDS/IPS y los pasos previos para su elaboración.

En el capítulo V, se efectúan las pruebas de funcionamiento respectivas y se elabora la documentación de resultados posteriores a la puesta en marcha del IDS/IPS.

En el Capítulo VI, se exponen las conclusiones obtenidas en la elaboración de este proyecto y las recomendaciones a tomar en cuenta, en caso de emprender este trabajo de investigación en otro escenario.

CAPÍTULO I

1. INTRODUCCIÓN A LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Este capítulo describe los conceptos preliminares referentes a la Seguridad de la Información, indica la importancia de su alcance en redes corporativas, así como también señala los tipos de amenazas informáticas y mecanismos de protección más comunes dentro de estos escenarios. Finalmente, señala las Normas ISO 27000 referentes a la Seguridad de la Información, priorizando la descripción de la ISO/IEC 27002, cuyo documento servirá de guía para el desarrollo de un tramo de esta tesis.

1.1 INTRODUCCIÓN

Actualmente el escenario en el cual las organizaciones enlazan sus redes internas a la Internet es más común cada día, debido a la infinidad de bondades que ésta ofrece, entre ellas, la obtención de información de interés potencial para la empresa, la optimización de la comunicación interna o externa sin límites geográficos, la creación de nuevas oportunidades de negocio a través del comercio electrónico, entre otras, las cuales podrían contribuir en gran proporción al aumento de la eficiencia y competitividad de cualquier entidad. Sin embargo, esto también las hace más vulnerables, pues cada sistema de computadores involucrado en la red es un blanco potencial y apetecible para cualquier atacante y la probabilidad de sufrir problemas de seguridad aumenta. Al mismo tiempo, la facilidad de ejecución o propagación de nuevos ataques, y el nivel de daño provocado por los mismos, llegan cada vez a escalas

mayores, volviéndose imprescindible el estudio y elaboración de estrategias que permitan alcanzar un nivel óptimo de seguridad de la información en una entidad.

1.2 SEGURIDAD DE LA INFORMACIÓN

La información constituye un recurso fundamental para el mantenimiento y desarrollo de cualquier organización, de modo que uno de los objetivos prioritarios de cualquier empresa será el aseguramiento de dicho activo y obviamente de los sistemas que lo procesan. Es por ello que esta temática se vuelve vital para el éxito de la actividad de cualquier entidad, pues intenta garantizar que sus recursos informáticos estén disponibles para cumplir sus propósitos, bajo cualquier circunstancia o factor que los pueda alterar.

"La seguridad de la información puede entenderse como aquellas técnicas y actividades destinadas a preservar la confidencialidad, integridad y disponibilidad de la información, así mismo se preocupa del resguardo y protección de los demás elementos del sistema informático[1], ya sea a nivel personal, grupal o empresarial" (Recuperado el 10 de Septiembre del 2011, de https://iepweb.sciencespo-rennes.fr/bibli_doc/download/224/).

1.2.1 PRINCIPIOS

La seguridad de la información, se fundamenta en tres principios básicos que debe cumplir todo sistema informático (Areitio, 2009):

[1] **Sistema informático:** conjunto que resulta de la integración de cuatro elementos importantes tales como: hardware, software, datos y usuarios.

- **Confidencialidad:** Se refiere a la privacidad de los elementos almacenados y procesados en un sistema informático, protegiéndolo de invasiones, intrusiones y accesos, por parte de personas o programas no autorizados.

- **Integridad:** Se basa en la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático, protegiéndolo de modificaciones o alteraciones inesperadas.

- **Disponibilidad:** Se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático.

  Para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran.

Figura 1.1: Principios de la Seguridad de Información

Referencia: http://www.satinfo.es/archivo/soporte/SOPORTE_seguridad-web.ppt

1.2.2 IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN

El resultado de la violación de los sistemas informáticos de innumerables entidades por parte de personas ajenas a la información, conocidas comúnmente como hackers[2] o crackers[3], han provocado la pérdida y/o modificación de los datos sensibles que circulan a través de sus redes, representando pérdidas económicas significativas y degradando el normal funcionamiento de sus procesos y servicios. Esta situación se complica debido a los esquemas ineficientes de seguridad con los que cuentan la mayoría de las compañías a nivel mundial y el limitado conocimiento relacionado con la planeación de una metodología de seguridad eficaz.

Por tal motivo, es fundamental que las empresas tomen precauciones no sólo para proteger su continuidad operativa al ser víctimas de un ataque, sino también consideren a la seguridad de la información como materia primordial para su normal desarrollo, y elaboren planes preventivos y correctivos que resguarden adecuadamente sus datos, recursos informáticos y en definitiva a sus usuarios que son su activo más valioso.

Actualmente se ha puesto de manifiesto una creciente masificación del tema de seguridad de la información en medios empresariales, sin embargo, los controles adoptados aún no garantizan un estado de seguridad aceptable. Con estas consideraciones las

[2] **Hackers o "White Hats":** Persona que busca vulnerabilidades en los sistemas o redes, con el objetivo de informar a los responsables o propietarios de sus recursos, para que tomen acciones sobre las mismas. Recientemente, este término se ha utilizado con frecuencia con un sentido negativo, para describir a una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa.

[3] **Cracker o "Black Hats":** Es un término más preciso para describir a una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa.

instituciones públicas como privadas deben implementar políticas que estén muy ligadas con su realidad y entorno, para que lo márgenes de error sean mínimos y el grado de protección se incremente. También es necesario que sus procesos contra incidentes de seguridad sean metódicos y cumplan con estudios previos que los lleven a identificar con plena certeza las amenazas que han de ser contrarrestadas.

En síntesis, considerar aspectos de seguridad demanda: **conocer el peligro**, **clasificarlo o evaluarlo** y **protegerse** de los impactos o daños de la mejor manera posible.

1.3 ATAQUES INFORMÁTICOS CONTRA SISTEMAS

Cada día aparecen nuevos y sofisticados métodos de ataques informáticos que buscan explotar las vulnerabilidades tanto en el diseño, como en la configuración y operación de los sistemas que conforman las redes conectadas a la Internet. Estos métodos de ataque se han ido automatizando, por lo que en muchos casos sólo se necesitan conocimientos técnicos básicos para realizarlos. De este modo, es trascendental la comprensión de estas técnicas para crear una visión real del escenario al cual se enfrentará un sistema informático a resguardar.

Se puede definir como ataques, "a todas aquellas acciones que suponen una violación de la seguridad de un sistema determinado, las cuales pueden o no tener éxito" (Recuperado el 25 de Septiembre del 2011, de http://www.dspace.espol.edu.ec/handle/123456789/20029?mode=full).

Estas acciones se pueden clasificar según los efectos causados, de la siguiente manera:

1.3.1 RECONOCIMIENTO DE SISTEMAS

Obtienen información previa sobre las organizaciones, redes y sistemas informáticos que son objetivo de posibles ataques.

Tabla 1.1: Técnicas de ataques por reconocimiento de sistemas
Referencia: http://www.mundointernet.es/IMG/pdf/ponencia95.pdf

TÉCNICAS	
Footprinting	Extrae toda la información posible del sistema objetivo utilizando herramientas como: la base de datos WHOIS (DNS, Direcciones IP) o People Search (Información de contactos).
Fingerprinting	Extrae información del sistema operativo (identifica las máquinas que actúan en la red) por medio de herramientas como Nmap.

1.3.2 DETECCIÓN DE VULNERABILIDADES EN LOS SISTEMAS

Detectan las posibles vulnerabilidades de un sistema informático, para posteriormente, desarrollar alguna herramienta que permita explotarlas fácilmente.

Tabla 1.2: Técnicas de ataques por detección de vulnerabilidades
Referencia: http://www.mundointernet.es/IMG/pdf/ponencia95.pdf

TÉCNICAS	
Escaneo de Puertos (Port Surfing)	Para conocer puertos abiertos o cerrados en las redes, servicios que son ofrecidos, chequear la existencia de firewalls o el funcionamiento de los mismos, etc. (Por ej.: Nmap).
Escaneo de red	Identifica hosts activos en una red para atacarlos (en el caso de un Cracker) o para realizar tareas de seguridad (en el caso de un administrador de redes). (Por ej.: AngryIP).

Escaneo de Vulnerabilidades	Detectar vulnerabilidades en los sistemas y redes. (Por ej.: Nessus).

1.3.3 INTERCEPTACIÓN PASIVA DE LA INFORMACIÓN (EAVESDROPPING)

Ataques que tratan de interceptar datos que se envían a través de redes de ordenadores como Internet de forma pasiva (sin modificar dicha información), vulnerando de este modo la confidencialidad del sistema informático y la privacidad de sus usuarios.

Tabla 1.3: Técnicas de ataques por eavesdropping
Referencia: http://www.mundointernet.es/IMG/pdf/ponencia95.pdf

TÉCNICAS	
Packet Sniffers	Programas que monitorean los paquetes entrantes y salientes de una red, capturándolos de forma promiscua. (Por ej.: WireShark).
Fisgoneo o Snooping	Esta técnica también extrae los paquetes del tráfico de la red sin realizar modificaciones, sin embargo, también basa sus funciones en el almacenamiento de dicha información obtenida (downloading). (Por ej.: ttysnoop).

1.3.4 MALWARE EN EQUIPOS

Entendemos por código malicioso o dañino (“malware”) cualquier programa, documento o mensaje susceptible de causar daños en las redes y sistemas informáticos. Puede ser clasificado según su propósito:

Tabla 1.4: Tipos de ataques por introducción de malware

Referencia: http://www.mundointernet.es/IMG/pdf/ponencia95.pdf

Malware Infeccioso	
Virus	Programa cuyo objetivo es destruir parte o la totalidad de los datos almacenados en algún soporte de información. Tiene la capacidad de copiarse a sí mismo y lo hace de forma transparente al usuario.
Gusanos	Programa cuya finalidad es la de ir consumiendo la memoria del sistema, mediante la realización de copias sucesivas de sí mismo, hasta desbordar la RAM, siendo ésta su única acción maligna.
Malware Oculto	
Troyanos	Un Caballo de Troya es un programa maligno que se oculta en otro programa legítimo, permitiendo al troyano realizar tareas ocultas y a menudo, malignas.
Drive by Downloads	Permite infectar masivamente a los usuarios simplemente ingresando a un sitio web determinado.
Para obtención de beneficios	
Spyware (Espías)	Software que recopila información del ordenador (como páginas web visitadas, información sobre números de tarjetas de crédito y claves de acceso) para transmitirla a una entidad externa con o sin el conocimiento de su propietario. Su infección generalmente genera también una pérdida considerable del rendimiento del sistema.
Adware (Advertising Software)	Muestran publicidad al usuario de forma intrusiva en forma de ventanas emergentes (pop-up) o de cualquier otra forma. Esta publicidad aparece inesperadamente en el equipo y resulta muy molesta.
Robo de Información personal	
Keyloggers	Monitorizan todas las pulsaciones del teclado y las almacenan para un posterior envío al creador.

1.3.5 ATAQUES POR SUPLANTACIÓN

Este tipo de ataque se dedica a dar información falsa, a negar una transacción y/o a hacerse pasar por un usuario conocido.

Tabla 1.5: Técnicas de ataques por suplantación

Referencia: http://www.mundointernet.es/IMG/pdf/ponencia95.pdf

TÉCNICAS	
IP Spoofing	Consiste en obtener acceso no autorizado a un sistema, usando una dirección de red que aparentemente proviene de un equipo de confianza. Esta técnica aprovecha las vulnerabilidades de una conexión TCP/IP [4] debido a que en este protocolo no existe información sobre el estado en la transacción que se usa para enrutar paquetes en la red y adicionalmente, la dirección origen situada en la cabecera de sus paquetes puede ser modificada por el atacante.
DNS Spoofing	Pretenden provocar un direccionamiento equívoco en los equipos afectados, debido a una traducción errónea de los nombres de dominio (DNS)[5] a direcciones IP, de este modo los usuarios de los sistemas afectados acceden a páginas Web falsas (Pishing) o bien sus mensajes de correo electrónico podrían ser interceptados. Otra posible consecuencia de la manipulación de los servidores DNS serían los ataques de Denegación de Servicio (DoS)[6], al

[4] **TCP/IP (Transmission Control Protocol/Internet Protocol):** Permite que diferentes tipos de PCs utilicen la red y se comuniquen unas con otras, indiferentemente de la plataforma o sistema operativo que usen.

[5] **DNS (Domain Name Service:)** Es un sistema que permite traducir de nombre de dominio a dirección IP y viceversa.

[6] **DoS (Denial of Service):** Tiene como objetivo imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo.

	provocar la redirección permanente hacia otros servidores en lugar de dirigirse al verdadero, inundando de paquetes a un servidor-objetivo determinado para intentar saturarlo.
SMTP (Mail) Spoofing	Basado en la suplantación de identidad del remitente de mensajes de correo falso, para tratar de engañar al destinatario o causar un daño en la reputación del supuesto remitente. Técnica empleada por varios virus para facilitar su propagación, o por "spammers", que envían gran cantidad de mensajes de "correo basura" bajo una identidad falsa. En la actualidad, falsificar mensajes de correo resulta bastante sencillo porque el protocolo SMTP carece totalmente de autenticación.
ARP Spoofing (ARP Poisoning)	ARP es un protocolo de capa 2 (enlace) que convierte una dirección IP a una dirección MAC. Se lo usa en redes TCP/IP ya que los hosts se conocen en la red a través de su dirección física (MAC) inicialmente, sin embargo, estas redes utilizan únicamente direcciones lógicas (IP) y se vuelve necesaria su traducción para el entendimiento de sus hosts. Entonces ARP Poisoning tiene como finalidad la falsificación de dichas asociaciones para ligar la dirección MAC del atacante con la dirección IP del nodo atacado. Por lo tanto, todo el tráfico dirigido a esta dirección IP, será erróneamente enviado al atacante, en lugar de a su destino real. El atacante, puede entonces elegir, entre reenviar el tráfico a su destino real (ataque pasivo o escucha), o modificar los datos antes de reenviarlos (ataque activo), convirtiéndose en un ataque de Hombre en Medio.

1.3.6 ATAQUES DE DENEGACIÓN DEL SERVICIO (DoS)

Buscan colapsar determinados equipos o redes informáticas, para impedir que puedan ofrecer sus servicios a sus clientes y usuarios. Cuentan con varias estrategias, entre ellas:

Tabla 1.6: Estrategias de ataques DoS

Referencia: http://www.mundointernet.es/IMG/pdf/ponencia95.pdf

Transmisión de paquetes de datos malformados o que incumplan las reglas de un protocolo, para provocar la caída de un equipo que no se encuentre preparado para recibir este tipo de tráfico malintencionado.	
Ping de la muerte	Surgió en los años noventa atacando a los sistemas operativos hasta antes de 1997, luego los mismos utilizarían parches para evitarlo. Este ataque implicaba el envío de un ping deformado (paquetes ICMP muy pesados mayores a 65635 bytes) a una computadora. Tomando en cuenta que un ping normal tiene un tamaño de 64 bytes, pings de mayor tamaño podrían bloquear el sistema.
Ataque LAND (Local Area Network Denial)	Consiste en enviar un paquete con la misma dirección IP o el mismo número de puerto en los campos fuente y destino. Esto puede provocar que un equipo empiece a generar Acuses de recibo ACK (Mensaje corto para informar a un transmisor que han llegado datos al destino) tratando de responderse a sí mismo, en un verdadero bucle sin fin, logrando colgar al equipo.
Generación de grandes cantidades de tráfico, generalmente desde múltiples equipos, y lograr un consumo excesivo de recursos cómo: ancho de banda, tiempo de CPU, memoria, disco duro, etc. hasta lograr agotarlos.	
Mail Bombing	Consiste en el envío masivo de miles de mensajes de correo electrónico provocando la sobrecarga del servidor de correo y/o de las redes afectadas.
SYN Flood	El sistema atacante utiliza una IP inexistente y envía multitud de peticiones de conexión (Tramas de Sincronización SYN) al equipo víctima. Como la víctima no puede contestar (porque su IP es inexistente) las peticiones llenan la cola de tal manera que las solicitudes reales no puedan ser atendidas.

Smurf	Este ataque utiliza el broadcast de la red. Envía paquetes ICMP de tipo echo-request (Ping[7]) con IP origen la de la máquina atacada y con IP destino la dirección broadcast de la red local. Con ello todas las máquinas de la red enviarán paquetes ICMP echo-reply (respuesta) a la máquina de la víctima, magnificando el ancho de banda usado y ralentizando la red e incluso llegando a colapsar a la víctima.

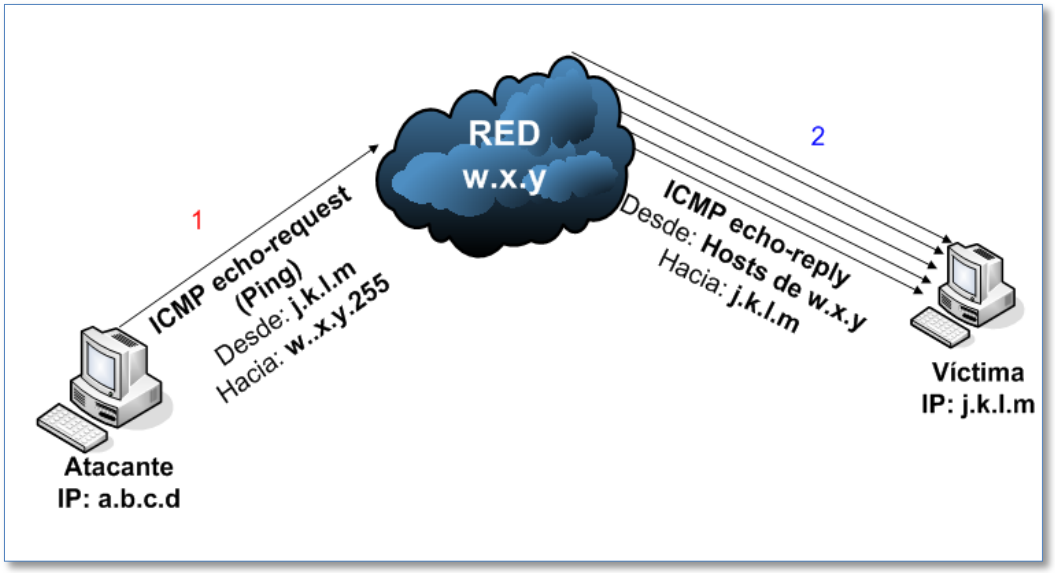


Figura 1.2: Ataque con SMURF

Referencia: http://it.aut.uah.es/enrique/docencia/ii/seguridad/documentos/t11-0506.pdf

1.3.7 ATAQUES DE DENEGACIÓN DE SERVICIO DISTRIBUIDOS (DDoS)

Cuando múltiples atacantes sincronizados dirigen sus acciones a un mismo destino, y consiguen su objetivo gracias a que agotan el ancho de banda de la víctima y sobrepasan la capacidad de procesamiento de los routers, consiguiendo que los servicios ofrecidos por la máquina atacada no puedan ser prestados. El atacante logra obtener el control de las máquinas infectadas por un cierto tipo de malware, las cuales se las conoce como "máquinas zombie", y

[7] **Ping (Packet Internet Groper):** Comprueba el estado de la conexión del host local con uno o varios equipos remotos de una red TCP/IP por medio del envío de paquetes ICMP de solicitud y de respuesta.

al conjunto de todas las que están a disposición de un atacante se le conoce como botnet[8] (red de bots).

La mayoría de estos ataques emplea un conjunto de exploits (explota vulnerabilidades) remotos para introducirse en los equipos. También pueden diseminarse mediante el envío masivo de correo no solicitado (spam), utilizando técnicas de ingeniería social para convencer al usuario de que ejecute un programa malicioso o accediendo a una página web con contenido falso.

1.4 HERRAMIENTAS PARA LA DETECCIÓN DE ATAQUES E INTRUSIONES

1.4.1 ANTIVIRUS Y ANTISPYWARE

El software antivirus puede utilizarse como herramienta preventiva o reactiva, que previene las infecciones, detecta y elimina virus, gusanos, caballos de Troya, entre otros. Sin embargo, los antivirus poseen limitaciones considerables, porque están enfocados a la protección individual de un ordenador más no de una red, y la protección que brinda no es total pues los virus mutan o se actualizan a mayor ritmo que los programas "buenos". Además no son capaces de contrarrestar ataques directos provenientes de crackers y por consiguiente, actividades criminales informáticas no logran ser impedidas por estas herramientas. A pesar de las limitaciones, nunca se deberá detener el funcionamiento del antivirus porque dejará al ordenador mucho más expuesto a ataques externos. De la misma forma, si no se lo actualiza,

[8] **botnet:** Colección de computadoras, conectadas a Internet, que interactúan entre sí para lograr la realización de cierta tarea de forma distribuida.

el software se volverá prácticamente inútil, ya que no logrará detectar ni remover los virus más recientes.

Por otro lado, el software antispyware detecta y elimina las aplicaciones de spyware impidiendo que dicho malware pueda recopilar información no autorizada, o utilice recursos importantes de la computadora que afecte su rendimiento.

1.4.2 FIREWALL

El firewall o cortafuego es el filtro que permite controlar el tráfico de entrada/salida de una red. Suele ubicarse entre la red interna y la conexión a Internet, sometiendo al tráfico circulante a las reglas establecidas, denegando o permitiendo comunicaciones desde una red a la otra, en función de las políticas de seguridad establecidas.

1.4.2.1 Ventajas

- Mantiene usuarios no autorizados fuera de la red protegida.
- Simplifica la administración (centraliza la seguridad).
- Se los considera como una línea de defensa de primera línea, que se puede complementar fácilmente con sistemas de detección/prevención de intrusos (ej.: SNORT[9]).

[9] **SNORT:** Sistema detector de intrusos muy extendido en el mercado desarrollado por Martin Roesch y disponible en código abierto.

1.4.2.2 Limitaciones

El firewall no puede ejecutar sus funciones en las siguientes circunstancias:

- Cuando los ataques provienen del tráfico que no pasa a través de él.
- Si los ataques son de carácter interno o se relaciona con la negligencia de sus usuarios, o a su vez son del tipo "Ingeniería Social".
- No realiza funciones de desinfección de archivos y software como si lo hacen los Antivirus.
- No protege del enmascaramiento de ataques dentro de protocolos permitidos como HTTP, ICMP o DNS.

1.4.2.3 Tipos de Firewall

Tabla 1.7: Tipos de Firewalls

Referencia:http://www.informatica.catamarca.gov.ar/multimedia/archivos/firewall.pdf

Firewall por Hardware	Son dispositivos que trabajan independientemente del computador y no consumen recursos del mismo. Normalmente se colocan entre el servidor y la conexión física al Internet. Una de sus desventajas es el mantenimiento ya que son más complicados de actualizar y configurar correctamente. Se recomiendan marcas tales como Cisco, HP, Linksys, entre otras.
Firewall por Software	Son los más comunes debido a que su costo es inferior a una implementación por hardware, adicionalmente su instalación y actualización es más sencilla aunque pueden presentar problemas debido al consumo de recursos del ordenador y ocasionar errores de

	compatibilidad con otro software instalado, de igual forma para su configuración se necesita poseer conocimientos en redes y saber los puertos necesarios para las aplicaciones utilizadas.

1.4.3 SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)

El IDS hace un análisis en tiempo real del tráfico en la red, en búsqueda de anomalías o intentos de intrusión, comparándolos con un conjunto de firmas cargadas previamente. Se define un intento de intrusión como "cualquier intento de comprometer la confidencialidad, integridad, disponibilidad o evitar los mecanismos de seguridad de una computadora o red" (Recuperado el 26 de Septiembre del 2011, de https://seguridadinformaticaufps.wikispaces.com/Documentacion2PrevioPractica).

Las intrusiones se pueden producir de varias formas: atacantes que acceden a los sistemas desde Internet, usuarios autorizados del sistema que intentan ganar privilegios adicionales para los cuales no están autorizados y usuarios autorizados que hacen un mal uso de los privilegios que se les han asignado.

El IDS se coloca en un lugar tal, que pueda observar una copia del tráfico de la red que debe analizar y no necesariamente el tráfico original (Modo Mirror), esto se logra configurando un puerto del switch en espejo.

1.4.3.1 Tipos de IDS

Se clasifican en dos tipos: de red y host. Cada tipo tiene unas capacidades diferentes en cuanto a los eventos detectables, por lo que en la práctica los IDS suelen nutrirse de sensores de ambos tipos.

a. NIDS (basados en red)

Puede monitorizar el tráfico que afecta a múltiples hosts que están conectados a un segmento de red.

Tabla 1.8: Ventajas y Desventajas de los NIDS
Referencia: http://www.rediris.es/cert/doc/pdf/ids-uv.pdf

Ventajas	Desventajas
▪ Bien localizado puede monitorizar una red grande. ▪ No interfieren en las operaciones habituales de la red (mínimo impacto).	▪ Pueden fallar en reconocer ataques lanzados durante periodos de tráfico alto. ▪ No analizan la información cifrada (p ej.: IPSec) ▪ Detectan el ataque, pero no conocen si tuvo éxito o no (debe realizarse una investigación manual por parte del administrador). ▪ Generación de Falsos Positivos[10].

[10] **Falsos Positivos:** Notifican que ha ocurrido algún evento (intrusión o anomalía), cuando realmente no ha ocurrido nada peligroso para el sistema. El Falso Negativo a su vez, se presenta cuando no se notifica una verdadera amenaza.

b. HIDS (basados en host)

Los HIDS se instalan en las máquinas que componen la red: tanto servidores como estaciones de trabajo. A diferencia de los NIDS estos entregan información de eventos más detallada (por ej.: se puede conocer si el ataque tuvo éxito o no).

Tabla 1.9: Ventajas y Desventajas de los HIDS
Referencia: http://www.rediris.es/cert/doc/pdf/ids-uv.pdf

Ventajas	Desventajas
▪ Pueden detectar ataques que no logran ser vistos por un NIDS. ▪ Puede analizar tráfico cifrado, ya que analiza antes de que los datos sean cifrados (host origen) y/o después de que sean descifrados (destino).	▪ Administración compleja, ya que deben ser configurados en cada host. ▪ Usan recursos del host que están monitorizando, influyendo en el rendimiento del sistema monitorizado. ▪ Cuando la máquina "cae" también lo hace el HIDS.

1.4.4 SISTEMA DE PREVENCIÓN DE INTRUSOS (IPS)

Los IPS a diferencia de los IDS, pueden tomar acciones específicas sobre los paquetes monitoreados, como impedir su paso por ejemplo, es decir siendo reactivos más no pasivos frente a un evento. De este modo, sus características se acercan más a la tecnología de los cortafuegos, pero basando su análisis en el comportamiento o contenido mismo del paquete, y no en la relación puerto/protocolo de la comunicación.

Para ello deben colocarse en medio del tráfico mismo que circula por un segmento de red, es decir, utilizando el puenteo o bridiging de sus interfaces y siendo transparente para el usuario (no posee dirección IP, lo cual evita la recepción de un determinado ataque).

A continuación se presenta una comparación de ciertas características tanto de IDS e IPS, para una mejor comprensión de sus funcionalidades:

Tabla 1.10: IDS vs IPS

Referencia: http://www.criptored.upm.es/guiateoria/gt_m142w.htm

Parámetro	**IDS**	**IPS**
Ubicación	Mirror	In line (puenteo)
Estabilidad	Caída del sistema quita información al analista de red. No es algo crítico.	Caída del sistema es catastrófica para la red.
Desempeño	La falta de procesamiento puede ser compensada con buffers de mucha memoria.	Requiere mayor capacidad de procesamiento.
Falsos Positivos	Carga de trabajo innecesaria para el analista en busca de falsas alarmas.	Produce bloqueos de paquetes válidos.
Falsos Negativos	Ataques resultan totalmente invisibles y pueden volver a ocurrir. Pérdida de información para el analista.	Paquetes maliciosos entran a la red.

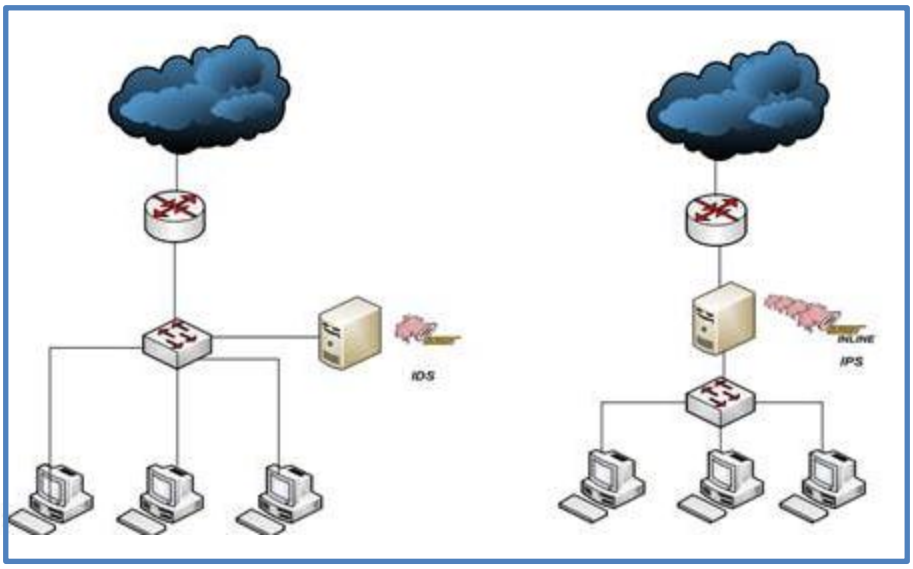


Figura 1.3: Ubicación IDS e IPS

Referencia: http://www.criptored.upm.es/guiateoria/gt_m142w.htm

1.4.4.1 Tipos de IPS

Los IPS se clasifican básicamente en dos tipos, según el extracto recuperado desde http://www.cybsec.com/upload/ESPE_IDS_vs_IPS.pdf.

a. IPS autónomos

Consisten en una aplicación en hardware, que utiliza su propia CPU y memoria. Se caracteriza por su elevado costo.

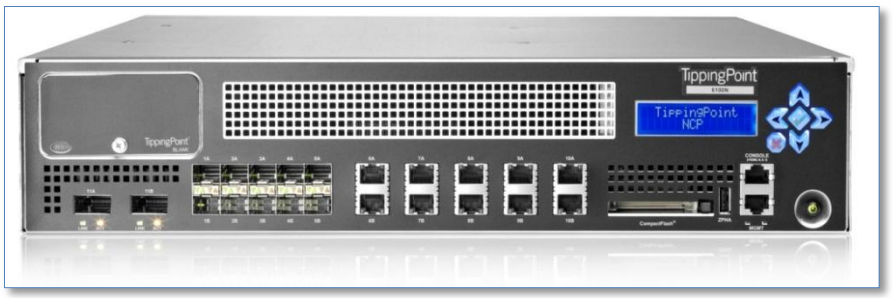


Figura 1.4: NIPS marca HP TippingPoint

Referencia: http://h17007.www1.hp.com/co/es/products/network-security/index.aspx

b. IPS Integrados

La estrategia de IPS ha evolucionado hacia los denominados IPS integrados, los cuales se orientan hacia una plataforma de software que busca integrarse a la infraestructura de red existente y que brinde opciones de implementación flexibles, inclusive estos IPS podrían acoplar sus funciones a los firewall tradicionales ya implementados en la red. Presentan los siguientes beneficios:

- **Menor costo:** Ahorro de costos, que incluye los gastos en compra de equipos y de capacitación continua.

- **Administración común:** El uso de múltiples soluciones de diferentes proveedores aumenta la dificultad de administración de la red y exige constantes capacitaciones al personal. Una solución integrada reduce la complejidad de la administración y reduce gastos por capacitaciones.

- **Política de seguridad unificada:** Pues todos los componentes de seguridad sean firewalls e IPS se guiarán en las mismas políticas establecidas, evitando fallos y ambigüedades.

La figura 1.5 muestra un ejemplo de IPS integrado en modo “in line”, trabajando de forma conjunta con un firewall, es decir, analizando alguna intrusión que no haya podido ser filtrada a priori por el mismo. Cabe indicar que esta ubicación requiere configuraciones de NAT al contrario de un IPS ubicado en un segmento de red interno.

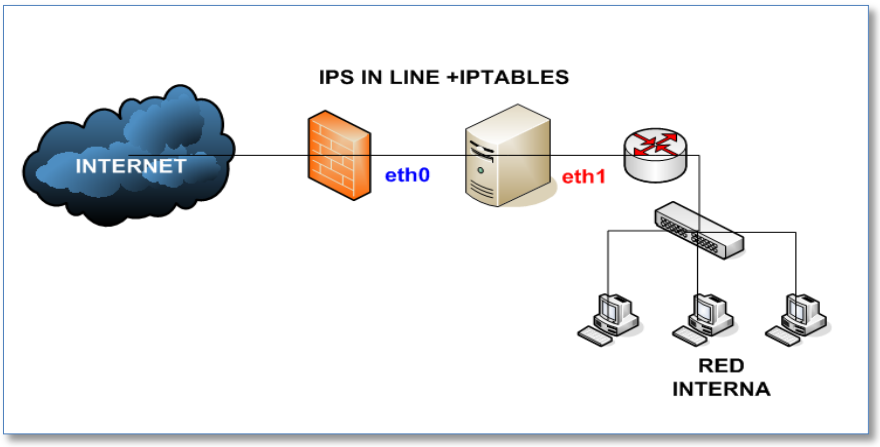


Figura 1.5: Arquitectura de IPS IN LINE

Referencia:http://www.adminso.es/index.php/Utilizaci%C3%B3n_de_Sistemas_de_Detecci%C3%B3n_de_Intrusos_como_Elemento_de_Seguridad_Perimetral

1.5 NORMAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN

Las organizaciones o empresas con el fin de proteger sus recursos informáticos, generalmente deciden invertir grandes cantidades de dinero en la implantación de medios técnicos que contrarresten amenazas externas múltiples, sin embargo, dejan de lado el factor humano, que es el eslabón más débil de la cadena de seguridad informática. Por ello es imprescindible la implantación de controles adecuados orientados tanto a usuarios, empleados y administradores de la red, mediante el establecimiento de políticas, buenas prácticas, procedimientos o estructuras organizativas, a fin de asegurar el cumplimiento de los objetivos de seguridad de la organización, alineados a estándares y normas internacionales de seguridad informática.

Nuestro país a través del Ministerio de Telecomunicaciones “ha adoptado a la Norma ISO 27000, como directriz para el establecimiento de los procesos que busquen minimizar los

riesgos en sistemas de información públicos". (Recuperado el 15 de Octubre del 2011, de http://www.mintel.gob.ec). Por tal motivo la investigación se centrará en el estudio de las mismas.

1.5.1 NORMA ISO 27000

Las normas ISO 27000 son una serie de estándares publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).El organismo encargado de la estandarización en el Ecuador es el Instituto Ecuatoriano de Normalización (INEN) el cual nombra a dicha Norma como NTE-INEN 27000 (Dentro de las Normas Técnicas Ecuatorianas).

La serie 27000 contiene las mejores prácticas recomendadas para desarrollar e implementar un Sistema de Gestión de la Seguridad de la Información (SGSI), entendiendo por SGSI como: "el proceso mediante el cual una organización conoce los riesgos a los que está sometida su información y los asume, minimiza o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente" (Recuperado el 16 de Octubre del 2011, de http://www.iso27000.es/sgsi).

Las Normas ISO 27000 tienen su origen en la Norma BS 7799-1 creada en 1995 por la primera entidad de normalización a nivel mundial llamada British Standards Institution (BSI), la cual se componía de un conjunto de buenas prácticas para la gestión de la seguridad de la información. En 1998 aparece la segunda parte de dicha norma como BS 7799-2 con los requisitos de un sistema de seguridad de la información. Para el año 2000, ISO adoptó la norma BS 7799-1 sin mayores cambios pero denominándola ISO 17799. En 2002 se revisó su

segunda parte para adecuarla a la filosofía de ISO y para el 2005 se publicó como ISO 27001, al mismo tiempo que se revisó y actualizó ISO17799 que sería renombrada como **ISO 27002:2005** el 1 de Julio de 2007. En 2009 fue publicada la ISO 27000 la cual contiene los términos y definiciones que se emplean en toda la serie 27000.La tabla siguiente resume las normas de la serie 27000 más importantes:

Tabla 1. 11: Resumen Normas Serie 27000

Referencia: http://www.iso27000.es

NORMA ISO	FECHA PUBLICACIÓN	CONTENIDO
27000	01 de Mayo de 2009.	Términos y definiciones, vocabulario.
27001	15 de Octubre de 2005.	Especifica los requisitos para la implantación del Sistema de Gestión de Seguridad de la Información (SGSI). Es la norma más importante de la familia.
27002	01 de Julio de 2007.	(Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799): Código de buenas prácticas para la gestión de Seguridad de la Información.
27003	01 de Febrero de 2010.	Directrices para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Es el soporte de la norma ISO/IEC 27001.
27004	7 de Diciembre de 2009.	Métricas para la gestión de Seguridad de la Información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información.
27005	4 de Junio de 2008.	Proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la

		Información, soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001.
27006	1 de Marzo de 2007	Específica requisitos específicos para la certificación del SGSI en las organizaciones.

1.5.1.1 Norma ISO 27002

Esta norma establece directrices y principios generales para iniciar, implementar o mantener la gestión de la seguridad de la información en una organización. Esta norma contiene objetivos de control y controles los cuales deben ser implantados para satisfacer los requerimientos de seguridad identificados previamente a través de una Evaluación de Riesgos (proceso de análisis y valoración de riesgos), y servirán de guía práctica para elaborar Normas de Seguridad para la Organización.

La norma contiene 11 dominios o capítulos principales que abarcan un total de 39 objetivos de control o categorías principales, además de un capítulo introductorio previo, como se presenta a continuación:

Tabla 1.12: Resumen Capítulos Normas 27002

Referencia: https://iso27002.es

CAPÍTULOS DE LA NORMA 27002	
Introducción	Contiene: • Conceptos e indicaciones generales. • Fechas de aprobación y revisión • Terminología, etc.
1. Política de seguridad	En este dominio se establecerá claramente los objetivos del documento, y se demostrará el apoyo y compromiso de la

	Gerencia con la seguridad de la información, a través de la publicación y mantenimiento de un documento de políticas de seguridad.
2.Aspectos organizativos para la seguridad	Se identifica a los participantes con responsabilidades para la elaboración, revisión y supervisión dentro del proceso de construcción de políticas y procedimientos.
3.Gestión de activos	En este dominio se debe realizar una clasificación de los activos, para asegurar que reciban un nivel de protección apropiado a sus niveles de riesgo.
4.Seguridad ligada a los recursos humanos	Este dominio trata de asegurar que cualquier empleado de una organización con acceso a los activos, adquiera un compromiso de confidencialidad, antes, durante y después de ejercer su cargo.
5.Protección Física y Ambiental	Este dominio trata de asegurar los activos físicos, a través del control de acceso y la protección contra contingencias externas (medioambientales).
6.Gestión de comunicaciones y operaciones	Este dominio trata de asegurar que la explotación de la infraestructura se realiza de forma segura y controlada. Para ello, define varios objetivos de control como: protección contra código malicioso, copias de seguridad, gestión de la seguridad de red, gestión de dispositivos de almacenamiento, etc.
7.Control de acceso	Este dominio cubre uno de los aspectos más importantes y evidentes respecto a la seguridad, la problemática del control de acceso a los sistemas de información. Para ello plantea los siguientes objetivos de control: gestión de los

	accesos de los usuarios, responsabilidades del usuario, control de acceso de red, control de acceso del sistema operativo, control de acceso a las aplicaciones, etc.
8.Adquisición, desarrollo y mantenimiento de los sistemas de información	Establece requisitos de seguridad en los sistemas de información, respecto al tratamiento correcto de las aplicaciones, uso de controles criptográficos, seguridad en los procesos, etc.
9.Gestión de incidentes de seguridad de la información	Este dominio trata de garantizar que los eventos y debilidades en la seguridad asociados sean notificados para de este modo, poder realizar las acciones correctivas oportunas y adecuadas.
10.Gestión de la continuidad del servicio	Este dominio trata de asegurar la disponibilidad de los servicios en caso de catástrofe, mediante un Plan de Continuidad del Servicio.
11.Cumplimiento	Este dominio trata de evitar el incumplimiento de las políticas y procedimientos de seguridad desarrollados.
Bibliografía:	Normas y publicaciones de referencia.
Índice	

CAPÍTULO II

2. ANÁLISIS DE RIESGOS EN LA RED DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA

Este capítulo describe el proceso de Análisis de Riesgos en la red administrativa del Gobierno Autónomo Descentralizado de Ibarra (GAD-I) mediante la Metodología MAGERIT v3, la cual propone técnicas y modelos estándar que simplifiquen las tareas de identificación de activos[11], amenazas[12] y niveles del riesgo[13] presentes en la red de la organización. Sus resultados permitirán obtener una visión real de las necesidades de seguridad presentes en la red, con el fin de crear medidas de protección efectivas para eliminar o controlar el riesgo de sufrir fallos en su seguridad.

2.1 MAGERIT

Los elementos de un sistema informático están expuestos a amenazas y niveles de riesgo que deberían ser plenamente identificados por su administrador para una adecuada gestión de la seguridad. Para ello han aparecido multitud de guías informales, metodologías y herramientas de soporte para la realización de este análisis. MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas) "es un método formal para investigar los riesgos que soportan los Sistemas de

[11] **Activos:** Son los elementos con los que cuenta un Sistema de Información dentro de una empresa los cuales aportan algún valor para la misma

[12] **Amenazas:** Causa potencial (intencional o fortuita), de un daño a cierto activo o grupo de activos.

[13] **Riesgo:** Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización

Información y para recomendar las medidas apropiadas que deberían adoptarse para controlarlos" (Recuperado el 23 de Abril del 2012, de http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=magerit).

Cabe destacar algunas ventajas que fueron tomadas en cuenta al momento de su elección:

- El texto de la Metodología originalmente fue escrita en idioma español, lo cual elimina las inexactitudes y ambigüedades de una traducción.
- El Análisis de Riesgos puede ser del tipo cuantitativo o cualitativo.
- Posee un extenso archivo de inventarios que facilita la identificación de Recursos de información, Activos y Amenazas.
- Contiene modelos estándar para homogenizar terminologías y criterios de análisis.
- Evalúa riesgos del tipo: intrínseco y efectivo.
- Valora en base a dimensiones distintas (disponibilidad, confidencialidad, integridad, autenticación y trazabilidad), para un análisis integral del riesgo.

2.1.1 OBJETIVOS

De acuerdo al Libro I: "Método" de MAGERIT v3, los objetivos principales que persigue la Metodología, son los siguientes:

- Concienciar a los responsables de manejar los sistemas de información, de la existencia de riesgo y la forma de minimizar o eliminar los mismos.

- Ofrecer un método ordenado para analizar los riesgos de una organización.
- Ayudar a descubrir y planificar los riesgos encontrados en una organización y así mantenerlos bajo control.
- Preparar a la organización para procesos de evaluación, auditoria y gestión, etc.

2.1.2 ESTRUCTURA DOCUMENTAL DE MAGERIT

MAGERIT v3**,** se ha estructurado en tres libros:

Tabla 2.1: Resumen libros MAGERIT

Referencia: Metodología MAGERIT –Libro I: Método

Método
• Expone de manera conceptual el proceso de Análisis y Gestión de Riesgos en general. • Describe los pasos para realizar un análisis del estado de riesgo y para gestionar su mitigación. • Muestra consejos prácticos para el desarrollo de cada uno de sus procesos.
Catálogo de Elementos
• Describe modelos estándar que sirvan de guías para el desarrollo de cada proceso del proyecto. • Promover una terminología y criterios uniformes que permitan homogeneizar los resultados del análisis.
Guía de Técnicas
• Describe un conjunto de Técnicas Específicas (Análisis mediante Tablas, Análisis Algorítmico, Arboles de ataque, etc.) y Generales (Análisis coste-beneficio, Diagramas de flujo de datos, Diagramas de procesos, Técnicas gráficas, Planificación de proyectos, Valoración Delphi, etc.) para proyectos de Análisis y Gestión de Riesgos.

2.1.3 FASES

MAGERIT se basa en el cumplimiento de tareas o fases, para llegar a determinar tanto el Riesgo intrínseco como el Riesgo efectivo, presentes en los sistemas de información, los cuales se describen a continuación:

Tabla 2.2: Fases MAGERIT

Referencia: Metodología MAGERIT-Libro I: Método

1) Estimación del Riesgo intrínseco
Mide la probabilidad de que una amenaza se materialice, sin tomar en cuenta el efecto de las salvaguardas[14] existentes en un sistema informático. Determina el efecto real de las amenazas.
Tareas: • Identificar y tipificar los activos relevantes de la institución. • Dimensionar los activos. • Valorar los activos en cada dimensión. • Determinar las amenazas a las que estarían expuestos los activos de la organización. • Valorar las amenazas sobre cada tipo de activo. Es decir, estimar las métricas Degradación [15] y Frecuencia[16]. • Calcular el impacto[17], al relacionar los parámetros: Valor del activo y Degradación. • Calcular el riesgo intrínseco, al relacionar el Impacto y Frecuencia (sin tomar en cuenta las salvaguardas existentes).

[14] **Salvaguardas:** Son las medidas de control que se despliegan para minimizar las amenazas que existan en la empresa.

[15] **Degradación:** Cuán perjudicado resultaría un activo en el supuesto de que se materializara cierta amenaza.

[16] **Frecuencia:** Cada cuanto se materializa una amenaza.

[17] **Impacto:** Es la medida del daño sobre el activo derivado de la materialización de una amenaza.

2) Estimación del Riesgo Efectivo
Mide la probabilidad de que una amenaza se materialice, pero tomando en cuenta el efecto de las salvaguardas existentes en un sistema informático. Diagnóstico de los niveles de riesgo actuales.
Tareas: • Identificar y tipificar las salvaguardas (del tipo preventiva[18] o limitante[19]) actualmente implementadas en la organización. • Estimar la eficacia de las salvaguardas, entre: No existente, Poco efectiva, Efectiva y Muy efectiva. • Revalorar las métricas Degradación y Frecuencia, esta vez tomando en cuenta las salvaguardas existentes. Utilizar estos nuevos valores para el cálculo del impacto y a su vez del Riesgo efectivo.

2.2 ANÁLISIS DE RIESGOS EN LA RED ADMINISTRATIVA DEL GAD IBARRA SIGUIENDO LA METODOLOGÍA MAGERIT

El proceso de Análisis del Riesgo en la red de una entidad, implica el conocimiento de los recursos que vale la pena proteger, de aquellos que son más importantes, de las amenazas de las que es necesario resguardarse y el potencial de cada una de ellas. De modo que se optimicen los esfuerzos dedicados a gestionar su protección y se determinen con precisión los requerimientos de la red en cuanto a seguridad.

[18] **Salvaguarda preventiva:** Reduce la frecuencia de las amenazas (aplicadas antes de su materialización).

[19] **Salvaguarda Limitante:** Limita el daño causado (reduce el impacto sobre el activo).

Para ello se utilizará un modelo cualitativo que caracterice los valores como: Altos, Medios, Bajos, etc., para la determinación del Riesgo Intrínseco y Efectivo, conforme se expone a continuación:

2.2.1 ESTIMACIÓN DEL RIESGO INTRÍNSECO

2.2.1.1 Identificación y Tipificación de Activos

MAGERIT muestra un catálogo estándar de activos dentro del Libro "Catálogo de Elementos" (ANEXO 1), donde los enlista y tipifica en grupos denominados: servicios, datos, aplicaciones (software), equipos informáticos, redes de comunicación, soportes de información, equipamiento auxiliar y personal.

De esta manera, se obtuvo un inventario de los activos más relevantes de la institución, el cual se detalla en el ANEXO 2 del presente proyecto. A continuación se resumen los resultados obtenidos:

Tabla 2.3: Resumen de la Identificación de Activos en el GAD-I
Referencia: Metodología MAGERIT

Activos del tipo SERVICIOS
Considerados como activos intangibles, que buscan satisfacer una necesidad del usuario. Su importancia para la organización, tiene que ver con el alto valor de pérdidas que supondría una interrupción de sus prestaciones.
Entre estos activos se encuentran los servicios finales (entregados), destinados a suplir las necesidades de la ciudadanía en general, tales como: servicios de rentas y recaudaciones, avalúos y catastros, actividades económicas, precios unitarios, administración de sistemas, gestión de privilegios, atención a usuarios internos y externos, etc. También constan los servicios recibidos

por la institución como: telefonía, internet, alarmas, entre otros.
Activos del tipo DATOS o ACTIVOS DE INFORMACIÓN Los datos o activos de información normalmente están agrupados en bases de datos o los almacenados en soportes de información. A través de los datos, una institución logra prestar sus servicios, de modo que su protección es ineludible.
Constan las bases de datos que dan soporte a aplicaciones importantes, tales como: bases de datos de Quipux, Olympo, Regyncont, Balance Score Card y correo electrónico. También se consideran los datos de respaldo, código fuente, código ejecutable y logs.
Activos del tipo APLICACIONES o SOFTWARE Se analizan aquellas aplicaciones o programas utilizados por la entidad para gestionar, analizar y transforman los datos, permitiendo la explotación de la información para la prestación de los servicios (se exceptúa el código fuente el cual es considerado como Activo de Información).
Se pueden agrupar como aplicaciones de desarrollo propio, donde constan los sistemas para: Avalúos y Catastros, Rentas y Recaudación, Actividades Económicas, Precios Unitarios, Transferencias de dominio, Administración de sistemas, entre otros. Aplicaciones subcontratadas como: Olympo (Contabilidad y Presupuestos), Balance Score Card (Gestión Municipal) y el Quipux (Gestión documental). Gestores de bases de datos PostgreeSQL, MySQL, Post GIS y sistemas operativos de servidores por ejemplo Debian, Windows Server 2000/2003, etc.
Activos del tipo EQUIPOS INFORMÁTICOS Activos físicos destinados a soportar directa o indirectamente los servicios que presta la organización, con responsabilidades para el procesado de datos, soporte de aplicaciones y almacenamiento de datos.
Forman parte de esta sección los servidores que alberga el Data Center de la entidad, con funciones para: el almacenamiento de bases de datos, soporte de aplicaciones como Olympo y Regycont, antivirus NOD32, gestión de correos y archivos, balanceo de cargas, entre otros. También forman parte de este ítem las estaciones de trabajo, impresoras tanto matriciales, de

tinta y láser, scánners y discos externos.
Activos del tipo REDES DE COMUNICACIÓN
Bienes físicos relacionados directamente al transporte de datos, entre equipos activos y pasivos de la red.
Se consideran aquellos equipos situados en el Data Center que se relacionan directamente con el transporte de datos en la red cableada, entre ellos: switchs, routers, patchpanels, racks, organizadores de cables, etc. Se identifica también el equipamiento wireless como: routers inalámbricos, radios, antenas y torres de los enlaces con las parroquias aledañas.
Activos del tipo SOPORTES DE INFORMACIÓN
Dispositivos físicos que la institución utiliza para almacenar su información de forma permanente o por periodos de tiempo considerables
Del tipo electrónicos como: storage, CD/DVD, discos externos y dispositivos USB o no electrónicos como material impreso.
Activos del tipo EQUIPAMIENTO AUXILIAR
Elementos físicos que dan soporte a los sistemas de información, sin estar directamente relacionados con datos.
Se encuentran los Sistemas de Alimentación Ininterrumpida (UPS), los equipos de aclimatación, tanto de precisión y el tipo split (de pared) que funciona como back up. Finalmente los recursos de suministro esencial como: papel para impresora, tóner, tinta para cartuchos, refrigerante, etc. Y los mobiliarios de la institución como: escritorios, sillas, mesas para computador, archiveros de documentos, armarios, entre otros, también forman parte de esta sección.
Activos del tipo INSTALACIONES
Se toma en cuenta el lugar donde se alojan los recursos del sistema informático y de comunicaciones en análisis.

Es así que en esta sección es considerado en primer lugar las instalaciones del edificio matriz del GAD Ibarra, las direcciones externas y ubicaciones donde están alojados equipos de comunicaciones desde centrales hasta torres para enlaces.
Activos del tipo PERSONAL En esta sección aparecen las personas relacionadas con los sistemas de información, desde usuarios, proveedores y administradores.
Constan usuarios internos (que acuden a las instalaciones) y externos a través de sitios web. También los administradores de bases de datos, analistas de sistemas, administradores de hardware y comunicaciones, técnicos de planta y proveedores tanto de aplicaciones como de equipos.

2.2.1.2 Dimensionamiento de los Activos

Esta tarea consiste en determinar en qué dimensión es valioso un activo, de acuerdo a su tipo. Entre las dimensiones a considerar están (MAGERIT v3, 2012):

- **Disponibilidad [D]:** Aseguramiento de que los usuarios autorizados tengan acceso a la información y sus activos asociados cuando éstos lo requieran. ¿Qué importancia tendría que el activo no estuviera disponible?
- **Integridad [I]:** Aseguramiento de que la información y los métodos de su procesamiento no hayan sido modificados sin autorización. ¿Qué importancia tendría que los datos o los métodos de su procesamiento fueran modificados fuera de control?
- **Confidencialidad [C]:** Aseguramiento de que el activo no sea accesible para aquellos usuarios no autorizados. ¿Qué importancia tendría que el activo fuera conocido por personas no autorizadas?

- **Autenticidad de los usuarios del servicio [A_S]:** Aseguramiento de que el usuario que acceda al servicio sea quien dice ser. ¿Qué importancia tendría que quien accede al servicio no sea realmente quien se cree?
- **Autenticidad del origen de los datos [A_D]:** Aseguramiento de que en todo momento se podrá conocer la fuente de los datos (No repudio). ¿Qué importancia tendría que los datos no fueran realmente atribuibles a quien se cree?
- **Trazabilidad del servicio [T_S]:** Aseguramiento de que en todo momento se podrá determinar cuál usuario hizo uso de un servicio, para qué y en qué instante. ¿Qué importancia tendría que no quedara constancia fehaciente del uso del servicio?
- **Trazabilidad de los datos [T_D]:** Aseguramiento de que en todo momento se podrá determinar cuál usuario accedió a los datos, para qué y en qué instante. ¿Qué importancia tendría que no quedara constancia del acceso a los datos?

2.2.1.3 Valoración de los Activos

En esta sección se valora un activo, al analizar el nivel del daño que provocaría a la institución, por ejemplo, en caso de que éste no estuviese disponible en todo momento (Disponibilidad), que haya sido modificado sin control (Integridad), que sea conocido por personas no autorizadas (Confidencialidad) o en alguna otra dimensión.

Para ello se puede utilizar cualquier escala de valores, siempre y cuando sea común para todas las dimensiones. Se ha elegido una escala de diez valores, dejando el valor 0 como un valor despreciable y valor 10 como máxima alerta de daño. En la siguiente tabla se detallan los criterios de valoración escogidos:

Tabla 2.4: Criterios de Valoración de los Activos

Referencia: Metodología MAGERIT-Libro II: Catálogo de Elementos

Valor	Nivel		Criterio
10	Muy Alto	MA	Daño muy grave a la organización
7-9	Alto	A	Daño grave a la organización
4-6	Medio	M	Daño importante a la organización
1-3	Bajo	B	Daño menor a la organización
0	Muy Bajo	MB	Irrelevante a efectos prácticos

A continuación se da una breve descripción de los resultados del proceso de Valoración de Activos, que se detalla en el ANEXO 2 del presente proyecto:

Tabla 2.5: Resumen de la Valoración de Activos en el GAD-I

Referencia: Metodología MAGERIT

Valoración de Activos del Tipo SERVICIOS
Dimensiones: ▪ Disponibilidad ▪ Autenticación del servicio ▪ Trazabilidad del servicio
✓ Los servicios entregados a usuarios internos generalmente tienen valores de disponibilidad elevados (entre altos y muy altos). ✓ El servicio de acceso a Internet, no genera valores importantes de daño al momento de evaluar su autenticación. ✓ El seguimiento al usuario (trazabilidad) no es prioridad para los servicios prestados por el GAD Ibarra.

Valoración de Activos del Tipo DATOS

Dimensiones:

- Disponibilidad
- Integridad
- Confidencialidad
- Autenticación de los datos
- Trazabilidad de los datos

- ✓ En el caso de tener datos no disponibles, genera inconvenientes a menor escala, en comparación con la indisponibilidad de un servicio.
- ✓ Los activos de información o datos, generan alertas máximas al momento de evaluar su integridad.
- ✓ Los datos confidenciales corresponden a los usados para el desarrollo de aplicaciones propias o información sensible (datos personales, claves, documentos individuales, respaldos, etc.) almacenada en las bases de datos.
- ✓ Es trascendental la acción de determinar el origen de los datos en todo momento (autenticación).
- ✓ Los valores de trazabilidad en los datos superan a la de los servicios, ya que indudablemente el manejo de datos necesita un mayor seguimiento, que informe acerca de: quien los usó, en qué instante y por qué razón.

Valoración de Activos del Tipo APLICACIONES

Dimensiones:

- Integridad
- Autenticación del servicio
- Autenticación de los datos
- Trazabilidad del servicio
- Trazabilidad de los datos

- ✓ Violaciones en la integridad de la estructura de las aplicaciones podrían generar, al igual que en los datos, daños graves o muy graves a la organización.
- ✓ La importancia de la autenticación en una aplicación, depende del tipo de datos a los que se quiere acceder y a los privilegios que vayan a ser entregados al usuario, que van desde realización de consultas hasta autorizaciones para modificar los datos.
- ✓ La importancia de la Trazabilidad del usuario de una aplicación (cuál usuario hizo uso de la aplicación, para qué y en qué instante), también obedece al nivel de permisos con los que éste cuente.

Valoración de Activos del Tipo EQUIPOS INFORMÁTICOS

Dimensiones:

- Disponibilidad
- Trazabilidad del servicio
- Trazabilidad de los datos

- ✓ Los activos de hardware no han sido valorados por su costo económico de adquisición, sino en base al nivel de daño que causaría a la institución, en el supuesto que no estuvieren disponibles.
- ✓ Los servidores soportan las aplicaciones, datos y por ende todos los servicios que presta la institución, de modo que su valoración (en todas las dimensiones) sobresale de la de los demás activos de hardware.

Valoración de Activos del Tipo REDES DE COMUNICACIÓN

Dimensiones:

- Disponibilidad
- Trazabilidad del servicio
- Trazabilidad de los datos

- ✓ Los activos más importantes, corresponden a switchs y routers ubicados en el Data Center de la institución, tomando en consideración que su indisponibilidad provocaría la

caída de la red principal.

- ✓ Las dimensiones trazabilidad del servicio y datos también generan valores altos, por la necesidad de dar seguimiento a sus usuarios con tareas de configuración y operación de estos activos.

Valoración de Activos del Tipo SOPORTES DE INFORMACIÓN

Dimensiones:

- Disponibilidad
- Trazabilidad del servicio
- Trazabilidad de los datos

- ✓ Destacan los soportes que almacenan mayor cantidad de información o la más sensible. Con esta consideración son prioridad en todas las dimensiones, los storage de los servidores y discos externos.

Valoración de Activos del Tipo EQUIPAMIENTO AUXILIAR

Dimensiones:

- Disponibilidad

- ✓ El valor de equipos auxiliares como equipos de aclimatación o sistemas de alimentación ininterrumpida, es superlativo para un sistema informático que busque disponibilidad absoluta, frente a posibles variaciones de temperatura que afecten el óptimo desempeño de los equipos o cortes inesperados de energía.

Valoración de Activos del Tipo INSTALACIONES y PERSONAL

Dimensiones:

- Disponibilidad
- Autenticación del servicio

- ✓ Respecto a las instalaciones, se consideran relevantes aquellas que alojan los equipos de valoración sobresaliente. De modo que las instalaciones del Data Center poseen valores de disponibilidad altos y con requerimientos de autenticación para su acceso.

- ✓ Sobre el personal, se valorizan con mayor magnitud a aquellas personas que están relacionadas con la configuración, manipulación y mantenimiento de los datos (administradores de BDD) y de los medios para su transporte (administradores de redes). Así mismo, estos administradores deben ser correctamente autenticados para evitar errores o ataques por parte de personal no permitido.

2.2.1.4 Identificación de Amenazas

Se considera amenaza a "cualquier causa potencial, ya sea intencional o fortuita, de un daño a un recurso de información y por ende a los activos de información que dicho recurso soporta" (Recuperado el 24 de Abril del 2012, de http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf).

Para el proceso de Identificación de Amenazas se ha tomado como base el inventario de Amenazas del libro "Catálogo de Elementos" de MAGERIT (ANEXO 3) del presente estudio. De esta manera se observa que las amenazas podrían ser de origen natural (terremotos, inundaciones, etc.) o industrial (contaminación, fallos eléctricos, etc.). Causadas por personas de manera accidental o intencional (ataques).

2.2.1.5 Valoración de las Amenazas

En esta tarea de Valoración de las Amenazas se determinará en primer lugar la Degradación del activo, es decir, se debe evaluar el valor que pierde cada activo (medida del daño en porcentaje) si fuese víctima de una amenaza.

Además se establecerá la Frecuencia (o Probabilidad) con la que puede ejecutarse una amenaza. Para este proyecto se ha optado por establecer la **Frecuencia** en la que se puede materializar una amenaza, por la facilidad de comprensión y manejo de este parámetro al momento de evaluarlo.

A continuación se muestran los valores a considerar al momento de la evaluación:

Tabla 2.6: Escalas de Degradación y Frecuencia
Referencia: Metodología MAGERIT-Libros I y II

DEGRADACIÓN del Activo	
MA	MUY ALTA (100% del Activo)
A	ALTA (80% del Activo)
M	MEDIA (50% del Activo)
B	BAJA (10% del Activo)
MB	MUY BAJA (1% del Activo)
FRECUENCIA de Materialización	
MF	MUY FRECUENTE (A diario)
F	FRECUENTE (Mensual)
FN	FRECUENCIA NORMAL (Anual)
PF	POCO FRECUENTE (Cada varios años)

Para el cálculo de la Degradación y Frecuencia en esta sección, no se considera el efecto de las salvaguardas actualmente implementadas. La tabla 2.7 muestra la Valoración de las Amenazas más importantes por cada grupo de activos (La valoración se muestra a detalle en el ANEXO 2).

Tabla 2.7: Resumen de la Valoración de Amenazas en el GADI

Referencia: Metodología MAGERIT

VALORACIÓN AMENAZAS (SIN SALVAGUARDAS)		
Sobre ACTIVOS del grupo SERVICIOS		
AMENAZA	**DEGRADACIÓN**	**FRECUENCIA**
E.24 (Caída por agotamiento de recursos)	A	FN
A.5 (Suplantación ident. Usuario)	MA	PF
A.24 (Denegación de servicio)	MA	FN
Sobre ACTIVOS del grupo DATOS		
AMENAZA	**DEGRADACIÓN**	**FRECUENCIA**
E.1 (Errores de los usuarios)	A	F
E.2 (Errores del administrador)	A	FN
E.8 (Difusión software dañino)	A	MF
E.16 (Introducción de información incorrecta)	MA	FN
E.19 (Divulgación de Información)	A	F
A.11 (Acceso no autorizado)	MA	PF
A.15 (Modificación información)	MA	PF
Sobre ACTIVOS del grupo APLICACIONES		
AMENAZA	**DEGRADACIÓN**	**FRECUENCIA**
E.2 (Errores del administrador)	A	FN
E.8 (Difusión software dañino)	A	MF
E.20 (Vulnerabilidades del software)	A	PF

E.21 (Errores de Mantenimiento software)	MA	FN
A.4 (Manipulación configuración)	MA	FN
A.11 (Acceso no autorizado)	MA	PF
Sobre ACTIVOS del grupo EQUIPOS INFORMÁTICOS		
AMENAZA	**DEGRADACIÓN**	**FRECUENCIA**
I.1 (Fuego)	MA	PF
I.2 (Agua)	MA	PF
I.5 (Avería física)	A	FN
E.2 (Errores del administrador)	A	FN
E.23 (Errores de Mantenimiento hardware)	A	FN
A.4 (Manipulación configuración)	A	PF
A.11 (Acceso no autorizado)	A	PF
Sobre ACTIVOS del grupo REDES DE COMUNICACIÓN		
AMENAZA	**DEGRADACIÓN**	**FRECUENCIA**
I.5 (Avería física)	A	FN
I.8 (Fallo servicios comunicaciones)	A	FN
E.2 (Errores del Administrador)	A	FN
A.4 (Manipulación configuración)	A	PF
A.11 (Acceso no autorizado)	A	PF
Sobre ACTIVOS del grupo SOPORTES DE INFORMACIÓN		
AMENAZA	**DEGRADACIÓN**	**FRECUENCIA**
I.5 (Avería física)	MA	FN

I.10 (Degradación de los S.I.)	A	PF
Sobre ACTIVOS del grupo EQUIPAMIENTO AUXILIAR		
AMENAZA	**DEGRADACIÓN**	**FRECUENCIA**
I.5 (Avería física)	A	FN
Sobre ACTIVOS del grupo INSTALACIONES		
AMENAZA	**DEGRADACIÓN**	**FRECUENCIA**
A.26 (Ataque destructivo)	A	PF
Sobre ACTIVOS del grupo PERSONAL		
AMENAZA	**DEGRADACIÓN**	**FRECUENCIA**
E.7 (Deficiencias organización)	A	FN
A.29 (Extorsión)	M	PF
A.30 (Ingeniería social)	A	PF

2.2.1.6 Estimación del Impacto

Impacto "es la medida del daño sobre el activo, derivado de la materialización de una amenaza". (Recuperado el 5 de Mayo del 2012, de www.rediris.es/difusion/eventos/forosseguridad/fs2012/archivo/analisis_riesgos_upct.pdf).

Para la valoración del Impacto, MAGERIT utiliza la técnica de Análisis mediante Tablas (descrita en el libro "Guía de Técnicas"), es decir, mediante una tabla de dos entradas que compara los parámetros: Valor del activo (en cada dimensión) y la Degradación causada por cierta Amenaza (Tabla 2.8).

Tabla 2.8: Estimación del Impacto a través del Análisis de Tablas (MAGERIT)

Referencia: Metodología MAGERIT-Libro III: Guía de Técnicas

IMPACTO		DEGRADACIÓN				
		1%(MB)	10%(B)	50%(M)	80%(A)	100%(MA)
VALOR (Nivel)	MA	M	A	A	MA	MA
	A	B	M	M	A	A
	M	MB	B	B	M	M
	B	MB	MB	MB	B	B
	MB	MB	MB	MB	MB	MB

Enseguida se muestra un ejemplo donde se calcula el Impacto en ciertos activos de la institución (El cálculo del Impacto se indica en el ANEXO 2).

Tabla 2.9: Ejemplo de Estimación del Impacto activos GADI

Referencia: Metodología MAGERIT

EQUIPOS INFORMÁTICOS

ACTIVO	AMENAZA	DISPONIBILIDAD [D]			
		Valor	Nivel	Degradación	Impacto
Servidor Blade 3000	I.1 (Fuego)	10	MA	MA	MA
	E.2 (Errores Admin.)	10	MA	A	MA
PC HP 6200 Pro	I.1 (Fuego)	5	M	MA	M
	E.2 (Errores Admin.)	5	M	A	M
Impresoras	I.1 (Fuego)	4	M	MA	M
	I.3 (C. Mecánica)	4	M	M	B

2.2.1.7 Determinación del Riesgo

El riesgo "es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos de una organización" (Recuperado el 10 de Mayo del 2012, de www.rediris.es/difusion/eventos/foros-seguridad/fs2012/archivo/analisis_riesgos_upct.pdf).

Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la frecuencia de ocurrencia**.**

Para la valoración del Riesgo, la Metodología MAGERIT compara el valor del Impacto y la Frecuencia, como muestra la Tabla 2.10. El riesgo resultante es llamado Riesgo Intrínseco, refiriéndose al riesgo en el sistema sin valorar la eficacia de las salvaguardas implantadas actualmente o las previstas en un Plan de Seguridad (de Gestión del Riesgo).

Tabla 2.10: Estimación del Riesgo a través del Análisis de Tablas (MAGERIT)
Referencia: Metodología MAGERIT-Libro III: Guía de Técnicas

RIESGO		FRECUENCIA			
		PF	**FN**	**F**	**MF**
IMPACTO	**MA**	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

En la tabla siguiente se muestra un ejemplo donde se estima el Riesgo Intrínseco en activos del tipo Equipos Informáticos de la institución (El cálculo del Riesgo Intrínseco se muestra en el ANEXO 2).

Tabla 2.11: Ejemplo de Estimación del Riesgo Intrínseco activos GADI

Referencia: Metodología MAGERIT

EQUIPOS INFORMÁTICOS

ACTIVO	AMENAZA	DISPONIBILIDAD [D]					
		Valor	Nivel	Degr	Imp	Frec.	R I
Servidor Blade 3000	I.1 (Fuego)	10	MA	MA	MA	PF	A
	E.2 (Errores Admin.)	10	MA	A	MA	FN	MA
PC HP 6200 Pro	I.1 (Fuego)	5	M	MA	M	PF	B
	E.2 (Errores Admin.)	5	M	A	M	FN	M
Impresoras	I.1 (Fuego)	4	M	MA	M	PF	B
	I.3 (C. Mecánica)	4	M	M	B	FN	B

2.2.2 ESTIMACIÓN DEL RIESGO EFECTIVO

2.2.2.1 Identificación de las Salvaguardas existentes

Las salvaguardas son las medidas establecidas por la institución para mitigar sus riesgos. Al ser implementadas permiten reducir la frecuencia de ocurrencia de las amenazas (salvaguardas preventivas), la degradación causada por ellas (salvaguardas limitantes) o ambas.

Los Niveles de efectividad que puede crear el despliegue de salvaguardas son los siguientes:

Tabla 2.12: Niveles de efectos de las salvaguardas

Referencia: Metodología MAGERIT

NIVELES DE EFECTIVIDAD	
No existe (NE)	Ninguna salvaguarda está implementada para una determinada amenaza.
Poca efectividad (PE)	La salvaguarda tiene un impacto indirecto o general sobre la amenaza.
Efectivo (E)	La salvaguarda reduce la frecuencia o el impacto de la amenaza de forma significativa.
Muy efectivo (ME)	Salvaguarda específicamente diseñada para la amenaza.

A continuación se describe a modo informativo las principales salvaguardas implantadas actualmente en la entidad:

- La Dirección de TIC ejecuta programas de mantenimiento preventivo de equipos con un intervalo de dos años, buscando minimizar las fallas por averías físicas que eviten mantenerlos disponibles en todo momento.

- Para contrarrestar ataques por difusión de malware, la entidad cuenta con un servidor de antivirus ESET NOD32, sin embargo, ataques más sofisticados no podrían ser detectados con estos mecanismos tradicionales.

- Existen claves y niveles de acceso para cada miembro del personal, que eviten la manipulación de aplicaciones y datos por personas no autorizadas.

- Se ejecutan automáticamente registros de auditorías dentro de aplicaciones, con las cuales se determina qué usuario y en qué instante realizó modificaciones en los datos.

- El acceso físico tanto a las instalaciones de la entidad como al Centro de Datos ubicado en la Dirección de TIC, es regulado mediante guardianía privada y un sistema electrónico de control de acceso respectivamente.

- Posee extinguidores de incendios, drenajes de agua y estructuras antisísmicas para contrarrestar amenazas del tipo industrial o natural.

En el ANEXO 4 se muestra el proceso completo de identificación de las salvaguardas desplegadas actualmente en la institución, se realiza la tipificación y estimación de la efectividad de las mismas.

2.2.2.2 Revalorización de las Amenazas

El siguiente paso para llegar a establecer el Riesgo Efectivo, es determinar las métricas Degradación y Frecuencia efectivas, es decir, considerando la efectividad de las salvaguardas actuales. De modo que, salvaguardas del tipo limitante influirán en los valores de Degradación (Tabla 2.13), a su vez salvaguardas del tipo preventivo, revalorizarán valores de Frecuencia (Tabla 2.14) y salvaguardas del tipo Limitante /Preventivo, generan nuevos valores en ambas métricas.

Tabla 2.13: Estimación de la Degradación Efectiva

Referencia: Metodología MAGERIT-Libro III: Guía de Técnicas

DEGRADACIÓN EFECTIVA		EFECTIVIDAD SALVAGUARDA LIMITANTE			
		NE	**PE**	**E**	**ME**
DEGRADACIÓN	**MA**	MA	A	M	B
	A	A	M	B	B
	M	M	B	MB	MB
	B	B	MB	MB	MB
	MB	MB	MB	MB	MB

Tabla 2.14: Estimación de la Frecuencia Efectiva

Referencia: Metodología MAGERIT-Libro III: Guía de Técnicas

FRECUENCIAEFECTIVA		EFECTIVIDAD SALVAGUARDA PREVENTIVA			
		NE	**PE**	**E**	**ME**
FRECUENCIA	**MF**	MF	F	FN	PF
	F	F	FN	PF	PF
	FN	FN	PF	PF	PF
	PF	PF	PF	PF	PF

A continuación se detalla un ejemplo que demuestra los nuevos valores de degradación o frecuencia, de acuerdo al tipo de salvaguarda desplegada en cada activo:

Tabla 2.15: Ejemplo de Revalorización Amenazas

Referencia: Metodología MAGERIT

EQUIPOS INFORMÁTICOS

ACTIVO	AMENAZA	SALVAG.		DISPONIBILIDAD [D]			
		Tipo	E	Deg	Deg E	Frec.	Frec. E
Servidor Blade 3000	I.1 (Fuego)	Lim.	E	MA	M	PF	PF
	E.2 (Errores Admin.)	_	NE	A	A	FN	FN
PC HP 6200 Pro	I.1 (Fuego)	Lim.	E	MA	M	PF	PF
	A.4 (Manip. config.)	Pre	E	A	A	FN	PF
	I.1 (Fuego)	Lim.	E	MA	M	PF	PF
	I.3 (C. Mecánica)	Pre. /Lim	E	M	MB	FN	PF

2.2.2.3 Estimación del Impacto y Riesgo Efectivo

Para el cálculo del Impacto y Riesgo Efectivo, se hace uso de las Tabla 2.8 y 2.10 antes indicadas, simplemente tomando en cuenta los valores de Degradación y Frecuencia Efectivas, tal como se muestra a continuación:

Tabla 2.16: Ejemplo de Estimación del Impacto y Riesgo Efectivos activos GADI

Referencia: Metodología MAGERIT

EQUIPOS INFORMÁTICOS

ACTIVO	AMENAZA	SALVAG.		DISPONIBILIDAD [D]				
		Tipo	E	Nivel Valor	Deg E	Frec. E	Imp. E	R E
Servidor	I.1 (Fuego)	Lim.	E	MA	M	PF	**A**	**M**

Blade 3000	E.2 (Errores Admin.)	_	NE	MA	A	FN	**MA**	**MA**
Impresoras	I.1 (Fuego)	Lim.	E	M	M	PF	**B**	**MB**
	I.3 (C. Mecánica)	Pre. /Lim	E	M	MB	PF	**MB**	**MB**

2.2.3 TRATAMIENTO DE LOS RESULTADOS

En síntesis, el proceso de Análisis de Riesgos tiene por objeto identificar "QUÉ ACTIVOS SE DEBEN PROTEGER", y "DE QUÉ SE LOS DEBE PROTEGER". Para ello se ha considerado los Activos con niveles de Riesgo Alto (A) y Muy Alto (MA), y aquellas Amenazas que los colocan en esa posición, en otras palabras se enlistan aquellas Amenazas resultantes y el grupo de Activos críticos. Los resultados finales del proceso se indican en el ANEXO 5.

A partir de estos resultados se procede a desarrollar soluciones para reducir o aceptar dicho riesgo (Gestión del Riesgo), a través de la incorporación de nuevas medidas técnicas o administrativas y el cumplimiento de otras ya existentes.

CAPÍTULO III

3. ELABORACIÓN DE POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

En este capítulo se desarrolla el Manual de Políticas y Procedimientos de Seguridad de la Información, destinados a usuarios y administradores de los activos informáticos del GAD Ibarra.

3.1 INTRODUCCIÓN

Esta medida está respaldada por los resultados obtenidos en el Análisis de Riesgos realizado en el capítulo anterior. A través de MAGERIT fueron revelados riesgos potenciales que provienen de amenazas relacionadas a errores intencionados y no intencionados por parte del personal de la institución, entre ellos: la introducción de información incorrecta, el escape, alteración o divulgación de datos, los errores de mantenimiento, la difusión de software dañino, entre otros. De esta manera se ha propuesto crear esta normativa que pretende guiar el comportamiento profesional y personal de los funcionarios de la institución, permitiendo unificar y/o modelar sus tareas y responsabilidades, para encontrar las mejores prácticas en el manejo de los recursos informáticos o simplemente para el cumplimiento de regulaciones legales o técnicas. En consecuencia, se han adoptado algunos de los controles de la Norma ISO 27002, como guía para la estructuración del documento, respecto al uso de términos, definiciones y demás directrices que forman parte de este reconocido estándar.

Finalmente cabe destacar que la guía en cuestión, no pretende ser la única estrategia para corregir las deficiencias de seguridad encontradas y tendrá como apoyo, el diseño e implementación de medios técnicos de protección, como es el caso del Sistema de Prevención de Intrusos sobre software libre (su diseño se muestra en el capítulo IV), el cual permite mitigar amenazas informáticas comunes con el fin de crear una solución eficiente, íntegra y de bajo costo.

GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA

MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

	Versión:	1.0.0
	Revisado por:	▪ Lcdo. Miguel Tobar Reina/*Jefe del Área de Hardware y Comunicaciones.* ▪ Ing. Irving Reascos Paredes/*ex Director de TIC GAD Ibarra.*
	Aprobado por:	▪ Ing. Paúl Barahona Salas/*Director de TIC*.
	Fecha de Aprobación:	

I. PROPÓSITO

El presente documento tiene como finalidad dar a conocer las Políticas y Procedimientos de Seguridad de la Información que deberán observar y cumplir los usuarios de los activos informáticos del GAD Ibarra, con el fin de resguardar su información, manteniendo la disponibilidad, confidencialidad e integridad de la misma.

II. CONCEPTOS PRELIMINARES

- **Seguridad de la Información**

Es el conjunto de reglas, planes y acciones, que buscan: proteger la información sensible de una organización, resguardar los recursos que la soportan, y las personas que la utilizan. Todo esto independientemente del lugar en que se encuentre, ya sea impresa en papel, registrada en medios de almacenamiento electrónicos o incluso en la memoria de las personas que la conocen.

- **Política de Seguridad**

Una política permite establecer un canal de comunicación con el usuario de un sistema informático, sea éste empleado, administrador, gerente o usuario final, indicándole cómo actuar frente a un recurso determinado del sistema, a través del establecimiento de reglas, normas o controles que determinan lo que está o no permitido realizar, con el fin de preservar la seguridad de los activos informáticos, especialmente los datos.

- **Procedimiento de Seguridad**

Un procedimiento se define como una sucesión de operaciones concatenadas entre sí, las cuales buscan orientar las tareas del usuario y/o administrador de los recursos informáticos, conforme a los objetivos planteados por las políticas de seguridad.

III. GENERALIDADES

a) Este documento está redactado de manera sencilla (sin tecnicismos), para que pueda ser interpretado por cualquier persona que ostente un cargo dentro de la entidad o terceros, con conocimientos informáticos o sin ellos.

b) Las políticas expuestas en este documento sirven de referencia, en ningún momento pretenden ser reglas absolutas, ya que están sujetas a cambios realizables en cualquier momento, siempre y cuando se tengan presentes los objetivos de seguridad.

c) Toda persona que haga uso de los activos informáticos del GAD Ibarra, deberá conocer y aceptar todo lo establecido en el documento de políticas de seguridad, el desconocimiento del mismo, no exonera de responsabilidad al usuario ante cualquier eventualidad que involucre la seguridad de la información o de la red institucional.

d) El lector de las políticas y procedimientos deberá enmarcar sus esfuerzos por cumplir todas las políticas pertinentes a su entorno de trabajo, sin importar el nivel organizacional en el que se encuentre dentro de la institución.

IV. NIVELES ORGANIZACIONALES

a) Gerencia.- Autoridad de nivel superior. Bajo su administración están la aceptación de las políticas de seguridad, en concordancia con el Gestor de Seguridad y la Unidad de Informática.

b) Gestor de Seguridad.- Persona encargada del análisis previo del estado de seguridad de la institución mediante evaluaciones del riesgo o auditorías, y de la gestión de los mismos a través de la elaboración de documentos de seguridad (políticas, normas, procedimientos) en coordinación con la Unidad de Informática.

c) Unidad de Informática.- Entidad o Departamento dentro de la institución, que vela por todo lo relacionado con la utilización de computadoras, sistemas de información, redes informáticas, procesamiento de datos e información.

Responsable de la elaboración de los documentos de seguridad, revisión y actualización del mismo. (Dirección de TIC).

d) Responsable de Activos.- Personal dentro de los diferentes departamentos administrativos de la institución, que tiene a cargo uno o más activos informáticos críticos o no críticos. Están obligados a velar por la seguridad y correcto funcionamiento de los mismos, entorno a sus respectivas áreas o niveles de mando.

V. VIGENCIA

La documentación presentada como normativa de seguridad entrará en vigencia desde el

momento en que éste sea aprobado como documento técnico de seguridad informática por las autoridades correspondientes del GAD Ibarra. Esta normativa deberá ser revisada y actualizada conforme a las exigencias de esta dependencia, o en el momento en que haya la necesidad de realizar cambios sustanciales en la infraestructura tecnológica de la Red Institucional.

VI. REFERENCIA

El documento se encuentra estructurado en base a los siguientes dominios y controles tomados de la Norma **ISO/IEC 27002:2005:**

1. Política de Seguridad de la Información

1.1 Objetivo de la Política de Seguridad

1.2 Compromiso de las Autoridades

2. Gestión de los Activos

2.1 Responsabilidad sobre los Activos

2.2 Clasificación de la Información

3. Seguridad Ligada a los Recursos Humanos

3.1 Antes del empleo

3.2 Durante el empleo

3.3 Cese del empleo

4. Seguridad Física y del Entorno

4.1 Seguridad de los equipos

4.2 Mantenimiento de los equipos

5. Gestión de Comunicaciones y Operaciones

5.1 Responsabilidades y procedimientos de operación

5.2 Planificación y aceptación del sistema

5.3 Protección contra el código malicioso y descargable

5.4 Copias de seguridad de la información

5.5 Manipulación de los medios de almacenamiento

5.6 Supervisión

6. Control de Acceso

6.1 Gestión de acceso de usuario

6.2 Responsabilidades del usuario

6.3 Control de acceso a la red

6.4 Control de acceso al sistema operativo

6.5 Control de acceso a las aplicaciones

7. Gestión de incidentes en la seguridad de la información.

7.1 Gestión de incidentes y mejoras de seguridad de la información

8. Cumplimiento

8.1Cumplimiento de las políticas y normas de seguridad

VII. TÉRMINOS Y DEFINICIONES

Activos	Conjunto de bienes tangibles e intangibles que son propiedad de una persona física o entidad. En el ambiente informático, llámese activo a los bienes de información y procesamiento que posee la institución.
Amenaza	Evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Archivo Log	Registros en los que se anotan los pasos que da un usuario dentro de una aplicación informática (horarios de conexión, terminales y direcciones involucradas en el proceso, etc.)
Área de trabajo	Lugar físico donde uno o más usuarios desarrollan sus tareas, en coordinación con recursos de hardware/software, dentro de un sistema informático.
Base de datos	Serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información de una entidad.
Data Center	Instalación empleada para albergar los sistemas de información y sus componentes asociados, como las comunicaciones y los sistemas de almacenamiento. Generalmente incluye fuentes de alimentación redundantes o de respaldo, conexiones redundantes de comunicaciones, controles de ambiente (por ejemplo, aire acondicionado) y otros dispositivos de seguridad.
Clave de acceso	Es la contraseña que un usuario emplea para acceder a un servicio, sistema o programa, creando un escudo ante los usuarios no autorizados.
Código Fuente	Es un programa en su forma original, tal y como fue escrito por el programador, no es ejecutable directamente por el computador, debe convertirse en lenguaje de máquina mediante compiladores.
Código malicioso	Software o fragmento del mismo que genera algún tipo de

(malware)	problema en el sistema en el cual se ejecuta, interfiriendo de esta forma con el normal funcionamiento del mismo. Virus, gusanos, troyanos son algunos ejemplos de código malintencionado.
Confidencialidad	Nadie puede acceder a la información sin haber sido autorizado.
Cuenta de acceso	Mecanismo de identificación de un usuario. Método de acreditación del usuario mediante procesos lógicos dentro de un sistema informático.
Dirección de TIC	Departamento perteneciente al GAD Ibarra, que vela por todo lo relacionado con la utilización de computadoras, sistemas de información, redes informáticas, procesamiento de datos e información y la comunicación en sí, a través de medios electrónicos.
Dirección IP	La dirección IP está compuesta por un número que permite identificar un dispositivo (por lo general, una computadora) que se encuentra dentro una red que utiliza el protocolo de Internet.
Disponibilidad	Los usuarios que necesitan la información y a quienes va dirigida dicha información siempre tienen acceso a ella.
Encriptación	Proceso mediante el cual cierta información es cifrada de forma que el resultado sea ilegible a menos que se conozcan los datos necesarios para su interpretación y así evitar que ésta no pueda ser obtenida con facilidad por terceros.

Estación de trabajo (Workstation)	Es un dispositivo final (generalmente un ordenador o PC) que facilita a los usuarios el acceso a los servicios que brinda la red.
Hardware	Dispositivos físicos (tangibles) dentro de un sistema informático.
Integridad	Nadie puede modificar el contenido de la información o los archivos y aún menos eliminarlos.
Intranet	Red de equipos que es interna a una organización y es compatible con aplicaciones de Internet.
ISO (Organización Internacional de Estándares)	Institución internacional reconocida y acreditada para normar en temas de estándares en una diversidad de áreas, aceptadas y legalmente reconocidas.
IEC (Comisión Electrotécnica Internacional)	Junto a la ISO, desarrolla estándares que son aceptados a nivel internacional.
Medios de almacenamiento	Dispositivos físicos donde se almacenan datos de forma temporal o permanente.
Niveles de permisos de acceso	Determina el conjunto de tareas que el usuario está permitido ejecutar en un entorno determinado, como dentro de una aplicación por ejemplo.
Norma ISO/IEC 27002:2005	Norma internacional que vela por que se cumplan los requisitos mínimos de seguridad, que propicien un nivel de seguridad aceptable y acorde a los objetivos institucionales, desarrollando buenas prácticas para la gestión de la seguridad

	informática.
Plan de Contingencia	Plan que contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y las operaciones de una entidad en caso de un desastre.
Red	Conjunto de computadoras y elementos interconectados que permiten una comunicación entre sí y forman parte de un mismo ambiente.
Responsabilidad	En términos de seguridad, significa determinar qué individuo en la institución, es responsable directo de mantener seguros los activos de cómputo e información.
Servidores	Es un ordenador de mayores prestaciones, capacidades de procesamiento y memoria, que se encarga de proveer servicios a otros ordenadores y programas clientes.
Sistema informático	Conjunto de elementos interrelacionados entre hardware y software, para el tratamiento de la información.
Software	Dispositivos lógicos (intangibles) dentro de un sistema informático. Compuesto por todos aquellos programas mediante los cuales se entregan órdenes a los equipos o dispositivos electrónicos.
UPS (Sistema de Alimentación Ininterrumpida)	Fuente de suministro eléctrico que posee una batería con el fin de seguir entregando energía a un dispositivo en el caso de interrupción eléctrica.
Usuario	Defínase a cualquier persona, que utilice los servicios

	informáticos de la red institucional del GAD Ibarra o tenga vinculación laboral con la institución.

VIII. DESARROLLO DE POLÍTICAS DE SEGURIDAD

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Dominio:	1.Políticas de Seguridad de la Información	**Destinatarios:**	Todos los usuarios
	Control:	1.1 Objetivo de la Política de Seguridad	**Fecha Elaboración:**	
Art. 1. Dotar de la información necesaria a los usuarios de los activos informáticos del GAD Ibarra, sobre las directrices que deben cumplir y utilizar para proteger el hardware y software de la red institucional, así como la información que es procesada y almacenada en sus recursos, apegadas a estándares internacionales desarrollados para tal fin.				

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Dominio:	1.Políticas de Seguridad de la Información	**Destinatarios:**	Todos los usuarios
	Control:	1.2 Compromiso de las autoridades	**Fecha Elaboración:**	
Art. 2. La Dirección de TIC y gestor de seguridad, como responsables de la elaboración del Manual de Políticas de Seguridad de la Información para el GAD Ibarra, asumen la responsabilidad de la creación, revisión periódica y socialización de los lineamientos y procedimientos de seguridad de la información descritos en este documento.				

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Dominio:	2. Gestión de los Activos	**Destinatarios:**	Todos los usuarios
	Control:	2.1 Responsabilidad sobre los Activos	**Fecha Elaboración:**	

Art. 3. El Gestor de Seguridad en concordancia con la Dirección de TIC, deberán identificar todos los activos críticos y documentar su importancia.

Art. 4. Se deberán definir los responsables por el/los activo/s crítico/s o de mayor importancia para el departamento y/o institución.

Art. 5. El personal responsable de los activos críticos o no críticos, velará por la salvaguarda de los mismos.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Dominio:	2. Gestión de los Activos	**Destinatarios:**	Todos los usuarios
	Control:	2.2 Clasificación de la Información	**Fecha Elaboración:**	

Art. 6. De forma individual, los departamentos del GAD Ibarra, son responsables de clasificar de acuerdo al nivel de importancia, la información que en ellos se procese.

Art. 7. Se tomarán como base los siguientes criterios, como niveles de importancia para clasificar la información:

a) Pública

b) Interna

c) Confidencial

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Dominio:	3. Seguridad ligada a los Recursos Humanos	**Destinatarios:**	Todos los usuarios
	Control:	3.1 Antes del Empleo	**Fecha Elaboración:**	

Art. 8. Los nuevos empleados deberán aceptar las condiciones sobre el uso adecuado de los recursos informáticos y de información confidencial del GAD Ibarra, así como del estricto apego al Manual de Políticas y Procedimientos de Seguridad de la Información vigente.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Dominio:	3. Seguridad ligada a los Recursos Humanos	**Destinatarios:**	Todos los usuarios
	Control:	3.2 Durante el empleo	**Fecha Elaboración:**	

Art. 9. Todo usuario debe respetar la intimidad, confidencialidad y derechos individuales de los demás usuarios.

Art. 10. La información procesada, manipulada o almacenada por el usuario no deberá ser divulgada a terceros, ya que es propiedad exclusiva del GAD Ibarra.

Art. 11. Para reforzar la seguridad de la información, el usuario conforme su criterio, deberá hacer respaldos de sus datos, dependiendo de la importancia y frecuencia de modificación de la misma. Los respaldos serán responsabilidad absoluta de los usuarios.

Art. 12. En ningún momento es aceptable la modificación de archivos no autorizada en los equipos informáticos, sino es bajo circunstancias especiales en las que de no hacerse de esa manera, el sistema quedaría inutilizable.

Art. 13. Cualquier falla efectuada en las aplicaciones o sistemas, por la manipulación errónea de archivos, deberá notificarse a la Dirección de TIC para su reparación.

Art. 14. Los usuarios de la red institucional, serán capacitados en cuestiones de seguridad de la información, según sea el área operativa y en función de las actividades que se desarrollan.

Art. 15. O a su vez, será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

Art. 16. El usuario es responsable de respetar la ley de derechos de autor, no abusando de este medio para inspeccionar, copiar y almacenar software o información sin conocimiento del autor.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Dominio:	3. Seguridad ligada a los Recursos Humanos	**Destinatarios:**	Todos los usuarios
	Control:	3.3 Cese del empleo	**Fecha Elaboración:**	

Art. 17. La Unidad de Recursos Humanos deberá reportar al personal de la Dirección de TIC, cuando un usuario deje de laborar o de tener una relación con la empresa.

Art. 18. Al darse por finalizado el contrato, se da por retirado los derechos de acceso hacia los activos de la institución utilizados durante el empleo.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Dominio:	4. Seguridad Física y del Entorno	**Destinatarios:**	Todos los usuarios
	Control:	4.1 Seguridad de los equipos	**Fecha Elaboración:**	

Art. 19. Los equipos de cómputo y comunicaciones estarán debidamente protegidos con la

infraestructura apropiada, de modo que se evite el acceso físico directo por terceras personas.

Art. 20.El acceso al interior del Centro de Datos se dará, única y exclusivamente al personal que ostente los siguientes cargos: responsables de Hardware, Comunicaciones y Bases de Datos.

Art. 21.El acceso al interior del Centro de Datos por parte del personal de mantenimiento, se dará siempre y cuándo se encuentren acompañados cuando menos por un responsable del área, designado por el Director de TIC.

Art. 22. Los servidores o estaciones de trabajo con problemas en su hardware, deberán ser reparados única y exclusivamente por los miembros del Área de Hardware, de no cumplirse lo anterior, deberán ser retirados sus medios de almacenamiento.

Art. 23. El cableado de red, se instalará físicamente separado de cualquier otro tipo de cables, llámese a estos de corriente o energía eléctrica, para evitar interferencias.

Art. 24. Los equipos deben contar con una adecuada instalación eléctrica, y abastecimiento de energía ininterrumpida mediante UPS.

Art. 25. Toda área de trabajo debe poseer herramientas auxiliares como extintores, de preferencia Clase B (incendios por líquidos inflamables, como grasa, gasolina, aceite, etc.) y C (fuego activados por electricidad), necesarios para salvaguardar los recursos tecnológicos y la información en el caso de producirse un flagelo.

Art. 26. El Centro de Datos deberá cumplir normas de seguridad referentes a:

- Acceso Restringido
- Temperatura y Humedad adecuada y estable para los equipos
- Protección contra descargas eléctricas
- Mobiliario adecuado que garantice la seguridad de los equipos.

Art. 27. Los usuarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, ni instalar o desinstalar dispositivos, sin la autorización de la Dirección de TIC, en caso de requerir este servicio deberá solicitarlo.

Art. 28. Mientras se opera el equipo de cómputo, no se deberá fumar, consumir alimentos o ingerir líquidos, ya que estas acciones pueden ocasionar daños en el equipo.

Art. 29. Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del CPU.

Art. 30. El usuario debe asegurarse que los cables de conexión no sean pisados o aguijoneados al colocar otros objetos encima o contra ellos.

Art. 31. La Dirección de TIC deberá establecer un inventario físico para préstamos de equipos o dispositivos de tecnología de información a usuarios internos del GAD Ibarra. Entre los más comunes (ordenadores portátiles, proyectores, UPS, cables y extensiones, CD/DVD, etc.)

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Dominio:	4. Seguridad Física y del Entorno	**Destinatarios:**	Todos los usuarios
	Control:	4.2 Mantenimiento de equipos	**Fecha Elaboración:**	

Art. 32.Los encargados del Área de Hardware del GAD Ibarra son los responsables de calendarizar y organizar al personal encargado del mantenimiento preventivo y correctivo de los equipos de cómputo.

Art. 33. El usuario no está facultado para intervenir física o lógicamente ninguna estación de trabajo que amerite reparación.

Art. 34. Los usuarios deberán asegurarse de respaldar la información que consideren

relevante, cuando el equipo sea enviado a reparación, previendo así la pérdida involuntaria de información que pueda ocurrir en el proceso de reparación del equipo.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Dominio:	5. Gestión de Comunicaciones y Operaciones	**Destinatarios:**	Administradores sistema
	Control:	5.1Responsabilidades y procedimientos de operaciones	**Fecha Elaboración:**	

Art. 35. El personal de la Dirección de TIC asignado al Área de Hardware y Comunicaciones, es responsable de la planeación para la adquisición de equipos de cómputo y comunicaciones, y de la verificación de su instalación, configuración e implementación.

Art. 36. El personal de la Dirección de TIC dedicado al Área de Software, efectuará todo el proceso propio de la planificación, desarrollo, adquisición, comparación, adaptación y actualización del software necesario para el GAD Ibarra.

Art. 37. La Dirección de TIC, es responsable absoluto de mantener el sistema de información en óptimo funcionamiento, fomentando una cultura de administración segura y servicios óptimos.

Art. 38. La Dirección de TIC, se encargará de regular el uso de los recursos del sistema y de la red a los usuarios, principalmente con la restricción de directorios, permisos y programas a ser ejecutados por los mismos.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Dominio:	5. Gestión de Comunicaciones y Operaciones	**Destinatarios:**	Administradores sistema
	Control:	5.2 Planificación y aceptación del sistema	**Fecha Elaboración:**	

Art. 39. La aceptación y posterior adquisición del software para la entidad, se hará efectiva

previo análisis y pruebas efectuadas por el personal de la Dirección de TIC en coordinación con la Gerencia.

Art. 40. Únicamente se utilizará software certificado o en su defecto software previamente revisado y aprobado, por personal calificado.

Art. 41. Es tarea del Analista de Sistemas, el realizar testing de calidad al software a prueba, respecto a entradas de datos en cuanto a:

- Caracteres inválidos, en los campos de datos.
- Datos incompletos.
- Datos con longitud excedente o valor fuera de rango.
- Datos no autorizados o inconsistentes.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Dominio:	5. Gestión de Comunicaciones y Operaciones	**Destinatarios:**	Todos los usuarios
	Control:	5.3 Protección contra el código malicioso y descargable	**Fecha Elaboración:**	

Art. 42. Se adquirirá y utilizará software únicamente de fuentes confiables.

Art. 43. En caso de ser necesaria la adquisición de software de fuentes no confiables, este se adquirirá en código fuente.

Art. 44. Los servidores, al igual que las estaciones de trabajo, tendrán instalado y configurado correctamente software antivirus actualizable y activada la protección en tiempo real.

Art. 45. Los usuarios de las estaciones de trabajo, deberán verificar que la información soportada por los medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deberán ejecutar el software antivirus autorizado e instalado por la Dirección de TIC.

Art. 46. Todos los archivos que sean proporcionados por personal interno o externo, considerando bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, deberá verificarse que los mismos no contengan ningún tipo de virus antes de su ejecución.

Art. 47. Ningún usuario, empleado o personal externo, deberá intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para auto replicarse, dañar, o en otros casos, impedir el funcionamiento de cualquier memoria de computadora, archivos de sistema o software. Menos aún, probarlos en cualquiera de los ambientes o plataformas de la institución.

Art. 48. Ningún usuario podrá descargar e instalar aplicaciones provenientes de sitios no confiables a partir redes de comunicaciones externas, sin la previa autorización de la Dirección de TIC.

Art.49. Cualquier usuario que sospeche de alguna infección por virus en su equipo de cómputo, deberá notificarlo inmediatamente a la Dirección de TIC para su erradicación.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Dominio:	5. Gestión de Comunicaciones y Operaciones	**Destinatarios:**	Administradores sistema
	Control:	5.4 Copias de seguridad de la información	**Fecha Elaboración:**	

Art. 50. El Responsable de Software, deberá realizar copias de seguridad teniendo en cuenta el tipo de información a almacenar y la frecuencia con que se debe realizar los respaldos para cada tipo. En este caso se ha definido lo siguiente:

Tipo de dato	Frecuencia
Portales Web	Mensual

Código Fuente	En cada cambio de versión.
BDD Espacial	Diario
BDD Alfanumérica	Diario
BDD Binaria	Mensual
BDD SQL Server	Diario
BDD Portales Web	Mensual
Proyectos, Informes e Investigaciones específicos de la Dirección de TIC	Mensual

Art. 51. Los medios de almacenamiento a usar serán: discos duros externos, servidores y DVD.

Art. 52. Las copias de respaldo se realizarán al final del día, fuera de horarios laborales.

Art. 53. Cada mes, los respaldos se harán por duplicado, una copia será entregada a la Dirección Administrativa para su respaldo seguro. La otra copia se la hará en un disco de respaldo de información en el equipo servidor de la Dirección TIC.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Dominio:	5. Gestión de Comunicaciones y Operaciones	**Destinatarios:**	Administradores sistema
	Control:	5.5 Manipulación de medios de almacenamiento	**Fecha Elaboración:**	

Art. 54. Los medios de almacenamiento serán etiquetados de acuerdo a la información que almacenan u objetivo que suponga su uso, detallando o haciendo alusión a su contenido, siguiendo la sintaxis:

BckupGAD-I_aaaa-mm-dd_DescripciónContenido

Art. 55. Los medios de almacenamiento con información crítica deberán ser manipulados

única y exclusivamente por el personal encargado de hacer los respaldos y el personal encargado de su salvaguarda.

Art. 56. Todo medio de almacenamiento con información crítica será guardado bajo llave en una caja especial a la cual tendrá acceso únicamente, el responsable de dicho activo, esta caja no debería ser removible.

Art. 57.Los miembros de la Dirección de TIC serán los encargados de ubicar los servidores donde se almacene la información, en instalaciones físicas debidamente administradas, con condiciones ambientales adecuadas y con planes de contingencia vigentes.

Art. 58. El responsable de Software es el encargado de garantizar el almacenamiento de las Copias de seguridad en condiciones ambientales óptimas, dependiendo del medio magnético empleado. Además deberá reemplazar las mismas, de forma periódica, antes que el medio magnético de soporte se pueda deteriorar.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Dominio:	5. Gestión de Comunicaciones y Operaciones	**Destinatarios:**	Administradores sistema
	Control:	5.6 Supervisión	**Fecha Elaboración:**	

Art. 59. Se registrará y archivará toda actividad procedente del uso de las aplicaciones, mediante los archivos log del sistema.

Art. 60. Los archivos log almacenarán nombres de usuarios, nivel de privilegios, direcciones IP del terminal, fecha y hora de acceso o utilización, actividad desarrollada, aplicación implicada en el proceso, entre otros.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Dominio:	6.Control de Acceso	**Destinatarios:**	Todos los usuarios
	Control:	6.1Gestión de acceso de usuario	**Fecha Elaboración:**	

Art. 61. Es usuario de la red institucional, toda persona que tenga contacto directo con sus activos informáticos y/o utilice los servicios de la red institucional del GAD Ibarra.

Art. 62. Se asignará una cuenta de acceso a los sistemas de la intranet, a todo usuario de la red institucional, siempre y cuando se identifique previamente el objetivo de su uso o permisos explícitos a los que éste accederá, junto a la información personal del usuario.

Art. 63. El acceso a la red por parte de terceros es estrictamente restrictivo y permisible únicamente mediante documentación de aceptación de confidencialidad hacia la institución.

Art. 64. No se proporcionará el servicio solicitado por un usuario o Departamento, sin antes haberse completado todos los procedimientos de autorización necesarios para su ejecución.

Art. 65. Las claves de acceso son personales e intransferibles.

Art. 66. La longitud mínima de caracteres permisibles en una contraseña se establece en 6 caracteres, entre alfanuméricos y especiales.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Dominio:	6.Control de Acceso	**Destinatarios:**	Todos los usuarios
	Control:	6.2 Responsabilidades del usuario	**Fecha Elaboración:**	

Art. 67. El usuario es responsable exclusivo de mantener a salvo su contraseña.

Art. 68. El usuario será responsable de las acciones que ejecute al acceder a los sistemas o servicios de la institución, desde su cuenta de acceso.

Art. 69. Se debe evitar el guardar o escribir las contraseñas en cualquier papel o superficie o

dejar constancia de ellas, a menos que ésta sea guardada en un lugar seguro.

Art. 70. El usuario es responsable de eliminar cualquier rastro de documentos proporcionados por el Gestor de Seguridad o Dirección de TIC, que contenga información que pueda facilitar a un tercero la obtención de la información de su cuenta de usuario.

Art. 71. El usuario es responsable de evitar la práctica de establecer contraseñas relacionadas con alguna característica de su persona o relacionado con su vida o la de parientes, como fechas de cumpleaños o alguna otra fecha importante.

Art. 72. Es responsabilidad del usuario cambiar periódicamente su contraseña, de acuerdo a la criticidad de la información, procurando no reutilizar las últimas contraseñas. En caso de no saber cómo realizar el cambio, la Dirección de TIC le brindará la asesoría necesaria.

Art. 73. El usuario deberá proteger su equipo de trabajo, evitando que personas ajenas a su cargo puedan acceder a la información almacenada en él, mediante una herramienta de bloqueo temporal (protegida por una contraseña), la cual deberá activarse en el preciso momento en que el usuario deba ausentarse.

Art. 74. Deberá utilizar únicamente la cuenta que le ha sido asignada y el nivel de privilegios predeterminado, para tener acceso a sistemas y recursos.

Art. 75. Cualquier usuario que encuentre un hueco o falla de seguridad en el control de acceso a los sistemas o aplicaciones de la institución, está obligado a reportarlo a los administradores del sistema.

Sobre el Uso del Correo Electrónico:

Art. 76. Se debe hacer uso de él, acatando todas las disposiciones de seguridad diseñadas para su utilización, evitando la introducción de software malicioso a la red institucional.

Art. 77. El correo electrónico municipal es de uso exclusivo, para los empleados del GAD Ibarra.

Art. 78. El usuario será responsable de la información que sea enviada desde su cuenta.

Art. 79. Los responsables de la Dirección de TIC del GAD Ibarra, se reservarán el derecho de monitorear las cuentas de usuarios, que presenten un comportamiento sospechoso para la seguridad de la red institucional.

Art. 80. No se permite enviar información clasificada como confidencial por correo electrónico.

Art. 81. No se deberá usar para envío de correo masivo de uso no institucional y ajeno a la organización, tales como cadenas, publicidad y propaganda comercial, política o social, etc.

Art. 82. Todo uso indebido del servicio de correo electrónico, será motivo de suspensión temporal de su cuenta de correo o según sea necesario la eliminación total de la cuenta dentro del sistema.

Sobre el Uso de Internet:

Art. 83. Los usuarios del GAD Ibarra, provistos de acceso a Internet, al aceptar este servicio están aceptando que:

- Serán sujetos de monitoreo de las actividades que realiza en Internet.
- Saben que existe la prohibición al acceso de páginas no autorizadas.
- Conocen sobre la prohibición de transmisión de archivos reservados o confidenciales no autorizados y la prohibición de descarga de software sin la autorización de la Dirección de TIC.
- La utilización de Internet es para el desempeño de su función y puesto dentro de la entidad y no para propósitos personales.

Art. 84. En caso de necesitar bajar archivos de la red, éstos deberán ser de un tamaño pequeño, a fin de no causar mucho tráfico y por consiguiente lentitud para los demás usuarios.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Dominio:	6. Control de Acceso	**Destinatarios:**	Administradores sistema
	Control:	6.3 Control de Acceso a la red	**Fecha Elaboración:**	

Art. 85. El acceso a la red interna, se permitirá siempre y cuando se cumpla con los requisitos de seguridad necesarios y éste será permitido mediante un mecanismo de autenticación.

Art. 86. Se debe eliminar cualquier acceso a la red sin previa autenticación o validación del usuario o el equipo implicado en el proceso.

Art. 87. La Dirección de TIC deberá emplear dispositivos de red para el filtrado de tráfico, evitando el acceso o flujo de información, no autorizada hacia la red interna o desde la red interna hacia el exterior.

Art. 88. Se registrará toda actividad originada en la red institucional, que genere un acceso a sus dispositivos, mediante archivos Log.

Art. 89. Se efectuará una revisión de Log de los dispositivos de acceso a la red en un tiempo máximo de 72 horas.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Dominio:	6. Control de Acceso	**Destinatarios:**	Todos los usuarios
	Control:	6.4 Control de acceso al sistema operativo	**Fecha Elaboración:**	

Art. 90. Al terminar una sesión de trabajo en las estaciones, los operadores evitarán dejar encendido el equipo o a su vez dejar sesiones abiertas, pudiendo proporcionar un entorno de utilización de la estación de trabajo por parte de personas ajenas.

Art. 91. El acceso a la configuración del sistema operativo de los servidores, es únicamente permitido al usuario administrador responsable.

Art. 92. Todo servicio provisto o instalado en los servidores, será ejecutado bajo cuentas restrictivas, estos privilegios tendrán que ser configurados correctamente.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Dominio:	6. Control de Acceso	**Destinatarios:**	Todos los usuarios
	Control:	6.5 Control de acceso a las aplicaciones	**Fecha Elaboración:**	

Art. 93. Al terminar una sesión de trabajo en las aplicaciones, los usuarios evitarán dejar sesiones abiertas o a su vez deberán activar en sus aplicaciones cierres de sesión automáticos luego de un tiempo de inactividad.

Art. 94. Se deberá definir y estructurar el nivel de permisos sobre las aplicaciones, de acuerdo a derechos de escritura, lectura, modificación, ejecución o borrado de información.

Art. 95. Se deberá registrar archivos Log de aplicaciones, que den seguimiento a las actividades de los usuarios en cuanto a accesos, horas de conexión, IP del terminal desde donde se conecta, entre otros, de manera que proporcionen información relevante y revisable posteriormente.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Dominio:	7.Gestión de incidentes en la seguridad de la información	**Destinatarios:**	Administradores sistema
	Control:	7.1Gestión de incidentes y mejoras	**Fecha Elaboración:**	

Art. 96. Deberá darse soluciones a problemas de seguridad en las estaciones de trabajo, en el menor tiempo posible.

Art. 97. La Dirección de TIC deberá elaborar un documento donde deba explicar los pasos que se deberán seguir en situaciones contraproducentes a la seguridad (Plan de

Contingencia).

Art. 98. Cualquier situación anómala y contraria a la seguridad deberá ser documentada, de forma escrita o a través de los archivos log de los sistemas, con el objetivo de verificar la situación y generar una respuesta eficiente.

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Dominio:	8.Cumplimiento	**Destinatarios:**	Administradores sistema
	Control:	8.1 Cumplimiento de Políticas	**Fecha Elaboración:**	

Art.99. La Dirección de TIC será el responsable de supervisar el cumplimiento de las políticas y lineamientos institucionales.

Art. 100. Las sanciones a que están sujetos los usuarios por incumplimiento de sus obligaciones e incurrir en las restricciones señaladas, son las siguientes:

- Llamada de atención de manera verbal o escrita.
- Suspensión temporal de los servicios de la Red.
- Suspensión definitiva de los servicios de la Red.
- Reposición o pago de los bienes extraviados, destruidos o deteriorados.

XI. DESARROLLO DE PROCEDIMIENTOS DE SEGURIDAD

En esta sección se describen los procedimientos de mayor relevancia, enfocados al resguardo de la información de la entidad y de los recursos que la procesan. A través de los cuales se busca organizar aquellas actividades ejecutadas por el personal del GAD Ibarra, que impliquen un manejo responsable de los recursos del sistema informático, sean estos físicos, datos o personal, evitando de esta manera malas prácticas o hábitos que expongan a los recursos y genere pérdida o robo de información.

De este modo, se exponen a continuación las directrices para un desarrollo metódico de actividades para: asesoría a usuarios frente a problemas en el sistema informático, mantenimiento correctivo de hardware y software, desarrollo de planes de mantenimiento preventivo, respaldo oportuno y seguro de datos por parte del usuario que manipula información sensible, respaldo o restauración de bases de datos por parte del administrador y gestión de permisos para usuarios de la red municipal.

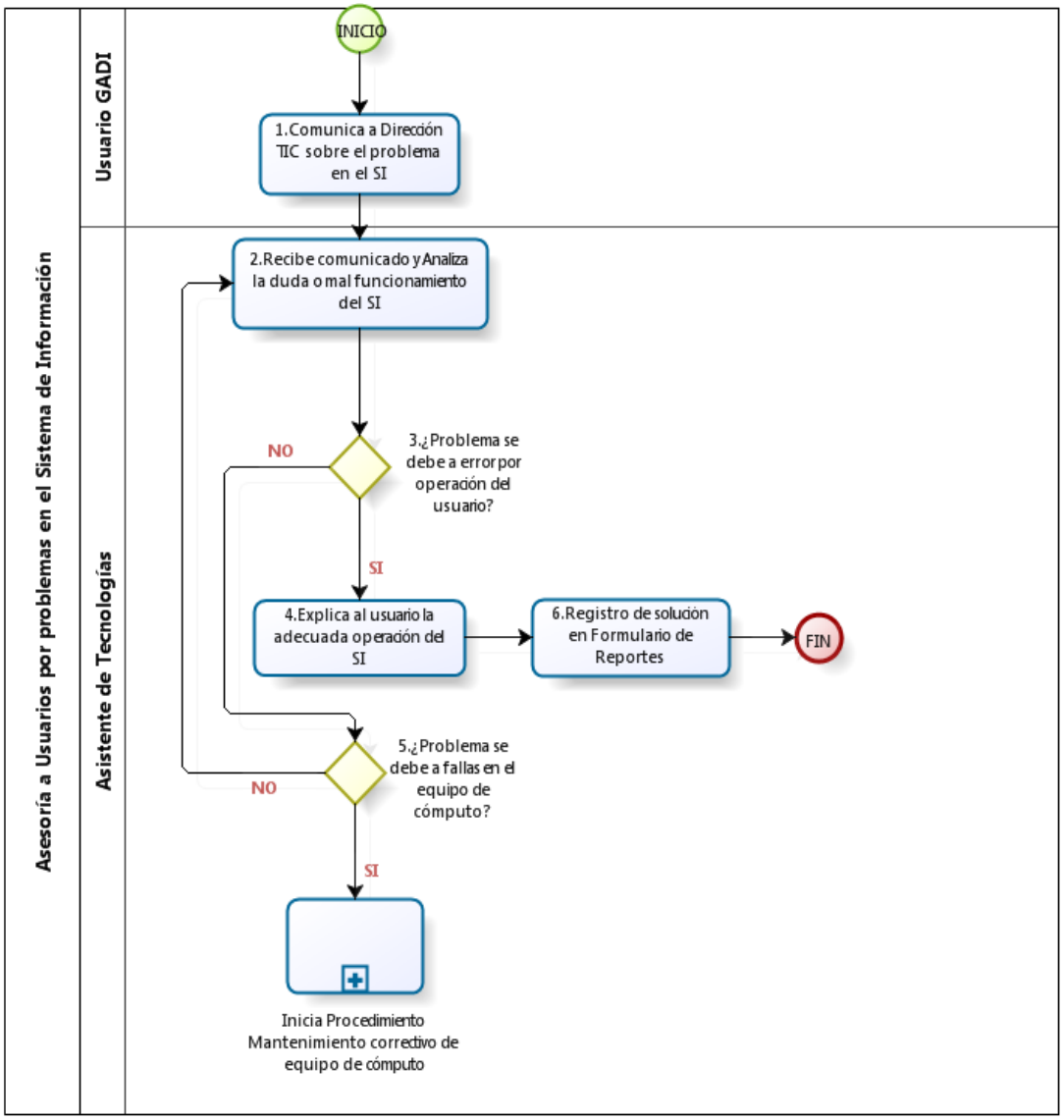
	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Procedimiento:	Asesoría para usuarios sobre problemas en el sistema de información.	**Versión:**	1.0
	Código:	PRO-1.0.1	**Fecha Elaboración:**	

1. **Objetivo:** Atender las necesidades de los funcionarios (usuarios) de los Departamentos del GAD-I, respecto a problemas en la operación del sistema de información.
2. **Alcance:** Aplica a las fallas originadas en el conjunto de hardware, software, datos y usuarios de la entidad.
3. **Abreviaturas y Definiciones:**

Abreviaturas		
Nº	**Término**	**Definición**
1	GAD-I	Gobierno Autónomo Descentralizado de Ibarra
2	TIC	Tecnología de la Información y Comunicaciones
3	SI	Sistema de Información

Definiciones		
Nº	**Término**	**Definición**
1	Análisis de Riesgo	Pretende descubrir qué recursos del sistema de información deben protegerse, de qué amenazas y en qué medida estos activos pueden verse afectados.
2	Datos	Representación simbólica (numérica, alfabética, algorítmica, etc.) de un atributo o característica de valor para la entidad.
3	Hardware	Recursos físicos dentro de un sistema informático, tales como: equipos de comunicaciones, cómputo, auxiliares, etc.
4	Sistema de información	Conjunto que resulta de la integración de cuatro elementos tales como: hardware, software, datos y usuarios.
5	Software	Recursos lógicos del sistema de información, tales como: programas o aplicaciones propias o subcontratadas.
6	Usuarios	Persona que hace uso de cualquier recurso del sistema de información.

4. Diagrama de Flujo



5. Desarrollo de Actividades

Nº	Actividad	Descripción	Responsable
1	Usuario comunica a la Dirección de TIC.	Se comunica con un miembro de la Dirección de TIC (miembro receptor del mensaje), describiendo el problema, acudiendo personalmente o vía telefónica.	Dirección TIC

2	Analiza la duda o mal funcionamiento del sistema de información.		Asistente de Tecnologías
4	¿Problema por Errores de operación por parte del usuario?	Si el problema se origina por fallas no intencionadas en la operación de los recursos, vea **Actividad 5**, caso contrario Ir a **Actividad 6**.	Asistente de Tecnologías
5	Explica al usuario la adecuada operación del sistema de información.	Con recomendaciones técnicas o administrativas, como las declaradas en las Políticas de Seguridad. Ir a **Actividad 7.**	Asistente de Tecnologías
6	¿Problema por fallas en el equipo de cómputo?	Inicia Procedimiento Mantenimiento Correctivo del Equipo de Cómputo, caso contrario regresa a **Actividad 2.**	Asistente de Tecnologías
7	Registra solución	Registra problema y actividades realizadas para su solución en Formulario de Reportes. Ver **Anexo B.**	Asistente de Tecnologías

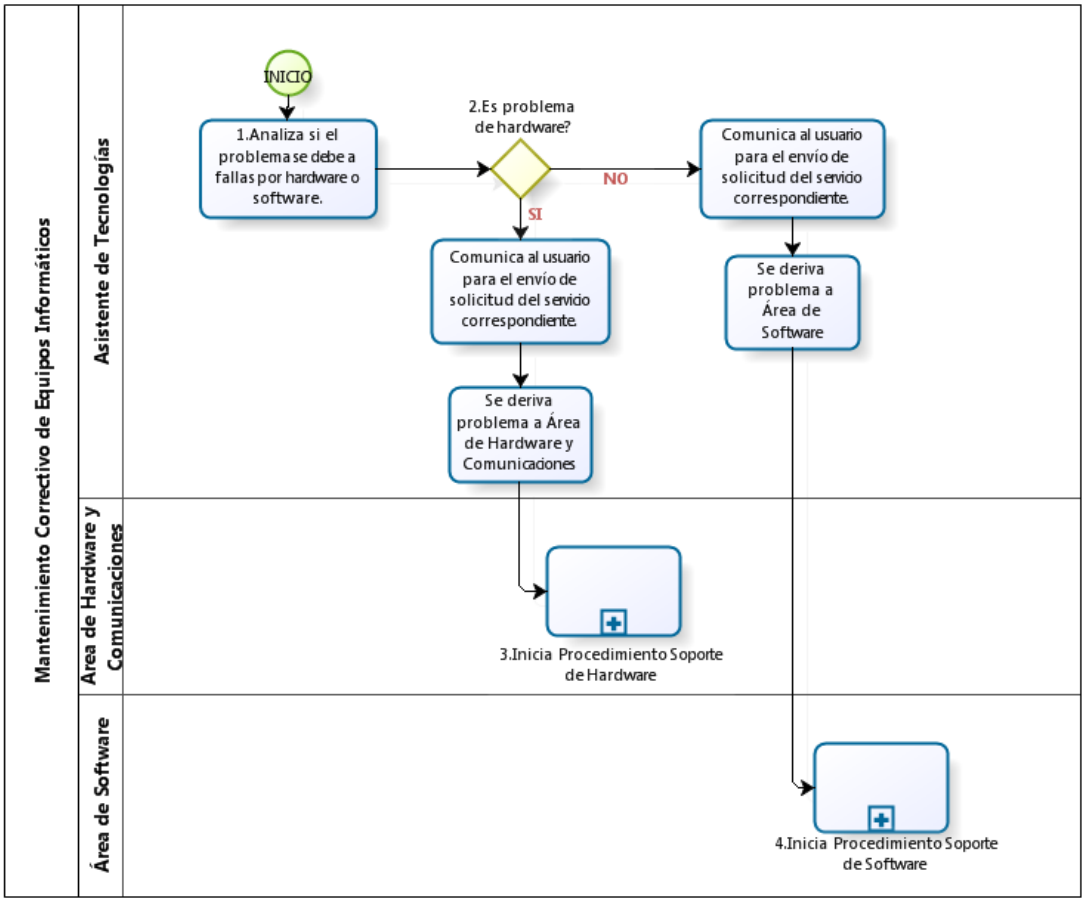
	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Procedimiento:	Mantenimiento correctivo de equipos informáticos	**Versión:**	1.0
	Código:	PRO-1.0.2	**Fecha Elaboración:**	

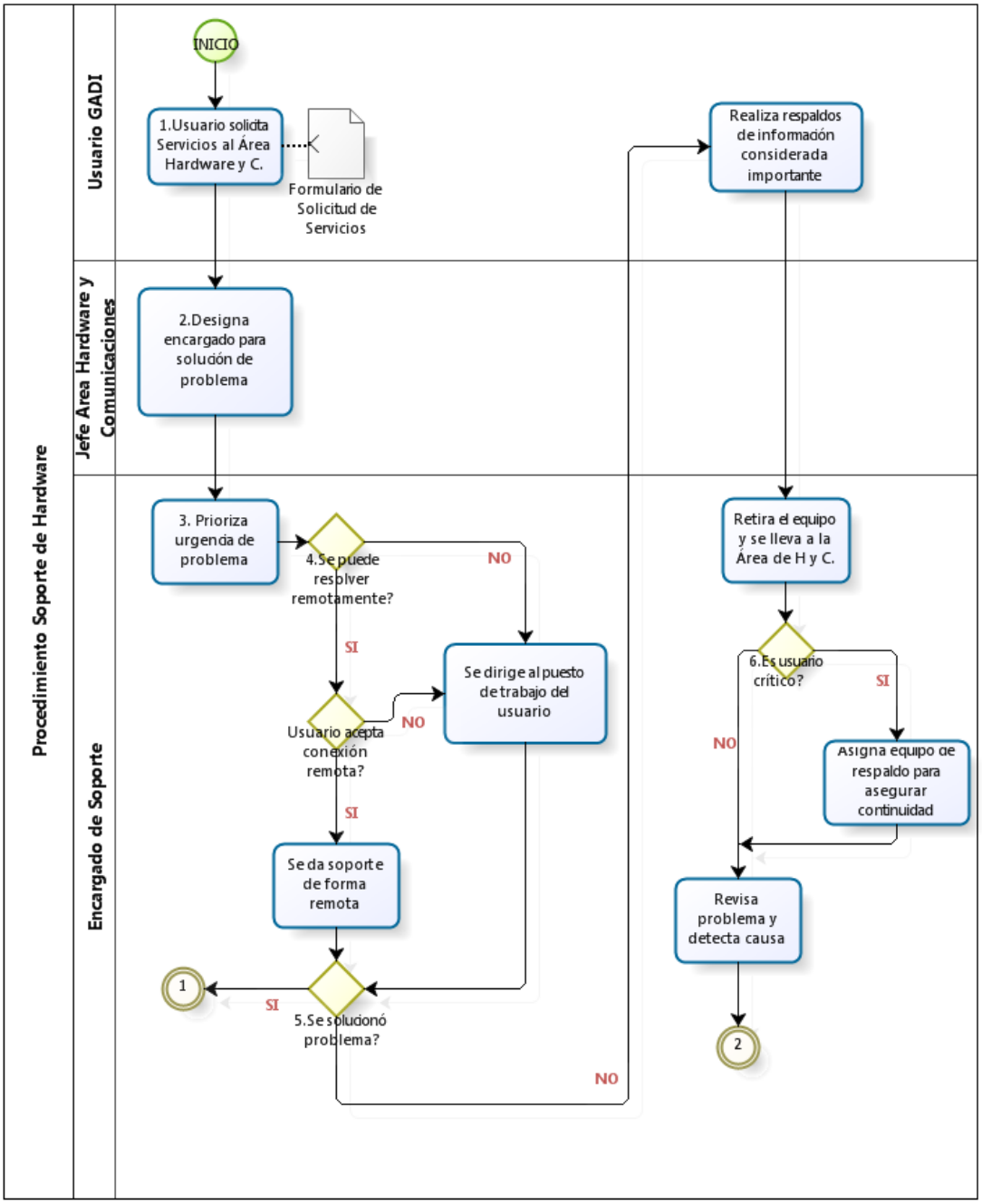
1. **Objetivo:** Garantizar la continuidad de operación de los recursos informáticos del GAD-I, a través de la revisión, reparación y adquisición de sus componentes de hardware y software.
2. **Alcance:** Aplica a los recursos de hardware y software de usuarios finales (PCs, impresoras, scanners, proyectores, UPS, aplicaciones, etc.)
3. **Abreviaturas y Definiciones:**

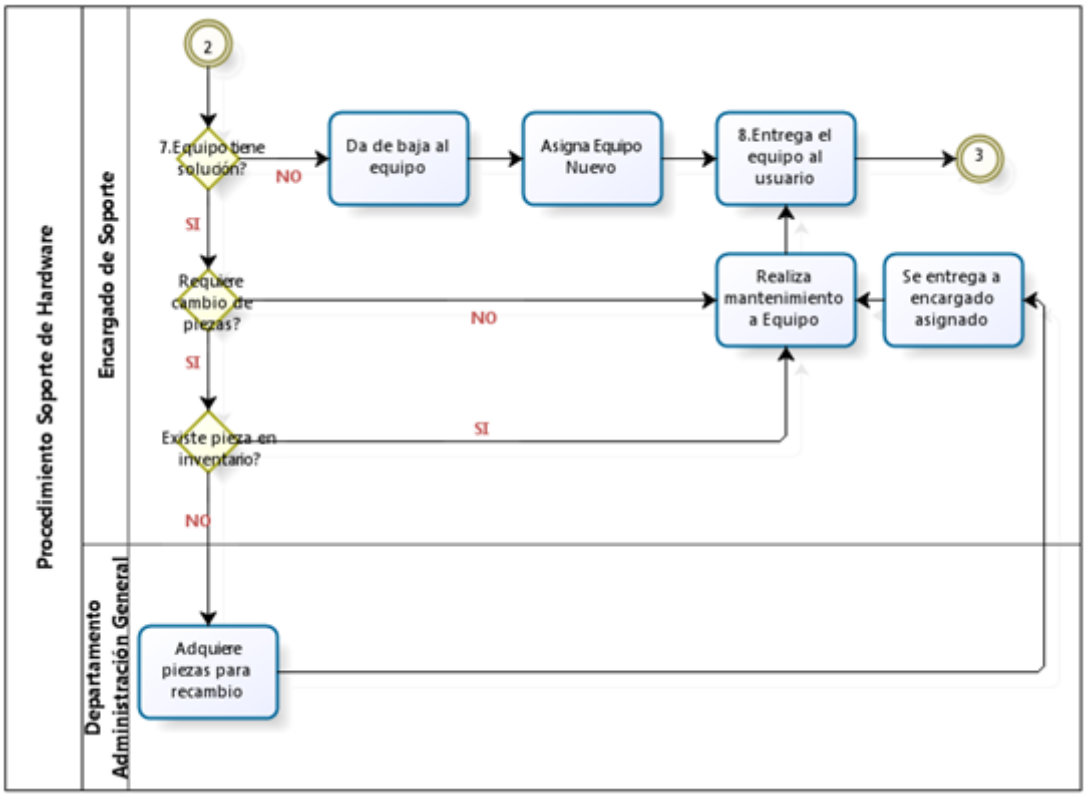
Abreviaturas		
Nº	**Término**	**Definición**
1	PC	Personal Computer (ordenador personal)
2	UPS	Sistema de Alimentación Ininterrumpida

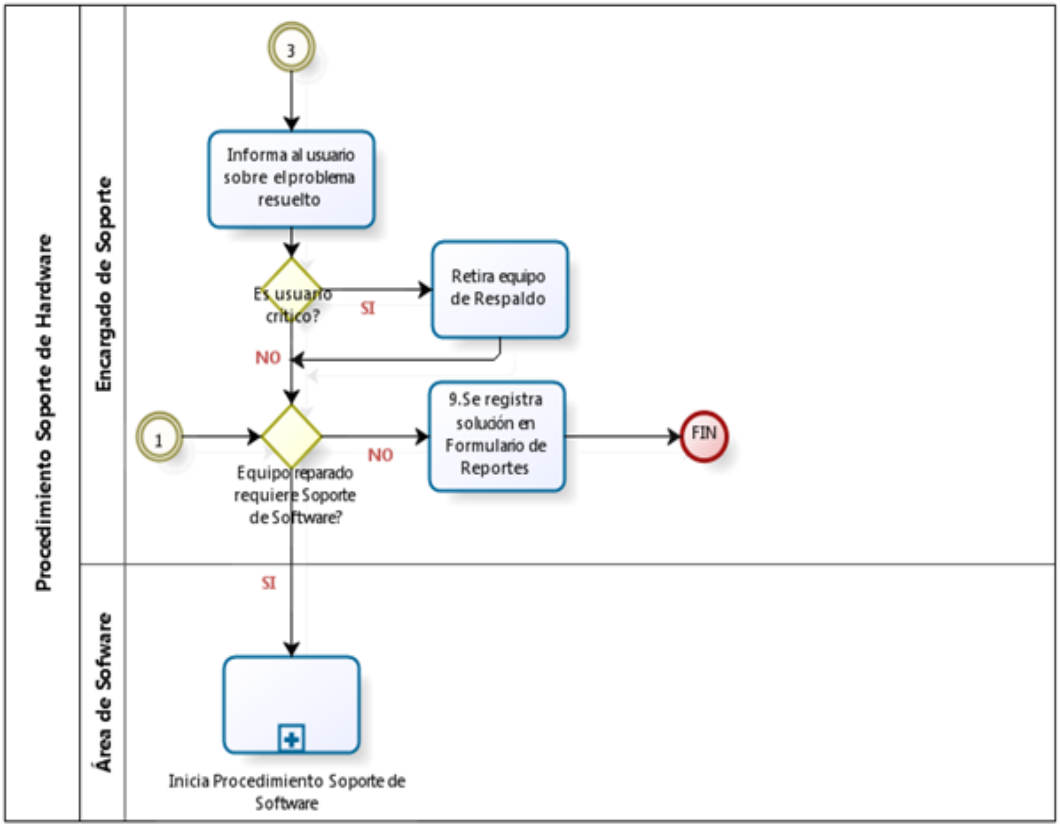
Definiciones		
Nº	**Término**	**Definición**
1	Aplicación propia	Software desarrollado por el personal interno del Área de software de la entidad.
2	Código	Denominado código fuente. Conjunto de instrucciones escritas en un lenguaje de programación, a través de las cuales el programa puede ejecutar sus funciones.
3	Conexión remota	Operación consistente en conectar un equipo con otro/s físicamente no próximos.
4	Mantenimiento correctivo	Mantenimiento que se realiza con el fin de corregir o reparar un fallo en el equipo o instalación.

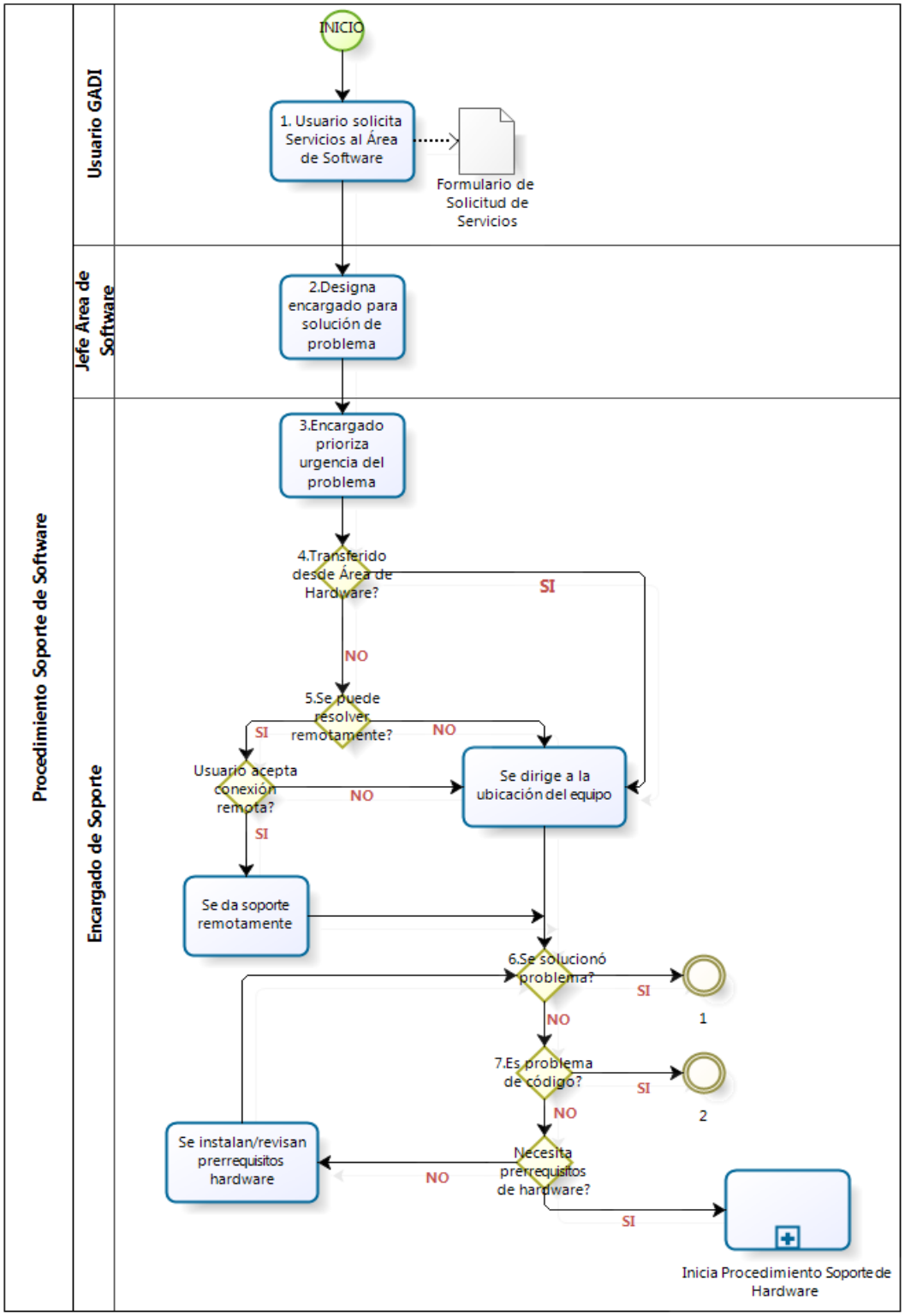
4. Diagramas de Flujo

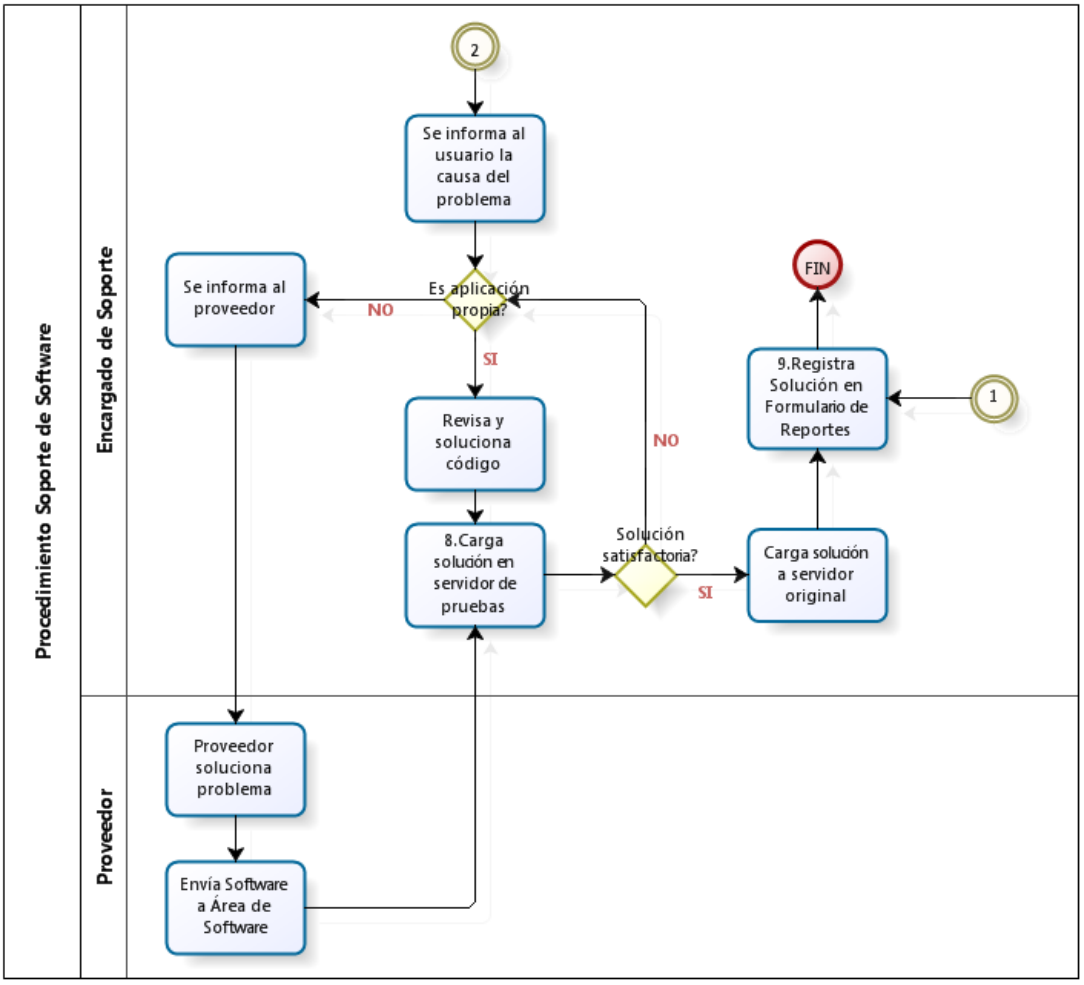



Procedimiento Soporte de Hardware
Usuario GADI
Jefe Área Hardware y Comunicaciones
Encargado de Soporte
INICIO
1.Usuario solicita Servicios al Área Hardware y C.
Formulario de Solicitud de Servicios
2.Designa encargado para solución de problema
3. Prioriza urgencia de problema
4.Se puede resolver remotamente?
NO
SI
Usuario acepta conexión remota?
NO
SI
Se dirige al puesto de trabajo del usuario
Se da soporte de forma remota
1
SI
5.Se solucionó problema?
NO
Realiza respaldos de información considerada importante
Retira el equipo y se lleva a la Área de H y C.
6.Es usuario crítico?
SI
NO
Asigna equipo de respaldo para asegurar continuidad
Revisa problema y detecta causa
2


Procedimiento Soporte de Hardware
Encargado de Soporte
Departamento Administración General
2
7.Equipo tiene solución?
NO
SI
Da de baja al equipo
Asigna Equipo Nuevo
8.Entrega el equipo al usuario
3
Requiere cambio de piezas?
NO
SI
Realiza mantenimiento a Equipo
Se entrega a encargado asignado
Existe pieza en inventario?
SI
NO
Adquiere piezas para recambio


Procedimiento Soporte de Hardware
Encargado de Soporte
Área de Sofware
3
Informa al usuario sobre el problema resuelto
Es usuario crítico?
SI
Retira equipo de Respaldo
NO
1
Equipo reparado requiere Soporte de Software?
NO
9.Se registra solución en Formulario de Reportes
FIN
SI
Inicia Procedimiento Soporte de Software


Procedimiento Soporte de Software
Usuario GADI
Jefe Área de Software
Encargado de Soporte
INICIO
1. Usuario solicita Servicios al Área de Software
Formulario de Solicitud de Servicios
2.Designa encargado para solución de problema
3.Encargado prioriza urgencia del problema
4.Transferido desde Área de Hardware?
SI
NO
5.Se puede resolver remotamente?
SI
NO
Usuario acepta conexión remota?
NO
SI
Se dirige a la ubicación del equipo
Se da soporte remotamente
6.Se solucionó problema?
SI
NO
1
7.Es problema de código?
SI
NO
2
Necesita prerrequisitos de hardware?
NO
SI
Se instalan/revisan prerrequisitos hardware
Inicia Procedimiento Soporte de Hardware



5. Desarrollo de Actividades

Procedimiento Mantenimiento Correctivo Equipos Informáticos

Nº	Actividad	Descripción	Responsable
1	Analiza si el problema se debe a fallas por hardware o software.	Identifica el problema y se lo deriva ya sea al Área de Hardware o Software de la institución, previo comunicado al usuario (el cual debe enviar solicitud de servicio según el caso).	Asistente de Tecnologías
2	¿Es problema de hardware?	Si es problema de hardware, ir a la **Actividad 3,** caso contrario ir a **Actividad 4**.	Asistente de Tecnologías

3	Inicia Procedimiento de Soporte de Hardware.	El equipo será revisado por personal del Área de Hardware y Comunicaciones.	Área de Hardware y C.
4	Inicia Procedimiento de Soporte de Software.	El equipo será llevado al Área de Software para su revisión.	Área de Software

Procedimiento Soporte Hardware

Nº	Actividad	Descripción	Responsable
1	Usuario envía Formulario de Solicitud de Servicios a la Dirección de TIC.	Llena el Formulario solicitando el tipo de servicio especificado. Ver **Anexo C**.	Usuario responsable del equipo
2	Se designa funcionario para solución de problema	Designa al personal para la solución del problema, de acuerdo a las cargas de trabajo.	Jefe Área Hardware y Comunicaciones
3	Prioriza urgencia del problema	Da prioridad a usuarios críticos, es decir, a aquellos que están relacionados directamente con la prestación de servicios de alta valoración para la entidad, de acuerdo a un Análisis de Riesgos Previo. **Ver Lista de Servicios Críticos. Anexo A.**	Encargado de dar soporte
4	¿Se puede resolver remotamente?	Decide si se puede solucionar el problema usando una conexión del equipo a la red (remotamente), caso contrario debe acudir al puesto de trabajo del usuario.	Encargado de dar soporte
5	¿Se solucionó el problema?	Si se solucionó el problema ir a la **Actividad 10**, caso contrario el usuario deberá sacar respaldos de su información y deberá ser retirado el equipo para su revisión.	Encargado de dar soporte Usuario responsable del equipo
6	¿Es usuario crítico?	Si lo es, se asigna un equipo de respaldo para evitar interrupciones	Encargado de dar soporte

		de los servicios críticos de la entidad. **Ver Lista de Servicios Críticos. Anexo A.**	
7	¿Equipo tiene solución?	Si tiene solución, decide si el problema ha de ser resuelto mediante mantenimiento únicamente, o cambio de componentes de hardware, caso contrario es necesario darlo de baja.	Encargado de dar soporte
8	Entrega del equipo al usuario	Posterior a haberse efectuado el mantenimiento respectivo, o la asignación de uno nuevo, según sea el caso.	Encargado de dar soporte
9	Reporte de solución	Se registra la actividad realizada por el personal que dio solución al problema. Ver **Anexo B.**	Encargado de dar soporte

Procedimiento Soporte Software

Nº	Actividad	Descripción	Responsable
1	Usuario envía Formulario de Solicitud de Servicios a la Dirección de TIC.	Llena el Formulario solicitando el tipo de servicio especificado. Ver **Anexo C**.	Usuario responsable del equipo
2	Se designa funcionario para solución de problema	Designa al personal para la solución del problema, de acuerdo a las cargas de trabajo.	Jefe Área Software
3	Prioriza urgencia del problema	Da prioridad a usuarios críticos, es decir, a aquellos que están relacionados directamente con la prestación de servicios de alta valoración para la entidad, de acuerdo a un Análisis de Riesgos Previo. **Ver Lista de Servicios Críticos. Anexo A.**	Encargado de dar soporte
4	¿Transferido desde Área	Examina si el equipo ha sido	Encargado de dar

	Hardware?	inspeccionado previamente en el Área de Hardware y Comunicaciones. Si es así, el encargado se dirige directamente a la ubicación del equipo, caso contrario, Ir a **Actividad 5**.	soporte
5	¿Se puede resolver remotamente?	Decide si se puede solucionar el problema usando una conexión del equipo a la red (remotamente), caso contrario debe acudir al puesto de trabajo del usuario.	Encargado de dar soporte
6	¿Se solucionó el problema?	Si es así, saltar a **Actividad 9** caso contrario ir a **Actividad 7.**	Encargado de dar soporte
7	¿Es problema de código?	Si se trata de una Aplicación de desarrollo propio, la revisión del código será efectuada por el Analista de sistemas encargado, caso contrario, será analizado por el proveedor de la aplicación.	Encargado de dar soporte Analista de Sistemas Proveedor
8	Se carga solución en Servidor de Pruebas	Cual sea el caso, la solución deberá ser probada en el servidor y observar que sea satisfactoria, antes de cargarlo en el servidor original	Encargado de dar soporte
9	Se registra solución en Formulario de Reportes	Se registra la actividad realizada por el personal que dio solución al problema. Ver **Anexo B.**	Encargado de dar soporte

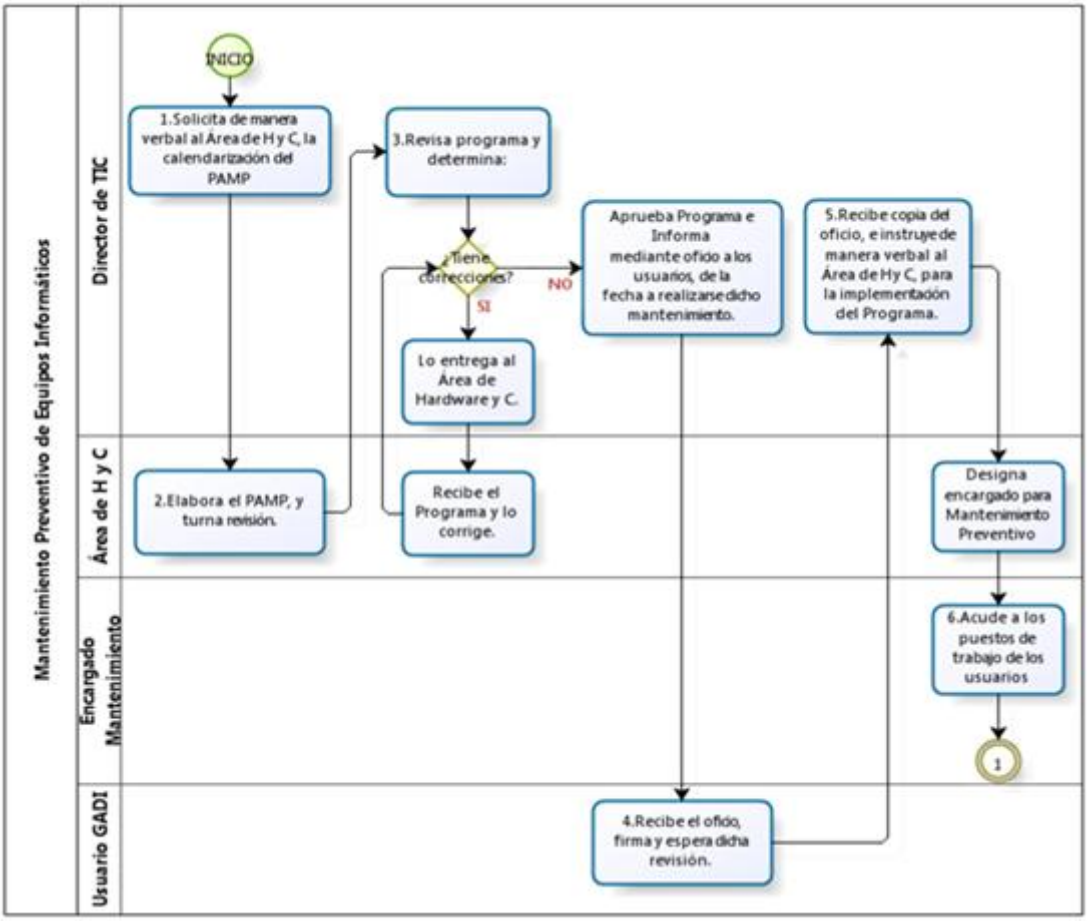
	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Procedimiento:	Mantenimiento preventivo de equipos informáticos	**Versión:**	1.0
	Código:	PRO-1.0.3	**Fecha Elaboración:**	

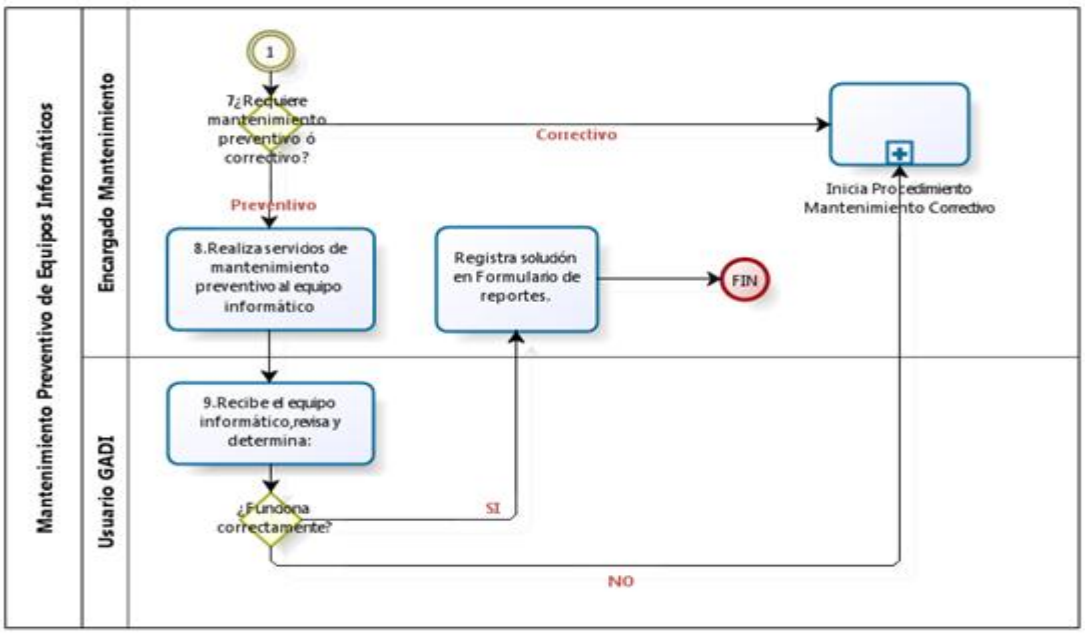
1. **Objetivo:** Mantener en óptimas condiciones de servicio los bienes informáticos de la entidad, garantizando su continuidad de operación.
2. **Alcance:** Aplica a los recursos de hardware y software de usuarios finales (PCs, impresoras, scanners, proyectores, UPS, aplicaciones, etc.)
3. **Abreviaturas y Definiciones:**

Abreviaturas		
Nº	**Término**	**Definición**
1	PAMP	Programa Anual de Mantenimiento Preventivo

Definiciones		
Nº	**Término**	**Definición**
1	Anti-Spam	Software para filtrado de correo electrónico con mensajes no solicitados, no deseados o de un remitente desconocido.
2	Anti-Spyware	Tipo de aplicación que se encarga de buscar, detectar y eliminar spywares o espías en el sistema.
3	Firmas de virus	Son pequeñas muestras de partes de virus que el antivirus usa para identificar uno o varios ejemplares de malware.

4. Diagrama de Flujo





5. Desarrollo de Actividades

Procedimiento Mantenimiento Preventivo Equipos Informáticos

Nº	Actividad	Descripción	Responsable
1	Solicita de manera verbal al Área de Hardware y C., la calendarización del (PAMP).		Director de TIC
2	Recibe comunicado, elabora el PAMP y turna revisión.	Elabora un informe de las distintas actividades a realizar, delegando responsabilidades y estableciendo fechas, para su posterior revisión.	Área de Hardware y Comunicaciones.
3	Revisa y aprueba informe previa corrección de errores.	Una vez aprobado, se envía oficio indicando fecha de revisión.	Director de TIC
4	Recibe el oficio, firma y espera dicha revisión.	Posterior a la entrega al usuario, se reenvía la copia del mismo al Director de TIC.	Usuario responsable del equipo
5	Instruye de manera verbal al Área de Hardware y C., para la implementación del Programa.	Autoriza la ejecución del PAMP por parte del Área de Hardware y C. de acuerdo a la fecha de inicio establecida.	Director de TIC
6	Acude a los puestos de trabajo de los usuarios	Revisión de los puestos de trabajo.	Encargado Mantenimiento Preventivo
7	¿Requiere mantenimiento preventivo o correctivo?	En el caso de ser Preventivo ir a la **Actividad 8,** caso contrario Inicia Procedimiento Mantenimiento Correctivo de Equipos Informáticos.	Encargado Mantenimiento Preventivo
8	Realiza servicios de mantenimiento preventivo al equipo informático	Entre estos servicios están: •Limpieza al CPU. •Revisión física, limpieza externa o interna al teclado y mouse.	Encargado Mantenimiento Preventivo

		•Reparación de cables de red e impresoras. •Configuración de servicios de red y de seguridad. •Actualización de las firmas de virus, antispyware, anti-spam y sistema operativo en general. •Configuración e instalación de impresoras. •Otras descritas en el cronograma.	
9	Recibe el equipo informático y determina si funciona correctamente.	Si funciona debidamente, el usuario emite la firma de conformidad en el Formulario de Reporte de Soluciones. **Ver Anexo B.** Caso contrario debe iniciar el Procedimiento de Mantenimiento Correctivo de Equipos Informáticos.	Usuario responsable del equipo

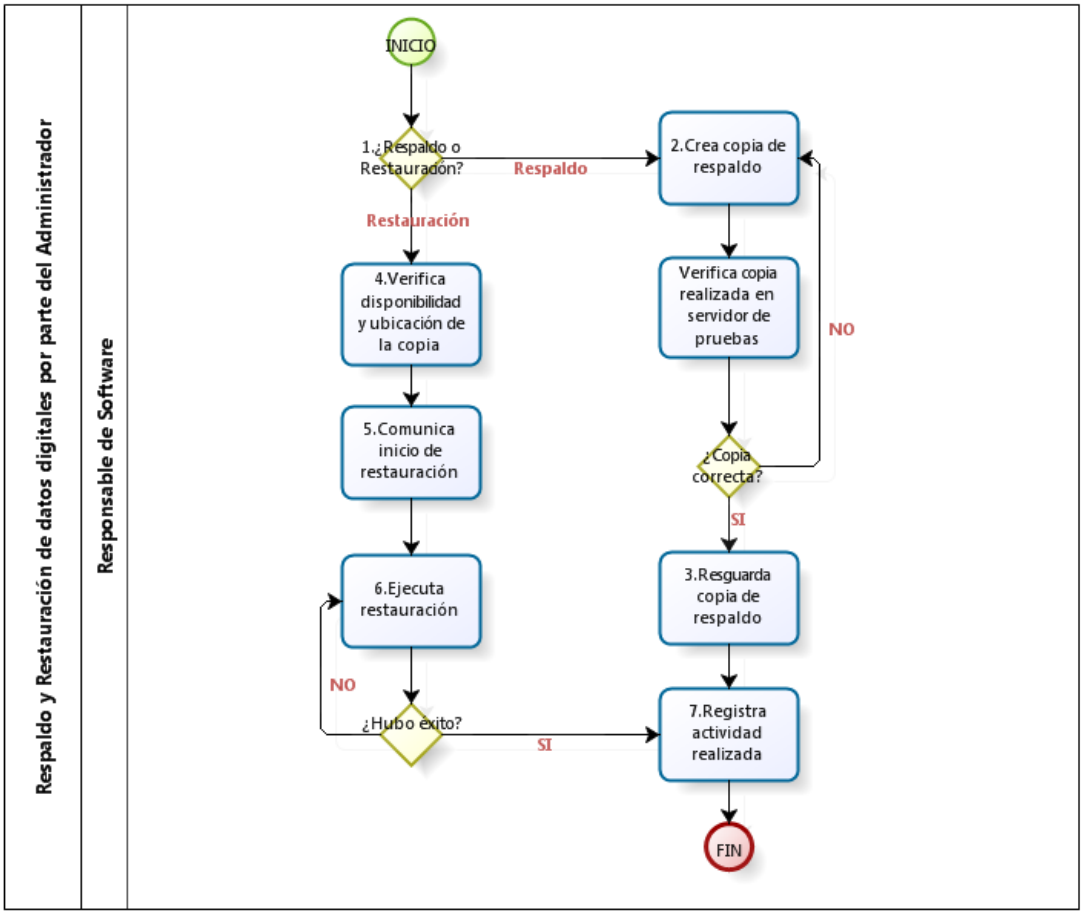
	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Procedimiento:	Respaldo y Restauración de Datos por parte del Administrador	**Versión:**	1.0
	Código:	PRO-1.0.4	**Fecha Elaboración:**	

1. **Objetivo:** Garantizar que los datos electrónicos mantengan su disponibilidad e integridad mediante la ejecución de respaldos o restauración de los mismos, en caso de pérdidas o modificaciones inesperadas.
2. **Alcance:** Aplica a los datos electrónicos administrados y custodiados por la Dirección de TIC, los cuales son:
   - Bases de Datos de las Aplicaciones Informáticas.
   - Bases de Datos de los Portales Web.
   - Código fuente y/o archivos de configuración de aplicaciones informáticas.
   - Portales Web.
3. **Abreviaturas y Definiciones:**

Abreviaturas		
Nº	**Término**	**Definición**
1	DVD	Digital Versatile Disc

Definiciones		
Nº	**Término**	**Definición**
1	Respaldo	Es la obtención de una copia de seguridad de los datos en otro medio, sea electrónico, magnético, impreso, etc. De modo que a partir de dicha copia es posible restaurar el sistema o datos al momento de haber realizado el respaldo.
2	Restauración	Tarea que se lleva a cabo cuando es necesario volver al estado del sistema o datos al momento del último respaldo.

4. Diagrama de Flujo



5. Desarrollo de Actividades

Procedimiento Respaldo y Restauración de Datos por parte del Administrador

Nº	Actividad	Descripción	Responsable
1	¿Respaldo o Restauración?	Se va a realizar una copia de respaldo de los datos o la restauración. Para el primer proceso Ver **Actividad 2**, caso contrario ir a **Actividad 4.**	Responsable de Software
2	Crea copia y verifica	Crea copia manual o automáticamente y procede a cargarla en el servidor de pruebas,	Responsable de Software

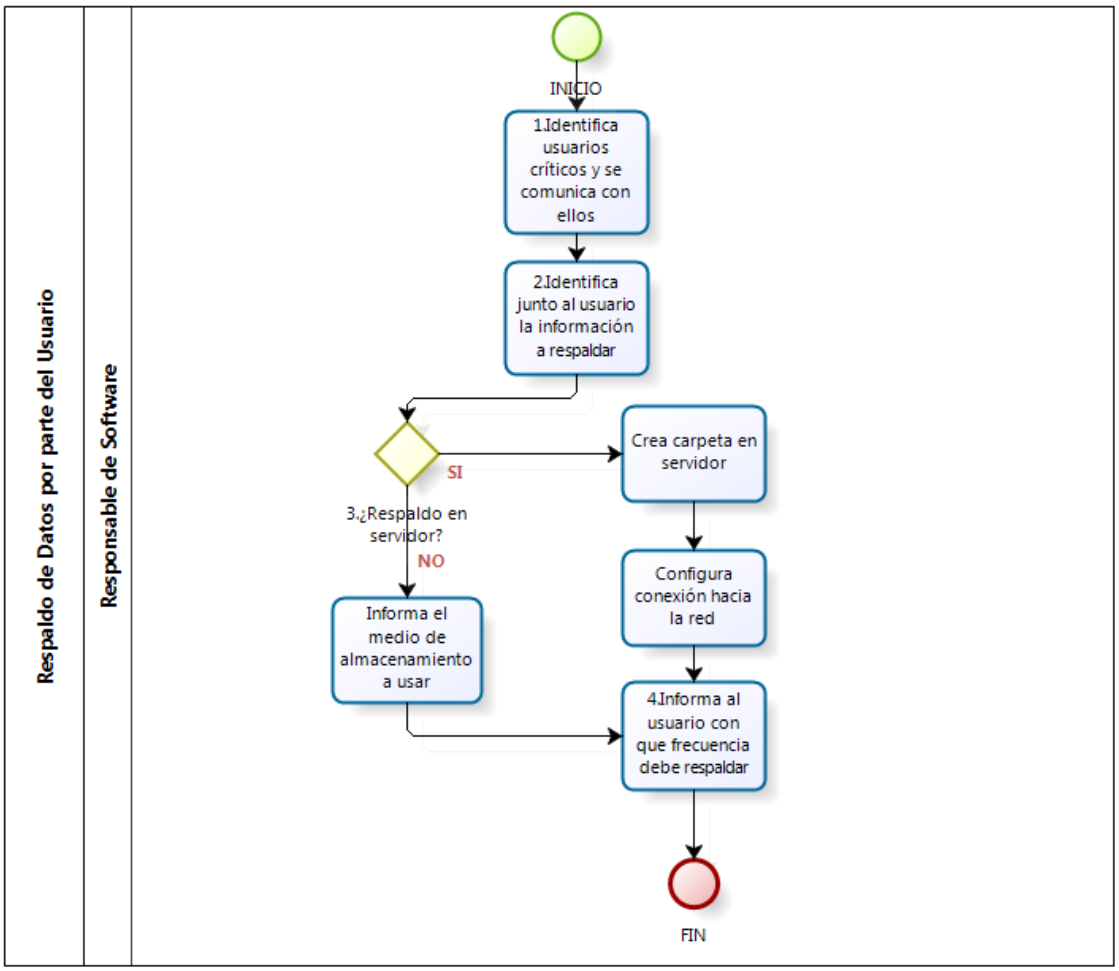
		para verificar que la copia está completa y sin errores.	
3	Resguarda copia	Diariamente carga la copia al servidor de respaldos y al final del mes, la almacena en medios magnéticos como DVDs, para enviarlos finalmente a la Dirección Financiera para su resguardo. Ir a **Actividad 7.**	Responsable de Software
4	Verifica disponibilidad y ubicación de la copia	Verifica en la Bitácora de Control de Respaldos y Restauración de Datos la disponibilidad y ubicación de la copia de respaldo. Busca la copia y la prepara. **Ver Anexo D.**	Responsable de Software
5	Comunica inicio restauración	Comunica (en caso de ser necesario) a los funcionarios del Área de Software, a los usuarios internos y externos de la Dirección de TIC, por medio de correo electrónico, acerca de la restauración de los datos, para que detengan las actividades de acceso durante el tiempo requerido.	Responsable de Software
6	Ejecución de la restauración	Involucra convertir la información a su estado original, es decir previo a las modificaciones almacenadas en dicha copia.	Responsable de Software
7	Registra actividad realizada	En caso de tener éxito, registra el trabajo realizado en la Bitácora de Control de Respaldos y Restauración de Datos**. Ver Anexo D.**	Responsable de Software

	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Procedimiento:	Respaldo de Datos por parte del Usuario.	**Versión:**	1.0
	Código:	PRO-1.0.5	**Fecha Elaboración:**	

1. **Objetivo:** Garantizar que los datos electrónicos mantengan su disponibilidad e integridad mediante la ejecución de respaldos o restauración de los mismos, en caso de pérdidas o modificaciones inesperadas.
2. **Alcance:** Aplica a los datos electrónicos administrados y custodiados por los funcionarios comunes dentro de cada Departamento del GAD-I, que manejan información considerada crítica.
3. **Abreviaturas y Definiciones:**

Definiciones		
Nº	**Término**	**Definición**
1	Data Center	Instalación empleada para albergar los sistemas de información y sus componentes asociados, como las comunicaciones y los sistemas de almacenamiento.
2	Medio de Almacenamiento	Dispositivo electrónico o no electrónico para el almacenamiento temporal o definitivo de datos.

4. Diagrama de Flujo



5. Desarrollo de Actividades

Procedimiento Respaldo de Datos por parte del Usuario

Nº	Actividad	Descripción	Responsable
1	Identifica usuarios críticos	A aquellos que brindan servicios considerados de máximo interés para la entidad. **Ver Lista de Servicios Críticos. Anexo A.**	Responsable de Software
2	Identifica la información a respaldar	Identifica los datos o información a respaldar en coordinación con el usuario	Responsable de Software

		responsable.	
3	¿Respaldo en servidor?	Opta si la información va a ser resguardada en el servidor de respaldos ubicado en el Data Center o en algún otro medio de almacenamiento (DVDs).	Responsable de Software
4	Informar al usuario con qué frecuencia debe realizar los respaldos de su información	De acuerdo a la importancia y el volumen de la información. Sea diaria o mensualmente.	Responsable de Software

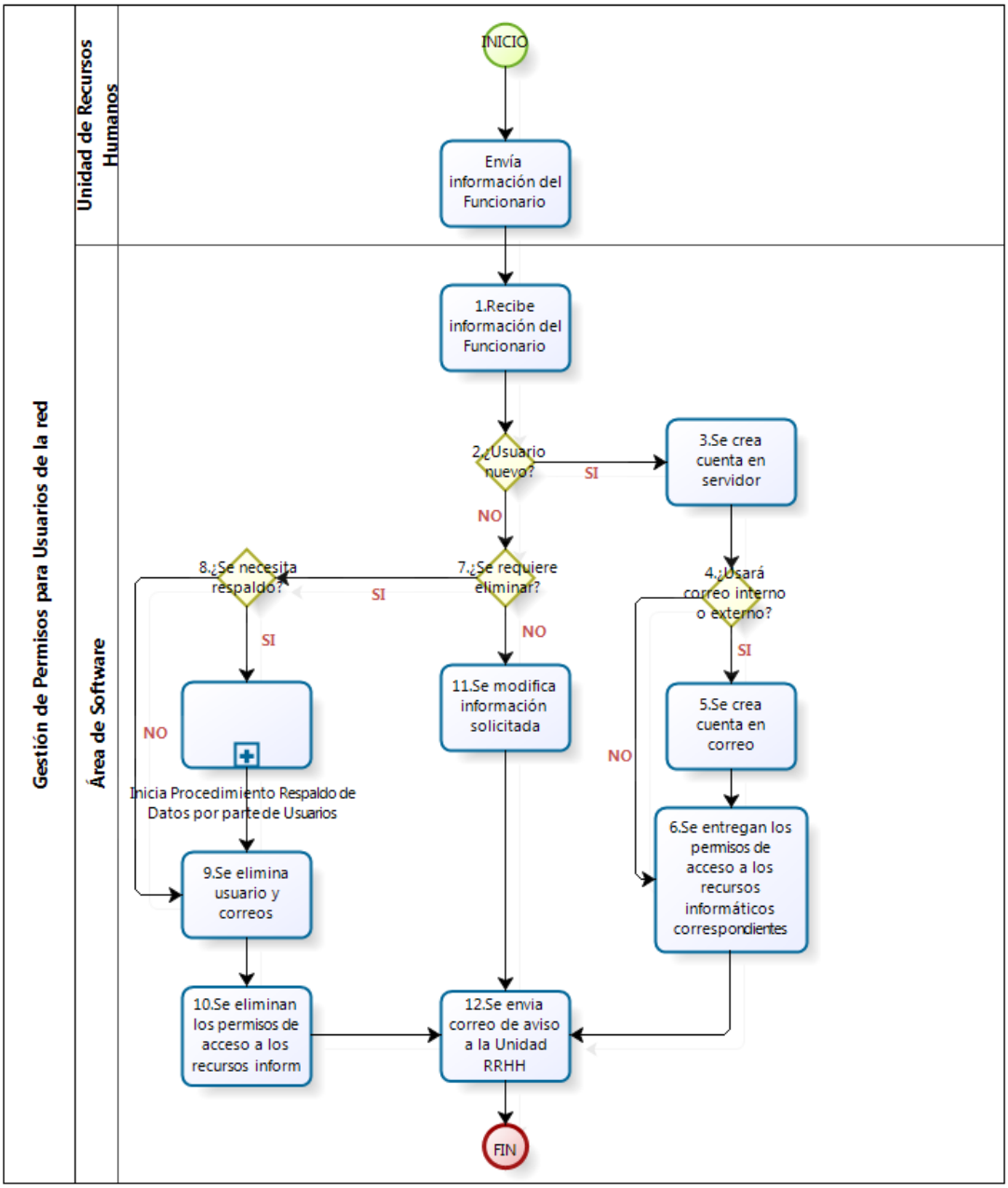
	GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA			
	Procedimiento:	Gestión de permisos para usuarios de la red	**Versión:**	1.0
	Código:	PRO-1.0.6	**Fecha Elaboración:**	

1. **Objetivo:** Proveer permisos de acceso hacia los activos informáticos de la institución, a funcionarios nuevos o antiguos, acorde con el cargo que ostenten y en un tiempo determinado. Así mismo, evitar pérdidas de información en caso de requerirse cambio de personal.
2. **Alcance:** Aplica a todo funcionario entrante o saliente, con acceso a información crítica a través de la red de comunicaciones institucional y sus recursos, ya sea de forma temporal o definitiva.
3. **Abreviaturas y Definiciones:**

Abreviaturas		
Nº	**Término**	**Definición**
1	BDD	Base de Datos
2	RRHH	Recursos Humanos

Definiciones		
Nº	**Término**	**Definición**
1	Permisos de acceso	Conjunto de permisos dados a un usuario o a un sistema para acceder a un determinado recurso.

4. Diagrama de Flujo



5. Desarrollo de Actividades

Procedimiento Gestión de Permisos para usuarios de la red

Nº	Actividad	Descripción	Responsable
1	Recibe información del funcionario, desde la Unidad de RRHH.	Recibe datos del funcionario, del tipo informativo y sobre el cargo designado. Se debe analizar el tipo de permisos a entregarse.	Área Software
2	¿Usuario nuevo?	Si es nuevo, Ver **Actividad 3**, caso contrario Ver **Actividad 7.**	Área Software
3	Crea cuenta en servidor	Se añade usuario a BDD de funcionarios.	Área Software
4	¿Usará correo?	Se analiza si el usuario necesita correo interno o externo, de acuerdo a sus funciones. Si no necesita Saltar a **Actividad 6.**	Área Software
5	Crea cuenta	Se crea cuenta con user name añadiendo @ibarra.gob.ec en caso del correo interno.	Área Software
6	Se entregan permisos correspondientes	Mediante memo, se envía lista de activos informáticos y nivel de permisos de acceso correspondientes al usuario. Saltar a **Actividad 12.**	Área Software
7	¿Eliminar a usuario antiguo?	Si se requiere eliminar los permisos de un usuario existente, ir a **Actividad 8**, caso contrario saltar a **Actividad 11.**	Área Software
8	¿Se necesita respaldo?	En caso de ser necesario, se respalda la información y correos, siguiendo el Procedimiento de Respaldo de Información por parte de Usuarios, caso contrario ir a **Actividad 9**.	Área Software
9	Se elimina usuario y correos	Sin respaldos.	Área Software
10	Se eliminan los permisos de	El cese de funciones en un usuario,	Área Software

	acceso	involucra la pérdida de privilegios entregados, para el acceso a los recursos informáticos correspondientes. Saltar a **Actividad 12.**	
11	Se modifica información solicitada	Modificaciones de permisos, información general del usuario, etc.	Área Software
12	Correo de aviso a RRHH	Envío de tipo y nivel de permisos otorgado al usuario (o aviso de modificaciones realizadas a su cuenta).	Área Software

En síntesis, a través del establecimiento de estos procedimientos se busca entre otros fines:

- Minimizar los errores del usuario y administrador del sistema informático mediante el establecimiento y cumplimiento de tareas metódicas.
- Delimitar las operaciones del personal de Hardware y Software a través del ordenamiento de sus responsabilidades dentro del departamento, en cuanto al mantenimiento de equipos.
- Llevar un registro de aquellos incidentes solucionados que sirvan como base para posteriores eventos, de tal manera que el administrador pueda resolver de manera ágil un problema ya detectado.
- Brindar un servicio de acuerdo al nivel de urgencia, es decir priorizando a aquellos funcionarios cuyas actividades se relacionan directamente con un servicio considerado crítico dentro de la institución (ANEXO A).
- Asegurar la integridad de la información a través del establecimiento de copias o respaldo de datos, por parte del usuario común y los administradores de las bases de datos.
- Garantizar el acceso a la red única y exclusivamente a personas autorizadas, a través de la entrega y retiro de permisos de forma organizada, en coordinación con la Unidad de Recursos Humanos.

CAPÍTULO IV

4. DISEÑO DEL SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS

En este capítulo se exponen las características y funciones de las principales herramientas que fueron escogidas para el diseño del IDS/IPS sobre software libre, además se describe el proceso para su elaboración, definiendo los parámetros de configuración necesarios para su correcto funcionamiento.

4.1 DESCRIPCIÓN DEL SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS

Anteriormente se dieron a conocer los lineamientos que regulan el uso de los recursos tecnológicos de la institución por parte de los usuarios, en pro de la preservación de la confidencialidad, integridad y disponibilidad de su información, a través del establecimiento de políticas y procedimientos. Sin embargo, estas medidas administrativas necesitan complementarse con herramientas técnicas que mitiguen aquellas amenazas netamente informáticas, relacionadas al contenido en sí del tráfico que circula por la red. De este modo, se ha propuesto ejecutar un Sistema de Detección y Prevención de Intrusos para la red administrativa del GAD Ibarra, debido a que forma parte de la nueva generación de técnicas de seguridad, adaptables a todo tipo de escenario informático.

"Los **Sistema de Detección y Prevención de Intrusos** fueron creados para contener las actividades maliciosas en la red. Con el simple deber de detectar, mantener un log y/o

tratar de bloquear estas actividades" (Recuperado el 10 de Diciembre del 2012, de http://www.clm.com.co/soluciones/idps.htm

El IPS ha sido elaborado sobre la versión 6.3 de CentOS (liberado en julio del 2012) y su base es la herramienta Snort inline 2.6.1.5 (liberada a partir de 2005). Además de aquello, se ha añadido el paquete Snort 2.6.1.5 como IDS, para el monitoreo constante de la red y el reconocimiento de ataques mediante firmas actuales. De esta manera se pretende aprovechar las funciones tanto para la detección como para la prevención de intrusos en una PC común, ubicada en un segmento de red interna.

En este sentido, es inevitable reconocer que: "La prevención de intrusos no constituye un reemplazo para la detección de intrusos, sino más bien un complemento" (Recuperado el 21 de Diciembre del 2012, de https:// http://190.90.112.209/http/articulos/hakin9_01_2008_ES.pdf).

4.2 HERRAMENTAS PARA EL DISEÑO DEL SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS

4.2.1 SNORT

Originalmente es un sistema de detección de intrusos (IDS) de código abierto, el cual permite registrar y alertar anomalías en un tramo de red, tales como: escaneos, inundaciones, sesiones no autorizadas, malware, entre otros, a través de sus preprocesadores o firmas por defecto. También puede prestar otras funciones básicas como: sniffer de paquetes (captura el

tráfico de la red y muestra en una consola en tiempo real) y registro de logs (permite guardar los logs generados para su posterior análisis), llamado también packet logger.

El motor de detección Snort posee algunas ventajas que han sido tomadas en cuenta al momento de su elección. Entre otras, son las que se muestran a continuación:

- Es basado en Open Source[20]
- Funciona bajo plataformas Linux y Windows.
- Puede desempeñarse como snnifer[21], packet logger y NIDS.
- Sus firmas de ataques se actualizan constantemente y son adaptables a cualquier escenario.
- Es ampliamente utilizado por profesionales en seguridad informática, a partir de 1998, año donde fue liberado por primera vez.

Snort como IDS, es una herramienta extremadamente útil para la recopilación de información sobre un ataque o el inicio del mismo, sin embargo, se limita a ser una herramienta pasiva (sin respuesta). Snort Inline es una modificación del mencionado paquete, y está diseñado precisamente para complementar esta funcionalidad, permitiendo la inspección y posterior rechazo de paquetes de red, suponiendo que cumplan con ciertos criterios predefinidos que los identifiquen como tráfico no permitido. En otras palabras, Snort

[20] **Open source:** Licencia que garantiza a cualquier persona el derecho de usar, modificar y redistribuir el código libremente.

[21] **Snnifer:** Es un software que permite el análisis y monitoreo del tráfico de la red, a través de la captura de paquetes de información.

Inline hace factible adaptar e implantar las funciones de un IPS o Sistema de Prevención de Intrusos y obtener una respuesta en tiempo real.

Este IPS filtra el tráfico mediante el módulo Queue, el cual permite enviar un paquete recibido hacia el espacio de usuario (alberga las aplicaciones de usuario final), para que Snort Inline pueda tomar acciones sobre éste, basándose en reglas cargadas previamente. Se ubica en medio del tráfico, usando dos tarjetas de red en modo bridge, evidentemente para asegurar que todos los paquetes a analizarse pasen a través de este mecanismo de control.

Por su parte Snort como IDS, puede analizar los paquetes ya sea mediante el puenteo de sus interfaces de red (similar a Snort Inline) o utilizando una réplica del tráfico, proveniente de un puerto espejo del switch.

Figura 4. 1: Logo Snort Inline
Referencia: http://snort-inline.sourceforge.net/

4.2.1.1 Elementos de Snort

Tanto Snort como Snort Inline procesan el tráfico entrante a través de los siguientes elementos:

Tabla 4. 1: Elementos de Snort

Referencia: http://www.snort.org

Módulo de captura	Se encarga de la captura de paquetes, mediante la librería libpcap.
Decodificador	Toma esos paquetes desde libpcap y los organiza en estructuras de datos de acuerdo a cada protocolo.
Preprocesadores	Ordena los paquetes de forma que pueda ser interpretada la información. De esta forma se facilita la aplicación de las distintas reglas para la búsqueda de un determinado ataque. Entre los preprocesadores destacan: **Sfportscan:** detecta ataques de reconocimiento, como por ejemplo, el escaneo de puertos. **Arpspoof:** detecta ataques por suplantación de ARP, tomando en consideración la auténtica correlación entre la dirección IP y MAC de cada host de la red. **Frag3:** sustituye a frag2 de versiones anteriores de Snort y tiene como objetivo el reensamblaje de paquetes fragmentados de modo que el motor de detección pueda analizar el contenido de dichos paquetes sin problemas, o a su vez evitar ataques por fragmentación. **Stream4:** hace un seguimiento de cada una de las conexiones TCP, UDP e ICMP, durante un tiempo o cantidad de paquetes previamente configurados. **HTTP Inspect:** examina el trafico HTTP, incluyendo URL's, cookies, etc.

Motor de detección	Es responsable de detectar si existe alguna actividad de intrusión, comparándolas con las reglas previamente definidas. Los factores que influyen en el tiempo de respuesta del motor de detección son los siguientes: _Características de la máquina anfitrión _Número de reglas o firmas definidas _Carga de la red De este modo, si la máquina anfitrión no posee las suficientes características para el procesamiento de todos los paquetes que circulan a través de ella, puede generarse cuellos de botella en el caso de los IPS o pérdidas de paquetes en los IDS.
Módulo de salida	Define el formato con el que se guardarán las alertas generadas por Snort.

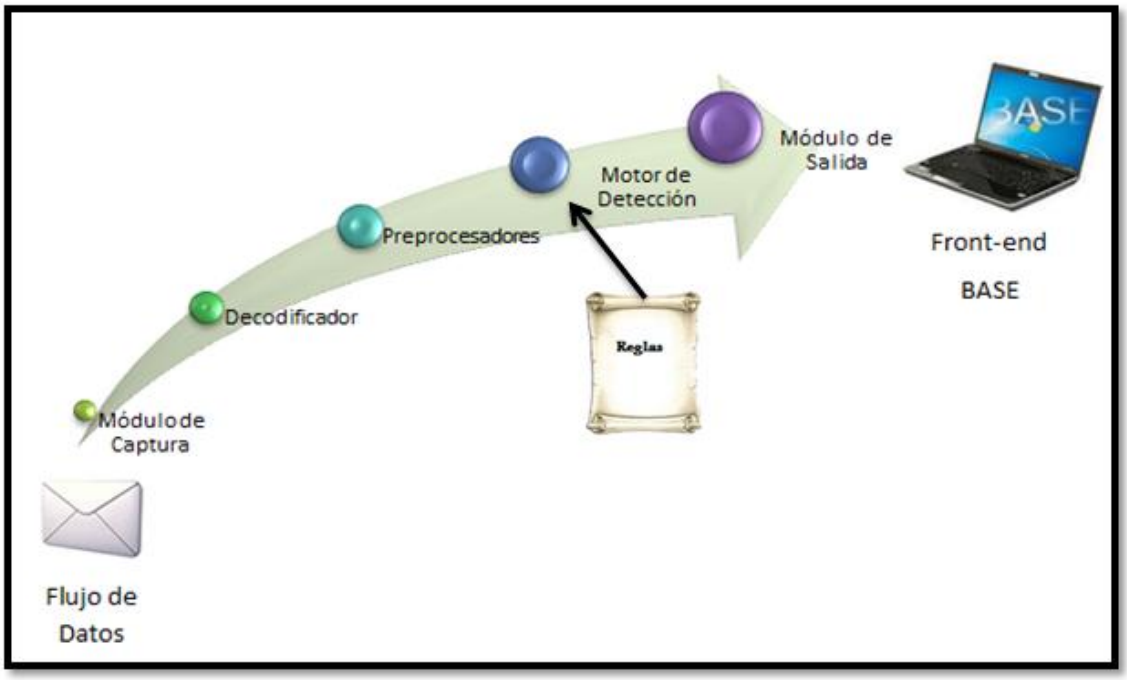


Figura 4. 2: Elementos de Snort

Referencia: http://www.snort.org

4.2.2 MYSQL

Es un gestor de base de datos en open source y de uso masivo, debido a su gran facilidad de instalación, rapidez, soporte multiplataforma, bajo consumo de recursos, etc. Es utilizado ampliamente para el almacenamiento de alertas generadas por Snort, debido a la facilidad de compilación y configuración con esta herramienta.

Figura 4. 3: Logo MySQL
Referencia: http://www.mysql.com

4.2.3 PHP (PHP HYPERTEXT PRE-PROCESSOR)

Es un lenguaje de programación de código abierto y muy popular, utilizado para la visualización y configuración de páginas web. Puede ser desplegado en la mayoría de los servidores web y en casi todos los sistemas operativos y plataformas sin costo alguno. Además permite la conexión con diferentes bases de datos tales como: MySQL, Postgres, Oracle, etc. En este sentido, esta herramienta servirá para la generación de la página web en la que se visualizarán las alertas de Snort.

Figura 4. 4: Logo PHP
Referencia: http://news.softpedia.es/

4.2.4 APACHE

Es un servidor web HTTP en código abierto, multiplataforma, con soporte para PHP y configurable para la aplicación de bases de datos como MySQL.

Figura 4. 5: Logo Apache
Referencia: http://www.apache.org

4.2.5 INTERFAZ BASE (BASIC ANALYSIS AND SECURITY ENGINE)

Es una derivación de ACID (Consola de Análisis para Bases de Datos de Intrusiones). Está escrita en PHP, tiene como objetivo analizar los contenidos de la base de datos de Snort.

Permite agrupar alertas, basándose en sus direcciones IP, protocolos y puertos, tipos de ataques, contenidos del paquete, etc., con el fin de realizar búsquedas detalladas de las alertas generadas.

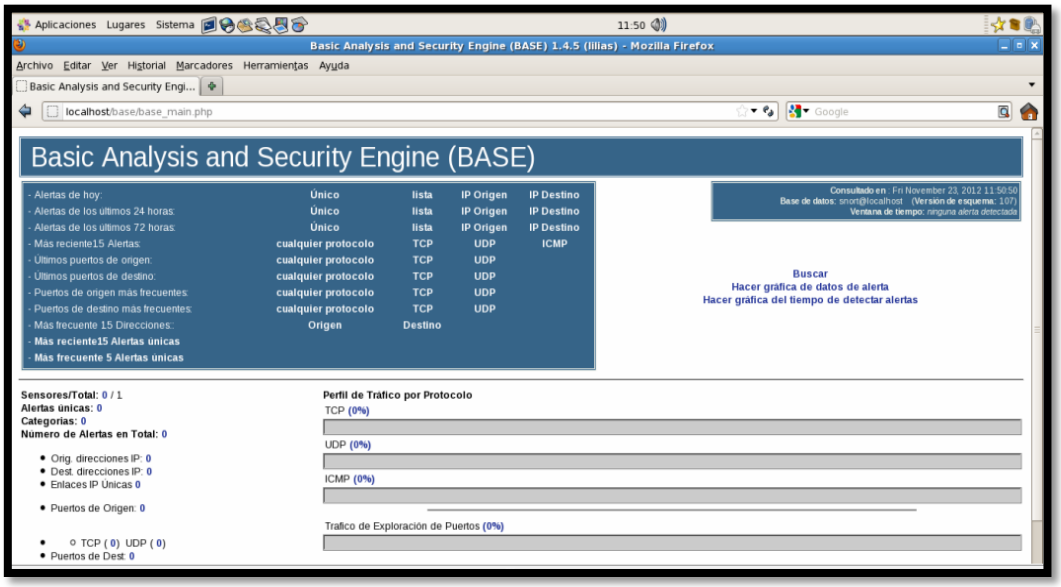


Figura 4. 6: Interfaz BASE

Referencia: http://www.snort.org

Adicionalmente a estas herramientas es necesario instalar otros paquetes de software para su correcto desempeño, entre los principales se encuentran:

Tabla 4. 2: Paquetes de software necesarios

Referencia: http://www.snort.org

Paquete	Versión	Descripción	Modo de ejecución
Barnyard	**0.2.0**	Permite que Snort optimice sus funciones y mejore su rendimiento, debido a que colabora con la interpretación de paquetes capturados y transporte de los mismos a la base de datos.	IDS

Snortrules-pr	**2.4**	Paquetes de reglas (Pertenece a Sourcefire[22])	IDS
Emerging rules	**_**	Paquete de reglas (Pertenece a Emerging Threaths Pro[23])	IDS
Pulledpork	**0.6.1**	Para la actualización automática del paquete de reglas.	IDS
Libpcap	**1.0.0**	Librería open source escrita en C para la captura de paquetes.	IDS/IPS
Libdnet	**1.12**	Librería que provee acceso a varios protocolos.	IDS/IPS
Iptables	**1.4.7**	Conjunto de reglas de filtrado de paquetes en prácticamente todas las distribuciones Linux.	IPS
Pcre	**7.8**	(Perl Compatible Regular Expressions) permite integrar Apache con PHP.	IDS/IPS
Adodb	**5.0**	Librería de código abierto para acceder a bases de datos con PHP.	IDS/IPS

A continuación, se presenta un diagrama de bloques que sintetiza el escenario que conforma Snort y sus herramientas complementarias:

[22] **Sourcefire:** Empresa especializada en soluciones de seguridad, fundada por Martin Roesch, creador de Snort.

[23] **Emerging Threaths Pro:** Empresa especializada en la creación de set de reglas tanto para Snort, Suricata, y otros motores de detección. Fue fundada por Matt Jonkman en 2006.

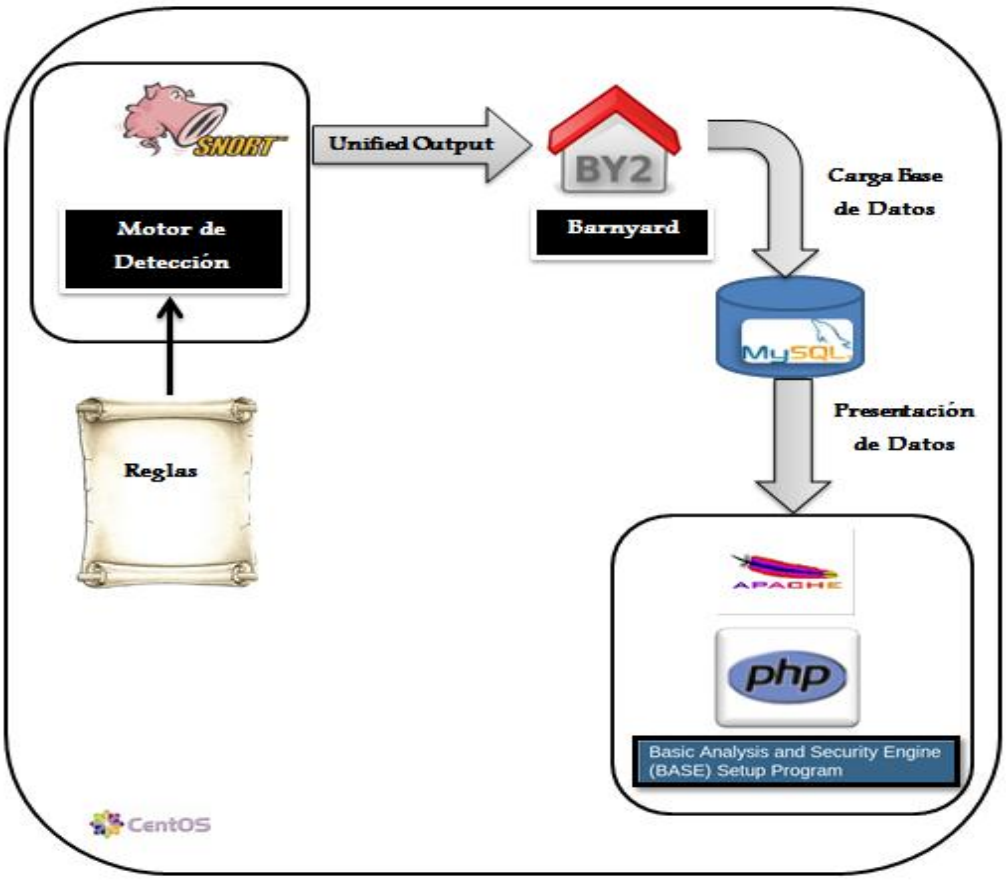


Figura 4. 7: Diagrama de Bloques de Snort (IDS) y sus herramientas complementarias
Referencia: http://polaris.umuc.edu/~sgantz/Install.html

Cabe destacar, que el paquete Snort Inline, no hace uso de la herramienta Barnyard, y la salida de sus datos se cargan directamente en la base de datos.

4.3 CARACTERÍSTICAS DEL EQUIPO

Las características del equipo deben satisfacer los requerimientos mínimos del software que está por instalarse (Tabla 4.3), pero también necesitan estar acorde con factores determinantes como el volumen del tráfico que circula por la red y el número de firmas que van a ser cargadas en el IDS/IPS. Por tal motivo es necesario considerar un dispositivo con muy buenas prestaciones tanto en capacidad de memoria, procesamiento y espacio de

almacenamiento en disco, para evitar errores en el monitoreo de la red o en el funcionamiento de la misma.

Tabla 4. 3: Requerimientos mínimos del sistema operativo

Referencia: http://www.snort.org

REQUERIMIENTOS MÍNIMOS CENTOS 6.3	
RAM	384 MB modo texto
	652 MB modo gráfico
Espacio en disco	10 GB
Arquitectura	32/64 bits

El artículo *"Capacity Planning for Snort IDS"* (Recuperado de http://mikelococo.com/2011/08/snort-capacity-planning/), señala que es factible utilizar una memoria RAM de 8 GB y de 2 a 4 procesadores, para abastecer a 200 Mbps de tráfico real y 7000 firmas cargadas.

En este sentido, se conoce que la red del GADI es Fast Ethernet, por lo que su volumen de datos real (throughput) será obviamente menor a 100 Mbps teóricos, a su vez, la cantidad de firmas (Emerging Threats) habilitadas es de 5000. De esta manera, un volumen de tráfico que bordea los 100 Mbps, requerirá una RAM de 3 a 4 GB y 2 procesadores.

De esta manera las características del equipo IDS/IPS son las que se muestran a continuación:

Tabla 4. 4: Características del equipo IDS/IPS

Referencia: http://www.intel.com

Características de Hardware		
Procesador	Intel Core i3	
RAM	4 GB	
Espacio en disco	750 GB	
Tarjetas de red	eth0	Marca: Intel 82579V Velocidad: 10/100/1000 Mbps Tipo de conexión: Integrada
	eth3	Marca: TP- link TG-3468 Velocidad: 10/100/1000 Mbps Tipo de conexión: PCIe
Direccionamiento (NIC para administración)		
Dirección IP	172.16.9.x	
Máscara	255.255.x.x	
Gateway	172.16.x.x	
DNS	172.16.8.94	

4.4 UBICACIÓN DEL IDS/IPS

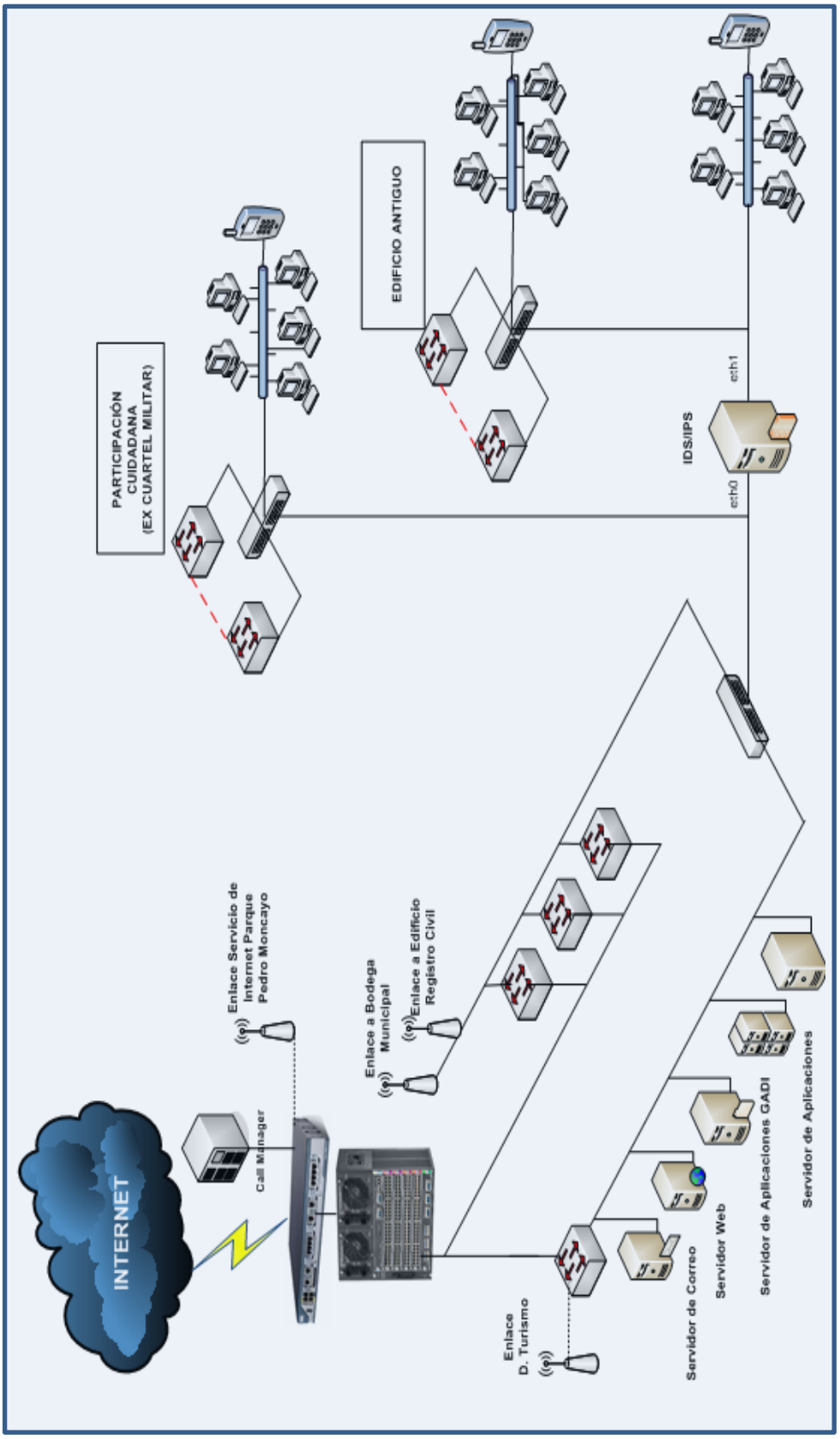


Figura 4. 8: Ubicación del IDS/IPS
Referencia: Red-administrativa GADI-2012

4.5 CONFIGURACIÓN DE PARÁMETROS

A continuación se expone la configuración del IDS/IPS, detallando los parámetros y herramientas que han sido utilizadas, dentro del entorno de CentOS 6.3.

4.5.1 INSTALACIÓN DE DEPENDENCIAS

Snort (IDS) y Snort Inline (IPS) requieren la instalación de prerrequisitos o dependencias para su correcto funcionamiento. Entre las cuales sobresalen la biblioteca de captura de paquetes multiplataforma Libpcap, MySQL como gestor de base de datos para el almacenamiento de alertas e Iptables usado por Snort Inline para el filtrado de tráfico. A continuación se muestra el comando para la instalación de cada paquete y la lista de las dependencias necesarias:

yum -y install ‹paquete›

Tabla 4. 5: Lista de prerrequisitos de instalación
Referencia: http://polaris.umuc.edu/~sgantz/Install.html

Librería para captura de datos: libpcap libpcap-devel
Librería para acceso a distintos protocolos de red: libdnet
Librerías Perl Compatible Regular Expressions (PCRE): pcre pcre-devel
Compiladores GNU C/C++: gcc gcc-c++
Generador de analizadores sintácticos: bison
Generador de analizadores léxicos: flex
Relacionados a la base de datos MySQL: mysql mysql-server mysql-devel mysql-bench

Servidor Web: httpd
PHP Hypertext Preprocessor: php **PHP command line interpreter**: php-cli **PHP extension and application repository (PEAR):** php-pear **PHP Graphics Drawing module:** php-gd **PHP module for using MySQL:** php-mysql **PHP module for optimizing ADOdb**: php-adodb **PHP graphing modules:** php-pear-Numbers-Roman php-pear-Numbers-Words php-pear-Image-Color php-pear-Image-Canvas php-pear-Image-Graph
Iptables: iptables-devel

4.5.2 INSTALACIÓN DE SNORT Y SNORT INLINE

Una vez descargados los paquetes snort 2.6.1.5 y snort_inline 2.6.1.5, se han descomprimido y compilado con soporte para la base de datos MySQL, mediante los comandos que se muestran a continuación:

Tabla 4. 6: Compilación de los paquetes Snort y Snort Inline
Referencia: http://polaris.umuc.edu/~sgantz/Install.html

```
tar xvzf ‹paquete.tar.gz›
cd ‹paquete›
./configure - -with-mysql
make
make install
```

4.5.2.1 Creación de directorios necesarios

Se crean directorios donde se alojarán los archivos de Snort y Snort Inline, las reglas a cargarse y los archivos log de las alertas.

Tabla 4. 7: Creación de directorios para resguardo de archivos de configuración y reglas necesarias.
Referencia: http://polaris.umuc.edu/~sgantz/Install.html

```
mkdir /etc/snort

mkdir /etc/snort/rules

mkdir /var/log/snort

mkdir /etc/snort_inline

mkdir /etc/snort_inline/reglas

mkdir /var/log/snort_inline
```

4.5.2.2 Edición del archivo de configuración snort.conf

En este archivo se han de establecer los parámetros generales de Snort en modo IDS, señalando el rango de dirección de red a monitorear, la ruta del archivo de reglas o firmas, los preprocesadores que desean ser activados y el formato del módulo de salida de las alertas generadas. En esta ocasión, se ha optado por un formato de salida binario (Unified), de tal manera que las alertas no ocupen demasiado espacio en las bases de datos y se generen de manera ágil.

Tabla 4. 8: Parámetros de configuración de Snort

Referencia: http://polaris.umuc.edu/~sgantz/Install.html

EDICIÓN DE VARIABLES PRINCIPALES
var HOME_NET ***172.0.0.0/8*** var EXTERNAL_NET any var RULE_PATH /etc/snort/rules
HOME_NET: Indica la red o subred a monitorear. **EXTERNAL_NET:** Se setea la variable any, para indicar que los ataques pueden provenir de cualquier dirección sea interna o externa. **RULE_PATH:** Determina la ruta del directorio donde se almacenan las reglas.
EDICIÓN DE LOS PARÁMETROS DEL PREPROCESADOR FRAG3
preprocessor frag3_global: max_frags ***65536*** preprocessor frag3_engine: policy first detect_anomalies bind_to ***172.0.0.0/8***
max_frags: Número máximo de fragmentos simultáneos a analizar (por defecto 65536). **bind_to:** Enlista las IPs que analiza frag3.
EDICIÓN DE LOS PARÁMETROS DEL PREPROCESADOR STREAM4
preprocessor stream4_reassemble:ports 21 23 25 53 80 110 111 139 143 445 513 1433
ports: Limita el número de puertos que analiza Stream4.
EDICIÓN DE LOS PARÁMETROS DEL PREPROCESADOR SFPORTSCAN
preprocessor sfportscan: proto { all } \ memcap { 10000000 } \

sense_level { low }
proto: Indica que protocolos va a analizar sfportscan (tcp, udp, icmp, ip, all) **memcap:** Máxima cantidad de memoria usada (bytes). A mayor cantidad, mayor capacidad de detección. **sense_level:** Nivel de sensibilidad de la detección, se recomienda usar un nivel bajo para evitar falsos positivos.
EDICIÓN DE LOS PARÁMETROS DEL PREPROCESADOR ARPSPOOF
preprocessor arpspoof preprocessor arpspoof_detect_host: ***172.16.8.160 00:0D:88:F5:B1:12***
arpspoof_detect_host: Se indica la relación entre la dirección física y lógica del host, para evitar falsos vínculos entre la IP y MAC.
CONFIGURACIÓN DEL MÓDULO DE LA SALIDA DE DATOS
output log_**unified**: filename snort.log, limit 128
Habilitar la salida de datos en el formato binario unified, los cuales serán interpretados por Barnyard antes de llegar a la base de datos.

4.5.2.3 Edición del archivo de configuración snort_inline.conf

Así mismo, Snort en modo IPS cuenta con un archivo de configuración similar, su diferencia radica en la configuración del módulo de salida, el cual necesita ser enlazado directamente a la base de datos MySQL. Con esto se elimina la necesidad de requerir el paquete Barnyard como intermediario, para el traslado de las alertas hacia la base de datos.

Tabla 4. 9: Parámetros de configuración de Snort Inline

Referencia: http://openmaniak.com/inline_tutorial.php

EDICIÓN DE VARIABLES PRINCIPALES
var HOME_NET 172.0.0.0/8 var EXTERNAL_NET any var RULE_PATH /etc/snort_inline/reglas
Modificar las variables HOME_NET y EXTERNAL_NET de la misma manera que en snort.conf. Además modificar la ruta RULE_PATH por el directorio donde se alojan las reglas para Snort Inline.
CONFIGURACIÓN DEL MÓDULO DE LA SALIDA DE DATOS
output database:log,mysql,user=snort1 password=snortpass1 dbname=snort1 host=localhost
La salida de datos se carga directamente a la base de datos snort1.

4.5.3 CREACIÓN DE LA BASE DE DATOS

Este proceso se divide en tres apartados. El primero corresponde al establecimiento de la contraseña de administrador para el acceso a la base de datos MySQL. Seguidamente se crea la base en sí, otorgándole todos los privilegios y finalmente deben ser cargadas las tablas incluidas en el directorio “schemas” de Snort y Snort Inline.

Tabla 4. 10: Configuración de MySQL

Referencia: http://polaris.umuc.edu/~sgantz/Install.html

/usr/bin/mysqladmin -u root password 'admin' mysql –u root –p

```
password:admin
mysql> create database snort;
grant INSERT,SELECT on root.* to snort@localhost;
SET PASSWORD FOR snort@localhost=PASSWORD('snortpass');
grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to
snort@localhost;
grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort;
exit;
mysql -u root -p < ~/snortinstall1/snort-2.6.1.5/schemas/create_mysql snort
```

4.5.3.1 Verificación de la base de datos

Se debe comprobar que la base de datos se ha generado y que las tablas han sido introducidas correctamente. Además se recomienda crear una base tanto para Snort como para Snort Inline.

Tabla 4. 11: Verificación de MySQL

Referencia: http://polaris.umuc.edu/~sgantz/Install.html

```
mysql -p
mysql> show databases;
mysql> use snort1;
mysql> show tables;
```

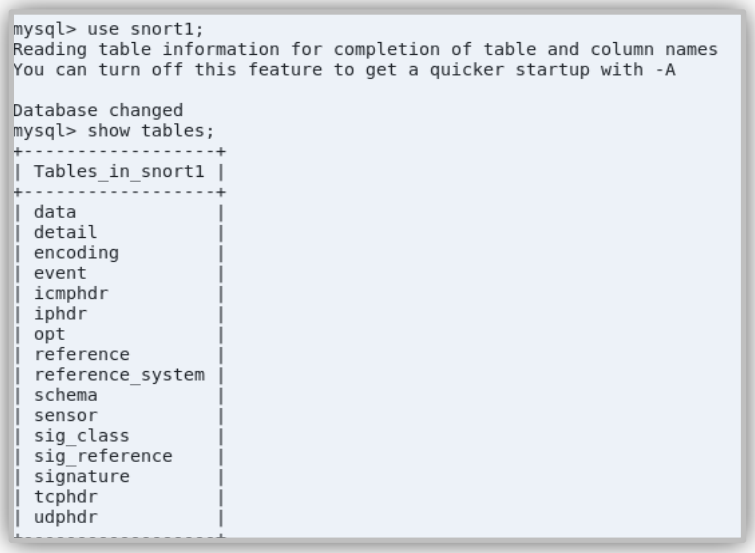


Figura 4. 9: Tablas base de datos snort1

Referencia: Fuente propia-software MySQL

4.5.4 PUENTEO DE INTERFACES

Mediante el bridging o puenteo, se logra atravesar el tráfico de red en medio del servidor, a partir de una interfaz virtual (br0) que enlaza en este caso dos interfaces físicas (eth0: entrada y eth3: salida), de modo que el tráfico en cuestión, pueda ser analizado y filtrado de acuerdo a las sentencias de Snort y Snort Inline.

Tabla 4. 12: Bridging de interfaces

Referencia: http://openmaniak.com/inline_tutorial.php

brctl addbr br0 brctl addif br0 eth0 brctl addif br0 eth3
Se obtiene una nueva interfaz virtual bridge br0 sin dirección IP. Si se requiere

administrar el IDS/IPS, será necesario el uso de una tercera interfaz.

4.5.5 INSTALACIÓN DE BARNYARD

Como se mencionó anteriormente esta herramienta colabora con la interpretación de la salida de datos en formato ***Unified*** provenientes de Snort en modo IDS y en el transporte de los mismos a la base de datos, logrando de esta manera minimizar las tareas de Snort, reducir la carga del servidor e incrementar su rendimiento.

Una vez descargado el paquete de Barnyard, se descomprime y compila con soporte para la base de datos MySQL, de forma similar a los paquetes Snort.

Tabla 4. 13: Conpilación de Barnyard
Referencia: http://polaris.umuc.edu/~sgantz/Install.html

```
tar –xvzf barnyard-0.2.0.tar.gz
cd barnyard-0.2.0
./configure --enable-mysql
make
make install
```

4.5.5.1 Edición del archivo configuración barnyard.conf

Se edita la interfaz por donde circula el tráfico a analizar, en este caso br0. Además se indica el nombre de la base de datos, el password y el usuario, necesarios para identificar la base de datos y credenciales para el enlace.

Tabla 4. 14: Parámetros de configuración de Barnyard

Referencia: http://polaris.umuc.edu/~sgantz/Install.html

```
config interface: br0
output alert_acid_db: mysql, sensor_id 1, database snort, server localhost, user
snort, password snortpass
output log_acid_db: mysql, database snort, server localhost, user snort, password
snortpass, detail full
```

4.5.5.2 Ejecución de Barnyard

```
/usr/local/bin/barnyard -c /etc/snort/barnyard.conf -d /var/log/snort/ -f
snort.log -w /var/log/snort/barnyard.waldo
```

La herramienta Barnyard debe ser activada, siempre y cuando se ejecute Snort en modo IDS, y se requiera la interfaz de visualización de BASE, ya que a través de dicha herramienta se envían las alertas en forma binaria hacia la base de datos MySQL para su posterior visualización.

4.5.6 INSTALACIÓN DE PULLEDPORK

Pulledpork permite actualizar constantemente las firmas cargadas en Snort IDS, con soporte tanto para reglas de la comunidad Sourcefire (creadora de Snort), como para aquellas pertenecientes a Emerging Threats, las mismas que fueron utilizadas para este proyecto.

El paquete Pulledpork fue extraído del sitio web: http://pulledpork.googlecode.com/files/pulledpork-0.6.1.tar.gz.

A continuación se muestra el procedimiento para su instalación:

Tabla 4. 15: Proceso de configuración de Pulledpork paso a paso.
Referencia: http://polaris.umuc.edu/~sgantz/Install.html

```
tar zxvf pulledpork.tar.gz
cd pulledpork-0.6.1
cp pulledpork.pl /usr/local/bin/
mkdir -p /usr/local/etc/pulledpork
cp etc/* /usr/local/etc/pulledpork/
chmod +x /usr/local/bin/pullepork.pl
```

4.5.6.1 Edición del archivo de configuración pulledpork.conf

En este archivo se ha de fijar la URL a través de la cual se descargarán las actualizaciones de las base de firmas seleccionadas y se ha de establecer la ruta del archivo donde van a ser almacenadas.

Tabla 4. 16: Parámetros de configuración de Pulledpork.
Referencia: http://polaris.umuc.edu/~sgantz/Install.html

rule_url=https://rules.emergingthreats.net/|emerging.rules.tar.gz|open rule_path=/etc/snort/rules/snort.rules
Descomentar la url de las firmas a utilizarse. Automáticamente se creará el

fichero snort.rules, el mismo que albergará las firmas Emerging Threaths descargadas, previa ejecución de Pulledpork.
distro=***RHEL-6.0*** enablesid=/usr/local/etc/pulledpork/enablesid.conf dropsid=/usr/local/etc/pulledpork/dropsid.conf disablesid=/usr/local/etc/pulledpork/disablesid.conf modifysid=/usr/local/etc/pulledpork/modifysid.conf
Editar la distribución Linux utilizada, en este caso cambiar a RHEL (Red Hat Enterprise Linux) versión 6. Descomentar los archivos para la administración de reglas, a través de los cuales se señala el conjunto de reglas habilitadas y deshabilitadas.

4.5.6.2 Ejecución de Pulledpork

perl /usr/local/bin/pulledpork.pl –c /usr/local/etc/pulledpork/pulledpork.conf

Figura 4. 10: Ejecución Pulledpork

Referencia: Fuente propia-software Pulledpork

4.5.7 CONFIGURACIÓN DE LA INTERFAZ GRÁFICA

4.5.7.1 Instalar Adodb

Este paquete actúa como un intermediario entre PHP y MySQL, necesario para la extracción de datos y la presentación de los mismos en una interfaz de visualización.

Tabla 4. 17: Proceso de configuración del paquete Adodb.
Referencia: http://nachum234.no-ip.org/security/snort/3-base-installation/

```
wget http://sourceforge.net/projects/adodb/files/adodb-php5-only/adodb-511-
for-php5/adodb511.tgz/download
cd /var/www/
tar -xvzf /root/snortinstall1/adodb-511 .tgz
mv adodb5/ adodb1
chmod 777 /var/www/adodb1
```

4.5.7.2 Instalar BASE

Basic Análisis and Security Engine (BASE), es la interfaz o consola de visualización escrita en PHP, a través de la cual se observarán y clasificarán las alertas en tiempo real.

Tabla 4. 18: Proceso de configuración del paquete BASE.
Referencia: http://nachum234.no-ip.org/security/snort/3-base-installation/

```
wget http://sourceforge.net/projects/secureideas/files/BASE/base-1.4.5/base-
1.4.5.tar.gz/download
cd /var/www/html
```

```
tar -zxvf /root/snortinstall/base-1.4.5.tar.gz

mv base-1.4.5/ base1/

chmod 777 /var/www/html/base1
```

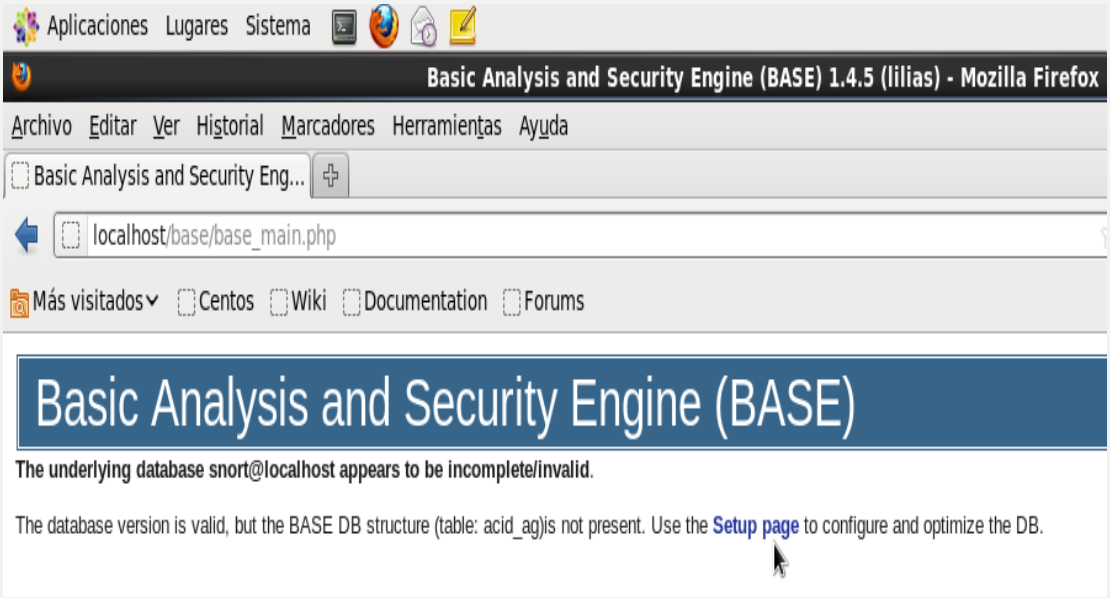
4.5.7.3 Configurar BASE

Se expone paso a paso el proceso de configuración de la interfaz gráfica BASE, para lo cual deben ser reiniciados previamente los servicios HTTP y MySQL:

Tabla 4. 19: Proceso de configuración de la interfaz gráfica BASE paso a paso.
Referencia: http://nachum234.no-ip.org/security/snort/3-base-installation/

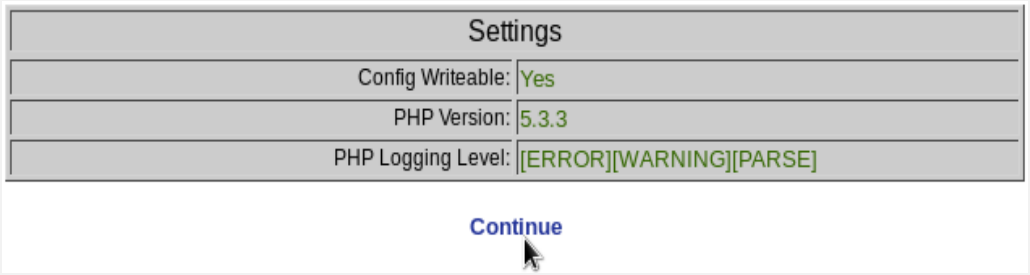
1)

- Acceder al navegador con la dirección: http://localhost/base1/.
- Clic en ***Setup page***.



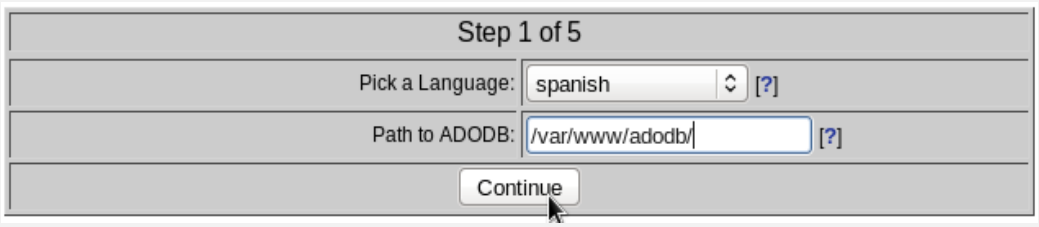
2)

- Clic en ***Continue.***



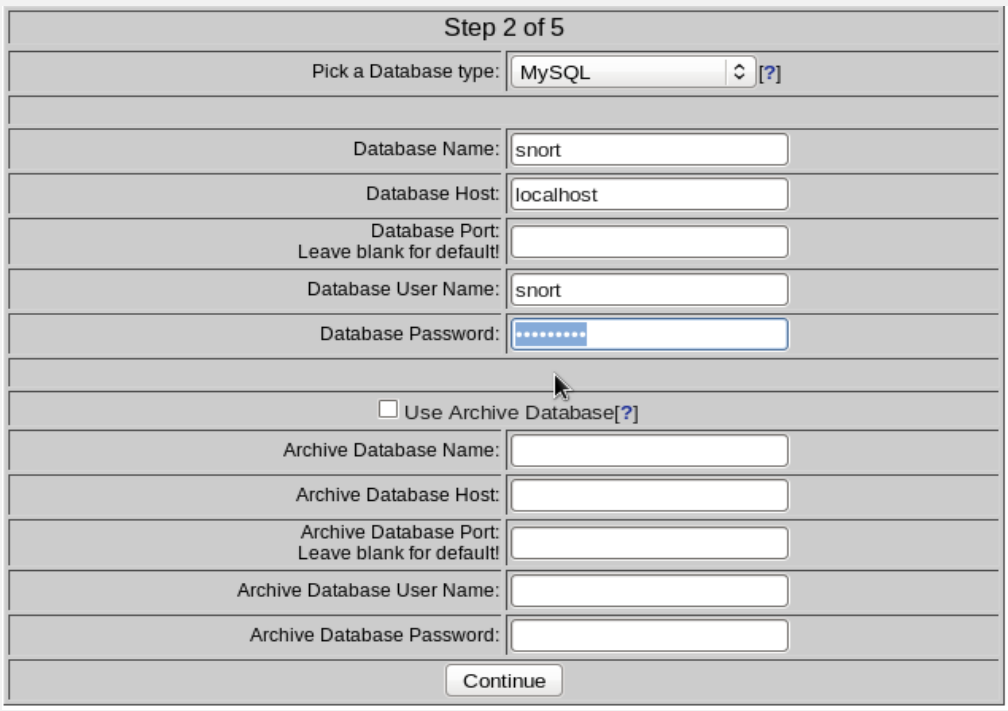
3)

- Elegir ***idioma*** y colocar ruta de archivo Adodb



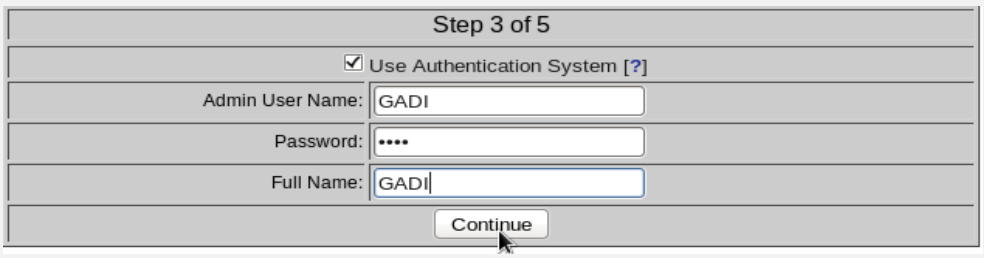
4)

- Especificar el tipo, ***nombre***, ***usuario*** y ***password*** de la base de datos.



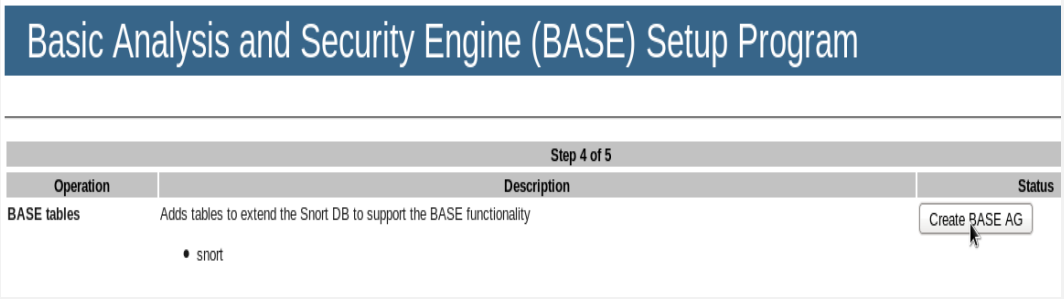
5)

- Activar la ***autenticación*** del sistema (opcional).



6)

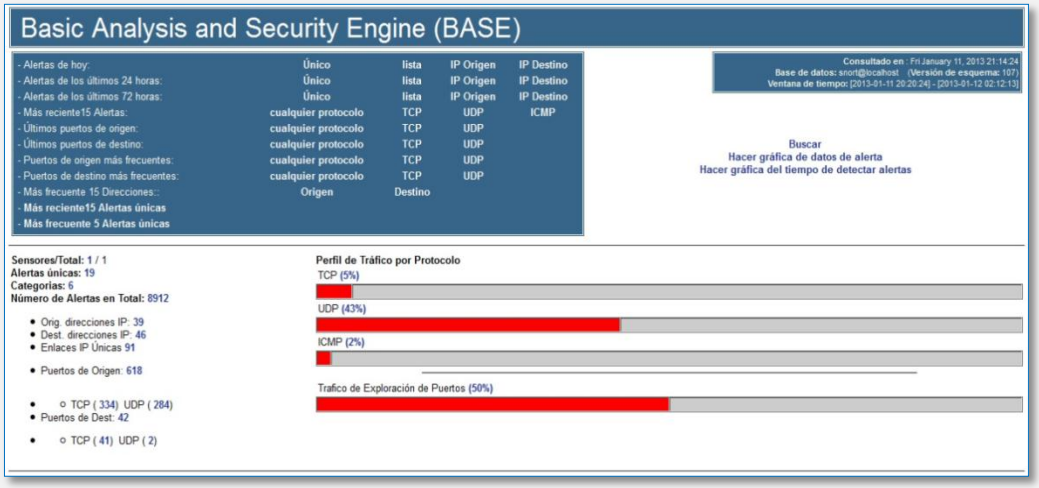
- Crear las tablas de la base de datos en la consola BASE.
- Clic en ***Create BASE AG.***



7)

- Comprobar la configuración. Ir a http://localhost/base1/

Resumen de Alertas de acuerdo al porcentaje detectado



Resumen de Alertas por protocolo

ID	< Firma >	< Marca de tiempo >	< Dirección Origen >	< Dirección Dest >	< Proto capa 4 >
#0-(1-256)	[snort] Snort Alert [1:10005:0]	2013-01-11 22:21:23	172.16.9.14:50372	172.16.8.93:3128	TCP
#1-(1-238)	[snort] Snort Alert [1:10005:0]	2013-01-11 22:11:03	172.16.8.93:3128	172.16.9.121:1115	TCP
#2-(1-237)	[snort] Snort Alert [1:10005:0]	2013-01-11 22:10:14	69.171.248.16:80	172.16.9.30:1850	TCP
#3-(1-231)	[snort] Snort Alert [1:10006:0]	2013-01-11 22:06:14	172.16.11.92:2796	172.16.8.93:3128	TCP
#4-(1-230)	[snort] Snort Alert [1:10005:0]	2013-01-11 22:06:13	172.16.11.92:2808	172.16.8.93:3128	TCP
#5-(1-228)	[snort] Snort Alert [1:10006:0]	2013-01-11 22:05:01	172.19.10.24:1375	172.16.8.93:3128	TCP
#6-(1-226)	[snort] Snort Alert [1:10005:0]	2013-01-11 22:03:19	172.19.10.34:49998	172.16.8.93:3128	TCP
#7-(1-213)	[snort] Snort Alert [1:10005:0]	2013-01-11 21:58:45	172.19.10.35:59343	172.16.8.93:3128	TCP
#8-(1-212)	[snort] Snort Alert [1:10005:0]	2013-01-11 21:56:43	172.19.10.35:59343	172.16.8.93:3128	TCP
#9-(1-211)	[snort] Snort Alert [1:10005:0]	2013-01-11 21:55:15	172.16.8.93:3128	172.16.9.93:1541	TCP
#10-(1-208)	[snort] Snort Alert [1:10005:0]	2013-01-11 21:55:02	69.171.248.16:80	172.16.9.30:1356	TCP
#11-(1-207)	[snort] Snort Alert [1:10006:0]	2013-01-11 21:53:33	172.16.11.92:2569	172.16.8.93:3128	TCP
#12-(1-206)	[snort] Snort Alert [1:10005:0]	2013-01-11 21:53:21	172.16.11.92:2605	172.16.8.93:3128	TCP
#13-(1-205)	[snort] Snort Alert [1:10005:0]	2013-01-11 21:53:21	172.19.10.35:59343	172.16.8.93:3128	TCP
#14-(1-203)	[snort] Snort Alert [1:10005:0]	2013-01-11 21:50:29	172.19.10.35:59274	172.16.8.93:3128	TCP
#15-(1-202)	[snort] Snort Alert [1:10005:0]	2013-01-11 21:50:23	172.16.8.93:3128	172.16.9.93:1380	TCP
#16-(1-183)	[snort] Snort Alert [1:10005:0]	2013-01-11 21:34:44	172.16.8.93:3128	172.16.9.14:50169	TCP
#17-(1-182)	[snort] Snort Alert [1:10005:0]	2013-01-11 21:34:44	172.16.9.14:50169	172.16.8.93:3128	TCP
#18-(1-178)	[snort] http_inspect: IIS UNICODE CODEPOINT ENCODING	2013-01-11 21:30:26	172.16.10.182:1264	172.16.8.103:80	TCP
#19-(1-146)	[snort] http_inspect: IIS UNICODE CODEPOINT ENCODING	2013-01-11 21:00:35	172.16.10.141:2012	172.16.8.110:80	TCP
#20-(1-120)	[snort] Snort Alert [1:10005:0]	2013-01-11 20:59:24	172.16.8.93:3128	172.16.9.93:1413	TCP
#21-(1-101)	[snort] Snort Alert [1:10005:0]	2013-01-11 20:52:42	172.16.8.93:3128	172.16.9.93:1380	TCP
#22-(1-88)	[snort] Snort Alert [1:10005:0]	2013-01-11 20:51:28	172.16.9.14:49935	172.16.8.93:3128	TCP
#23-(1-89)	[snort] Snort Alert [1:10005:0]	2013-01-11 20:51:28	172.16.8.93:3128	172.16.9.14:49935	TCP
#24-(1-90)	[snort] Snort Alert [1:10005:0]	2013-01-11 20:51:28	172.16.9.14:49938	172.16.8.93:3128	TCP
#25-(1-91)	[snort] Snort Alert [1:10005:0]	2013-01-11 20:51:28	172.16.8.93:3128	172.16.9.14:49938	TCP
#26-(1-87)	[snort] Snort Alert [1:10005:0]	2013-01-11 20:50:01	172.16.8.93:3128	172.16.9.93:1415	TCP
#27-(1-86)	[snort] http_inspect: IIS UNICODE CODEPOINT ENCODING	2013-01-11 20:49:55	172.16.9.62:1995	172.16.8.103:80	TCP
#28-(1-81)	[snort] http_inspect: IIS UNICODE CODEPOINT ENCODING	2013-01-11 20:49:33	172.16.11.126:4698	172.16.8.103:80	TCP
#29-(1-82)	[snort] Snort Alert [1:10005:0]	2013-01-11 20:49:33	172.16.9.14:49918	172.16.8.93:3128	TCP
#30-(1-83)	[snort] Snort Alert [1:10005:0]	2013-01-11 20:49:33	172.16.8.93:3128	172.16.9.14:49918	TCP
#31-(1-84)	[snort] Snort Alert [1:10005:0]	2013-01-11 20:49:33	172.16.9.14:49917	172.16.8.93:3128	TCP
#32-(1-85)	[snort] Snort Alert [1:10005:0]	2013-01-11 20:49:33	172.16.8.93:3128	172.16.9.14:49917	TCP
#33-(1-74)	[snort] http_inspect: IIS UNICODE CODEPOINT ENCODING	2013-01-11 20:44:37	172.16.9.49:1851	172.16.8.103:80	TCP

Resumen de Alertas por tipo de ataque

Basic Analysis and Security Engine (BASE)

Inicio | Buscar | Preferencias | Logout

[Atrás]

Añadido 4 alerta(s) al escondrijo de alertas

Consultado en : Fri January 11, 2013 20:53:12

Meta Criterio	*any*
Criterio IP	*any*
Layer 4 Criteria	*none*
Criterio Carga	*any*

Mostrando alertas 1-6 de 6 en total

< Clasificación >	< Total # >	< Sensor # >	< Firma >	< Dirección Origen >	< Dirección Dest >	< First >	< Ultimo >
desclasificado	4387 (52%)	1	8	19	25	2013-01-11 20:21:00	2013-01-12 01:53:09
non-standard-protocol	679 (8%)	1	1	18	20	2013-01-11 20:20:24	2013-01-12 01:51:57
trojan-activity	1 (0%)	1	1	1	1	2013-01-11 22:06:51	2013-01-11 22:06:51
attempted-recon	11 (0%)	1	2	1	3	2013-01-11 22:45:11	2013-01-12 00:38:48
misc-activity	3303 (39%)	1	2	1	3	2013-01-11 22:45:15	2013-01-12 01:50:35
attempted-dos	6 (0%)	1	4	1	1	2013-01-12 00:10:33	2013-01-12 01:13:14

4.6 PUESTA EN MARCHA DE SNORT IDS

- **Ejecutar Snort IDS:**

snort –i br0 –c /etc/snort/snort.conf

- **Ejecutar Barnyard:**

/usr/local/bin/barnyard -c /etc/snort/barnyard.conf -d /var/log/snort/ -f snort.log -w /var/log/snort/barnyard.waldo

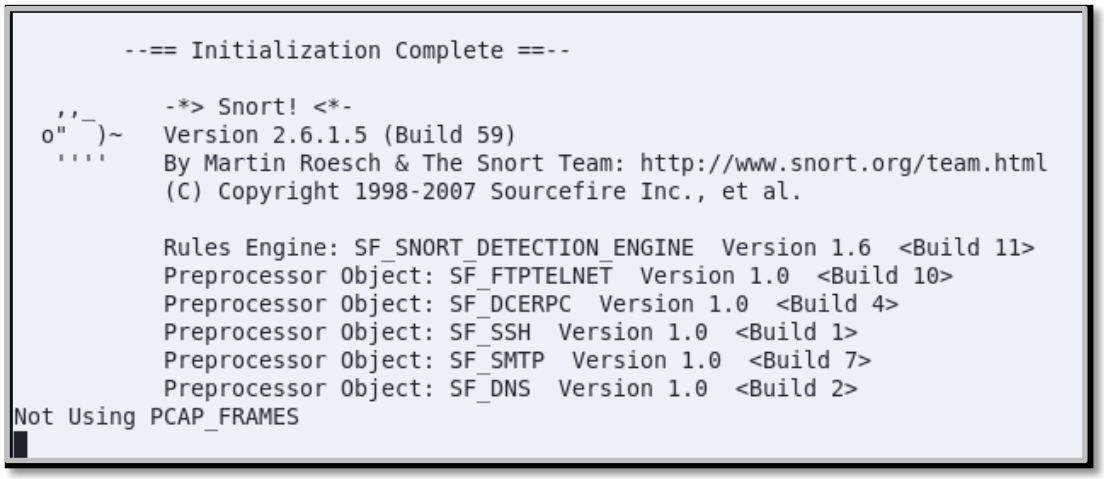


Figura 4. 11: Ejecución Snort modo IDS

Referencia: Fuente propia-software Snort

4.7 PUESTA EN MARCHA DE SNORT INLINE

- **Cargar módulo ip_queue:**

Necesario para enviar los paquetes a cola para su respectivo análisis por parte de Snort Inline.

modprobe ip_queue

- **Configurar iptables;**

Para señalar los paquetes que se desea enviar al user space, marcándolos con el módulo QUEUE.

iptables -A INPUT -j QUEUE

- **Ejecutar Snort Inline:**

snort_inline -Q -v -c /etc/snort_inline/snort_inline.conf -l /var/log/snort_inline/

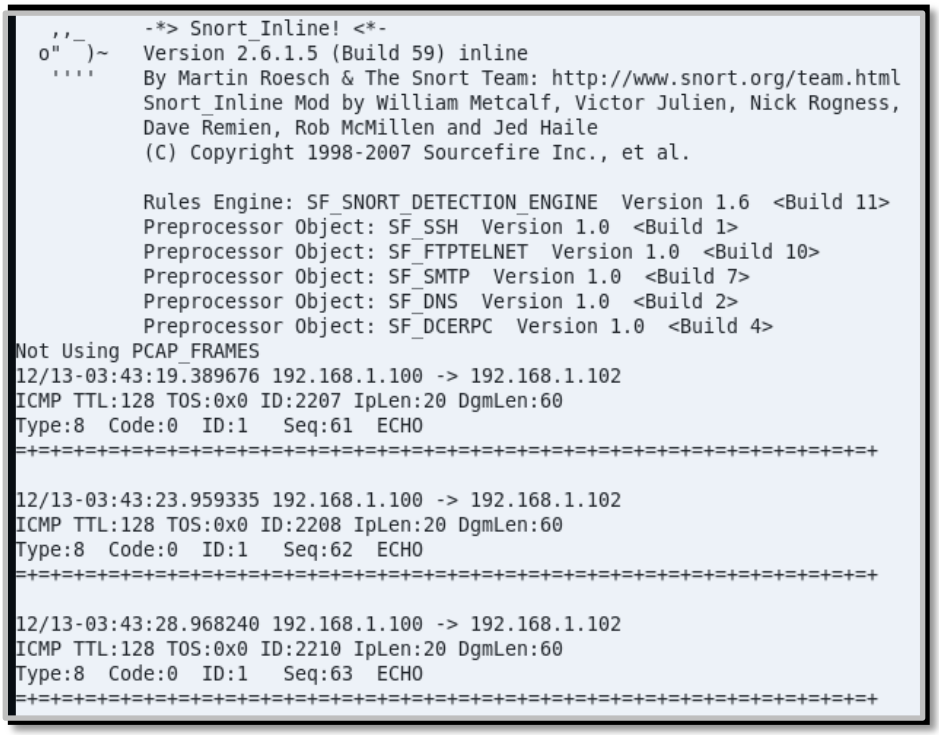


Figura 4. 12: Ejecución Snort modo IPS

Referencia: Fuente propia-software Snort Inline

CAPÍTULO V

5. IMPLEMENTACIÓN Y PRUEBAS

En este capítulo se muestran los resultados de las pruebas de funcionamiento, posteriores a la implementación del IDS/IPS en la red administrativa, con el fin de observar y comprobar su correcto desempeño. Para lo cual, se propone efectuar la simulación de determinados ataques informáticos y el establecimiento de un conjunto de reglas para filtrado de tráfico específico, acorde a ciertas políticas de seguridad establecidas anteriormente.

5.1 SIMULACIÓN DE ATAQUES INFORMÁTICOS

A continuación se señalan los tipos de ataques informáticos que van a ser generados en las pruebas planteadas, los cuales corresponden a aquellos ataques más comunes, dentro del entorno de la seguridad de la información, según el extracto recuperado de https://sites.google.com/site/sykrayolab/ataques-informaticos, entre ellos: ataques por DoS, suplantación de identidad, fuerza bruta y detección de vulnerabilidades. Además se señalan las distintas técnicas y herramientas utilizadas para su ejecución dentro de la red municipal.

5.1.1 DETECCIÓN DE VULNERABILIDADES

El atacante inicialmente busca adueñarse de datos informativos de la organización (números telefónicos, direcciones, información del personal), ya sea utilizando herramientas básicas como servidores whois[24] o de ingeniería social. Sin embargo, también requerirá

[24] **Whois:** Es una base de datos de Internet que contiene información acerca de una IP, de un dominio o de una organización.

identificar aquellas debilidades presentes en el sistema (puertos abiertos, hosts vivos, servicios activos, entre otros.) que le permitan ejecutar ataques más complejos y dañinos.

De esta manera se ha optado por simular la técnica de escaneo de puertos con la herramienta Nmap, tanto para plataformas Windows (Nmap 6.00) y Linux (Zenmap de Back Track[25]), cuya principal función es la identificación de puertos abiertos, que estén a la espera de nuevas conexiones, permitidas o no.

Nmap permite llevar a cabo de forma relativamente sencilla varios tipos de scanning de puertos, entre los que destacan:

- **Escaneo por defecto:** Brinda un reporte acerca del estado de los puertos, servicios encontrados o el estado de la máquina. Se lo realiza a través del comando:

nmap ‹*IP host objetivo*›

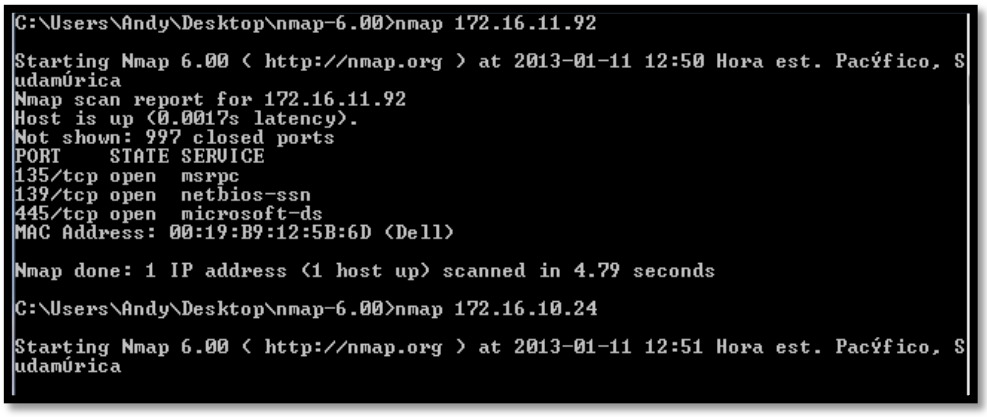


Figura 5. 1: Comando de ejecución escaneo por defecto

Referencia: Fuente propia-software Nmap

---

[25] **Back Track:** Es una de las distribuciones de mayor aceptación por parte de profesionales de seguridad informática, diseñada con una amplia gama de herramientas para la realización de test de penetración, auditorias de seguridad, análisis forense, etc.

En la figura 5.2 se muestra el despliegue de la alerta en la consola de Snort:

```
[**] [122:1:0] (portscan) TCP Portscan [**] {PROTO255} 172.16.9.14 -> 172.16.11.92
[**] [122:1:0] (portscan) TCP Portscan [**] {PROTO255} 172.16.9.14 -> 172.16.11.92
[**] [122:1:0] (portscan) TCP Portscan [**] {PROTO255} 172.16.9.14 -> 172.16.11.92
```

Figura 5. 2: Alerta generada por Snort (Escaneo básico)

Referencia: Fuente propia-software Snort

- **Escaneo TCP SYN:** Envía un paquete SYN. Si la respuesta es un paquete SYN/ACK, el puerto está abierto, mientras que si es un RST, se encuentra cerrado. TCP SYN scan se ejecuta a través del siguiente comando:

```
nmap –sS –O ‹IP host objetivo›
```

Se despliega la siguiente alerta:

```
SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 172.16.9.14:57154 -> 172.16.11.92
SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 172.16.9.14:57154 -> 172.16.11.92
SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 172.16.9.14:57154 -> 172.16.11.92
```

Figura 5. 3: Alerta generada por Snort (Escaneo TCP SYN)

Referencia: Fuente propia-software Snort

- **Escaneo TCP FIN:** Considerado como uno de los escáner nmap más silencioso, el cual se apoya también en el establecimiento de una conexión TCP/IP, al enviar paquetes FIN. Si se obtiene como respuesta un paquete RST, se concluye que el puerto está cerrado y al no recibir respuesta (se ignora paquete FIN), se determina que el puerto puede encontrarse abierto o silencioso. Esta técnica se ejecuta mediante el comando:

```
nmap –sF –O ‹IP host objetivo›
```

En la figura siguiente, indica el despliegue de la alerta en la consola de Snort:

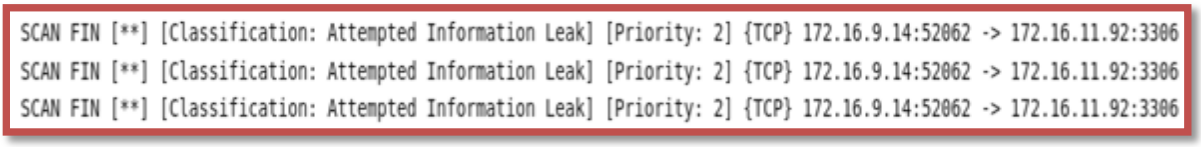


Figura 5. 4: Alerta generada por Snort (Escaneo TCP FIN)

Referencia: Fuente propia-software Snort

Otros tipos de escaneos:

- **UDP**: nmap –sU –O ***‹IP host objetivo›*** (Escanea servicios UDP).
- **Ping**: nmap –sP –O ***‹IP host objetivo›*** (Identifica host activos).

Como se observa el monitoreo de cada una de éstas conexiones no legítimas, lo puede realizar Snort a través del preprocesador *Sfportscan*, el cual es capaz de identificar diferentes tipos de escáneres (TCP, UDP, IP), o a su vez, mediante las reglas creadas previamente en su directorio rules, con el objetivo de producir alertas específicas por cada evento.

"Los preprocesadores no están basados en reglas, son programas autónomos, cada uno con su propia configuración, realizando cada uno una tarea independiente, pero funcionando en conjunto para ofrecer a Snort una visión simplificada del tráfico supervisado". (Recuperado de: http: //e-archivo.uc3m.es/bitstream/10016/11213/1/PFC_Hugo_Gascon_Polanco.pdf.)

5.1.2 ATAQUE POR SUPLANTACIÓN (SPOOFING)

Generalmente se produce cuando el atacante se hace pasar por un host conocido, simulando su identidad para conseguir acceso a los recursos del sistema, al aprovechar algún tipo de confianza basada en el nombre de dominio o dirección IP del host suplantado. El Capítulo I expone las diversas técnicas de Spoofing de acuerdo a la tecnología en la que se basan: IP Spoofing, DNS Spoofing, ARP[26] Spoofing, entre otros.

Se ha seleccionado la técnica de ARP Spoofing, con la cual el atacante intenta asociar su dirección MAC con la dirección IP del host víctima y su gateway, de modo que cualquier tráfico enviado a dicha víctima, sea erróneamente dirigido hacia el atacante. La simulación del ataque se lo efectúa empleando la herramienta Ettercap que está por defecto en Back Track. Ettercap es un potente sniffer multipropósito diseñado para realizar ataques Man in the Middle (Hombre en Medio), dado que sitúa al atacante en medio del tráfico, pudiendo éste solo escucharlo (interactuación pasiva) o modificarlo (interceptación activa), previo su reenvío al host original.

La figura siguiente muestra el comando de ejecución del ataque, ingresando simplemente las direcciones IP del gateway de la red y de la PC objetivo.

[26] **ARP (Address Resolution Protocol)**: Protocolo que permite averiguar la dirección física MAC de un host determinado, partiendo de su dirección lógica IP.

Figura 5. 5: Comando ejecución Ettercap

Referencia: Fuente propia-software Back Track 5

Cabe destacar que el proceso que cumple ARP Spoofing, para falsear la tabla ARP de su víctima, se lo puede analizar mediante el sniffer Wireshark[27], como muestra la figura 5.6, el cual ha sido desarrollado en una red doméstica para facilitar su observación.

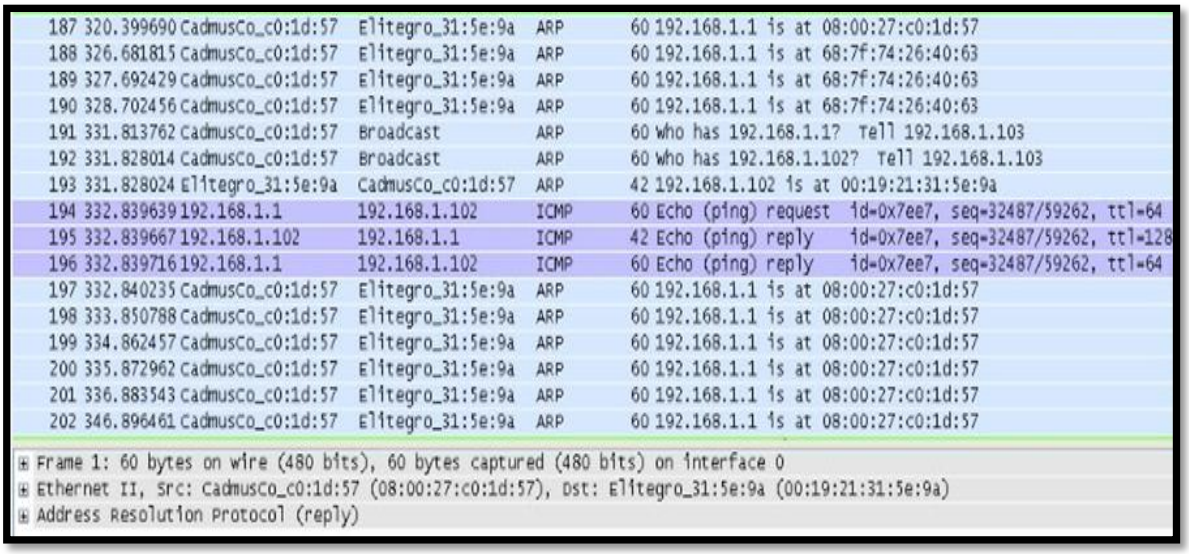


Figura 5. 6: Análisis del Ataque ARP Spoofing

Referencia: Fuente propia-software Wireshark

[27] **Wireshark**: Sniffer que permite capturar tramas y paquetes que pasan a través de una interfaz de red. Además cuenta con todas las características estándar de un analizador de protocolos.

- **Paquetes 191 y 192:** El atacante con IP 192.168.1.103 y MAC (08:00:27:c0:1d:57), ha lanzado un *ARP request* a la dirección broadcast preguntando por la MAC de las IP 192.168.1.1 (gateway de la red-objetivo) y la IP 192.168.1.102 (PC-objetivo).

- **Paquete 193:** Acto seguido, el router contesta con un *ARP reply* indicando cuál es la dirección MAC de la PC-objetivo, es decir la (00:19:21:31:5e:9a). De este modo el atacante con la IP 192.168.1.103, ya tiene la MAC de la PC-objetivo, con lo cual ya puede compartir tráfico Ethernet.

- El problema viene a partir del paquete 197, donde la máquina atacante envía reiteradamente a la PC-objetivo y al router, paquetes *ARP reply* falsos, asociando la IP del router con su propia MAC (08:00:27:c0:1d:57). De esta forma, todo el tráfico que transite entre el gateway de la LAN y la PC-objetivo pasará a través de la máquina atacante.

Como respuesta a este tipo de ataque, Snort dispone de un preprocesador denominado *Arpspoof,* el cual valida la relación entre la dirección IP del gateway de la red en este caso la 172.16.8.160 y su dirección MAC 00:0D:88:F5:B1:12, de modo que cuando exista un intento de suplantación se despliegue la siguiente alerta:

Figura 5. 7: Alerta generada por Snort (Ataque ARP Spoofing)

Referencia: Fuente propia-software Snort

5.1.3 ATAQUE POR FUERZA BRUTA

Es el procedimiento ilícito mediante el cual se obtienen las claves o códigos necesarios para acceder a un equipo, sistema, sitio web, etc., a través de la generación de posibles combinaciones de caracteres provenientes de diccionarios de palabras previamente definidos, que han de ser probados hasta la obtención de la combinación idónea.

Esta técnica explota las vulnerabilidades del factor humano, el cual hace uso de claves y códigos poco robustos, con un mínimo número de caracteres y/o poca variedad en los mismos, facilitando las labores de los atacantes al momento de descifrarlos.

Se ha optado por utilizar la técnica de ataque por fuerza bruta con diccionario, utilizando la herramienta Medusa dentro de Back Track, en contra del servicio ssh de la víctima. Para lo cual se deberá primero comprobar si el puerto 22 (ssh) está presto a aceptar conexiones, caso contrario no se completará la conexión. Se hará uso nuevamente de Nmap mediante la siguiente línea de comando:

nmap –p 22 ‹*IP host objetivo*›

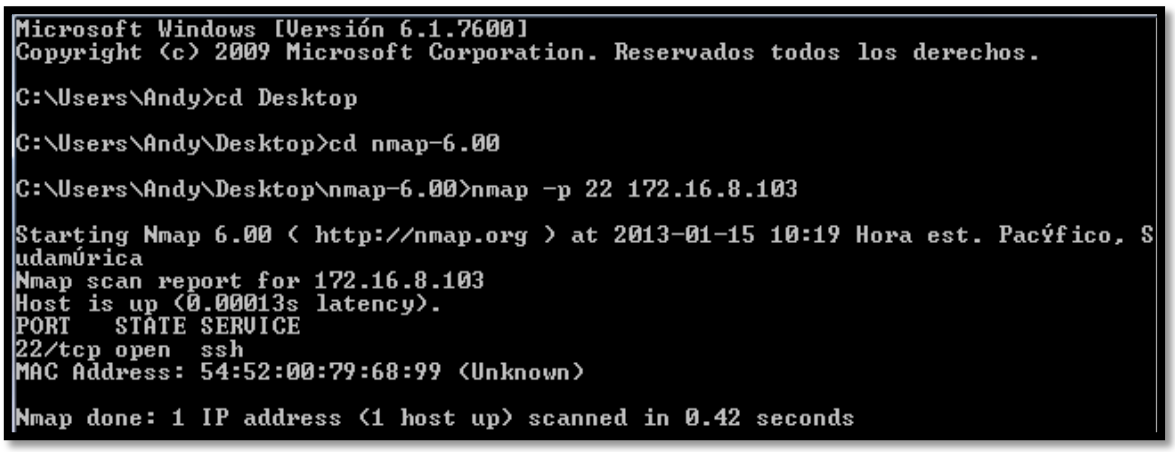


Figura 5. 8: Comando ejecución escaneo al puerto 22

Referencia: Fuente propia-software Nmap

Luego de comprobar que el puerto 22 está abierto, se lleva a cabo la simulación del ataque con medusa, utilizando el diccionario John the Ripper, de la siguiente manera:

Figura 5. 9: Comando ejecución Medusa

Referencia: Fuente propia-software Back Track 5

Como respuesta a este tipo de ataque, el IDS/IPS despliega la siguiente alerta, que corresponde a una regla cargada:

Figura 5. 10: Alerta generada por Snort (Ataque Fuerza Bruta)

Referencia: Fuente propia-software Snort

5.1.4 ATAQUE DE DENEGACIÓN DEL SERVICIO

Como su nombre bien lo señala, estos ataques intentan imposibilitar el acceso normal a los servicios y recursos de una organización durante un tiempo indefinido. Los ataques DoS hacen uso de ciertas estrategias como las que se mencionan a continuación:

- Denegaciones del servicio por inundación, saturando un equipo con solicitudes para que no pueda responder a las peticiones reales.

- Denegaciones de servicio por explotación de vulnerabilidades, que aprovechan una vulnerabilidad en el sistema para volverlo inestable.

Se ha hecho uso de la técnica de Denegación del Servicio por Inundación o Flooding, la misma que consiste en bombardear un sistema mediante un flujo continuo de tráfico, que acaba por consumir todos los recursos del mismo y el ancho de banda de la red atacada. Utilizan diversos mecanismos tomando en cuenta el protocolo involucrado en la ejecución del ataque, entre los que destacan:

- **SYN Flood:** Consiste en el envío simultaneo de banderas TCP/SYN, de modo que la víctima intente reiteradamente establecer una conexión a cada una de estas peticiones, respondiendo con paquetes TCP/SYN ACK y esperando por la respuesta TCP/ACK.

  Estos intentos de conexión consumen recursos en el equipo de la víctima y copan el número de conexiones que se pueden establecer, reduciendo la posibilidad de responder peticiones legítimas de conexión.

- **ICMP y UDP Flood:** Persiguen los mismos objetivos de un ataque por inundación, pero haciendo uso de tráfico con paquetes ICMP Echo Request y UDP respectivamente.

En este sentido se ha seleccionado la herramienta Hping3 de Back Track, para generar este tipo de ataques, por su capacidad de originar flujos de paquetes del tipo TCP, ICMP y UDP, ocultando la dirección IP real del atacante.

Las figuras 5.11 y 5.12 muestran los resultados tras la ejecución de un Ataque SYN Flood con IP falsa (192.168.1.1):

Figura 5. 11: Comando ejecución hping3 (Ataque SYN Flood con IP falsa)

Referencia: Fuente propia-software Back Track 5

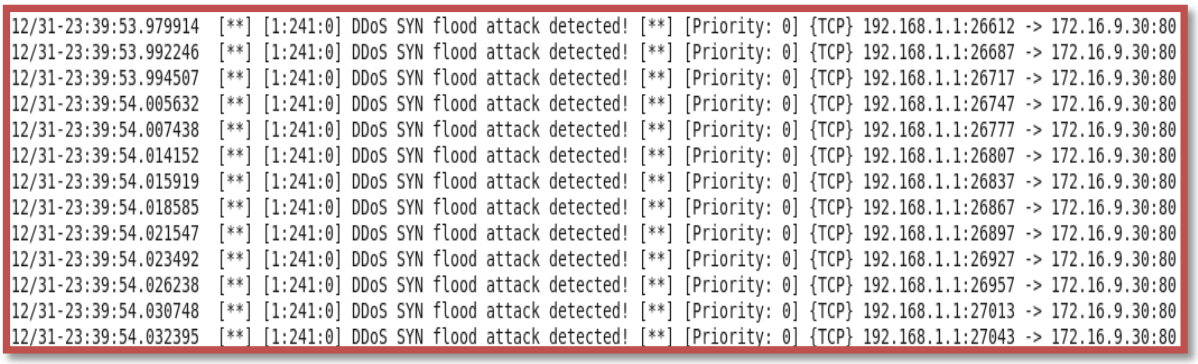


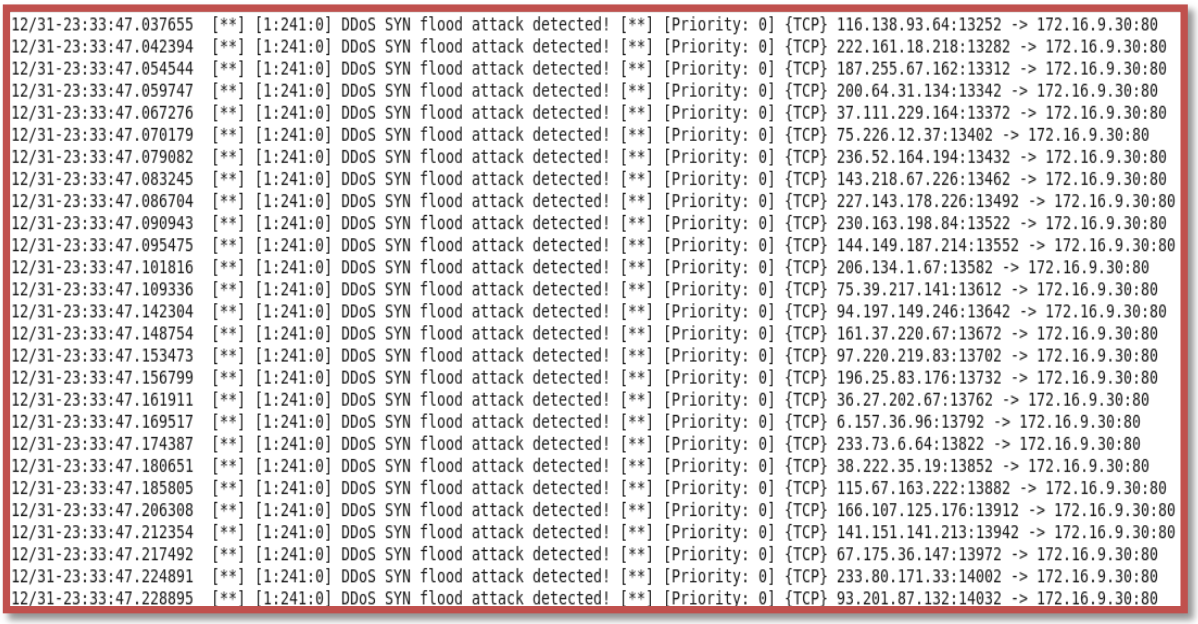
Figura 5. 12: Alerta generada por Snort (Ataque SYN Flood con IP falsa)

Referencia: Fuente propia-software Snort

Así mismo, Las figuras 5.13 y 5.14 exponen los resultados tras lanzar un Ataque SYN Flood con IP aleatoria (random):

Figura 5. 13: Comando ejecución hping3 (Ataque SYN Flood con IP aleatoria)

Referencia: Fuente propia-software Back Track 5



```
12/31-23:33:47.037655  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 116.138.93.64:13252 -> 172.16.9.30:80
12/31-23:33:47.042394  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 222.161.18.218:13282 -> 172.16.9.30:80
12/31-23:33:47.054544  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 187.255.67.162:13312 -> 172.16.9.30:80
12/31-23:33:47.059747  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 200.64.31.134:13342 -> 172.16.9.30:80
12/31-23:33:47.067276  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 37.111.229.164:13372 -> 172.16.9.30:80
12/31-23:33:47.070179  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 75.226.12.37:13402 -> 172.16.9.30:80
12/31-23:33:47.079082  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 236.52.164.194:13432 -> 172.16.9.30:80
12/31-23:33:47.083245  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 143.218.67.226:13462 -> 172.16.9.30:80
12/31-23:33:47.086704  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 227.143.178.226:13492 -> 172.16.9.30:80
12/31-23:33:47.090943  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 230.163.198.84:13522 -> 172.16.9.30:80
12/31-23:33:47.095475  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 144.149.187.214:13552 -> 172.16.9.30:80
12/31-23:33:47.101816  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 206.134.1.67:13582 -> 172.16.9.30:80
12/31-23:33:47.109336  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 75.39.217.141:13612 -> 172.16.9.30:80
12/31-23:33:47.142304  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 94.197.149.246:13642 -> 172.16.9.30:80
12/31-23:33:47.148754  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 161.37.220.67:13672 -> 172.16.9.30:80
12/31-23:33:47.153473  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 97.220.219.83:13702 -> 172.16.9.30:80
12/31-23:33:47.156799  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 196.25.83.176:13732 -> 172.16.9.30:80
12/31-23:33:47.161911  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 36.27.202.67:13762 -> 172.16.9.30:80
12/31-23:33:47.169517  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 6.157.36.96:13792 -> 172.16.9.30:80
12/31-23:33:47.174387  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 233.73.6.64:13822 -> 172.16.9.30:80
12/31-23:33:47.180651  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 38.222.35.19:13852 -> 172.16.9.30:80
12/31-23:33:47.185805  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 115.67.163.222:13882 -> 172.16.9.30:80
12/31-23:33:47.206308  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 166.107.125.176:13912 -> 172.16.9.30:80
12/31-23:33:47.212354  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 141.151.141.213:13942 -> 172.16.9.30:80
12/31-23:33:47.217492  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 67.175.36.147:13972 -> 172.16.9.30:80
12/31-23:33:47.224891  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 233.80.171.33:14002 -> 172.16.9.30:80
12/31-23:33:47.228895  [**] [1:241:0] DDoS SYN flood attack detected! [**] [Priority: 0] {TCP} 93.201.87.132:14032 -> 172.16.9.30:80
```

Figura 5. 14: Alerta generada por Snort (Ataque SYN Flood con IP aleatoria)

Referencia: Fuente propia-software Snort

También es posible generar ataques del tipo ICMP Flood y UDP Flood respectivamente, a través de los comandos siguientes:

```
hping3 ‹IP host objetivo› -a ‹IP atacante falsa› -1 - -destport 80 - -flood - -debug

hping3 ‹IP host objetivo› --rand-source -1 - -destport 80 - -flood - -debug
```

```
hping3 ‹IP host objetivo› -a ‹IP atacante falsa› -2 –destport 80 –flood –debug

hping3 ‹IP host objetivo› --rand-source -2 - -destport 80 - -flood - -debug
```

Estas herramientas de ataque hoy en día, son cada vez más accesibles y su lanzamiento involucra la menor complejidad posible. Tal es el caso del software LOIC (Low Orbit Ion Cannon) que corre sobre plataforma Windows, capaz de desplegar ataques por inundación

tanto a sitios web como a direcciones IP específicas de forma relativamente sencilla. Como se indica en la figura siguiente:

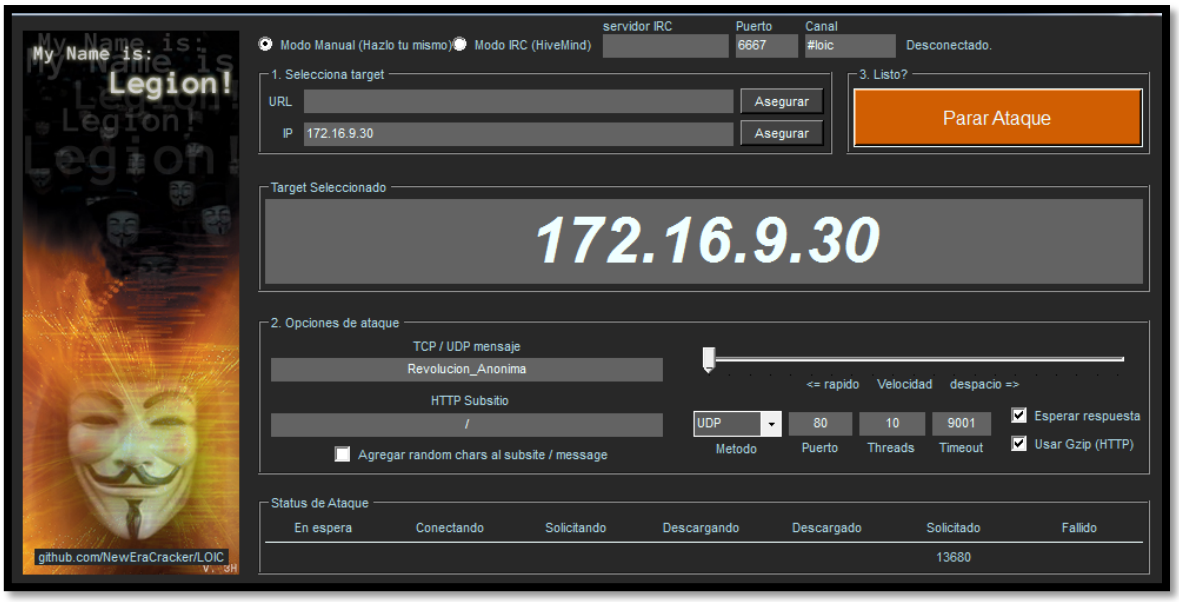


Figura 5. 15: Ejecución LOIC (Ataque UDP Flood)

Referencia: Fuente propia-software Back Track 5

A continuación, se despliega la alerta de Snort, donde se señala que el software LOIC en modo UDP, ha sido lanzado en contra de una PC perteneciente a la red que gobierna el IDS/IPS:

```
3] {UDP} 172.16.9.14:62502 -> 172.16.9.30:80
01/11-20:45:25.003744  [**] [1:19318:1] SLR - LOIC DoS Tool (UDP Mode)  - Behavior Rule (tracking/threshold) [**] [Classification: Misc activity] [Priority:
3] {UDP} 172.16.9.14:62503 -> 172.16.9.30:80
01/11-20:45:25.013775  [**] [1:19318:1] SLR - LOIC DoS Tool (UDP Mode)  - Behavior Rule (tracking/threshold) [**] [Classification: Misc activity] [Priority:
3] {UDP} 172.16.9.14:62505 -> 172.16.9.30:80
01/11-20:45:25.023738  [**] [1:19318:1] SLR - LOIC DoS Tool (UDP Mode)  - Behavior Rule (tracking/threshold) [**] [Classification: Misc activity] [Priority:
3] {UDP} 172.16.9.14:62504 -> 172.16.9.30:80
01/11-20:45:25.033792  [**] [1:19318:1] SLR - LOIC DoS Tool (UDP Mode)  - Behavior Rule (tracking/threshold) [**] [Classification: Misc activity] [Priority:
3] {UDP} 172.16.9.14:62503 -> 172.16.9.30:80
01/11-20:45:25.043842  [**] [1:19318:1] SLR - LOIC DoS Tool (UDP Mode)  - Behavior Rule (tracking/threshold) [**] [Classification: Misc activity] [Priority:
3] {UDP} 172.16.9.14:62503 -> 172.16.9.30:80
01/11-20:45:25.053749  [**] [1:19318:1] SLR - LOIC DoS Tool (UDP Mode)  - Behavior Rule (tracking/threshold) [**] [Classification: Misc activity] [Priority:
3] {UDP} 172.16.9.14:62503 -> 172.16.9.30:80
01/11-20:45:25.063853  [**] [1:19318:1] SLR - LOIC DoS Tool (UDP Mode)  - Behavior Rule (tracking/threshold) [**] [Classification: Misc activity] [Priority:
3] {UDP} 172.16.9.14:62503 -> 172.16.9.30:80
```

Figura 5. 16: Alerta generada por Snort (Ataque UDP Flood con LOIC)

Referencia: Fuente propia-software Snort

5.2 REGLAS EN BASE A POLÍTICAS PLANTEADAS

Como se mencionó en capítulos anteriores, el paquete Snort Inline efectúa funciones de un sistema de prevención de intrusos real, filtrando el tráfico entrante o saliente de forma inteligente y en base a las necesidades o requerimientos del administrador.

Precisamente, se emplea esta herramienta para introducir un conjunto de reglas "drop", que aporten en las tareas de depuración del tráfico circulante en la red municipal, pero en base a las condiciones o restricciones descritas en las políticas de seguridad de la información propuestas.

A continuación se exponen las políticas escogidas y las estrategias empleadas para alcanzar sus propósitos:

	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN GAD IBARRA**	
	Dominio:	3. Seguridad ligada a los Recursos Humanos
	Control:	3.2 Durante el empleo
Artículo 16. El usuario es responsable de respetar la ley de derechos de autor, no abusando de este medio para inspeccionar, copiar y almacenar software o información sin conocimiento del autor.		

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN GAD IBARRA	
	Dominio:	5. Gestión de Comunicaciones y Operaciones
	Control:	5.3 Protección contra el código malicioso y descargable

Artículo 42. Se adquirirá y utilizará software únicamente de fuentes confiables.

Artículo 48. Ningún usuario podrá descargar e instalar aplicaciones provenientes de sitios no confiables a partir redes de comunicaciones externas, sin la previa autorización de la Dirección de TIC.

Estrategia: Evitar la descarga de contenidos maliciosos o aquellos protegidos por derechos de autor y que puedan conducir a la vulneración de las leyes de propiedad intelectual, los mismos que a su vez generan carga innecesaria de tráfico en la red. Para ello se propone bloquear archivos con extensiones .exe, .mp3, mp4, entre otros.

A continuación se expone el evento generado por la consola de Snort Inline, indicando que se está bloqueando la descarga de un archivo P2P, además brinda información acerca de la dirección IP del usuario infractor y el puerto utilizado:

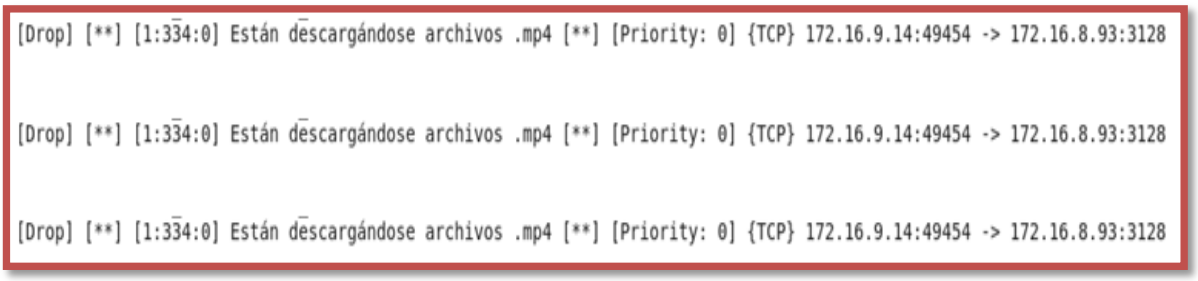


Figura 5. 17: Evento generado por Snort Inline (Debido a la descarga de archivos P2P)

Referencia: Fuente propia-software Snort Inline

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN GAD IBARRA	
	Dominio:	6.Control de Acceso
	Control:	6.2 Responsabilidades del usuario

Artículo 83. Los usuarios del GAD Ibarra, provistos de acceso a Internet, al aceptar este servicio están aceptando que:

- Saben que existe la prohibición al acceso de páginas no autorizadas.
- La utilización de Internet es para el desempeño de su función y puesto dentro de la entidad y no para propósitos personales.

Estrategia: Bloquear la navegación a determinados sitios web, que por política institucional no serán accesibles desde los puestos de trabajo, en horas laborables, como por ejemplo los sitios: facebook, youtube, yahoo, entre otros.

El evento generado por la consola de Snort Inline, confirma el intento de un usuario por acceder a sitios prohibidos:

```
[Drop] [**] [1:1002:0] Bloquear facebook [**] [Priority: 0] {TCP} 172.16.9.14:45116 -> 172.16.8.93:3128
[Drop] [**] [1:1002:0] Bloquear facebook [**] [Priority: 0] {TCP} 172.16.9.14:45116 -> 172.16.8.93:3128
[Drop] [**] [1:1002:0] Bloquear facebook [**] [Priority: 0] {TCP} 172.16.9.14:45116 -> 172.16.8.93:3128
```

Figura 5. 18: Evento generado por Snort Inline (Debido al acceso a páginas prohibidas)

Referencia: Fuente propia-software Snort Inline

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN GAD IBARRA	
	Dominio:	5. Gestión de Comunicaciones y Operaciones
	Control:	5.1Responsabilidades y procedimientos de operaciones

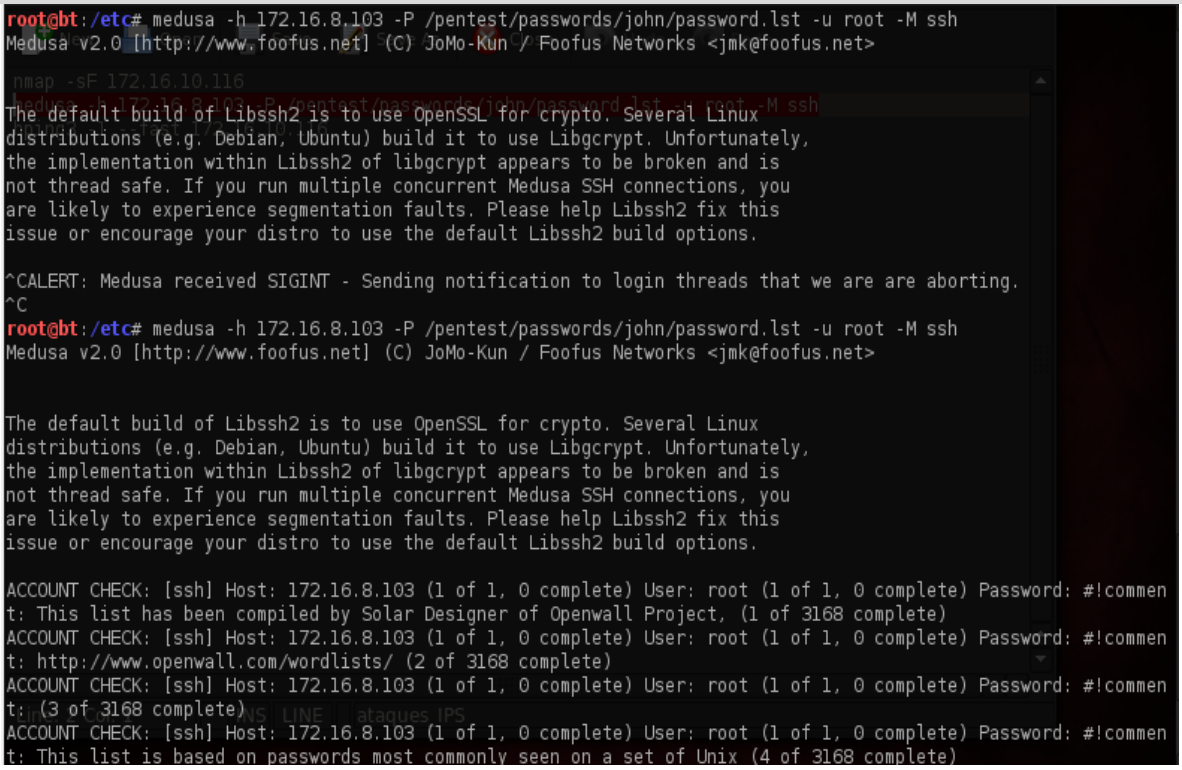
Artículo 37. La Dirección de TIC, es responsable absoluto de mantener el sistema de información en óptimo funcionamiento, fomentando una cultura de administración segura y servicios óptimos.

Estrategia: Garantizar la seguridad del sistema de información y sus componentes, a través del bloqueo o monitoreo de determinados tipos de ataques informáticos, mediante la herramienta Snort Inline, que compone el servidor IDS/IPS propuesto.

A continuación, se exhiben los resultados correspondientes al bloqueo del ataque por fuerza bruta con diccionario, demostrando que el mismo no tuvo éxito o no completó efectivamente su ataque tras la activación de Snort Inline como mecanismo preventivo, así mismo, se exponen los eventos generados en la consola de visualización posteriores a su identificación.

- **Ataque por Diccionario (Fuerza Bruta)**

IPS desactivado



IPS activado

Figura 5. 19: Ejecución Ataque Medusa con IPS activado/desactivado

Referencia: Fuente propia-software Back Track 5

Con el IPS activo, no se puede completar el ataque luego de tres primeros intentos y aparece el puerto 22 como cerrado, evitando de esta forma un ataque por ssh.

Figura 5. 20: Evento generado por Snort Inline (Bloqueo ataque Medusa)

Referencia: Fuente propia-software Snort Inline

Previa la implementación de las medidas técnicas propuestas, la red municipal ofrecía un entorno propicio para la ejecución de ataques internos, los cuales fueron descubiertos a lo largo del proceso de pruebas, y que en su mayoría tuvieron éxito sin dejar huellas o evidencias por analizar, además se comprobó la existencia de herramientas de fácil acceso, cuya ejecución no requería de un elevado nivel de conocimiento y esfuerzo, como son: LOIC (Low Orbit Ion Cannon) y Nmap-6.00 para Windows.

A través de la activación de los mecanismos de detección y prevención propuestos, se ha logrado captar en tiempo real la ejecución de un ataque, identificar su origen y tipo, pero sobre todo, lograr su bloqueo. También es importante señalar el aporte que brindan las medidas organizativas, las cuales buscan encauzar al usuario hacia el uso responsable de los recursos informáticos. En definitiva, la suma de todas las medidas aplicadas intentan ubicar al atacante en un ambiente mucho más hostil.

CAPÍTULO VI

6. CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- Se obtuvo una metodología de seguridad informática integral, cuyo plan para la protección de los recursos del sistema se basa en la combinación de medidas técnicas y administrativas, concebidas mediante la ejecución del IDS/IPS y la elaboración del Manual de Políticas y Procedimientos.

- La unión de las herramientas IDS e IPS en el servidor propuesto, brinda mayores alternativas para contrarrestar intrusiones inesperadas en la red, al juntar la capacidad de monitoreo constante de Snort y un filtrado de tráfico basado en políticas a través de Snort Inline. Sin embargo, esto también conlleva al aumento de las características del hardware del servidor, con el fin de mantener las capacidades de procesamiento en niveles normales, al requerirse un doble análisis de paquetes.

- La integración IDS/IPS identificó satisfactoriamente los ataques simulados con la herramienta Back Track, la cual es ampliamente utilizada para pentesting (pruebas de penetración) en redes, comprobando su eficiencia frente a una serie de pruebas con diversas técnicas.

- El IDS al contrario del firewall, hace un monitoreo de la red en búsqueda de intrusiones de forma inteligente, basándose en el contenido mismo de los paquetes y

no únicamente relacionando el puerto/protocolo de la comunicación. El IPS a su vez, añade la posibilidad de tomar acciones sobre los paquetes monitoreados, como su bloqueo por ejemplo.

- Snort es una herramienta poderosa de detección de intrusos, sin embargo, requiere pruebas previas donde se seleccione un conjunto de reglas acordes al entorno donde va a ejecutar sus funciones, con el objeto de eliminar los falsos positivos y malas interpretaciones de alertas.

- A través de MAGERIT se concluyó que los valores de riesgo alto, son generados por amenazas relacionadas a errores intencionados o no intencionados por parte del usuario, comprobando una tendencia que señala una probabilidad mayor de sufrir ataques de tipo interno antes que externo. De esta manera es imprescindible que se dé con el cumplimiento de las políticas del manual propuesto, para orientar al usuario hacia el uso adecuado y responsable de los recursos.

- El Análisis de Riesgos en los activos del GAD Ibarra adicionalmente arrojó como resultado, un grupo de activos críticos, es decir aquellos que son más propensos a sufrir problemas de seguridad, o a su vez, aquellos cuyo daño o indisponibilidad supondría grandes pérdidas para la entidad (ver ANEXO 5). De este modo se ha definido responsables para cada uno de ellos, los mismos que velarán por la salvaguarda y control de los mismos, siguiendo los estamentos de las políticas de seguridad planteadas.

- Los servicios críticos identificados con el uso de MAGERIT, fueron tomados en cuenta para el desarrollo de los procedimientos correspondientes al Mantenimiento Correctivo de Equipos y el Respaldo de Información por Parte del Usuario. En el primer caso, con la finalidad de dar prioridad de atención a aquellos usuarios que están relacionados directamente con la prestación de estos servicios altamente valorados y en el segundo, con el objetivo asegurar que la información que generan dichos servicios sea respaldada oportunamente.

- Es una solución de seguridad informática de bajo costo, al ser íntegramente basado en freeware y compuesto de recursos mínimos de hardware, recomendable para redes con presupuestos limitados. De esta manera, puede replicarse este proyecto en redes pequeñas anexas a la entidad, como aquellas ubicadas en las juntas parroquiales, establecimientos educativos, bibliotecas, infocentros, etc.

6.2 RECOMENDACIONES

- Es importante tomar como referencia a aquellas metodologías, normas o guías reconocidas, para al desarrollo de procesos importantes como el Análisis de Riesgos, o el desarrollo de las Políticas de Seguridad, evitando así errores de estructura, mal manejo de términos o el incumplimiento de estándares a nivel mundial.

- El proceso de valoración de los activos y amenazas del sistema de información, correspondiente a una de las tareas de la Metodología MAGERIT, deben ser llevadas a cabo con plena coordinación y colaboración por parte del personal que labora en el

Departamento de Tecnologías de la institución, quienes están capacitados para dar un veredicto en base a su experiencia y conocimiento.

- Es recomendable efectuar un proceso de inducción al personal, sobre las actividades que deben cumplirse en los Procedimientos propuestos, de modo que se evite el desacato, conflictos y discrepancias de los mismos.

- Es necesario contar con un servidor de buenas características de hardware, necesarias para evitar cuellos de botella al momento de ubicarse en medio del tráfico.

- Se debe disminuir el consumo de recursos del servidor, ya sea deshabilitando procesos innecesarios, evitando manejar el entorno gráfico del sistema operativo o disminuyendo el número de firmas de Snort.

- Al momento de adquirir las tarjetas de red, es recomendable conocer la compatibilidad de sus drivers con el kernel del sistema operativo anfitrión, de modo que sean reconocidas automáticamente, evitando conflictos y pérdidas de tráfico posteriores a su instalación. Todo ello con el objetivo de evadir procedimientos de solución tediosos, como la compilación de un nuevo kernel por ejemplo.

- Verificar si el procesador del servidor trabaja a la velocidad real, mediante el comando *pgrep -lf ondemand.*, de forma que se aproveche fielmente sus características, caso contrario realizar las correcciones necesarias para evitar problemas por falta de recursos.

- Deshabilitar el firewall por defecto de CentOS y la opción SE Linux (seguridad avanzada), para evitar conflictos al momento de configurar la cadena iptables con el módulo QUEUE.

- Es recomendable usar varios sensores IDS en distintos tramos de la red, para monitorearla en su totalidad, preferentemente analizando una réplica del tráfico real, de modo que se produzca el menor impacto posible sobre la red.

REFERENCIAS BIBLIOGRÁFICAS

Areitio, J. (2009). *Seguridad de la información: redes, informática y sistemas de información*. Recuperado de: http://www.kilibro.com/book/preview/67196_seguridad-de-la-informacion.

Crescentino, L. (2009). *El software libre y su implementación en la administración pública de América del Sur.* Recuperado de: http://iepweb.sciencespo-rennes.fr/bibli_doc/download/224/.

CTTC (Centre Tecnològic de Telecomunicacions de Catalunya). (s.f.). *Glosario de términos de seguridad.* Recuperado de: http://www.cttc.es/resources/doc/080122-glosario-48230.pdf.

Digital Metamorphosis of a Shuttered Butterfly. (2013). *Snort (Intrusion Detection Utility) Installation in Centos 6.* Recuperado de: http://shutteredbutterfly.com/2013/02/06/snort-intrusion-detection-utility-installation-in-centos-6/.

Ditech. (2010). *Prevención de intrusos (IPS)*. Recuperado de: http://ditech.com.co/soluciones-integrales/seguridad-informatica-en-redes/revencion-de-intrusos-ips/.

Gascón, H. (2010). *Estudio de un IDS open source frente a herramientas de análisis y explotación de vulnerabilidades*. (Tesis de Ingeniería en Telecomunicaciones, Universidad Carlos III de Madrid). Recuperado de: http://e-archivo.uc3m.es/bitstream/10016/11213/1/PFC_Hugo_Gascon_Polanco.pdf.

García, J. (s.f.). Mucho más que un cortafuego. *Haking revista,2008*(1),10-16. Recuperado de: http://190.90.112.209/http/articulos/hakin9_01_2008_ES.pdf.

Giménez, M. (2008). *Utilización de sistemas de detección de intrusos como elemento de seguridad perimetral*. (Tesis de Ingeniería en Informática, Universidad de Almería). Recuperado de: http://www.adminso.es/images/1/1d/PFC_marisa.pdf.

Gómez, A. (s.f.). *Prevención de ataques e intrusos en las redes informáticas.* Recuperado de http://www.mundointernet.es/IMG/pdf/ponencia95.pdf.

Lee, P., Chuang, H., Yaou, C., Chao, W., & Hsueh ,G.(2012). Making linux an IPS device using snort. Recuperado de: https://www.ibm.com/developerworks/community/blogs/58e72888-6340-46ac-b488-d31aa4058e9c/entry/august_8_2012_12_01_pm6?lang=en.

Lococo, M. (2011). *Capacity planning for snort IDS.* Recuperado de: http://mikelococo.com/2011/08/snort-capacity-planning/.

Matalobos, J. (2009). *Análisis de riesgos de seguridad de la información.* (Tesis de Ingeniería del Software, Universidad Politécnica de Madrid). Recuperado de: http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf.

Pabón, Y. (2012). *Instalación, configuración, funcionamiento y ejecución de snort*. (Tesis de Ingeniería en Sistemas Computacionales, Universidad Francisco de Paula Santander). Recuperado de https://seguridadinformaticaufps.wikispaces.com/Documentacion2PrevioPractica.

PAE (Portal de Administración Electrónica, Esp.).(2012). *Libros de MAGERIT v3-idioma-español*. Recuperado de: http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_Area_Descargas&langPae=es&iniciativa=184.

Portal de soluciones técnicas y organizativas a los controles de ISO/IEC 27002, Esp. (2012). *Controles ISO 27002*. Recuperado de: https://iso27002.es.

Sánchez, E. (2012). *Análisis de riesgos en la Universidad Politécnica de Cartagena*. Recuperado de: http://www.rediris.es/difusion/eventos/foros-seguridad/fs2012/archivo/analisis_riesgos_upct.pdf.

Simulación de ataques informáticos en entornos virtuales. (2011). Recuperado de: http://infosececuador.wordpress.com/2011/01/17/76/.

Servernoobs, US. (2013). *Avoiding CPU speed scaling-running CPU at full speed.* Recuperado de http://www.servernoobs.com/avoiding-cpu-speed-scaling-in-modern-linux-distributions-running-cpu-at-full-speed-tips/.

University of Maryland, US. (s.f.). *Installing snort from source code on linux.* Recuperado de: http://polaris.umuc.edu/~sgantz/Install.html.

Viteri, M., Orellana, P. (2011). *Metodología de seguridad en redes T.A.M.A.R.A: testeo, análisis y manejo de redes y accesos*. (Tesis de Ingeniería en Telemática, ESPOL). Recuperado de http://www.dspace.espol.edu.ec/handle/123456789/20029?mode=full.

Zabala, S. (2009). *Guía a la redacción en el estilo APA, 6ta edición*. Recuperado de: http://www.suagm.edu/umet/biblioteca/pdf/guia_apa_6ta.pdf.

GLOSARIO DE TÉRMINOS

ACK.- Acrónimo de Acknowledgement (Confirmación). Confirmación positiva a un mensaje recibido, corroborando la integridad de los datos.

Análisis de riesgos.- Estudio de los activos, sus vulnerabilidades y las probabilidades de materialización de amenazas, con el propósito de determinar la exposición al riesgo de cada activo ante cada amenaza.

Angry IP.- Aplicación que rastrea cada dirección IP de una red, con el fin de verificar si está activa o no, o as u vez obtener información como: nombre de host, dirección MAC y estado de puertos.

ARP.- (Address Resolution Protocol) Es el encargado de convertir las direcciones IP a direcciones MAC. Partiendo del hecho de que en una red los host se conocen a través de sus direcciones físicas MAC, una máquina que quiere comunicarse con otra, primero pregunta por su dirección IP destino, pero para entenderla la traduce a una física.

Ataque de diccionario.- Método empleado para romper la seguridad de los sistemas basados en passwords (contraseñas) en la que el atacante intenta dar con la clave adecuada probando todas (o casi todas) las palabras posibles o recogidas en un diccionario.

Auditoria de seguridad.- Es el estudio que comprende el análisis y gestión de las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.

Autenticación.- Confirmación de la identidad de un usuario. Verificar que un usuario que intente acceder a los recursos de un sistema informático o que genera una determinada información, es quien dice ser.

Cabecera de paquetes.- Parte inicial de un paquete que precede a los datos propiamente dichos y que contiene las direcciones del remitente y del destinatario, control de errores y otros campos.

CentOS.- (Community ENTerprise Operating System) Es un clon a nivel binario de la distribución Linux Red Hat Enterprise Linux RHEL, compilado por voluntarios a partir del código fuente liberado por Red Hat, tiene licencia GPL.

Código abierto.- El código abierto tiene un punto de vista más orientado a los beneficios prácticos de poder acceder al código fuente, con la posibilidad de modificarlo y mejorarlo. Al contrario del concepto de software libre más amplio, que promueve la libertad de: reproducción, estudio, modificación, y redistribución del producto.

Controles criptográficos.- Transforma el texto plano a datos ilegibles, para quienes no poseen los métodos ni permisos para restaurarlos. Con el fin de ocultar dicha información a entes ajenos, detectar su modificación no autorizada y prevenir su uso no permitido.

Desbordamiento de Buffer.- Error de software que tiene lugar cuando se copia una cantidad más grande de datos sobre un área más pequeña, sobre-escribiendo otras zonas de datos no previstas.

Direccionamiento.- Permite la transmisión de datos entre host de la misma red o redes diferentes.

Dirección MAC.- La dirección MAC (Media Access Control Address) es un identificador de 48 bits (6 bytes) que corresponde de forma única a una tarjeta o interfaz de red.

Enrutamiento.- Busca un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad. También es el proceso usado por el router para enviar paquetes a la red de destino.

Espacio de usuario.- El espacio de usuario (user space) o espacio de aplicación comprende la región de memoria donde se ejecutan las aplicaciones de usuario propiamente dichas.

Exploit.- Programa o código que "explota" una vulnerabilidad del sistema o de parte de él para aprovechar esta deficiencia en beneficio del creador del mismo.

FIN flag.- Si se activa es porque no hay más datos a enviar por parte del emisor, esto es, el paquete que lo lleva activo es el último de una conexión.

GNU.- El proyecto GNU fue iniciado por Richard Stallman con el objetivo de crear un sistema operativo completamente libre. GNU es un acrónimo recursivo que significa GNU No es Unix (GNU is Not Unix).

GPL.- La Licencia Pública General de GNU (GNU General Public License), garantiza a los usuarios finales la libertad de usar, estudiar, compartir (copiar) y modificar el software. Su propósito es declarar que el software cubierto por esta licencia es software libre y protegerlo de intentos de apropiación que restrinjan esas libertades a los usuarios.

HTTP.- El Protocolo de Transferencia de Hipertexto tiene como propósito el permitir la transferencia de archivos (principalmente, en formato HTML), entre un navegador (el cliente) y un servidor web.

ICMP.- El Protocolo de Mensajes de Control de Internet (Internet Control Message Protocol) se utiliza para efectuar el diagnóstico y notificación de errores durante una comunicación.

INEN.- (Instituto Ecuatoriano de Normalización) Es una entidad cuyas funciones principales son: La normalización (creación o adaptación de normas), control de importaciones y certificaciones de calidad.

Ingeniería Social.- Es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Se usará comúnmente el teléfono o Internet para engañar a la gente y llevarla a revelar información sensible, o bien a violar las políticas de seguridad típicas.

IPSec.- Conjunto de protocolos para soportar intercambio seguros de paquetes a nivel IP donde el emisor y receptor deben compartir una llave pública. Ampliamente extendido para la implementación de Redes Privadas Virtales (VPNs), soporta dos modos de cifrado: Transporte y Túnel.

Iptables.- Herramienta de espacio de usuario mediante la cual el administrador puede definir políticas de filtrado del tráfico que circula por la red, o a su vez, realizar traducción de direcciones de red (NAT).

Kernel.- Es el núcleo del sistema operativo y la parte fundamental del mismo. Es el encargado de gestionar recursos, planificar la ejecución de los procesos, supervisar la transmisión de datos entre las aplicaciones y los dispositivos periféricos, etc.

Keylogger.- Programa que intercepta todas las pulsaciones realizadas en el teclado (e incluso a veces también el mouse), y las guarda en un archivo para obtener datos críticos como contraseñas, etc. Posteriormente puede ser enviado a un tercero sin conocimiento ni consentimiento del usuario.

Libpcap.- Librería usada para captura de paquetes, por parte de herramientas como: analizadores de tráfico, sistemas de detección de intrusos en la red, programas de captura de las tramas de red (packet sniffers), etc.

Linux.- El núcleo de Linux fue creado a partir de ideas de Unix, por Linus Torvalds (Helsinki, 1969) a principios de los 90. Este proyecto se une con Free Software Foundation (FSF) para el proyecto GNU, con el fin de hacer un sistema operativo libre, conformando lo que hoy se conoce como sistema GNU/Linux.

Log.- Fichero de texto en el que queda recogida toda la actividad que tiene lugar en un determinado ordenador, permitiendo para ciertos programas que su propietario o administrador detecte actividades ilícitas e identifique, por medio de su dirección IP, al usuario correspondiente.

MySQL.- Es un sistema de gestión de bases de datos, licenciado bajo la GPL de la GNU. Su diseño le permite soportar una gran carga de forma muy eficiente. MySQL fue creada por la empresa sueca MySQL AB.

NAT.- (Network Address Translation) Entre sus funciones están la de permitir el acceso a Internet a varias máquinas a partir de una sola IP pública u ocultar (por razones de seguridad) dichas direcciones IP de la red interna detrás de una dirección IP que se desea hacer pública.

Nessus.- Programa de escaneo de vulnerabilidades para diversos sistemas operativos. El proyecto Nessus comenzó en 1998, cuando Renaud Deraison quiso que la comunidad de Internet tenga un escaner remoto de seguridad que sea libre.

Nmap.- Rastrea los puertos de la máquina o máquinas en cuestión y establece si un puerto está abierto, cerrado o protegido por un firewall.

OSI.- (Open System Interconnection) Define cómo se integran el hardware y software, en función de las diferentes capas, para permitir la comunicación entre ordenadores.

Packet Logger.- Escucha todo el tráfico de la red, y registra los paquetes en un determinado directorio.

Parche de seguridad.- Conjunto de ficheros adicionales al software original de una herramienta o programa informático, que sirven para solucionar sus posibles carencias, vulnerabilidades, o defectos de funcionamiento.

Pentesting.- Corresponde a las pruebas de intrusión o análisis de vulnerabilidades.

People Search.- Permiten encontrar a personas en las diferentes redes sociales, o a su vez, acceder a su teléfono, dirección, portales web, fotos, empleo, etc.

Política.- Permite establecer un canal de comunicación con el usuario de un sistema informático, sea éste empleado, administrador, gerente, usuario final, etc., indicándole cómo actuar frente a un recurso determinado del sistema, a través del establecimiento de reglas, normas o controles que determinan lo que está o no permitido realizar.

Procedimiento.- Un procedimiento se define como una sucesión de operaciones concatenadas entre sí, enfocadas a cumplir con los objetivos de las políticas de seguridad de la información previamente desarrolladas.

Protocolo.- Conjunto de reglas o normas a seguir en una cierta comunicación, las cuales deben ser idénticas tanto en el emisor como receptor.

Queue.- Lleva al paquete a una cola destinada al procesamiento en espacio de usuario. Para que esto sea útil, necesita un proceso en espacio de usuario que recibe, posiblemente manipula, y dicta veredicto sobre los paquetes.

SGSI.- (Sistema de Gestión de Seguridad de la Información) Se basa en el diseño, implantación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos.

SMTP.- (Protocolo simple de transferencia de correo electrónico). Protocolo de red basado en texto, utilizado para el intercambio de mensajes de correo electrónico entre computadoras o distintos dispositivos.

Snnifer.- Programa y/o dispositivo que monitoriza la circulación de datos a través de una red. Los sniffers pueden emplearse tanto con funciones legítimas de gestión de red como para el robo de información.

Software Libre.- Denominación del software que respeta la libertad de todos los usuarios que adquirieron el producto y, por tanto, una vez obtenido el mismo puede ser usado, copiado, estudiado, modificado, y redistribuido libremente de varias formas. Puede estar disponible gratuitamente o al precio de costo, por tanto no debe ser confundido con software gratuito (freeware).

Spam.- Correo electrónico no deseado que se envía aleatoriamente a gran cantidad de usuarios. No es una amenaza directa, pero la cantidad de correo basura recibido y el tiempo que supone identificarlo y eliminarlo, representa un elemento molesto para los usuarios de Internet.

SSH.- (Secure SHell) es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente.

SYN.- El cliente realiza una conexión enviando un paquete SYN al servidor, en el servidor se comprueba si el puerto está abierto, si el puerto no está abierto se le envía al cliente un reset RST, esto significa un rechazo de intento de conexión. Si el puerto está abierto, el servidor responde con un SYN/ACK. Entonces el cliente respondería al servidor con un ASK, completando así la conexión.

Trazabilidad.- Se refiere a la actividad que compromete al administrador, para dar un seguimiento al usuario en lo que se refiere al uso adecuado de un activo o servicio determinado, dentro de un sistema de información.

Ttysnoop.- Es una aplicación para espiar literalmente a un usuario que accede a una maquina determinada mediante ssh.

UDP.- Es un protocolo del nivel de transporte que permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión (No orientado a conexión), ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

Unified.- Es un formato binario usado por Snort para escribir sus alertas en tiempos y espacios reducidos. Este formato tiene un intérprete llamado Barnyard, el cual a su vez lleva está información a la base de datos para su respectivo almacenamiento.

Unix.- Es un sistema operativo, con funciones multitarea y multiusuario, desarrollado en los laboratorios Bell (por Kernighan & Thompson) en 1969. En sus inicios fue distribuido de forma gratuita en muchas universidades ganando gran aceptación, sin embargo con el tiempo

se fueron creando licencias cada vez más restrictiva. Provisto básicamente por tres partes: el kernel (control de la máquina y supervisión de los programas de usuario), el shell (intérprete de órdenes, se ocupa de la comunicación entre el usuario y el sistema) y los programas de utilidad (resto de programas que no están incluidos en el kernel, útiles para tareas básicas como edición de ficheros, ordenamiento de números, gráficas, etc.)

Vulnerabilidad.- Fallos o huecos de seguridad detectados en algún programa o sistema informático. Estos errores de programación y/o diseño permiten que un tercero se aproveche de ellos para realizar acciones tales como ataques, intrusiones o cualquier otro uso indebido.

ANEXOS

ANEXO 1

CATÁLOGO ESTÁNDAR PARA LA IDENTIFICACIÓN DE ACTIVOS SEGÚN EL LIBRO "CATÁLOGO DE ELEMENTOS" DE MAGERIT

El objetivo de este catálogo de elementos que aparecen en un proyecto de análisis y gestión de riesgos es doble:

- Por una parte, facilitar la labor de las personas que acometen el proyecto, en el sentido de ofrecerles ítem estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis.

- Por otra, homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios que permitan comparar e incluso integrar análisis realizados por diferentes equipos.

Servicios [S]
Función que satisface una necesidad de los usuarios (del servicio). Para la prestación de un servicio se requieren una serie de medios. Los servicios aparecen como activos de un análisis de riesgos bien como servicios finales (prestados por la Organización a terceros), bien como servicios instrumentales (donde tanto los usuarios como los medios son propios), bien como servicios contratados (a otra organización que los proporciona con sus propios medios). Así se encuentran servicios públicos prestados por la Administración para satisfacer necesidades de la colectividad; servicios empresariales prestados por empresas para satisfacer necesidades de sus clientes; servicios internos prestados por departamentos especializados dentro de la Organización, que son usados por otros departamentos u empleados de la misma; etc. Al centrarse esta guía en la seguridad de las tecnologías de la información y las comunicaciones, es natural que aparezcan servicios de información, servicios de comunicaciones, servicios de seguridad, etc. sin por ello ser óbice para encontrar otros servicios requeridos para el eficaz desempeño de la misión de la organización.

```
[pub] al público en general (sin relación contractual)
[ext] a clientes (bajo una relación contractual)
[int] interno (usuarios y medios de la propia organización)
[cont] contratado a terceros (se presta con medios ajenos)
```

Datos/Información [D]

Elementos de información que, de forma singular o agrupada de alguna forma, representan el conocimiento que se tiene de algo. Los datos son el corazón que permite a una organización prestar sus servicios. Son en cierto sentido un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado en forma de bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.

Es habitual que en un análisis de riesgos e impactos, el usuario se limite a valorar los datos, siendo los demás activos meros sirvientes que deben cuidar y proteger los datos que se les encomiendan.

```
[bdd] datos vitales
[com] datos de interés comercial
[adm] datos de interés administrativo
[source] código fuente
[exe] código ejecutable
[conf] datos de configuración
[log] registro de actividad (log)
[per] datos de carácter personal
```

Aplicaciones/Software [SW]

Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.

No preocupa en este apartado el denominado “código fuente” o programas que serán datos de interés comercial, a valorar y proteger como tales. Dicho código aparecería como datos.

```
[prp] desarrollo propio (in house)
[sub] desarrollo a medida (subcontratado)
[dbms] sistemas de gestión de bases de datos
[office] ofimática
[os] sistemas operativos
```

Equipos Informáticos/Hardware [SW]

Dícese de bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.

```
[host] grandes equipos
[mid] equipos medios
[pc] informática personal
[mobile] informática móvil
[pda] agendas electrónicas
[print] medios de impresión
[scan] escáneres
```

Redes de Comunicaciones [COM]

Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.

```
[modem] módems
[hub] concentradores
[switch] conmutadores
[router] encaminadores
[bridge] pasarelas
[firewall] cortafuegos
```

Soportes de Información [SI]

En este epígrafe se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

```
[disk] discos
[disquette] disquetes
[cd] cederrón (CD-ROM)
[usb] dispositivos USB
[dvd] DVD
[tape] cinta magnética
[mc] tarjetas de memoria
[ic] tarjetas inteligentes
[printed] material impreso
```

Equipamiento Auxiliar [SI]

En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

```
[ups] sistemas de alimentación ininterrumpida
[gen] generadores eléctricos
[ac] equipos de climatización
[cabling] cableado
[furniture] mobiliario: armarios, etc
```

Instalaciones [L]

En este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones.

```
[site] emplazamiento
[building] edificio
[mobile] plataformas móviles
[car] vehículo terrestre: coche, camión, etc.
[plane] vehículo aéreo: avión, etc.
```

Personal [P]

En este epígrafe aparecen las personas relacionadas con los sistemas de información.

```
[op] operadores
[adm] administradores de sistemas
[com] administradores de comunicaciones
[dba] administradores de BBDD
[des] desarrolladores
[sub] subcontratas
```

ANEXO 2

CÁLCULO DEL RIESGO INTRÍNSECO SOBRE LOS ACTIVOS DE LA RED ADMINISTRATIVA DEL GAD IBARRA

ANEXO 3

CATÁLOGO ESTÁNDAR PARA LA IDENTIFICACIÓN DE AMENAZAS SEGÚN EL LIBRO "CATÁLOGO DE ELEMENTOS" DE MAGERIT

1. Desastres Naturales [N]

Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

1.1 Fuego [N.1]

Tipos de activos:	**Dimensiones:**
_ [HW] equipos informáticos (hardware) _ [COM] redes de comunicaciones _ [SI] soportes de información _ [AUX] equipamiento auxiliar _ [L] instalaciones	1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos

Descripción: Incendios: posibilidad de que el fuego acabe con los recursos del sistema.

1.2 Daños por Agua [N.2]

Tipos de activos:	**Dimensiones:**
_ [HW] equipos informáticos (hardware) _ [COM] redes de comunicaciones _ [SI] soportes de información _ [AUX] equipamiento auxiliar _ [L] instalaciones	1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos

Descripción: Inundaciones: posibilidad de que el agua acabe con los recursos del sistema.

1.3 Otros desastres naturales [N.*]

Tipos de activos:	**Dimensiones:**
_ [HW] equipos informáticos (hardware) _ [COM] redes de comunicaciones _ [SI] soportes de información _ [AUX] equipamiento auxiliar	1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos

_ [L] instalaciones	
Descripción: Otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, etc.	

2. De origen Industrial [I]

Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.

2.1 Fuego [I.1]

Tipos de activos:	**Dimensiones:**
_ [HW] equipos informáticos (hardware) _ [COM] redes de comunicaciones _ [SI] soportes de información _ [AUX] equipamiento auxiliar _ [L] instalaciones	1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripción: Incendio: posibilidad de que el fuego acabe con los recursos del sistema.	

2.2 Daños por agua [I.2]

Tipos de activos:	**Dimensiones:**
_ [HW] equipos informáticos (hardware) _ [COM] redes de comunicaciones _ [SI] soportes de información _ [AUX] equipamiento auxiliar _ [L] instalaciones	1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripción: Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.	

2.3 Contaminación mecánica [I.3]

Tipos de activos:	**Dimensiones:**
_ [HW] equipos informáticos (hardware) _ [COM] redes de comunicaciones _ [SI] soportes de información _ [AUX] equipamiento auxiliar	1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos

Descripción: Vibraciones, polvo, suciedad, etc.

2.4 Contaminación electromagnética [I.4]

Tipos de activos:	**Dimensiones:**
_ [HW] equipos informáticos (hardware) _ [COM] redes de comunicaciones _ [SI] soportes de información (electrónicos) _ [AUX] equipamiento auxiliar	1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos

Descripción: Interferencias de radio, campos magnéticos, luz ultravioleta, etc.

2.5 Avería de origen físico o lógico [I.5]

Tipos de activos:	**Dimensiones:**
_ [SW] aplicaciones (software) _ [HW] equipos informáticos (hardware) _ [COM] redes de comunicaciones _ [SI] soportes de información _ [AUX] equipamiento auxiliar	1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos

Descripción: Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.

2.6 Corte del suministro eléctrico [I.6]

Tipos de activos:	**Dimensiones:**
_ [HW] equipos informáticos (hardware) _ [COM] redes de comunicaciones _ [AUX] equipamiento auxiliar	1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos

Descripción: Cese de la alimentación de potencia

2.7 Condiciones inadecuadas de temperatura y/o humedad [I.7]

Tipos de activos:	**Dimensiones:**
_ [HW] equipos informáticos (hardware) _ [COM] redes de comunicaciones _ [SI] soportes de información	1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos

_ [AUX] equipamiento auxiliar	

Descripción: Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, etc.

2.8 Fallo de servicios de comunicaciones [I.8]

Tipos de activos:	**Dimensiones:**
_ [COM] redes de comunicaciones	1. [D] disponibilidad

Descripción: Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.

2.9 Interrupción de otros servicios y suministros esenciales [I.9]

Tipos de activos:	**Dimensiones:**
_ [AUX] equipamiento auxiliar	1. [D] disponibilidad

Descripción: Otros servicios o recursos de los que depende la operación de los equipos.

2.10 Degradación de los soportes de almacenamiento de la información [I.10]

Tipos de activos:	**Dimensiones:**
_ [SI] soportes de información	1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos

Descripción: Como consecuencia del paso del tiempo

2.11 Emanaciones electromagnéticas [I.11]

Tipos de activos:	**Dimensiones:**
_ [D] datos / información	1. [C] confidencialidad

Descripción: Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque.

Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información (incluyendo los teclados).

Esta amenaza se denomina, incorrecta pero frecuentemente, ataque TEMPEST (del inglés *"Transient Electromagnetic Pulse Standard").* Abusando del significado primigenio, es frecuente oír hablar de que un equipo disfruta de "*TEMPEST protection"*, queriendo decir que se ha diseñado para que no emita, electromagnéticamente, nada de interés por si alguien lo captara.

No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, etc. que estarán amenazadas de intercepción.

2.12 Otros desastres industriales [I.*]

Tipos de activos:	**Dimensiones:**
_ [HW] equipos informáticos (hardware) _ [COM] redes de comunicaciones _ [SI] soportes de información _ [AUX] equipamiento auxiliar _ [L] instalaciones	1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos

Descripción:

Otros desastres debidos a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, etc.

3. Errores y fallos no intencionados [E]

Fallos no intencionales causados por las personas.

3.1 Errores de los usuarios [E.1]

Tipos de activos:	**Dimensiones:**
_ [S] servicios _ [D] datos / información _ [SW] aplicaciones (software)	1. [I] integridad 2. [D] disponibilidad

Descripción: Equivocaciones de las personas cuando usan los servicios, datos, etc.

3.2 Errores del administrador [E.2]

Tipos de activos:	**Dimensiones:**
_ [S] servicios _ [D] datos / información	1. [D] disponibilidad 2. [I] integridad

_ [SW] aplicaciones (software) _ [HW] equipos informáticos (hardware) _ [COM] redes de comunicaciones	3. [C] confidencialidad 4. [A_S] autenticidad del servicio 5. [A_D] autenticidad de los datos 6. [T_S] trazabilidad del servicio 7. [T_D] trazabilidad de los datos
Descripción: Equivocaciones de personas con responsabilidades de instalación y operación.	
3.3 Errores de monitorización *(log)* [E.3]	
Tipos de activos: _ [S] servicios _ [D] datos / información _ [SW] aplicaciones (software)	**Dimensiones:** 1. [T_S] trazabilidad del servicio 2. [T_D] trazabilidad de los datos
Descripción: Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, etc.	
3.4 Errores de configuración [E.4]	
Tipos de activos: _ [S] servicios _ [D] datos / información _ [SW] aplicaciones (software) _ [HW] equipos informáticos (hardware) _ [COM] redes de comunicaciones	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad 4. [A_S] autenticidad del servicio 5. [A_D] autenticidad de los datos 6. [T_S] trazabilidad del servicio 7. [T_D] trazabilidad de los datos
Descripción: Introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	
3.5 Deficiencias en la organización [E.7]	
Tipos de activos: _ [P] personal	**Dimensiones:** 1. [D] disponibilidad

Descripción: Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc.

3.6 Difusión de software dañino [E.8]

Tipos de activos:	**Dimensiones:**
_[D] datos / información _ [SW] aplicaciones (software)	1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad 4. [A_S] autenticidad del servicio 5. [A_D] autenticidad de los datos 6. [T_S] trazabilidad del servicio 7. [T_D] trazabilidad de los datos

Descripción: Propagación inocente de virus, espías *(spyware)*, gusanos, troyanos, bombas lógicas, etc.

3.7 Errores de [re-]encaminamiento [E.9]

Tipos de activos:	**Dimensiones:**
_ [S] servicios _[D] datos / información _ [SW] aplicaciones (software) _ [COM] redes de comunicaciones	1. [C] confidencialidad 2. [I] integridad 3. [A_S] autenticidad del servicio 4. [T_S] trazabilidad del servicio

Descripción: Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.
Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.

3.8 Errores de secuencia [E.10]

Tipos de activos:	**Dimensiones:**
_[D] datos / información _ [SW] aplicaciones (software)	1. [I] integridad

Descripción: Alteración accidental del orden de los mensajes transmitidos.

3.9 Escapes de información [E.14]	
Tipos de activos: _ [D] datos / información	**Dimensiones:** 1. [C] confidencialidad
Descripción: La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.	
3.10 Alteración de la información [E.15]	
Tipos de activos: _ [D] datos / información	**Dimensiones:** 1. [I] integridad
Descripción: Alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	
3.11 Introducción de información incorrecta [E.16]	
Tipos de activos: _ [D] datos / información	**Dimensiones:** 1. [I] integridad
Descripción: Inserción accidental de información incorrecta. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	
3.12 Degradación de la información [E.17]	
Tipos de activos: _ [D] datos / información	**Dimensiones:** 1. [I] integridad
Descripción: Degradación accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	
3.13 Destrucción de información [E.18]	
Tipos de activos: _ [D] datos / información	**Dimensiones:** 1. [D] disponibilidad
Descripción: Pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	

3.14 Divulgación de información [E.19]	
Tipos de activos: _ [D] datos / información	**Dimensiones:** 1. [C] confidencialidad
Descripción: Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc.	
3.15 Vulnerabilidades de los programas (software) [E.20]	
Tipos de activos: _ [SW] aplicaciones (software) _[D] datos / información	**Dimensiones:** 1. [I] integridad 2. [D] disponibilidad 3. [C] confidencialidad
Descripción: Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.	
3.16 Errores de mantenimiento / actualización de programas (software) [E.21]	
Tipos de activos: _ [SW] aplicaciones (software) _[D] datos / información	**Dimensiones:** 1. [I] integridad 2. [D] disponibilidad
Descripción: Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante	
3.17 Errores de mantenimiento / actualización de equipos (hardware) [E.23]	
Tipos de activos: _ [HW] equipos informáticos (hardware)	**Dimensiones:** 1. [D] disponibilidad
Descripción: Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.	
3.18 Caída del sistema por agotamiento de recursos [E.24]	
Tipos de activos: _ [S] servicios _ [HW] equipos informáticos (hardware)	**Dimensiones:** 1. [D] disponibilidad

_ [COM] redes de comunicaciones	

Descripción: La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

3.19 Indisponibilidad del personal [E.28]

Tipos de activos:	**Dimensiones:**
_ [P] personal interno	1. [D] disponibilidad

Descripción: Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, etc.

4. Ataques intencionados [A]

Fallos deliberados causados por las personas.

4.1 Manipulación de la configuración [A.4]

Tipos de activos:	**Dimensiones:**
_ [S] servicios	1. [I] integridad
_ [D] datos / información	2. [C] confidencialidad
_ [SW] aplicaciones (software)	3. [A_S] autenticidad del servicio
_ [HW] equipos informáticos (hardware)	4. [A_D] autenticidad de los datos
_ [COM] redes de comunicaciones	5. [T_S] trazabilidad del servicio
	6. [T_D] trazabilidad de los datos
	7. [D] disponibilidad

Descripción: Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.

4.2 Suplantación de la identidad del usuario [A.5]

Tipos de activos:	**Dimensiones:**
_ [S] servicios	1. [C] confidencialidad
_[D] datos / información	2. [A_S] autenticidad del servicio
_ [SW] aplicaciones (software)	3. [A_D] autenticidad de los datos

	4. [I] integridad
Descripción: Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.	
4.3 Abuso de privilegios de acceso [A.6]	
Tipos de activos: _[D] datos / información _ [SW] aplicaciones (software)	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad
Descripción: Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.	
4.4 Uso no previsto [A.7]	
Tipos de activos: _ [S] servicios _ [HW] equipos informáticos (hardware) _ [COM] redes de comunicaciones _ [SI] soportes de información _ [AUX] equipamiento auxiliar _ [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.	
4.5 Difusión de software dañino [A.8]	
Tipos de activos: _[D] datos / información _ [SW] aplicaciones (software)	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad 4. [A_S] autenticidad del servicio 5. [A_D] autenticidad de los datos

	6. [T_S] trazabilidad del servicio 7. [T_D] trazabilidad de los datos
Descripción: Propagación intencionada de virus, espías *(spyware)*, gusanos, troyanos, bombas lógicas, etc.	
4.6 [Re-]encaminamiento de mensajes [A.9]	
Tipos de activos: _ [S] servicios _[D] datos / información _ [SW] aplicaciones (software) _ [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [A_S] autenticidad del servicio 4. [T_S] trazabilidad del servicio
Descripción: Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información hacia donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe.	
4.7 Alteración de secuencia [A.10]	
Tipos de activos: _[D] datos / información _ [SW] aplicaciones (software)	**Dimensiones:** 1. [I] integridad
Descripción: Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados.	
4.8 Acceso no autorizado [A.11]	
Tipos de activos: _ [S] servicios _ [D] datos / información	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad

_ [SW] aplicaciones (software) _ [HW] equipos informáticos (hardware) _ [COM] redes de comunicaciones _ [SI] soportes de información _ [AUX] equipamiento auxiliar _ [L] instalaciones	3. [A_S] autenticidad del servicio
Descripción: El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.	
4.9 Análisis de tráfico [A.12]	
Tipos de activos: _[D] datos / información	**Dimensiones:** 1. [C] confidencialidad
Descripción: El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina "monitorización de tráfico".	
4.10 Repudio [A.13]	
Tipos de activos: _ [S] servicios	**Dimensiones:** 1. [T_S] trazabilidad del servicio
Descripción: Negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: negación de haber recibido un mensaje o comunicación. Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro	
4.11 Intercepción de información (escucha) [A.14]	
Tipos de activos: _ [D] datos / información	**Dimensiones:** 1. [C] confidencialidad
Descripción: el atacante llega a tener acceso a información que no le corresponde, sin que	

la información en sí misma se vea alterada.

4.12 Modificación de la información [A.15]

Tipos de activos:	**Dimensiones:**
_ [D] datos / información	1. [I] integridad

Descripción: Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.

Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

4.13 Introducción de falsa información [A.16]

Tipos de activos:	**Dimensiones:**
_ [D] datos / información	1. [I] integridad

Descripción: Inserción interesada de información falsa, con ánimo de obtener un beneficio o causar un perjuicio.

Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

4.14 Corrupción de la información [A.17]

Tipos de activos:	**Dimensiones:**
_ [D] datos / información	1. [I] integridad

Descripción: Degradación intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.

Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

4.15 Destrucción la información [A.18]

Tipos de activos:	**Dimensiones:**
_ [D] datos / información	1. [D] disponibilidad

Descripción: Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio. Esta amenaza sólo se identifica sobre datos en general, pues cuando

la información está en algún soporte informático, hay amenazas específicas.

4.16 Divulgación de información [A.19]

Tipos de activos:	**Dimensiones:**
_ [D] datos / información	1. [C] confidencialidad

Descripción: Revelación de información

4.17 Manipulación de programas [A.22]

Tipos de activos:	**Dimensiones:**
_ [SW] aplicaciones (software) _[D] datos / información	1. [C] confidencialidad 2. [I] integridad 3. [A_S] autenticidad del servicio 4. [A_D] autenticidad de los datos 5. [T_S] trazabilidad del servicio 6. [T_D] trazabilidad de los datos

Descripción: Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.

4.18 Denegación de servicio [A.24]

Tipos de activos:	**Dimensiones:**
_ [S] servicios _ [HW] equipos informáticos (hardware) _ [COM] redes de comunicaciones	1. [D] disponibilidad

Descripción: La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

4.19 Robo [A.25]

Tipos de activos:	**Dimensiones:**
_ [HW] equipos informáticos (hardware) _ [COM] redes de comunicaciones _ [SI] soportes de información _ [AUX] equipamiento auxiliar _[D] datos / información	1. [D] disponibilidad 2. [C] confidencialidad

Descripción: La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.

El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales.

El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias.

En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.

4.20 Ataque destructivo [A.26]

Tipos de activos:	**Dimensiones:**
_ [HW] equipos informáticos (hardware) _ [COM] redes de comunicaciones _ [SI] soportes de información _ [AUX] equipamiento auxiliar _ [L] instalaciones	1. [D] disponibilidad

Descripción: Vandalismo, terrorismo, acción militar, etc.

Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal

4.21 Ocupación enemiga [A.27]

Tipos de activos:	**Dimensiones:**
_ [HW] equipos informáticos (hardware) _ [COM] redes de comunicaciones _ [SI] soportes de información _ [AUX] equipamiento auxiliar _[D] datos / información _ [L] instalaciones	1. [D] disponibilidad 2. [C] confidencialidad

Descripción: Cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.

4.22 Indisponibilidad del personal [A.28]

Tipos de activos:	**Dimensiones:**
_ [P] personal interno	1. [D] disponibilidad

Descripción: Ausencia deliberada del puesto de trabajo: como huelgas, absentismo

laboral, bajas no justificadas, bloqueo de los accesos, etc.

4.23 Extorsión [A.29]	
Tipos de activos: _ [P] personal interno _ [S] servicios _[D] datos / información	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [A_S] autenticidad del servicio 4. [A_D] autenticidad de los datos 5. [T_S] trazabilidad del servicio 6. [T_D] trazabilidad de los datos
Descripción: Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.	

4.24 Ingeniería social [A.30]	
Tipos de activos: _ [P] personal interno _ [S] servicios _[D] datos / información	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [A_S] autenticidad del servicio 4. [A_D] autenticidad de los datos 5. [T_S] trazabilidad del servicio 6. [T_D] trazabilidad de los datos
Descripción: Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.	

ANEXO 4

IDENTIFICACIÓN DE SALVAGUARDAS EXISTENTES-GAD IBARRA

ANEXO 5

RESULTADOS FINALES POSTERIORES A LA IMPLEMENTACIÓN DE MAGERIT SOBRE LOS ACTIVOS DE LA RED ADMINISTRATIVA-GAD IBARRA

ANEXO 6

IDENTIFICACIÓN DEL PERSONAL RESPONSABLE PARA LOS ACTIVOS CRÍTICOS DETECTADOS CON MAGERIT

TIPO	ACTIVO CRÍTICO	RESPONSABLE
SERVICIOS	Actividades económicas	**Ing. Jairo Álvarez**
	Administración de sistemas	**Ing. Jairo Álvarez**
	Avalúos y catastros	**Ing. Manuel Lara**
	Precios unitarios	**Ing. Manuel Lara**
	Rentas y recaudaciones	**Ing. Jairo Álvarez**
	Registro de propiedad	**Ing. Byron Cueva**
	Gestión de privilegios	**Ing. Jairo Álvarez**
DATOS	BDD alfanumérica	**Ing. Manuel Lara**
	BDD Olympo	**Lcda. Sonia Bossano**
	BDD portal web	**Ing. Gladys Potosí**
	BDD espacial	**Ing. Byron Cueva**
	BDD binaria y BSC	**Ing. Manuel Lara**
	BDD correo electrónico	**Ing. Gabriel Bucheli**
	BDD Quipux	**Ing. Cristian Romero**
	Código fuente	**Ing. David Bolaños**
	Código ejecutable	**Todos**
	Respaldos	**Ing. Manuel Lara**
	Máquinas virtuales servidores	**Ing. Gabriel Bucheli**
	Datos de recursos humanos	**Ing. Manuel Lara**
	Archivos de configuración	**Todos**
APLICACIONES	Sist. avalúos y catastros	**Ing. Manuel Lara**
	Sist. rentas y recaudaciones	**Ing. Jairo Álvarez**

	Sist. actividades económicas	**Ing. Jairo Álvarez**
	Sist. análisis de precios unitarios	**Ing. Manuel Lara**
	Sist. registro de la propiedad	**Ing. Byron Cueva**
	Sist. transferencia de dominio	**Lcda. Sonia Bossano**
	Sist. de notificaciones y multas	**Ing. Jairo Álvarez**
	Sist. administración de sistemas	**Ing. Jairo Álvarez**
	Portales web	**Ing. Gladys Potosí**
	Sist. Olympo	**Lcda. Sonia Bossano**
	Sist. Quipux	**Ing. Cristian Romero**
	SO Debian	**Ing. Gabriel Bucheli**
	SO Windows Server 2000/2003	**Ing. Gabriel Bucheli**
	BDD MySQL- PostgreSQL	**Ing. Manuel Lara**
	Apache Tompcat	**Todos**
	Sun Aplication Server	**Ing. Cristian Romero**
EQUIPOS INFORMÁTICOS	Sevidor BLADE 3000	**Lcdo. Miguel Tobar**
	Servidor de correos y archivos	**Lcdo. Miguel Tobar**
	Servidor de balanceo de carga	**Lcdo. Miguel Tobar**
	Servidor de pruebas	**Lcdo. Miguel Tobar**
	Servidor de BDD	**Lcdo. Miguel Tobar**
	Servidor para virtualización	**Lcdo. Miguel Tobar**
REDES DE COMUNICACIÓN	Switch Catalyst 4503 E	**Lcdo. Miguel Tobar**

ANEXO 7

MODELO DE TRÍPTICO DESTINADO A LOS USUARIOS DEL GAD IBARRA

El tríptico presentado a continuación, ha sido entregado a los Directores de los diversos Departamento y Unidades de Gestión del Gobierno Autónomo Descentralizado de Ibarra, los cuales a su vez, han entregado copia del mismo con memo, a cada uno de los funcionarios de la entidad, de esta manera, se busca dar a conocer las principales Políticas de Seguridad de la Información propuestas en el "Manual de Políticas y Procedimientos de la Información", desarrollados en este proyecto.

CUARTO: Sobre el uso y manipulación de claves o contraseñas

El usuario es responsable exclusivo de mantener a salvo su contraseña o clave de acceso.

Las claves de acceso son personales e intransferibles.
La longitud mínima de caracteres permisibles en una contraseña se establece en 6 caracteres, entre alfanuméricos y especiales.

Se debe evitar el guardar o escribir las contraseñas en cualquier papel o superficie o dejar constancia de ellas, a menos que ésta sea guardada en un lugar seguro.

El usuario es responsable de evitar la práctica de establecer contraseñas relacionadas con alguna característica de su persona o relacionado con su vida o la de parientes, como fechas de cumpleaños o alguna otra fecha importante, que pueda ser adivinada fácilmente.

Es responsabilidad del usuario cambiar periódicamente su contraseña, de acuerdo a la criticidad de la información, procurando no reutilizar las últimas contraseñas. En caso de no saber cómo realizar el cambio, informar a la Dirección de TIC.

QUINTO: Sobre el uso del correo electrónico.

El correo electrónico municipal es de uso exclusivo, para los empleados del GAD Ibarra.

El usuario será responsable de la información que sea enviada desde su cuenta.

No se permite enviar información clasificada como confidencial por correo electrónico.

No está permitido el envío de correo masivo de uso no institucional y ajeno a la organización, tales como cadenas, publicidad y propaganda comercial, política o social, etc.

SEXTO: Sobre el uso de Internet

Los usuarios del GAD Ibarra, provistos de acceso a Internet, al aceptar este servicio están aceptando que:

- Serán sujetos de monitoreo de las actividades que realiza en Internet.
- Saben que existe la prohibición al acceso de páginas no autorizadas.
- Conocen sobre la prohibición de transmisión de archivos reservados o confidenciales no autorizados y la prohibición de descarga de software sin la autorización de la Dirección de TIC.
- La utilización de Internet es para el desempeño de su función y puesto dentro de la entidad y no para propósitos personales.

DEPARTAMENTO DE TECNOLOGÍAS Y COMUNICACIONES DEL GAD IBARRA

ELABORADO POR: Andrés Cevallos M.
Gestor de Seguridad-Proyecto "Metodología de Seguridad Informática con base en la Norma ISO 27002 y en herramientas de prevención de intrusos para el GAD Ibarra".

m.andrescevallos@gmail.com

Ibarra-2013

GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA

RESUMEN DEL MANUAL "POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA USUARIOS DEL GAD IBARRA"

Introducción.-

La información constituye un recurso fundamental para el mantenimiento y desarrollo de cualquier organización, de modo que uno de los objetivos prioritarios de cualquier empresa será el aseguramiento de dicho activo y obviamente de los sistemas que lo procesan.

Propósito.-

El presente documento tiene como finalidad dar a conocer un resumen de las Políticas de Seguridad de la Información que deberán observar y cumplir los usuarios de los activos informáticos del GAD Ibarra, con el fin de resguardar su información, manteniendo la disponibilidad, confidencialidad e integridad de la misma.

Políticas de Seguridad de la Información.-

Son esencialmente orientaciones o instrucciones que determinan lo que está o no permitido realizar, con el fin de preservar la seguridad de los activos informáticos, especialmente los datos.

PRIMERO: Sobre la seguridad de la información

La información procesada, manipulada o almacenada por el usuario no deberá ser divulgada a terceros, ya que es propiedad exclusiva del GAD Ibarra.

Para reforzar la seguridad de la información, el usuario conforme su criterio, deberá hacer respaldos de sus datos, dependiendo de la importancia y frecuencia de modificación de la misma. Los respaldos serán responsabilidad absoluta de los usuarios.

SEGUNDO: Sobre la seguridad de los equipos de cómputo

Los equipos de cómputo con problemas en su hardware, deberán ser reparados única y exclusivamente por los miembros del Área de Hardware.

El usuario no está facultado para intervenir física o lógicamente ningún equipo de cómputo que amerite reparación.

Los usuarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, ni instalar o desinstalar dispositivos, sin la autorización de la Dirección de TIC, en caso de requerir este servicio deberá solicitarlo.

Mientras se opera el equipo de cómputo, no se deberá fumar, consumir alimentos o ingerir líquidos, ya que estas acciones pueden ocasionar daños en el equipo.

Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del CPU.

El usuario debe asegurarse que los cables de conexión no sean pisados o aguijoneados al colocar otros objetos encima o contra ellos.

TERCERO: Sobre la protección contra código malicioso

Los equipos de cómputo, deberán tener instalado y configurado correctamente software antivirus actualizado.

Los usuarios de los equipos de cómputo, deberán verificar que la información soportada por los medios de almacenamiento (memorias flash, CD/DVD, discos externos, entre otros), estén libres de cualquier tipo de código malicioso, para lo cual deberán ejecutar el software antivirus autorizado e instalado por la Dirección de TIC.

Ningún usuario podrá descargar e instalar aplicaciones provenientes de sitios no confiables a partir redes de comunicaciones externas, sin la previa autorización de la Dirección de TIC.

Cualquier usuario que sospeche de alguna infección por virus en su equipo de cómputo, deberá notificarlo inmediatamente a la Dirección de TIC para su erradicación.

ANEXO A

LISTA DE SERVICIO CRÍTICOS PRESTADOS POR EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE IBARRA DE ACUERDO AL ANÁLISIS DE RIESGOS CON MAGERIT

ANEXO B

FORMULARIO DE REPORTE DE SOLUCIONES

Este formulario debe registrar y organizar las actividades de soporte realizadas por el personal de las Áreas de Hardware y Software de la entidad. Para llevar constancia fehaciente de los problemas que han sido atendidos y de las actividades que conllevan su solución, para crear un historial que sirva como base para posteriores problemas técnicos o de seguridad.

FORMULARIO REPORTE DE SOLUCIONES	
Usuario equipo informático	(Expresar el nombre del responsable del equipo que fue atendido)
Fecha/hora ingreso	
Fecha/hora salida	
Problema	(Enunciar las dificultades que tuvo el usuario, las mismas que lo llevaron a solicitar atención)
Tipo de servicio	(Exponer el tipo de servicio que fue requerido por el usuario, los mismos que están descritos en el Formulario de Solicitud de servicios-anexo)
Solución	(Describir las actividades (o estrategias) ejecutadas para llegar a la solución del problema)

Observaciones:……
……
……

_____ _____

(f) Conformidad Usuario **(f) Encargado soporte**

ANEXO C

FORMULARIO DE SOLICITUD DE SERVICIOS PARA LA DIRECCIÓN DE TIC

A través de este formulario el usuario podrá solicitar servicio o atención al personal de la Dirección de TIC de manera formal y organizada, especificando previamente sus requerimientos, de tal forma que se pueda destinar al personal de soporte idóneo para tal petición.

FORMULARIO DE SOLICITUD DE SERVICIOS PARA LA DIRECCIÓN DE TIC	
1.CAMPOS	
Fecha:	
Funcionario Solicitante:	
Departamento al que pertenece:	
Objetivo:	(Enunciar lo que se pretende lograr con el servicio solicitado)

2.SELECCIONE SERVICIOS

Reubicación de Equipo	**Instalación de Equipo**	**Instalación Software**	**Actualización de Software**	**Correo**
Mantenimiento de Equipo	**Reparación de Equipo**	**Reporte de errores**	**Internet**	**Otros**

- **Reubicación de Equipo:** Ubicar el equipo en las áreas en donde se requiere para su óptimo aprovechamiento.
- **Mantenimiento de Equipo:** Mantenimiento preventivo del equipo.
- **Instalación de Equipo:** Instalar algún equipo o sistema de hardware/software.
- **Reparación de Equipo:** Restauración del equipo, cuando presente falla.
- **Instalación Software:** Instalación de programas de cómputo.
- **Reporte de errores:** Información de los errores que esté generando el sistema, a fin de tomar medidas pertinentes.
- **Internet:** Provisión del servicio de Internet.
- **Correo:** Solicitud para la creación de cuentas de correo electrónico.

ANEXO D

BITÁCORA DE CONTROL DE RESPALDOS Y RESTAURACIÓN DE DATOS

Por medio de esta bitácora se lleva un registro y control de los respaldos y restauraciones por parte de los administradores, describiendo las Bases de Datos de las que se obtuvo las copias de seguridad y señalando la ubicación donde van a ser almacenadas, garantizando además que sean manipuladas única y exclusivamente por personal autorizado.

BITÁCORA DE CONTROL DE RESPALDOS Y RESTAURACIÓN DE DATOS				
Fecha:				
Hora de inicio:				
Hora de finalización:				
Responsable:				
Tipo de Operación: (Señalar con una X)	a) Respaldo ☐		b) Restauración ☐	
1.DESCRIPCIÓN DE RECURSOS RESPALDADOS				
BASE DE DATOS DEL GAD-I	**BASE DE DATOS DE PORTALES WEB**		**APLICACIONES INFORMÁTICAS**	**PORTALES WEB**
(Señalar con una X la Base respaldada)	(Describir los nombres de las BDD de portales web, aplicaciones informáticas o portales web, de los cuales se obtuvo el respaldo)			
Base Alfanumérica Base Binaria Base Espacial	☐ ☐ ☐			
1.1Ubicación del archivo				
Nombre del Servidor:		Código del DVD:		

Dirección IP:	Ubicación:
Directorio:	

2.DESCRIPCIÓN DE RECURSOS RESTAURAURADOS

Causa/Motivo de la Restauración:	

BASE DE DATOS DEL GAD-I	**BASE DE DATOS DE PORTALES WEB**	**APLICACIONES INFORMÁTICAS**	**PORTALES WEB**
Base Alfanumérica ☐ Base Binaria ☐ Base Espacial ☐			

Resultado/Observaciones

……

……

……....

_____ _____

(f) Responsable **Sello de verificación**