ESCUELA SUPERIOR POLITECNICA DEL LITORAL

FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN

MAESTRÍA EN SEGURIDAD INFORMATICA APLICADA (MSIA)

Tema:

"DESARROLLO DEL ESQUEMA DE SEGURIDAD, PLAN DE RECUPERACIÓN ANTE DESASTRES INFORMÁTICOS Y SOLUCIÓN PARA EL NIVEL DE EXPOSICIÓN DE AMENAZAS Y VULNERABILIDADES APLICADA A LOS SERVIDORES Y EQUIPOS DE COMUNICACIÓN DEL CENTRO DE DATOS DE LA MUNICIPALIDAD DE LA CIUDAD DEL ESTE."

TESIS DE GRADO

Previa a la obtención del Título de:

MAGÍSTER EN SEGURIDAD INFORMÁTICA APLICADA

Presentada por:

LSI. DANIEL IVÁN QUIRUMBAY YAGUAL

GUAYAQUIL – ECUADOR

AÑO: 2015

AGRADECIMIENTO

Agradezco a Dios y a cada uno de los profesores de esta maestría que fueron guías esenciales en el desarrollo y culminación de esta nueva meta profesional.

DEDICATORIA

Este trabajo está dedicado a mi familia, a mi esposa e hijos, así como también a mis Padres, Suegros y Hermanos quienes han sido los pilares fundamentales de apoyo a la obtención de este logro profesional.

TRIBUNAL DE GRADUACIÓN

_____	_____
Msig. Robert Andrade	**Msig. Albert Espinal**
DIRECTOR DE LA TESIS	**MIEMBRO PRINCIPAL**

DECLARACIÓN EXPRESA

“ La responsabilidad del contenido de esta Tesis de Grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL.“

(Reglamento de Graduación de la ESPOL.)

_____

Lsi. Daniel Iván Quirumbay Yagual

RESUMEN

Este documento identifica una propuesta para implementar un plan piloto de recuperación de desastres y respaldo que sea viable y factible;encaso de que ocurra algún tipo de incidente la Institución pueda poner en operatividad el Plan, ayudando inmediatamente a la reactivación y funcionamiento de todos sus sistemas informáticos, redes y servidores de manera oportunaminimizando costos.

Conjuntamente se realizó un análisis de Riesgo y Vulnerabilidades al área TIC’s del Municipio, que permita ver resultados eidentificar unacorrecta y oportuna preparación al personal demostrando un empoderamiento de sus responsabilidades y saber cómo actuar ante amenazaso siniestrosinformáticos a la que se está expuesto hoy en día toda Institución Pública.

Además se diseñópolíticas, normas y procedimientos de protección de datos y recursos informáticos basados en estándares ISO, permitiendo minimizar los riesgos de los activos físicos y lógicos informáticos más críticos de la Institución.

Finalmente el aporte profesional que se realiza a esta Institución Pública, está enfocado a optimar recursos tecnológicos y económicos, utilizando software adecuados como medios de soporte para la ejecución y continuidad del Sistema de Seguridad Institucional.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ABREVIATURAS Y SIMBOLOGÍA

AS/NZS	Estándar Australiano/Neozelandés
Ciberataque	Ataque Informático
DBA	Administrador de la Base de Datos
DMZ	Zona desmilitarizada
DNS	Sistema de nombres de Dominio
Firewall	Corta fuego o pared de fuego
FTP	Protocolo de Transferencia de Archivos
Full Duplex	En redes: transmisión y recepción de datos simultáneos
GPL	Licencia Pública General
IDS	Sistema de Detección de Intrusos
IPS	Sistema de Prevención de Intrusos
ISO/IEC	Organización de Estándares Internacionales /Comisión Electrotécnica Internacional
NIST	Instituto Nacional de Estándares y Tecnología
NMAP	Rastreo de puertos escrito originalmente por Gordon Lyon
Pentesting	Método mediante el cual se evalúa la seguridad de un sistema informático, mediante un ataque simulado.
TICs	Tecnología de la Información y la Comunicación
Wireshark	Analizador de Tráfico en la red

INTRODUCCIÓN

Este documento contiene la realización del análisis de riesgos, amenazas y vulnerabilidades al área tecnológica del Municipio de la Ciudad del Este, permitiendo garantizar la integridad y disponibilidad de la información, basado en un estudio previo de posibles amenazas utilizando como guía la normativa AS/NZS ISO 31000:2009 de riesgos Informáticos.

La detección de vulnerabilidades basada en la técnica de ethical hacking y la utilización de herramientas de Pentesting, permite salvaguardar los sistemas informáticos de cualquier amenaza sea esta interna o externa a la que hoy en día se encuentra expuesta toda Institución Pública, para dar solución a toda inseguridad detectada con el objetivo de minimizar el riesgo y su impacto económico.

El desarrollo de un plan de recuperación de desastres y respaldo de la información permite establecer responsabilidades a los usuarios dueños de los procesos y tener la capacidad operacional para la recuperación inmediata ante cualquier incidente que suceda en la institución

Finalmente la implementación dela política de seguridadalineadabajo la guía del estándar Británico ISO/IEC 27002:2013, se orienta específicamente a una institución pública municipal, permite entonces enfocarse a la capacitación y socialización de buenas prácticas del manejo de Servicios y equipos tecnológicos pertenecientes a la institución.

CAPÍTULO 1

1. ANTECEDENTES Y DIAGNÓSTICO DE LA INFRAESTRUCTURA DE TIC.

1.1. ANTECEDENTES

La Ciudad del Este a consecuencia del crecimiento notable de la población fue elevado a parroquia rural del Cantón Santa María el 11 de diciembre de 1935, luego cuando la población de la parroquia Salinas se cantonizó, La Ciudad del Este se convirtió en parroquia de esta localidad en 1937.

El crecimiento poblacional y económico fue acelerado gracias a la exportación del petróleo, esto hizo que se desarrolle rápidamente y el 14 de abril de 1993, “Ciudad del Este” se convirtió oficialmente en Cantón de la Provincia de Santa María mediante Decreto No. 23 publicado en el Registro Oficial No. 168 del 14 de abril de 1.993, con una superficie de 25,6 Km2.

Una vez convertida la Ciudad del Este en cantón fue el inicio de la Ilustre Municipalidad Ciudad del Este, la Constitución de la República del Ecuador aprobada en el 2008 da la apertura a nuevos esquemas de descentralización planteados por el gobierno actual a través de la Constitución Política, los Municipios de los Cantones de cada una de las Provincias, componentes de la división política del Ecuador, ahora se denominan “Gobiernos Autónomos Descentralizados (GAD´s) ” y tienen competencias exclusivas en planificación territorial, obras públicas y movilidad.

Estos Gobiernos Autónomos Descentralizados gozan de autonomía política, administrativa y financiera, y se deben regir a los principios de solidaridad, subsidiariedad, equidad interterritorial, integración y participación ciudadana. Actualmente está establecido en la Constitución de la República del Ecuador que los Gobiernos Autónomos Descentralizados deben generar sus propios recursos financieros, conjuntamente también participarán de las rentas del

Estado; además, se prevé que participen de al menos el quince por ciento de ingresos permanentes y de un monto no inferior al cinco por ciento de los no permanentes correspondientes al Estado Central. Los principios que rigen estas participaciones son: asignaciones anuales que sean predecibles, directas, oportunas y automáticas

Los criterios para la distribución de los recursos entre los Gobiernos Autónomos Descentralizados son los siguientes:

1. Tamaño y densidad de la población.
2. Necesidades básicas insatisfechas, jerarquizadas y consideradas en relación con la población residente en el territorio de cada uno de los Gobiernos Autónomos Descentralizados.
3. Logros en el mejoramiento de los niveles de vida, esfuerzo fiscal y administrativo, y cumplimiento de metas del Plan Nacional de Desarrollo y del plan de desarrollo del Gobierno Autónomo Descentralizado.

1.2. MISIÓN

Somos un gobierno local líder, que promueve el desarrollo humano sostenible, entregando a la comunidad servicios de calidad y calidez; con tal

propósito desarrolla una gestión eficiente, transparente y participativa; contribuyendo de esta manera, al bienestar material y espiritual de la colectividad.

1.3. VISIÓN

El Gobierno Autónomo Descentralizado Municipal del Cantón Ciudad del Este, con la participación activa de la ciudadanía y la planificación articulada con los distintos o iguales niveles de gobierno, contribuirá a construir un modelo de desarrollo humano sostenible y equitativo, que privilegia la consecución del buen vivir; constituyéndose de esta manera, en el motor del progreso Cantonal y Provincial. Su talento humano es solidario, altamente competitivo, honesto y comprometido con su institución y su cantón.

1.4. OBJETIVOS GENERALES

Mejorar la calidad de vida del Cantón Ciudad del Este garantizando el ejercicio de los derechos de la ciudadanía, en iguales condiciones, mediante la capacitación e integración familiar en un ambiente social, aplicando políticas de manejo ambiental, conservando los espacios naturales y desarrollndo actividades sosteniblemente que garanticen el buen vivir de las

ciudadanas y ciudadanos de este cantón, a través de la ejecución de proyectos de biodiversidad.

1.5. DESCRIPCIÓN DEL PROBLEMA

La rápida evolución informática en estos tiempos requiere que todas las organizaciones privadas y estatales adopten un conjunto mínimo de controles de seguridad para proteger sus sistemas de información. En vista de esta situación el GAD Municipal del Cantón Ciudad del Este tiene la necesidad de implementar políticas y normas de seguridad basados en estándares que permita regular los servicios que ofrece a través de todo el equipo tecnológico utilizado en la Institución Municipal.

La falta de estos controles de seguridad informática causan que esta área se encuentre expuesta a un nivel de amenaza muy alto que a su vez pudiera provocar la pérdida de información crítica y originar la paralización de todos los servicios que ofrece la institución, adicionalmente es importante destacar que las Instituciones Públicas dispongan además de un Plan de Recuperación ante Desastres que permita de una manera oportuna y optima mantener la continuidad operativa y que sea aplicable específicamente al Centro de Procesamiento de Datos Municipal.

1.6. Solución Propuesta

Como solución se propone implementar un plan de recuperación ante desastres que sea viable y factible, y en caso de que ocurra algún tipo de incidente, el GAD Municipal pueda poner en operatividad el Plan que permita ayudar a la reactivación del funcionamiento de todos sus sistemas informáticos, redes y servidores.

Conjuntamente se propone diseñar, implantar y mantener políticas, normas y procedimientos de protección de datos y recursos informáticos basados en estándares internacionales que minimicen los riesgos de los activos físicos y lógicos informáticos más críticos de la Institución, además de implementar medidas de seguridad en el Centro de Datos que mitiguen las vulnerabilidades y amenazas informáticas a la que se está expuesto todo equipo informático.

1.7. Evaluación de la Infraestructura Tecnológica y Software

El GAD Municipal del Cantón Ciudad del Este, actualmente cuenta con una infraestructura básica, estable y robusta que le permite estar a la vanguardia en el desarrollo tecnológico que ésta demanda, con el fin de ofrecer un buen

servicio a la comunidad de una forma óptima y ágil, tal y como se detalla a continuación en cada una de las descripciones técnicas.

1.7.1. Hardware

El crecimiento continuo de la Institución en estos últimos años ha permitido generar grandes cambios en el área del Centro de Procesamiento de Datos Municipal, actualmente cuenta con su propio espacio físico y sistema de enfriamiento. Los equipos Informáticos tales como Servidores Datos, Voz y Video son mantenidos gracias al constante Mantenimiento preventivo y actualización de Software al que son sometidos, para que de esta manera garanticen la continuidad de la gestión administrativa y se pueda brindar un servicio de excelente calidad a la comunidad.

El Centro de Procesamiento de Datos cuenta con Servidores de la línea de IBM y HP, los mismos que cumplen distinto roles para brindar los servicios de base de datos, internet, correo electrónico, respaldo, entre otros.

1.7.1.1. Roles

Rol de Servidores	Sistema Operativo
Servidor de Base de Datos	Windows 2003 Server R2
Servidor de Aplicaciones2	
Server de Aplicaciones 1	Linux Centos 5.3
Server Web	
Server de Respaldo	
Server DNS	
Servidor de Impresiones	
Server de Correo Electrónico	
Server Proxy	
Server Firewall	
Server FTP	
Server PBX	Software Libre

Tabla 1-1. Roles

En la Institución se promueve la utilización del software libre tanto en los servidores y los equipos de oficina, generando de esta manera un ahorro considerable en la compra de licencias y como se observa en la tabla 1-1 Roles la mayoría de los Servidores de Datos poseen este tipo de Software.

Es importante recalcar que los Sistema Operativos con Licencia y que cumplen un rol especifico, son utilizados por que aún no se han encontrado dentro de la paquetería Software Libre algún aplicativo que los reemplace.

1.7.1.2. Características de Servidores

ROL	MARCA	MODELO	PROCESADOR		Tipo de Tarjeta de Red	MEMORIA RAM	Características Disco Duro
			Tipo	# Núcleos			
APLICACIONES 1	IBM	System X3200 M2	1Xeon 3.0 Ghz.	2	1 Gbps	6 GB.	Disco 1: 250GB.
APLICACIONES 2	IBM	System X3650	1Xeon 2.0 Ghz.	2	1 Gbps	4 GB.	Disco 1: 300Gb Disco 500Gb. Disco3: 1 TB.
WEB	HP	Proliant ML 150 G2	2 Xeon 3.2 Ghz.	4	1 Gbps	8 GB.	Disco1: 250Gb. Disco2: 250Gb.
Base de Datos	HP	Proliant ML 370 G3	1 Xeon 3.06 Ghz.	1	1 Gbps	4 GB.	Disco1:146.8 Disco2: 36.4 Disco3: 36.4
Server Backup	IOMEGA	NAS 450R	1 Xeon 1.86 Ghz.	2	1 Gbps	2 GB.	Cuatro Disco:500 Gb.
Server PBX	DENWA	DENWA MICRO	1 Intel 1.8 Ghz.	2	Dual Gigabit Ethernet	1GB.	32GB.
Server DNS y FTP	PC Clon Genérico	ATX Tower	1 QuadCore 2.33 Ghz.	2	1 Gbps	3 GB.	Disco: 500Gb.

Server Proxy-Firewall	PC Clon Genérico	ATX Tower	1QuadCore 2.33 Ghz.	2	1 Gbps	4 GB.	Disco: 500Gb.

Tabla 1-2.Características de Servidores

Cabe indicar que en la actualidad el Centro Procesamiento de Datos cuenta con un UPS de 10 KVA monofásico que mantiene la continuidad de la energía eléctrica cuando existen los cortes imprevistos de la misma. Además de que se cuenta con un generador trifásico 200 KW 208-120V, con un transformador 400 KVA, 13200/208-120V que mantiene la continuidad de energía eléctrica al Centro de Procesamiento de Datos Municipal de los cortes de energía repentinos que sufre la Ciudad.

1.7.2. Software

El equipamiento lógico o Sistemas Informáticos con la que cuenta el Municipio se centra específicamente en las siguientes plataformas que enlistamos en la Tabla 1-3.Catálogos de Sistemas Informáticos

1.7.2.1. Catálogo de Sistemas Informáticos

Sistema	S.O.	Plataforma	Función	Transaccionabilidad
Sistema de Gestión Municipal	Linux CentOS 5.3	Oracle 10g	Sistema de Información para la Gestión Administrativa de todo el Municipio, los módulos son los siguientes: Ordenes de Pago, Control de Multas, bodega, Catastro, Coactiva, Seguridad y Control, Terrenos, Contabilidad, Planificación, Presupuesto, Nomina, Rentas, Recaudación, Centro Medico	MEDIA- ALTA

SITAC (SISTEMA INTEGRADO DE TRIBUTACION ASESOR CONTABLE)	Windows 2003 Server	FOXPRO	Software diseñado para exigencias tributarios, con este sistema puedes obtener lo siguiente: - anexos transaccionales y reoc - formularios 103. 104. 107	MEDIA ALTA
Sistema de Información Registral (SIRE)	Windows 2003 Server	Visual Studio y Access.	Sistema de control de los cambios en la información de dominios que experimenta un bien inmueble registrado dentro del Cantón.	MEDIA

Tabla 1-3.Catálogos de Sistemas Informáticos

Categorización de la Transacionabilidad de las operaciones	
ALTA	Aproximadamente 80,000 Transacciones
MEDIA-ALTA	Aproximadamente 50,000 Transacciones
MEDIA	Menores a 50,000 transacciones

Tabla 1-4. Categorización de la Transacionabilidad de las operaciones

Cabe mencionar que el Sistema Municipal fue desarrollado por personal que laboró en el mismo Municipio en el año 2002 y actualmente se realiza mantenimiento a la Base de Datos y actualizaciones de acuerdo como se vaya reformando las ordenanzas o leyes gubernamentales.

1.8. Evaluación de la Infraestructura de Red

Actualmente la Institución Pública cuenta con una infraestructura de Red confiable, que permite agilitar la gestión administrativa, a través de la RED LAN y MAN, mantiene enlaces de datos desde varias dependencias internas y externas del GAD Municipal, de las cuales se describe en la continuidad del documento.

1.8.1. Red LAN

En lo que concierne a la Red LAN, el Municipio cuenta con un cableado estructurado certificado de 25 años por los tipos de conectividad y sistema de cableado, cuya marca del cable UTP utilizado es “Signamax” de categoría 6 solido con una velocidad de transmisión de 10/100/1000 Mbps, que garantiza la fiabilidad en conectividad de la estructura informática, permitiendo acceder a los servicios y recursos de forma rápida y segura.

En relación a la Certificación del Cableado Estructurado instalada en todo el Edificio se evaluaron los siguientes parámetros tanto para los puntos de datos, como de voz.

- Diafonía
- Perdida de Retorno
- Atenuación
- ACR
- ELFEXT
- Diafonía power sum
- Power Sum ACR
- ELFEXT Power Sum

Estándares Aplicados:

IEEE 802.3 10 BaseT

IEEE802.3u 100BaseTX

IEEE 802.3ab 1000BaseT

IEEE 802.3 z 1000BaseSX

IEEE 802.3z 1000BaseLX

IEEE 802.3x Flow Control

Cantidad de Puntos de Red Certificados e instalados en los dos Edificios Administrativos:

- Por dato Edificio Principal: 210 puntos
- Por voz Edificio Principal: 210 puntos
- Por dato Edificio Segundo: 28 Puntos
- Por voz Edificio Segundo: 28 Puntos

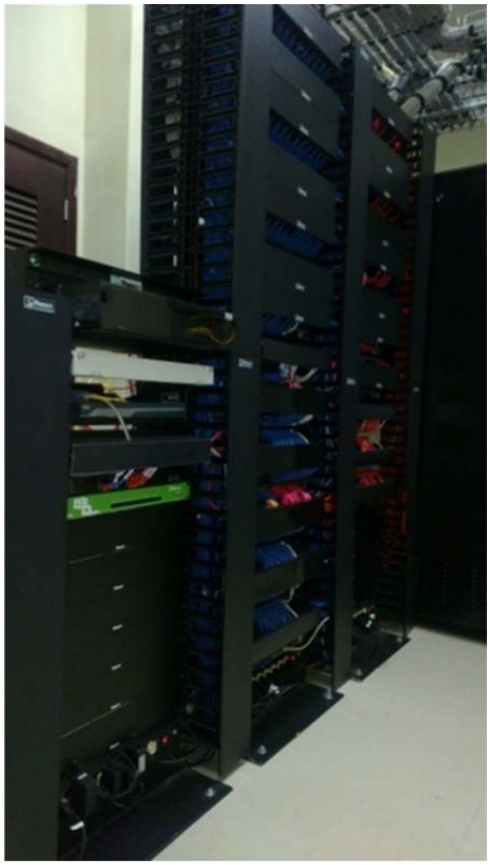


Figura 1-1. Cableado Estructurado del Centro de Procesamiento de Datos

1.8.1.1. Características del Cable UTP

Tipo de Cable	Descripción General
	**RENDIMIENTO DE TRANSMISIÓN:** ANSI/TIA/EIA-568-C.2: supera la categoría 6 (1-250MHz) ISO / IEC 11801, CENELEC EN 50173: supera la categoría 6 (1-250 MHz) **COMPORTAMIENTO:** Impedancia: 125 Ohm ± 20% @ 64 kHz **CONDUCTOR:** Material de cobre desnudo Tamaño 23 AWG, 1000Ft. **FUNDA:** PVC CMR material Media Espesor: 0,50 mm (0,020 in), min en cualquier punto: 0,40 mm (0,016 in) Diámetro 6,3 ± 0,3 mm (0,25 ± 0,01 in) Color de 7 colores estándar
Cable Categoria 6-4pares UTP solido	

Tabla 1-5. Características del Cable UTP

1.8.1.2. Acceso al Internet

En la actualidad el servicio de internet es facilitado por la Corporación Nacional de Telecomunicaciones(CNT) que a través de una línea de Fibra de tipo dedicada 1:1, monomodo, con un ancho de banda de 6 Mbps es conectado a través de un Servidor Proxy con el Sistema Operativo CentOS versión 5.3 que a través del servicio de Nateo o encaminamiento de paquetes es enviado a la red LAN de la Institución para que todas las máquinas clientes pueda obtener el servicio de internet, así como también los departamentos que se encuentran en puntos remotos.

1.8.1.3. Topología

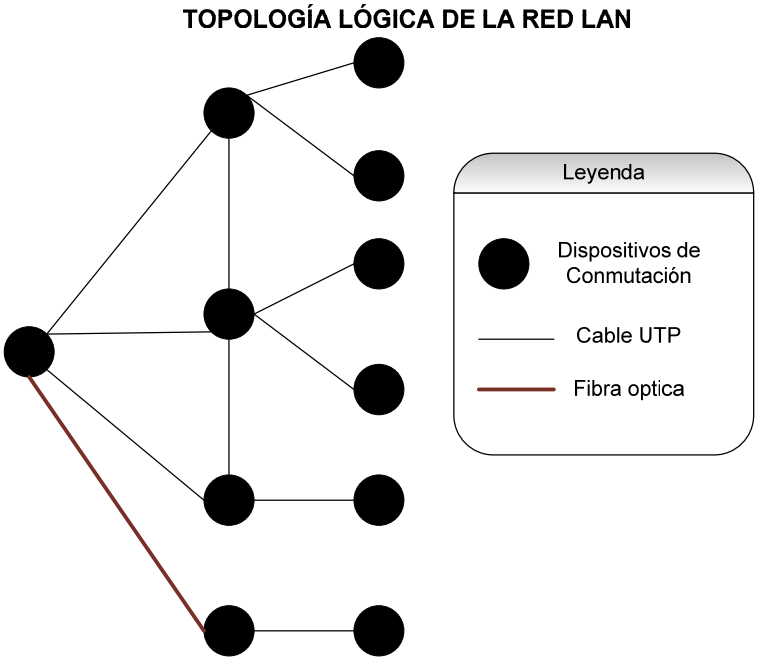


Figura 1-2. Topología lógica de la Red LAN

Tal como se puede visualizar en la Figura 2, el tipo de topología utilizado es el Tipo Estrella, el mismo que le permite una comunicación rápida y redundante entre cada uno de los piso del edificio Municipal, capaz de tener un rendimiento alto y totalmente disponible al momento de realizar alguna transacción.

Debido a la existencia de dos edificios contiguos, la conectividad entre edificios Municipales está realizada a través de fibra óptica Monomodo y fusionados en un organizador de fibra en ambos extremos de conexión, con 6 hilos activos de las cuales 2 son para transmisión de datos y dos para transmisión de voz ambos transmiten a 1000Base BX, quedando 2 puntos de respaldo.

Figura 1-3. Organizador de Fibra Óptica Edificio Principal

Figura 1-4. Organizador de Fibra Óptica Edificio Segundo

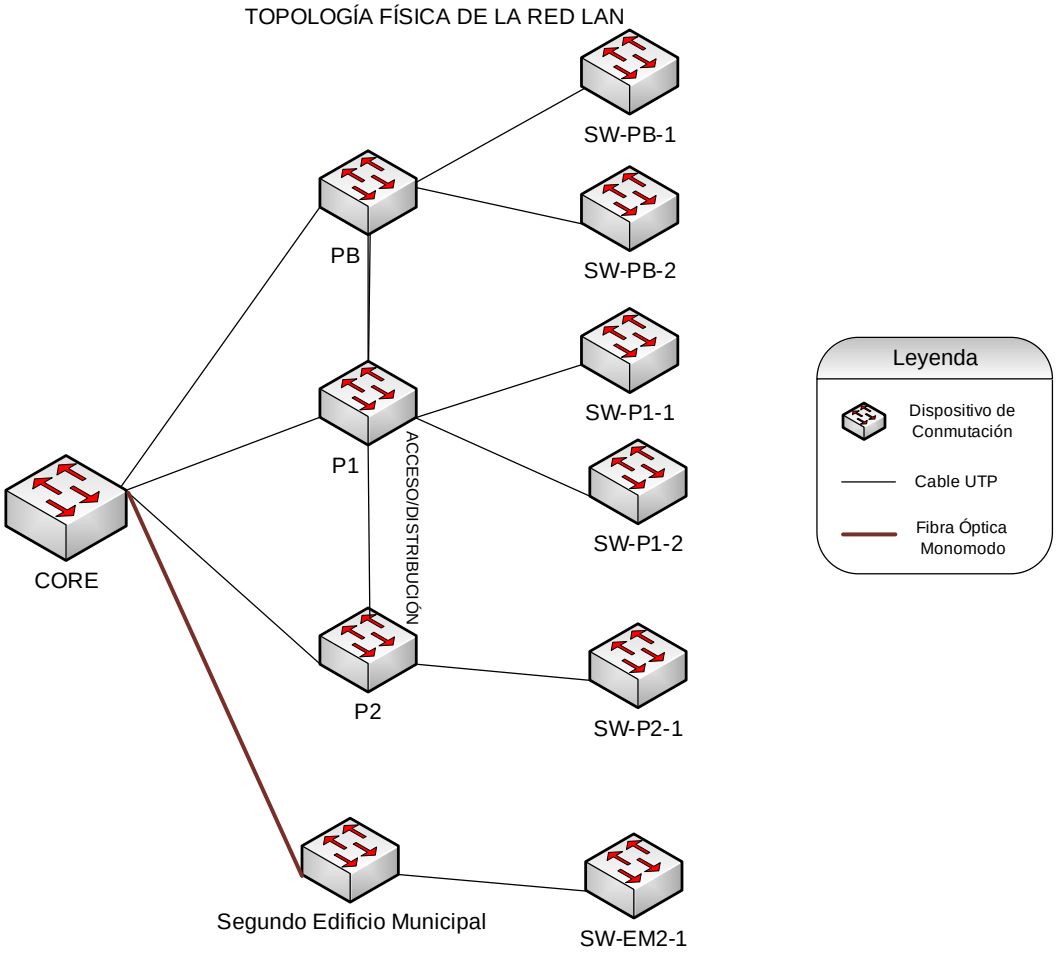


Figura1-5. Topología física de la Red LAN

Como se observará en la Figura 5, la red LAN se divide en cuatro sub redes principales, Planta Baja, Primer Piso, Segundo Piso y Segundo Edificio Administrativo que son administrados a través de redes segmentadas. La velocidad de transmisión de esta red es de 1000 Mbps y la Categoría del Cable es de tipo 6. Solo en la interconexión del Core y el Segundo Edificio es por Fibra Óptica.

1.8.1.4. Dispositivos de Conmutación

Todos los dispositivos de conmutación con los que cuenta el Municipio de Ciudad del Este se encuentra distribuidos en la capa Core, Capa Distribución y Capa de Acceso, de las cuales se pasan a detallar en la siguiente forma:

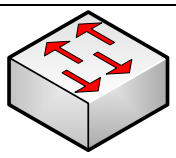
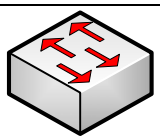
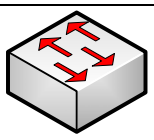
Capa Core	Capa Distribución	Capa de Acceso
 CORE	 PB	 SW-PB-1
Switch Administrables TP-LINK TL-SG3424	Switch Administrables ZyXel - GS1910-24	Switch UNICOM SMART GST2402

Tabla 1-6. Dispositivos de Conmutación

1.8.1.5. Características de Equipos

Figura 1-6. SWTICH TP-LINK MANAGER TL-SG3424

Descripción General	
Interfaces: 24 puertos RJ45 a 10/100/1000 Mbps (Negociación automática, MDI/MDIX automático) 4 slots SFP combo a 100/1000 Mbps* 1 puerto de consola **Ancho de banda/Backplane:** 48Gbps **Tabla de direcciones MAC:**8K **VLAN:** Soporte IEEE802.1Q con 4000 grupos VLAN y 4000 VIDs VLAN basada en puerto/MAC/protocolo GARP/GVRP	**Listas de Control de Acceso:** Filtrado de paquetes L2～L4 basado en el origen y destino de las direcciones MAC, IP, puertos TCP/UDP, 802.1p, DSCP, protocolo e identificador VLAN **Seguridades:** Vinculación IP-MAC-puerto-VID Autenticación según puerto IEEE 802.1X/MAC, Radius, VLAN para invitados Defensa contra ataques DoS Inspección ARP dinámica (DAI) SSH v1/v2 SSL v2/v3/TLSv1

Tabla 1-7. Dispositivos de Conmutación 1

Figura 1-7. SWITCH ZyXel - GS1910-24

Descripción General	
Gestión de Red: Gestión basada en web, SNMP v1, v2c, v3, Grupos RMON 1, 2, 3, 9, NTPv4,Relé DHCP, Syslog, Duplicación de puertos, DNS, sFlow **Gestión y QoS de tráfico:** VLAN basada en puerto, VLAN basada en MAC VLAN basada en protocolo- IEEE 802.1Q	**Seguridades:** IEEE 802.1x, Seguridad Portuaria, Autenticación MAC, Límite de direcciones MAC, Layer 2 filtrado MAC, Filtrado IP de nivel 3,Capa 4 filtrado socket TCP / UDP, Guardia BPDU, Reenvío MAC estática, Múltiples servidores RADIUS, Varios servidores TACACS +, RADIUS, TACACS + ,SSL, Snooping DHCP, Inspección ARP ,UPNP, Filtrado de paquetes ACL

Figura 1-8. UNICOM SMART GST2402G

Descripción General	
• Velocidad de Transmisión 10/100/1000	• IGMP Snooping • Port mirroring

• Gestión de red SNMP • Static VLANs • GVRP • VLAN tagging	• Port security.

Tabla 1-8. Dispositivos de Conmutación 2

1.8.1.6. Dispositivo de Enrutamiento

Equipo

Figura 1-9. Router Cisco 1841
Descripción General
Memoria RAM: 256 MB (instalados) / 38 4 MB (máx.) - SDRAM Memoria Flash: 64 MB (instalados) / 128 MB (máx.) **Conexión de Redes** Ethernet, Fast Ethernet IPSec SNMP Protección firewall, criptografía 128 bits, cifrado del hardware, VPN, soporte

VLAN, Sistema de prevención de intrusiones (IPS), cifrado de 256 bits **Sistema Operativo,** Cisco IOS Advanced Security

Tabla 1-9. Dispositivo de Enrutamiento

1.8.2. Red MAN

Todas las conexiones que se realicen de forma inalámbrica a través de equipos de comunicación a una distancia mínima de 200 mts. hasta una distancia máxima de 3 Km aproximadamente, es identificado como una Red Metropolitana para el Municipio de la Ciudad del ESTE, por tal motivo se ha considerado identificar mediante la Figura 10 la siguiente información.

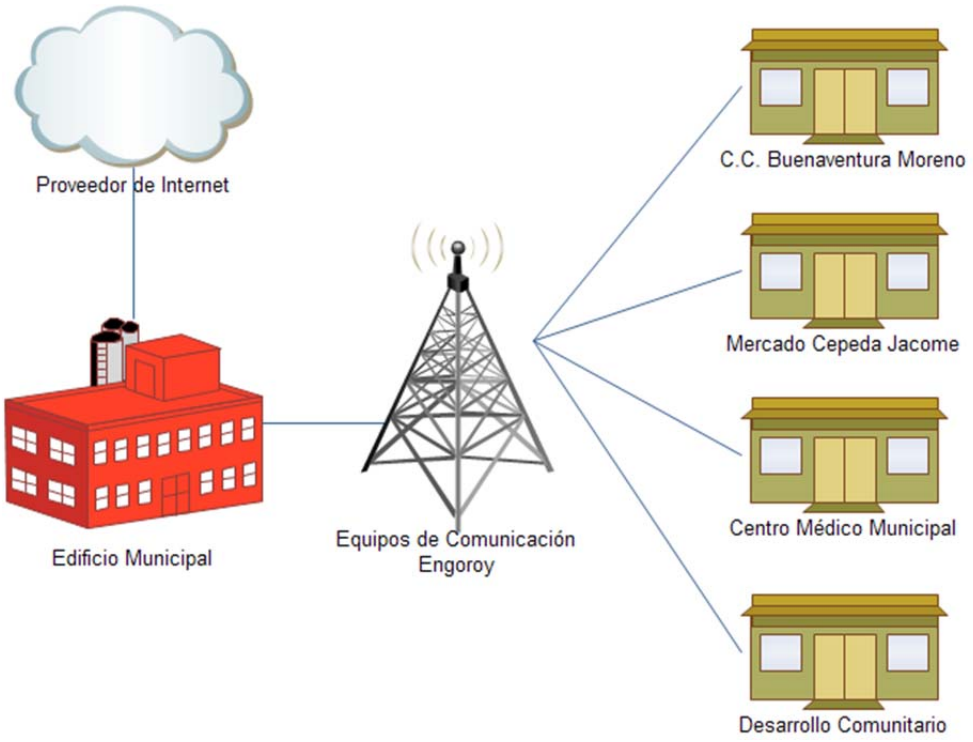


Figura 1-10. Red MAN

1.8.2.1. Arquitectura de la Red MAN

La existencia de oficinas corporativas cercanas en una ciudad, genera la presencia de este tipo de arquitectura dentro de la Institución, para esto se cuenta con un nodo de retransmisión de datos ubicada en el Cerro de nombre Engoroy que permite la conexión con 4 oficinas externas que pertenecen al Municipio.

Esta red privada cuya distancia entre nodo de conexión no es mayor 2.5 milla (4 Kms), medio de comunicación se realiza a través de equipos de Radio frecuencia de 2.4 a 5 Ghz. A continuación se muestra una gráfica detallando la forma de Comunicación en la Red MAN y la recepción del Servicio de Internet, dando una visión global a fin de posteriormente determinar los puntos de riesgo y debilidades tecnológicas a nivel de la infraestructura.

Arquitectura de RED Metropolitana

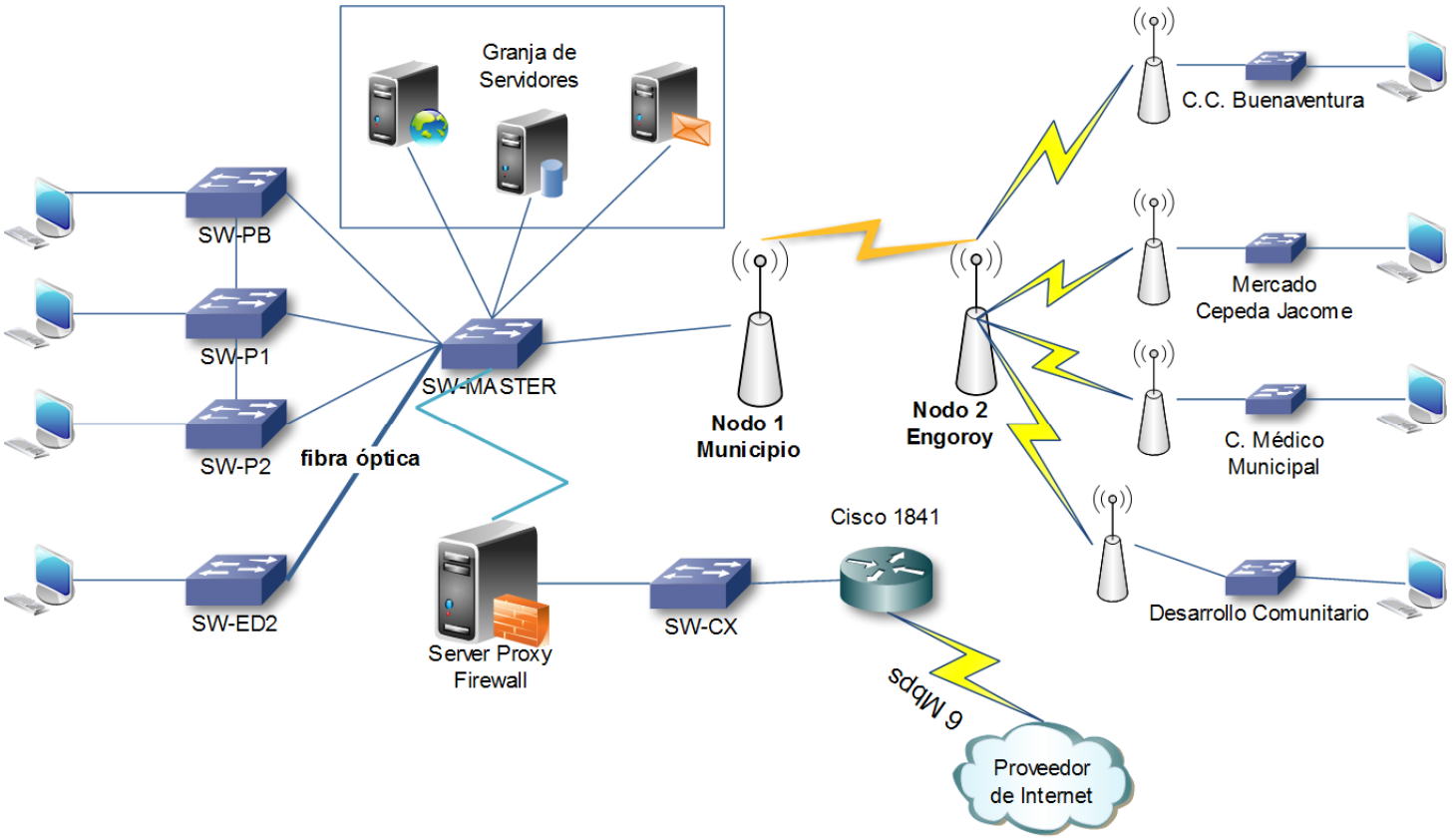


Figura 1-11. Arquitectura de Red Metropolitana

1.8.2.2. Dispositivos de Radio Enlace

Equipo

Figura 1-12. Airmax5N
Descripción General y Ubicación
Hardware *1 Puerto LAN 10/100Mbps compatible con estándar IEEE802.3af,* *AUTO MDI/MDI-X* *8MB Flash, 32MB SDRAM* *Carcasa resistente al agua y radiaciones UV* ***Antena*** *Incluye antena direccional 14dBi* *Angulo de emisión: 30 grados sobre plano vertical y horizontal* *R-SMA conector para antenna externa* ***Modos de funcionamiento*** *Soporta Modo Cliente,ModoAP,Modo Bridge WDS, Modo* *Repetidor, Bridge, Infrastructura ,Router y WISP* ***Seguridad*** *Soporte 802.1x Radius, Soporte WPA con PSK/TKIP/AES ,WPA2* ***Ubicación:*** *Enlace Municipio- Centro de Datos Engoroy*

Tabla 1-10. Dispositivo de Radio Enlace 1

Equipo


Figura 1-13. CanopyBackhaul 5.7 Ghz 5700bh20

Descripción General y Ubicación	
Description	5.7 GHz Backhaul, 20 Mb
CanopyPartNumber	5700BH20USG
MarketAvailability	North America, Europe, South America, Asia
SignalingRate	20 Mbps
Typical LOS Range	1 mi (1.6 km)
TypicalAggregateUsefulThroughput	14.0 Mbps
Frequencyrange of band	ISM 5725-5850 MHz
Non-overlappingChannels	3
ChannelWidth	20 MHz
ChannelSpacing	every 5 MHz
Encryption	DES capable
ProtocolsUsed	IPV4, UDP, TCP, ICMP, Telnet, HTTP, FTP, SNMP
Network Management	HTTP, TELNET, FTP, SNMP Version 2c
Ubicación:	
Enlace Centro de Desarrollo Humano(CDH) y Centro de Comunicaciones Engoroy	

Tabla 1-11. Dispositivo de Radio Enlace 2

Equipo

Figura 1-14. Ubiquiti NS2 NanoStation2 2.4 GHz 10dBi 400mW
• Processor Specs - Atheros AR2315 SOC, MIPS 4KC, 180MHz • Memory Information - 16MB SDRAM, 4MB Flash • Networking Interface - 1 X 10/100 BASE-TX (Cat. 5, RJ-45) Ethernet Interface • Wireless Approvals - FCC Part 15.247, IC RS210 • RoHS Compliance - Yes • Antenna - Integrated 10dBi Dual Pol + External RP-SMA • Outdoor Range - over 15km **Ubicación:** Enlace Centro de Comunicaciones Engoroy y Centro Comercial Buenaventura

Tabla 1-12. Dispositivo de Radio Enlace 2

1.9. Seguridad de la Información

1.9.1. Introducción

La seguridad de los datos para una Institución Pública es fundamental, debido que la divulgación de la información puede ocurrir a través de publicaciones en redes sociales, correo electrónico o a través de filtración de información por parte de los empleados.

El costo de las infracciones de seguridad de datos, en términos monetarios y de credibilidad de las Institución siempre es muy alto, por tanto es necesario considerar soluciones integrales a esta problemática para el beneficio de la Institución.

EL GAD Municipal cuenta con las seguridades básicas y con configuraciones de equipos de comunicación personalizadas necesarias para garantizar la integridad de los datos, es importante identificar que el concepto de “Seguridad de la Información” no debe ser confundido con el de “Seguridad Informática”, ya que este último sólo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas.

1.9.2. Seguridad Perimetral e Interna

La seguridad lógica sea esta interna o externa son aspectos fundamentales a tener en cuenta dentro del Municipio, así como también el disponer de los equipos y configuraciones necesarias para dar la debida seguridad de la información.

El filtrado de Paquetes se realiza a través de un servidor con sistema operativo CentOS 5.3 que tiene configurado el Servicio de firewall a través del software “Shorewall” que permite que el equipo se convierta en un Cortafuego lógico y pueda prestarlas debida seguridad y salvaguardar la integridad de la información de la red LAN

1.9.3. Firewall Lógico

En la actualidad el software firewall Shorewall, es una herramienta de alto nivel para la configuración de Netfilter y permite la configuración de un firewall de host, de un servidor, un firewall enrutador, y lograr manejar complejas configuraciones. Esta herramienta cuenta con soporte para IPV4 e IPV6.

1.9.4. DMZ

DMZ (zona desmilitarizada) es un diseño conceptual de red donde los servidores de acceso público se colocan en un segmento de red aislado. La intención de DMZ es asegurar que los servidores de acceso público no puedan comunicarse con otros segmentos de la red interna, en el caso de que un servidor se encuentre comprometido., tal es el caso del Servidor de Correo electrónico, Servidor de Pagina Web y el Servidor de respaldo, cabe recalcar que las empresas por lo general al momento de ingresar un empleado, establece acuerdos de confianza y niveles de acceso controlados, sin embargo si se presentara algún intento de acceso no autorizado hacia LAN (red interna) estos son bloqueados por el firewall.

A continuación se observa a través de la siguiente Figura la estructura lógica de cómo se encuentra instalados los equipos de seguridad de la institución:

1.9.5. Diseño lógico del DMZ

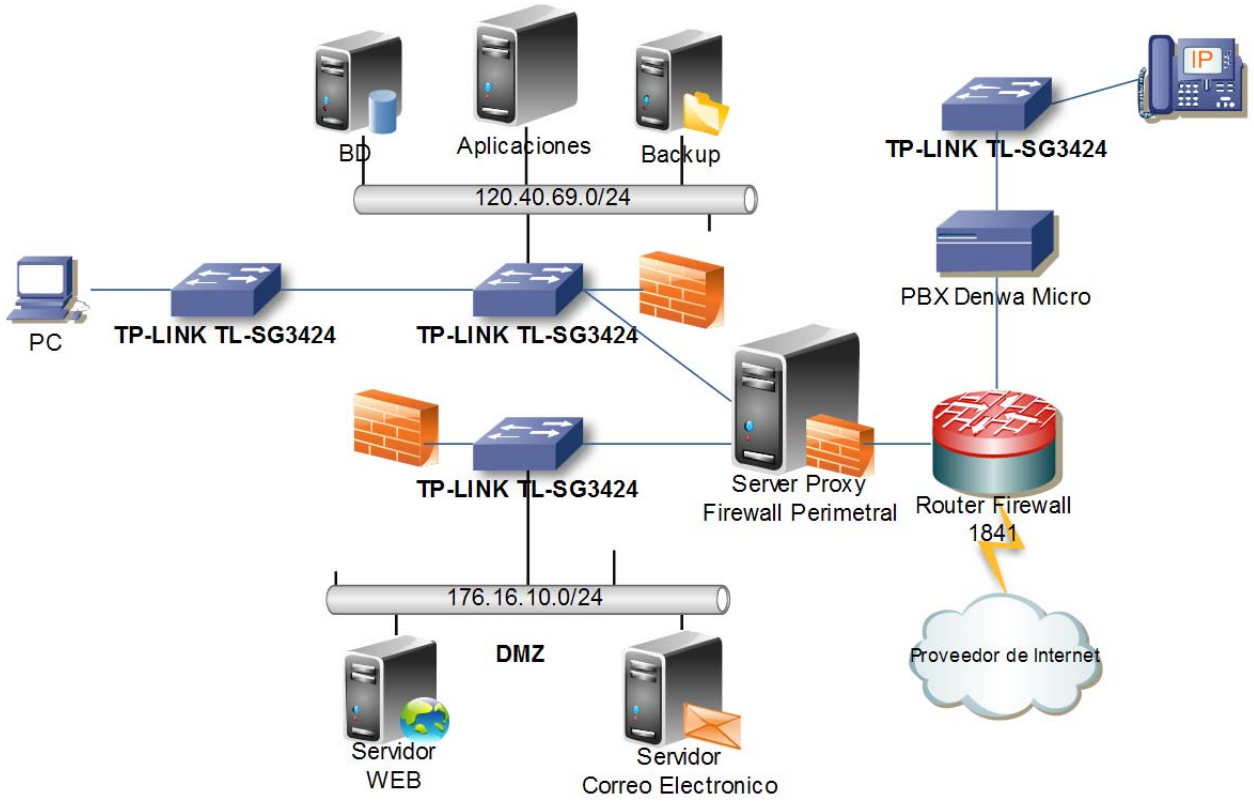


Figura1-15. Diseño Lógico del DMZ

CAPÍTULO 2

2. MARCO TEÓRICO.

2.1. Introducción

El Implementar Seguridad Informática a las infraestructuras Tecnológicas específicamente para el Centro de Procesamiento de Datos se ha convertido en necesarias debido a que si se logra estimar la frecuencia con la cual se materializan los riesgos o vulnerabilidades, así como determinar la magnitud de sus posibles consecuencias considerando las debidas precauciones,

podemos de modo preventivo tomar medidas para reducir su impacto y evitar la paralización de las organizaciones o empresas.

Con la realización de un análisis de riesgo informático como también la Implantación de Políticas de Seguridad basados en estándares ISO(Organización Internacional por la Normalización)se puede identificar fácilmente sus vulnerabilidades y amenazas a la que se encuentra expuesta, permitiendo a las organizaciones o empresas minimizar pérdidas económicas y maximizar oportunidades de negocio dentro de los parámetros de una Institución Pública.

Conocedores de que la tecnología de la información actual facilita las operaciones de negocio, es necesario considerar siempre que aquellas tecnologías pueden presentar riesgos que causan que la información se pierda o se modifique perjudicando a los interesados. Entre las amenazas que pueden aumentar el riesgo de una Institución depende de la zona donde se encuentre ubicada, para este caso se está analizando los siguientes: cortes de energía eléctrica, ciberataques, sucesos de origen físico, negligencia o decisiones institucionales, entre otros.

2.2. Análisis del Riesgo del Sistema de Información

El Análisis de riesgos de la Información tiene la intención de garantizar la seguridad de los datos, aplicar políticas de acceso a los diferentes niveles de autorización de acceso a la información, identificar las amenazas, vulnerabilidades y riesgo operativos de la Infraestructura Tecnológica Municipal con la que cuenta actualmente.

2.2.1. El Riesgo Informático

Se entiende como la gestión de riesgo Informático a la probabilidad de ocurrencia de incidentes que causen la paralización a los Sistemas Informáticos o de la red de comunicación, de forma que imposibilite el cumplimento de un objetivo o ponga en peligro a los bienes de la Organización, ocasionando de esta manera pérdidas o daños económicos irreversibles.

La Organización Internacional por la Normalización (ISO) define el riesgo tecnológico como: “La probabilidad de que una amenaza se materialice, utilizando vulnerabilidad existentes de un activo o un grupo de activos, generándole pérdidas o daños” (Guías para la gestión de la seguridad de TI /TEC TR 13335-1, 1996).Otras de las normativas con una madurez para la

definición del riesgo es la de origen Australiana y Nueva Zelandia AS/NZS 4360:2004 que lo define como “Posibilidad de que un suceso tenga un impacto en los objetivos”(AS/NZS 4360:2004),normativa que ha sido incorporada y actualizada internacionalmente como ISO 31000:2009, aplicada mundialmente y que define al riesgo como: “efecto de la Incertidumbre en los objetivos” (ISO 31000:2009).

2.2.2. Características

En el análisis de riesgo es importante reconocer que cada proceso de riesgo tiene características, tales como:

- **Activos:** Elementos que forman parte de los sistemas informáticos y redes de comunicación.

- **Amenazas:** Todo tipo de circunstancias que puede suceder a los sistemas y redes de comunicación. Las amenazas pueden ser de carácter físico como por ejemplo un incendio o lógico como por ejemplo acceso no autorizado a una base de datos.

- **Probabilidad:** Establecer la probabilidad de ocurrencia que puede realizarse de manera cuantitativa o cualitativa, pero siempre

considerando que la medida no debe contemplar la existencia de ninguna acción paliativa, o sea, debe considerarse en cada caso qué posibilidades existen que la amenaza se presente independientemente del hecho que sea o no contrarrestada.

- **Vulnerabilidades:** Agujeros de seguridad, debilidad de los activos que son aprovechadas por las amenazas para dañar un activo.

- **Impacto:** Consecuencia de la materialización de una amenaza sobre un activo.

- **Controles:** Mecanismos que permiten reducir las vulnerabilidades de equipos y sistemas informático.

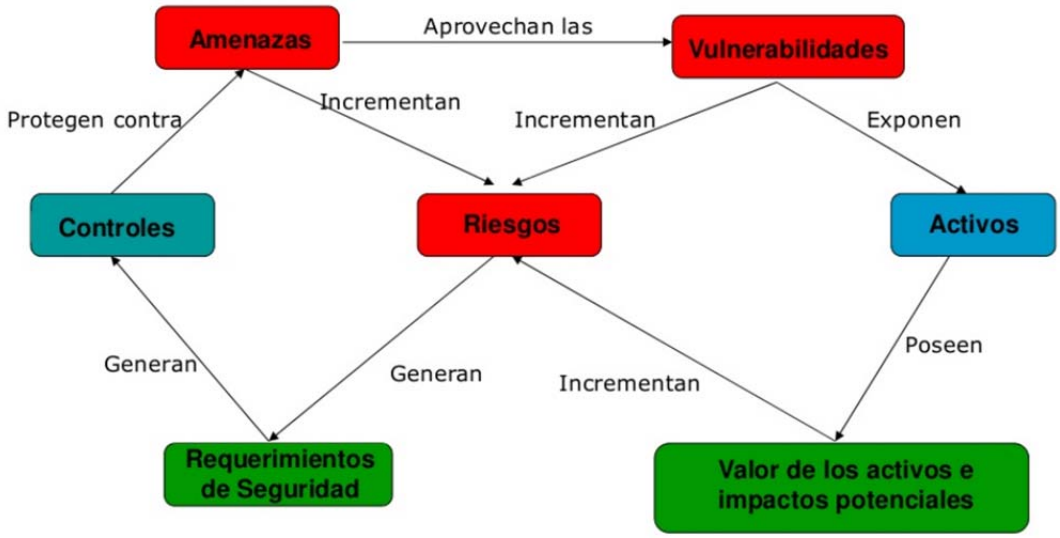


Figura2-16. Elementos del Análisis de Riesgo Informático

Además al hablar de la Seguridad de la Información es necesario considerar para el análisis de riesgo informático los siguientes componentes:

- **Integridad:** mantener la información libre de modificaciones no autorizadas.
- **Confidencialidad:** La información solo puede ser legible y modificado por personas autorizadas, tanto en el acceso a datos almacenados como también durante la transferencia de ellos.
- **Disponibilidad:** La información debe estar disponible cuando se necesite
- **Autenticación:** Que no se pueda negar la autoría (irrefutabilidad, no repudio).

2.2.3. Clasificación de Riesgo de TI (Tecnología de la Información)

Según el ambiente en el que se desenvuelve la empresa u organización investigada se puede identificar y relacionar los cuatro siguientes tipos de riesgo:

Riesgo Inherente: Es la posibilidad de errores o irregularidades en la información financiera, administrativa u operativa, antes de considerar la efectividad de los controles internos diseñados y aplicados por la institución.

Riesgos Financieros: Es todo lo relacionado a la parte financiera de la entidad, dicho riesgo se relaciona con el manejo de los recursos de la empresa.

Riesgo Operativo: Comprende tanto el riesgo en sistemas como operativo provenientes de deficiencias en los sistemas de información, procesos, estructura, que conducen a ineficiencias, oportunidad de corrupción o incumplimiento de los derechos fundamentales.

Riesgos de Tecnológico: Riesgo que se asocia con la capacidad tecnológica disponible por la entidad, con el objetivo de satisfacer sus necesidades actuales, futuras y de soporte al cumplimiento de su misión.

2.2.4. Metodología

Para la gestión de riesgo tecnológico, existen varios estándares que pueden servir como apoyo al análisis de riesgo de la TICs, para el Municipio de la Ciudad del Este, para la cual es importante destacar los siguientes:

Estándares orientados al Riesgo Tecnológico

- BS 31100
- ISO/IEC 27005
- ITGI-Risk IT Framework
- NIST-SP800-30
- AS/NZS ISO 31000:2009
- ISO 31010:2009
- AS/NZS 4360
- MAGERIT
- CRAMM
- UNE 71504

Desde un principio una de las normas aplicadas mundialmente a todo tipo de Instituciones es la norma AS/NZS 4360, pero este no cubre los mismos espectros que la ISO 27001 en sus disciplinas, ya que solo afecta a la forma

de cómo se deben analizar los riesgos, y en consecuencia planificar las medidas de seguridad, mientras que la ISO 27001 determina específicamente como gestionar el Sistema de la Gestión de la Seguridad Informática comúnmente llamado Plan de Seguridad.

Sin embargo, según Alfonso Bilbao Iglesias, en su artículo llamado "**La Necesaria Normativa ISO sobre la Seguridad**" elaborado en junio del 2010[1], expresa lo siguiente: "Desde la Empresa Cueva valiente Ingenieros, hemos participado algunas veces en el establecimiento de un Sistema de Gestión de Seguridad conjunto de Seguridad Física y Seguridad Lógica (por llamarlo de alguna manera) y hemos vivido las contradicciones de que la norma ISO 27001 se adapte como una protección a las necesidades de la gestión de la Seguridad Lógica (o Seguridad de la Información) y que no hay forma de encajar en ese modelo las particularidades de la gestión de la Seguridad Física".

La necesidad de esta Institución Pública para el Centro de Procesamiento de Datos no solo requiere la implementación de seguridad lógica, sino también llegar a un punto de evaluar todos los riesgo posibles a nivel tecnológico que

[1] Alfonso Bilbao and De Cuevavaliente Ingenieros, "La Necesaria Normativa ISO Sobre Seguridad Artículo Técnico", 2010 <http://www.cuevavaliente.com/es/documentos>.

puedan ocurrir al momento ofrecer servicios a la comunidad a través de los Sistemas Informáticos.

Basados en estos antecedentes se ha considerado la mejor alternativa del listado de normas antes presentado para la implementación de la gestión de riesgo, esta normativa es AS/NZS ISO 31000:2009 orientada a Riesgos, remplazando a la conocida mundialmente AS/NZS 4360, que tiene como objetivo ayudar a las organizaciones de todo tipo y tamaño a gestionar el riesgo con efectividad y posibilitar una mejora continua en el proceso de toma de decisiones en todo lo relacionada a la Gestión de Riesgo Tecnológico.

La ISO 31000 da una mejor alternativa para los riesgos deliberados en el ámbito de la Seguridad tanto físico como lógico que puedan suscitarse en cualquier momento en el Municipio de la Ciudad del Este, y que están basados en dos razones fundamentales:

- Cubrir todo el espectro de la Gestión de la Seguridad (tal como el ISO 27001).
- Orientación a la mejora continua con el esquema Plan-Do-Check-Act, PDCA (Planificar, Realizar, Comprobar y Reaccionar), comúnmente utilizado por la norma ISO.

Es importante dejar en claro que al alinearnos a la normativa ISO 31000 no significa que la ISO 27005 de Riesgo de la Seguridad de la Información, pierda relevancia debido a que su uso se puede justificar para tratar riesgos técnicos, mientras que la ISO 31000 provee un marco abierto y adecuado a los riesgo de una institución Pública si lo aplicamos correctamente a los equipos y sistemas informáticos.

2.2.5. La Norma AS/NZS ISO 31000:2009

Esta normativa que surge en noviembre del 2009 y tiene su origen Australiano y de Nueva Zelanda, permitió paralelamente la Actualización de la Guía ISO 73 que ofrece una lista de 50 términos referidos a la gestión de riesgo, además la AS/NZS ISO 31000:2009 suministra orientaciones genéricas para la gestión de riesgos y puede aplicarse a una gran variedad de actividades, decisiones u operaciones de cualquier Institución pública, privada, organizaciones sin fines de lucro, asociación, grupo o individuo.

Esta norma pueden ser aplicada a cualquier tipo de riesgo, cualquiera sea su naturaleza, causa u origen, así presente resultados positivas o negativas para la organización.

A partir de la ISO 31000, la palabra riesgo se define en términos del “Efecto de la incertidumbre en los objetivos”, esta nueva definición implica que se refiera tanto a las situaciones negativas tradicionales de riesgo que provocan perdidas, como a las situaciones positivas de riesgos, que constituyen oportunidades, cada uno de estos conceptos han sido incorporados actualmente por la ISO 27001[2]**,** Esta norma provee de principios, el marco de trabajo (framework) y un proceso destinado a gestionar cualquier tipo de riesgo en una manera transparente, sistemática y creíble dentro de cualquier alcance o contexto.

La implementación de esta norma en el Municipio de la Ciudad del Este permitirá contar con un conjunto de procedimiento y normativas internas que garantizaran lo siguientes aspectos:

- Contar con un cuerpo normativo especifico, armonizado y relacionado con la política interna de la institución.
- Disponer de un Análisis de riesgo consensuado con los responsables de la Organización que determinaran de forma directa la disposición de los recursos de seguridad necesarios.

[2] ISO, “Consejos de Implantación Y Métricas de ISO/IEC 27001 Y 27002” <http://www.iso27000.es/download/ISO_27000_implementation_guidance_v1_Spanish.pdf> [accessed 8 March 2015].

- Disponer de una métrica de desempeño de la seguridad, que permita analizar las desviaciones sobre objetivos propuestos.
- Contar con procedimientos de análisis de desempeño (a partir de la métrica) y de las consiguientes tomas de decisiones tendentes a corregir las desviaciones.

2.2.5.1. Estructura de la ISO 31000

La norma ISO propone un esquema procedural, tal como se presenta en la siguiente Figura.

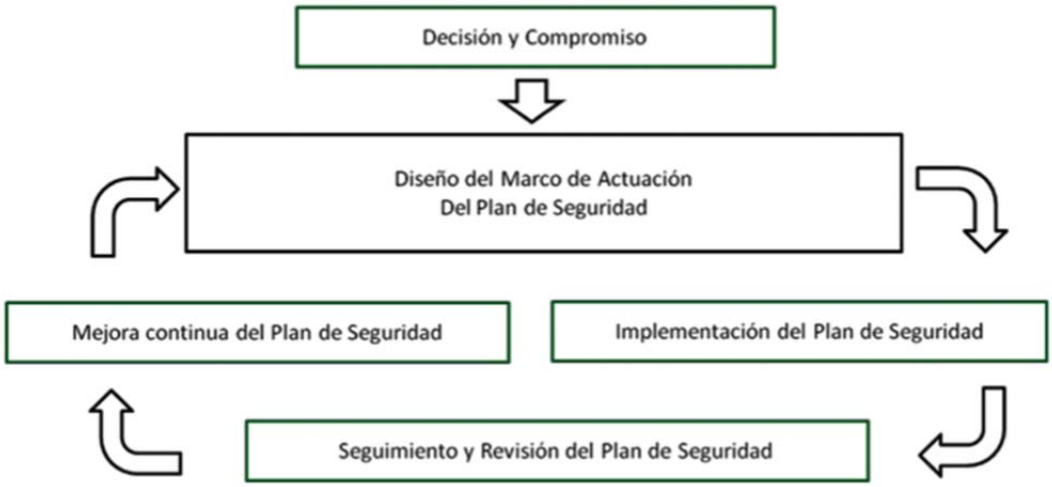


Figura 2-17. Estructura procedural del la normativa ISO 31000

Decisión y Compromiso: Para la implementación de un plan de seguridad se requiere un fuerte compromiso e implicación de la Dirección en los niveles más altos posibles.

Diseño del Marco de Actuación: Disponer de una serie de documentos en las que se determine los mecanismos y Políticas de Seguridad de la Institución.

Implementación del Plan de Seguridad: Se aplica el marco de Actuación, y se pondrá en marcha el modelo definido por la ISO 31000 muy parecido al norma AS/NZS 4360)

Seguimiento y Revisión: Es considerado los informes de Seguridad sobre los progresos de implementación del Plan de Seguridad.

Mejora Continua del Plan de Seguridad: Esto se consigue con las actuaciones de redefiniciones del Plan que permitan readecuar la política de Seguridad, el propio Plan y el marco de actuación.

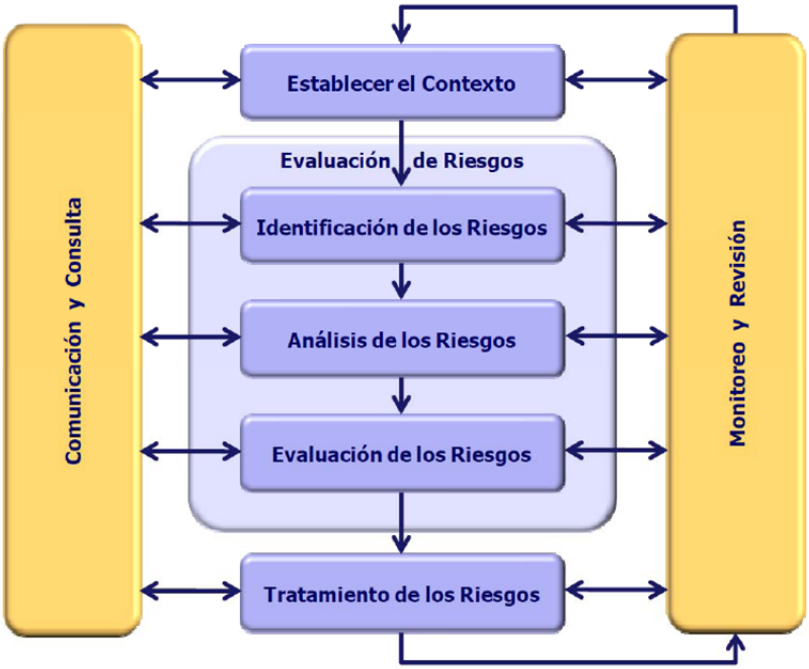


Figura 2-18. Estándar ISO 31000:2009 de Gestión de Riesgo

Los planes de seguridad de acuerdo con la norma ISO 31000[3] son los siguientes:

- Redacción de las directivas y normas internas del Marco de Actuación del Plan de Seguridad, adecuándolas a las estructuras de normativa interna existente.
- Desarrollo del Plan de Seguridad, utilizando herramienta de Análisis de riesgo y propuesta de medidas de seguridad, adaptada a las normas ISO 31000.

[3] ISOTOOLS, "Norma ISO 31000:2009. Gestión de Riesgos. Principios Y Directrices.", 2013 <http://www.isotools.com.co/norma-iso-310002009-gestion-de-riesgos-principios-y-directrices/> [accessed 15 October 2014].

- Determinación de los indicadores de desempeño del Plan de Seguridad y diseño de los informes de medición y de información sobre incidentes.
- Asesoramiento para la organización de las reuniones periódicas de seguimiento y mejora continua del Plan de Seguridad.

2.3. Análisis de Vulnerabilidades

Antes de realizar cualquier estudio o análisis de seguridad a la Institución se debe tomar en cuenta cuales son los estándares que van a servir de guía para identificar de forma ordenada y diversa a las auditorias Informáticas que se vayan a ejecutar al Municipio.

2.3.1. Tipos de Análisis

1. **Análisis de vulnerabilidades (Vulnerability Assessment)**

Este tipo de análisis no es intrusivo, el objetivo es buscar vulnerabilidades en los sistemas evaluados, con el fin de clasificarlas y presentarlas de forma estructurada.

2. Test de Intrusión (Penetration Testing)

Consiste en realizar varios tipos de pruebas, aprovechando las vulnerabilidades encontradas y de esta manera comprometer los sistemas. Este tipo de auditorías de seguridad es más invasiva que el análisis de vulnerabilidades y puede ser dirigido a un solo objetivo.

3. Hacking Ético:

La diferencia específica con el test de intrusión, es que es más completa la auditoria en relación con los dispositivos (Servidores de Datos, Firewall, IDS, router) las pruebas que se realizan son más rigurosas, además de la existencia de un pacto previo con el cliente, para poder hacer pruebas de tipo de “denegación de Servicio e Ingeniería social” en horarios planificados que no perjudique el normal funcionamiento laboral de la Institución.

Existen varios documentos de este tipo reconocidos como metodologías para el proceso de Auditoría de Seguridad Ofensiva o Hacking ético que nos puede servir de guía para este proyecto, las mismas que enlistamos a continuación:

- Open Source Security Testing Methodology Manual (OSSTMM)

- The Penetration Testing Execution Standard (PTES)
- About the Open Web Application Security Project (OWASP)
- VulnerabilityAssessment.co.uk

Se debe dejar especificado que para la ejecución de este trabajo también existe la necesidad de realizar acuerdos de confidencialidad y pactos sobre el trato de la información, esto antes de realizar cualquier prueba de Seguridad en los sistemas evaluados. Este tipo de procedimiento es un proyecto de seguridad informática que ayudará a garantizar el trabajo realizado sobre la auditoria a los sistemas operativos o aplicaciones.

La Metodología que se utilizará para el Análisis de Seguridad que se ejecutara al Municipio de la Ciudad del Este es una **auditoria de tipo "Hacking Ético" con el apoyo de la documentación OWASP,** las mismas que tiene las siguientes fases:

- Definición de reglas de auditoria
- Recolección de información
- Network Mapping, Scanning de Puertos y Enumeración
- Análisis y Clasificación de Vulnerabilidades
- Explotación de Vulnerabilidades
- Post-explotación de vulnerabilidades

- Presentación de Reportes y resultados

Cada una de estas fases es documentada en el capítulo 3, ilustrando de mejor manera el desarrollo de cada una de ellas.

2.4. Plan de Recuperación ante Desastres

El plan de recuperación ante desastres no es más que procedimientos, políticas y procesos que se deben establecer en una Institución para actuar en caso de eventos adversos o siniestros inesperados que afecten a sus operaciones diarias. Para esto se debe constituir un plan que permita al Municipio restaurar con sus operaciones críticas en el menor tiempo posible y actuar de manera adecuada ante el problema suscitado.

2.4.1. Tipos de Contingencia

Existen diferentes tipos de contingencia de acuerdo a los daños sufridos:

Menor: es la que tiene repercusiones solo en las operaciones diarias y se puede recuperar en menos de 8 horas laborables.

Grave: Es la que causa daños a las instalaciones, pero puede reiniciar operaciones en menos de 24 horas.

Critica: Afecta a las operaciones y las instalaciones, este no es recuperable en corto tiempo y puede suceder porque no existe normas preventivas o bien porque estas no son suficientes; relacionado también con desastres naturales incendios, inundación o terremoto, etc.

2.4.2. Diferencia entre Emergencia y Contingencia

Según Elio Ríos[4], la diferencia entre Contingencia y Emergencia es la siguiente:

a. Es **Contingencia** (lo que puede o no suceder) si se tenía previsto por los organismos de atención y/o por la comunidad de los afectados que esto pudiera ocurrir y si se adquirió logística, se prepara personal especializado y a la comunidad para atenderlo en forma integral.

b. Es **Emergencia** el caso que este hecho no esté contemplada por los organismos de atención y/o por la comunidad de los afectados la posibilidad de aparición y desarrollo de la eventualidad, con todos los

[4] Elio Ríos Serrano, "Los Desastres - Por: Elio Ríos Serrano" <http://www.aporrea.org/actualidad/a13255.html>.

rasgo de la sorpresa y por supuesto sin tener una logística, sin preparación de personal especializado ni a la comunidad para atenderlo en forma integral.

Es importante saber que la pérdida de información provoca daño de fondo en la Institución como los mencionados a continuación:

- Contribuyentes decepcionados y molestos
- Perdida de Reputación Institucional
- Retraso en gestiones administrativas

Es importante destacar esta información para la creación de un Plan de Recuperación ante Desastres y Respaldo de Información eficiente, y que se llegue a ejecutar de forma óptima al momento de suscitarse el siniestro.

2.5. Políticas de Seguridad Informática

Para conseguir mejoras en el campo de la Seguridad Tecnológico se debe implementar Políticas que fomente la buena práctica y el correcto manejo de la información para el Centro de Procesamiento de Datos de esta institución

Pública, por tal situación es necesario trabajar con la normativa ISO 27002:2013[5]

2.5.1. Descripción de la Norma 27002

Esta Norma contiene 35 objetivos de control y 114 controles que se encuentran agrupados en 14 dominios principales. A continuación se presenta un resumen de la Norma ISO/IEC 27002:

5. Políticas de Seguridad.

5.1 Directrices de la Dirección en seguridad de la información.

5.1.1 Conjunto de políticas para la seguridad de la información.

5.1.2 Revisión de políticas para la seguridad de la información.

6. Aspectos organizativos de la Seguridad de la Información

6.1 Organización interna.

6.1.1 Asignación de responsabilidades para la segur. de la información.

6.1.2 Segregación de tareas.

6.1.3 Contacto con las autoridades.

[5] Iso27000.es, "ControlesISO27002-2013", 2013, 27002 <http://iso27000.es/download/ControlesISO27002-2013.pdf>.

6.1.4 Contacto con grupos de interés especial.

6.1.5 Seguridad de la información en la gestión de proyectos.

6.2 Dispositivos para movilidad y teletrabajo.

6.2.1 Política de uso de dispositivos para movilidad.

6.2.2 Teletrabajo.

7. Seguridad ligada a los Recursos Humanos.

7.1 Antes de la contratación.

7.1.1 Investigación de antecedentes.

7.1.2 Términos y condiciones de contratación.

7.2 Durante la contratación.

7.2.1 Responsabilidades de gestión.

7.2.2 Concienciación, educación y capacitación en seguridad de la información

7.2.3 Proceso disciplinario.

7.3 Cese o cambio de puesto de trabajo.

7.3.1 Cese o cambio de puesto de trabajo.

8. Gestión de Activos.

8.1 Responsabilidad sobre los activos.

8.1.1 Inventario de activos.

8.1.2 Propiedad de los activos.

8.1.3 Uso aceptable de los activos.

8.1.4 Devolución de activos.

8.2 Clasificación de la información.

8.2.1 Directrices de clasificación.

8.2.2 Etiquetado y manipulado de la información.

8.2.3 Manipulación de activos.

8.3 Manejo de los soportes de almacenamiento.

8.3.1 Gestión de soportes extraíbles.

8.3.2 Eliminación de soportes.

8.3.3 Soportes físicos en tránsito.

9. Control de Accesos.

9.1 Requisitos de negocio para el control de accesos.

9.1.1 Política de control de accesos.

9.1.2 Control de acceso a las redes y servicios asociados.

9.2 Gestión de acceso de usuario.

9.2.1 Gestión de altas/bajas en el registro de usuarios.

9.2.2 Gestión de los derechos de acceso asignados a usuarios.

9.2.3 Gestión de los derechos de acceso con privilegios especiales.

9.2.4 Gestión de información confidencial de autenticación de

usuarios.

9.2.5 Revisión de los derechos de acceso de los usuarios.

9.2.6 Retirada o adaptación de los derechos de acceso

9.3 Responsabilidades del usuario.

9.3.1 Uso de información confidencial para la autenticación.

9.4 Control de acceso a sistemas y aplicaciones.

9.4.1 Restricción del acceso a la información.

9.4.2 Procedimientos seguros de inicio de sesión.

9.4.3 Gestión de contraseñas de usuario.

9.4.4 Uso de herramientas de administración de sistemas.

9.4.5 Control de acceso al código fuente de los programas.

10. Cifrado

10.1 Controles criptográficos.

10.1.1 Política de uso de los controles criptográficos.

10.1.2 Gestión de claves.

11. Seguridad Física y Ambiental.

11.1 Áreas seguras.

11.1.1 Perímetro de seguridad física.

11.1.2 Controles físicos de entrada.

11.1.3 Seguridad de oficinas, despachos y recursos.

11.1.4 Protección contra las amenazas externas y ambientales.

11.1.5 El trabajo en áreas seguras.

11.1.6 Áreas de acceso público, carga y descarga.

11.2 Seguridad de los equipos.

11.2.1 Emplazamiento y protección de equipos.

11.2.2 Instalaciones de suministro.

11.2.3 Seguridad del cableado.

11.2.4 Mantenimiento de los equipos.

11.2.5 Salida de activos fuera de las dependencias de la empresa.

11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.

11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.

11.2.8 Equipo informático de usuario desatendido.

11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. Seguridad en la Operativa.

12.1 Responsabilidades y procedimientos de operación.

12.1.1 Documentación de procedimientos de operación.

12.1.2 Gestión de cambios.

12.1.3 Gestión de capacidades.

12.1.4 Separación de entornos de desarrollo, prueba y producción.

12.2 Protección contra código malicioso.

12.2.1 Controles contra el código malicioso.

12.3 Copias de seguridad.

12.3.1 Copias de seguridad de la información.

12.4 Registro de actividad y supervisión.

12.4.1 Registro y gestión de eventos de actividad.

12.4.2 Protección de los registros de información.

12.4.3 Registros de actividad del administrador y operador del sistema.

12.4.4 Sincronización de relojes.

12.5 Control del software en explotación.

12.5.1 Instalación del software en sistemas en producción.

12.6 Gestión de la vulnerabilidad técnica.

12.6.1 Gestión de las vulnerabilidades técnicas.

12.6.2 Restricciones en la instalación de software.

12.7 Consideraciones de las auditorías de los sistemas de información.

12.7.1 Controles de auditoría de los sistemas de información.

13. Seguridad en las telecomunicaciones.

13.1 Gestión de la seguridad en las redes.

13.1.1 Controles de red.

13.1.2 Mecanismos de seguridad asociados a servicios en red.

13.1.3 Segregación de redes.

13.2 Intercambio de información con partes externas.

13.2.1 Políticas y procedimientos de intercambio de información.

13.2.2 Acuerdos de intercambio.

13.2.3 Mensajería electrónica.

13.2.4 Acuerdos de confidencialidad y secreto

14. Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información.

14.1 Requisitos de seguridad de los sistemas de información.

14.1.1 Análisis y especificación de los requisitos de seguridad.

14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.

14.1.3 Protección de las transacciones por redes telemáticas.

14.2 Seguridad en los procesos de desarrollo y soporte.

14.2.1 Política de desarrollo seguro de software.

14.2.2 Procedimientos de control de cambios en los sistemas.

14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.

14.2.4 Restricciones a los cambios en los paquetes de software.

14.2.5 Uso de principios de ingeniería en protección de sistemas.

14.2.6 Seguridad en entornos de desarrollo.

14.2.7 Externalización del desarrollo de software.

14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.

14.2.9 Pruebas de aceptación.

14.3 Datos de prueba.

14.3.1 Protección de los datos utilizados en pruebas.

15. Relaciones con Suministradores.

15.1 Seguridad de la información en las relaciones con suministradores.

15.1.1 Política de seguridad de la información para suministradores.

15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.

15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.

15.2 Gestión de la prestación del servicio por suministradores.

15.2.1 Supervisión y revisión de los servicios prestados por terceros.

15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. Gestión de Incidentes en la Seguridad de la Información.

16.1 Gestión de incidentes de seguridad de la información y mejoras.

16.1.1 Responsabilidades y procedimientos.

16.1.2 Notificación de los eventos de seguridad de la información.

16.1.3 Notificación de puntos débiles de la seguridad.

16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.

16.1.5 Respuesta a los incidentes de seguridad.

16.1.6 Aprendizaje de los incidentes de seguridad de la información.

16.1.7 Recopilación de evidencias.

17. Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio.

17.1 Continuidad de la seguridad de la información.

17.1.1 Planificación de la continuidad de la seguridad de la información.

17.1.2 Implantación de la continuidad de la seguridad de la información.

17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

17.2 Redundancias.

17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. Cumplimiento.

18.1 Cumplimiento de los requisitos legales y contractuales.

18.1.1 Identificación de la legislación aplicable.

18.1.2 Derechos de propiedad intelectual (DPI).

18.1.3 Protección de los registros de la organización.

18.1.4 Protección de datos y privacidad de la información personal.

18.1.5 Regulación de los controles criptográficos.

18.2 Revisiones de la seguridad de la información.

18.2.1 Revisión independiente de la seguridad de la información.

18.2.2 Cumplimiento de las políticas y normas de seguridad.

18.2.3 Comprobación del cumplimiento.

La descripción de los 14 dominios son:

1. Políticas de seguridad (1 control)

2. Aspecto Organizativos de la seguridad de Información (2 controles)
3. Seguridad ligada a recursos humanos (3 controles)
4. Gestión de activos (3 controles)
5. Control de acceso (4 controles)
6. Cifrado (1 control)
7. Seguridad física y ambiental (2 controles)
8. Seguridad en la Operativa (7 controles)
9. Seguridad en las Telecomunicaciones (2 controles)
10. Adquisición, desarrollo y Mantenimiento de los Sistemas de Información (3 controles)
11. Relaciones con suministradores (2 controles)
12. Gestión de Incidentes en la Seguridad de la Información (1 control)
13. Aspectos de la Seguridad de la Información en la Gestión de la Continuidad del Negocio (2 control)
14. Cumplimiento (2 controles)

Tabla 2.13 Normativa ISO 27002:2013

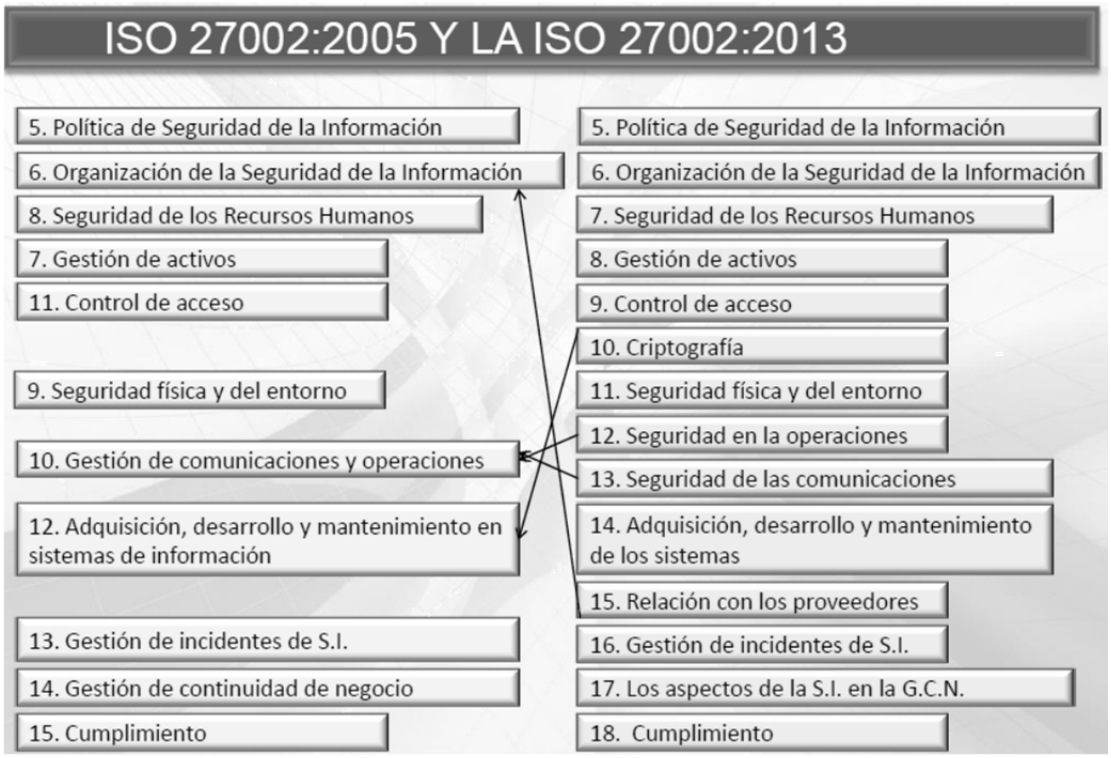


Figura2-19. ISO 27002:2005 vs. ISO 27002:2013

En la gráfica antes observada se identifica que en la Normativa ISO 27002:2013 posee menos controles tecnológicos que la ISO 27002:2005[6], adicionalmente se cuenta con políticas de control más claras y se debe considerar esta actualización para la aplicación en este documento.

La Normativa ISO 27002:2013, es una herramienta que permite establecer políticas y controles con el objetivo de disminuir los riesgos informáticos en la Institución.

[6] Iso/iec 27002:2005., "Iso/iec 27002:2005.", 2011, 27002 <http://www.iso27000.es/download/ControlesISO27002-2005.pdf>.

Al implementar esta normativa lograremos reducir las amenazas y riesgos hasta llegar a un nivel considerable de seguridad para la Institución, luego del análisis de la normativa se ha considerado necesario enfocarse principalmente en aplicar tres controles:

a) Documentos de la Política de Seguridad de la información
b) Asignación de responsabilidades relativas a la seguridad de la información
c) Cumplimiento de la Política y normas de seguridad

2.5.2. Parámetros para Establecer Políticas de Seguridad de Información.

Para la generación de la política debe ser considerado como un proceso técnico administrativo que debe contar siempre con el Apoyo administrativo y en especial de la máxima autoridad de la Entidad, sin este apoyo este proceso puede fracasar o no llegar a su término de forma satisfactoria.

Es importante que al diseñar las políticas de seguridad basados en una Institución Pública se considere primeramente los siguientes aspectos:

- ✓ Reunirse con los Departamentos que poseen mayor experiencia para establecer el alcance y definir las violaciones a las Políticas.
- ✓ Identificar a los líderes de áreas para la toma de decisión a fin de que ellos son los más interesados por preservar la integridad de la información que manejan
- ✓ Monitorear constantemente los procedimientos y operaciones que realiza el área de Tecnología.
- ✓ Detallar explícitamente y concretamente el alcance de la política con el propósito de evitar tensiones por parte del personal de área y de toda la institución.

Finalmente el principal objetivo de estos aspectos ya expresados, es lograr que sea aprobado cada una de las políticas, las mismas que deben integrarse a la estrategia de negocio que lleva el Municipio, a su misión y visión con el fin de que las altas autoridades de la Institución reconozcan de forma inmediata la importancia y utilidad para el Municipio.

Es Importante recalcar que las políticas por sí solas no constituyen una garantía para la Seguridad del Municipio, ellas deben responder a intereses y necesidades Institucionales basadas en su visión, que lleven a un esfuerzo conjunto de sus actores por administrar correctamente sus recursos, factor

que facilita la formalización y materialización de los compromisos adquiridos como Institución Pública.

2.6. Cifrado de los Sistemas de Información

2.6.1. Criptografía

Criptografía[7] (del griego (criptos), «oculto», y (grafé), «escritura», literalmente «escritura oculta»). Tradicionalmente se ha definido como el ámbito de la criptografía que se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados. Estas técnicas se utilizan tanto en el arte como en la ciencia. Por tanto, el único objetivo de la criptografía es conseguir la confidencialidad de los mensaje, para ello se diseñaban sistemas de cifrado y códigos. En esos tiempos la única criptografía existente era la llamada criptografía clásica.

Actualmente la tecnología más apropiada dentro de la criptografía para defender servicio de Correo Electrónico y hoy en día el más utilizado para envió de información es la firma digital.

[7] Wikipedia.org, "Criptografía - Wikipedia, La Enciclopedia Libre" <http://es.wikipedia.org/wiki/Criptografía>.

Es necesario que los usuarios aprendan a proteger su información de los peligrosde la nube del Internet, seleccionando contraseñas adecuadas para sus cuentas y cifrando la información que almacenan en los servidores. Además deben saber cómo observar lasanomalías que se aprecian en el uso de los servicios y reportarlas oportunamente, Esto puede alertar sobre cualquiera de las variantes de ataques que se utilizan hoy en día.

2.6.2. Métodos de Encriptación y Protección de la Información

En la actualidad se han incrementado precipitadamente los Ciberataques dirigidas a las Instituciones Públicas debido a que el volumen de información que se maneja en el Internet en muchas situaciones es muy grande, situación por la que se requiere garantizar transmisiones segura de datos dentro de la nube de internet, razón por la cual debemos emplear técnicas de forma que los datos que se envían de una computadora a otra sea de forma segura, en cuanto a que el receptor lo comprenda de acuerdo al algoritmo establecido y sea idéntico al enviado por el emisor y que este a su vez este codificado para evitar que sea interpretado por usuarios ajenos a la comunicación realizada.

Este proceso es completamente transparente para el usuario final, no incrementa el tamaño de los paquetes y solo puede ser desencriptado por

quien tenga la clave para realizar esta acción. De esta manera estaremos considerando los siguientes puntos de seguridad informática:

- ✓ Autenticidad de los usuarios.
- ✓ Confidencialidad.
- ✓ Integridad.
- ✓ No repudio.

Los métodos de encriptación[8] existentes se dividen en dos grandes grupos los cuales son:

- ✓ Clave secreta o privada (simétrica).
- ✓ Clave pública (asimétrica).

2.6.3. Clave Privada (Simétrica)

Utiliza una clave para la encriptación y desencriptación del mensaje a transmitir, esta clave se debe intercambiar entre los equipos por medio de un canal seguro; ambos extremos deben tener la misma clave para cumplir con el proceso.

[8]Textoscientificos.com, "Encriptación" <http://www.textoscientificos.com/redes/redes-virtuales/tuneles/encriptacion> .

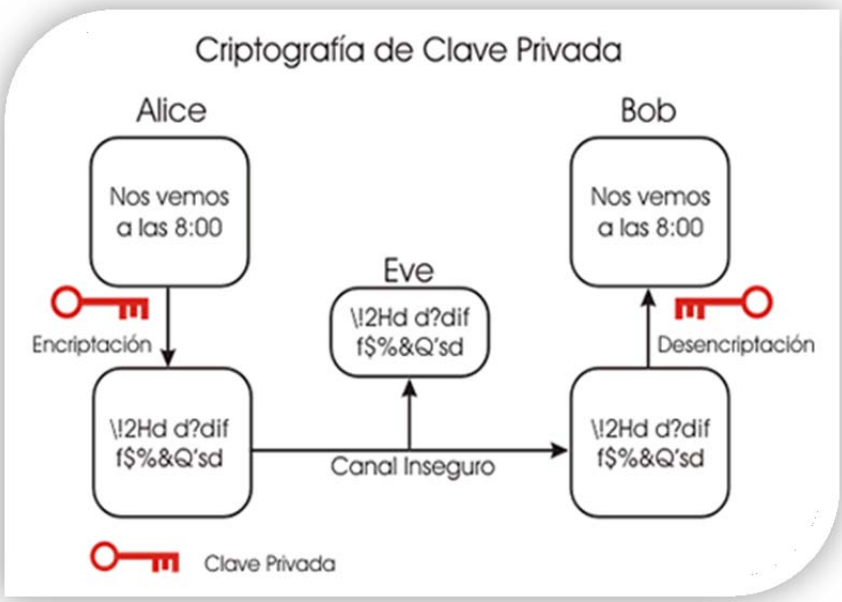


Figura 2-20. Clave Privada

Entre los principales algoritmos simétricos tenemos los siguientes: DES, IDEA y RC5.

Las principales desventajas de los métodos simétricos son la distribución de las claves, el peligro de que muchas personas deban conocer una misma clave y la dificultad de almacenar y proteger muchas claves diferentes.

2.6.4. Clave Pública (Asimétrica)

También llamada asimétrica, se basa en el uso de dos claves diferentes, que

poseen una propiedad fundamental: una clave puede desencriptar lo que la otra ha encriptado.

Una de las claves de la pareja, llamada clave privada, es usada por el propietario para cifrar los mensajes, mientras que la otra, llamada clave pública, es usada para desencriptar el mensaje.

El primer sistema de clave pública que apareció fue el de Diffie-Hellman, en 1976, y fue la base para el desarrollo de los que después aparecieron, entre los que cabe destacarel RSA (el más utilizado en la actualidad).

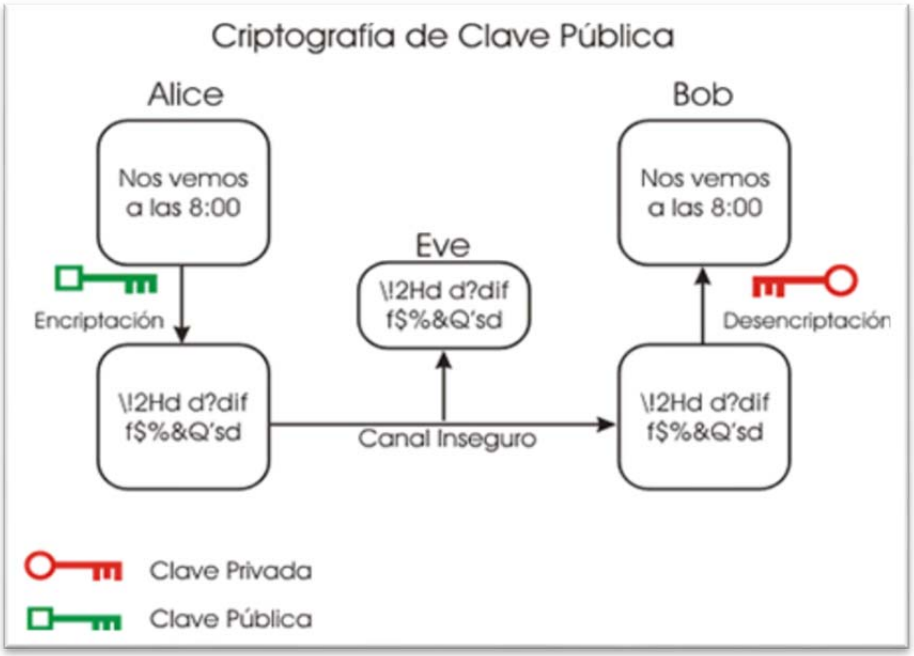


Figura 2-21. Clave Pública

Las claves públicas y privadas tienen características matemáticas especiales, de tal forma que se generan siempre a la vez por parejas, estando cada una de ellas ligada intrínsecamente a la otra, mientras que la clave privada debe mantenerla en secreto de su propietario, ya que es la base de la seguridad del sistema, la clave pública es difundida, para que esté al alcance del mayor número posible de personas, existiendo servidores que guardan, administran y difunden dichas claves.

Para que un algoritmo de clave pública sea considerado seguro debe cumplir con los siguientes puntos:

- Conocido el texto cifrado no debe ser posible encontrar el texto en claro ni la clave privada.
- Conocido el texto cifrado (criptograma) y el texto en claro debe resultar más caro en tiempo o dinero descifrar la clave, que el valor posible de la información obtenida por terceros.
- Conocida la clave pública y el texto en claro no se puede generar un criptograma correcto encriptado con la clave privada.
- Dado un texto encriptado con una clave privada sólo existe una pública capaz de desencriptarlo, y viceversa.

2.6.5. Diferencias entre los algoritmos Simétricos y los Asimétricos.

Al hablar de los algoritmos simétricos estos permiten encriptar y desencriptar con la misma llave. Las principales ventajas de los algoritmos simétricos son su seguridad y su velocidad y tiene un nivel de seguridad de 128bits.

Los algoritmos asimétricos pueden encriptar y desencriptar con diferentes llaves. Los datos se cifran con una llave pública y se desencriptan con una privada, siendo ésta su principal ventaja. Los algoritmos asimétricos, también conocidos como algoritmos de llave pública, necesitan al menos una llave de 3.000 bits para alcanzar un nivel de seguridad similar al de uno simétrico de 128 bits.

Los algoritmos asimétricos son increíblemente lentos, tanto que no pueden ni se recomiendan ser utilizados para cifrar grandes cantidades de información. Los algoritmos simétricos son aproximadamente 1.000 veces más rápidos que los asimétricos.

En la siguiente tabla, se modela una comparativa entre los dos tipos de criptografía:

Tabla comparativa entre criptografía simétrica y asimétrica

	Ventajas	Desventajas	Garantías de seguridad	Uso	Algoritmos más usados
Simétrica	sistema eficiente en grupos muy reducidos, ya que sólo es necesaria una única clave no es necesario disponer de una tercera parte confiable Infraestructura sencilla	es necesario compartir la clave entre emisor y receptor por medios que pueden no ser seguros si se compromete la clave, se compromete toda la comunicación no permite autenticar al emisor ya que una misma clave la utilizan dos personas se necesita un elevado número de claves: n*(n-1)/2; siendo n el número de personas implicadas en una comunicación cifrada	confidencialidad integridad	• cifrado de mensajes	**DES** con tamaño de clave de 56 bits. **Triple-Des** con tamaño de clave de 128 bits a 256 bits. **Blowfish** con tamaño de clave de 128 bits a 256 bits **AES** con tamaños de clave de 128, 192 o 256 bits.
Asimétrica	número de claves	alto coste computacional en el	confidencialida	cifrado de	**RSA** con tamaño de

	Ventajas	Desventajas	Garantías de seguridad	Uso	Algoritmos más usados
	reducido, ya que cada individuo necesitará únicamente un par de claves computacionalmente es complicado encontrar la clave privada a partir de la pública no es necesario transmitir la clave privada entre emisor y receptor	proceso de generación de claves la necesidad de un tercero (autoridad de certificación) en el proceso necesidad de una gran infraestructura independientemente del número de individuos. Se precisa mayor tiempo de proceso y claves más grandes	d integridad autenticidad de origen no repudio	mensajes firma digital intercambio de claves	clave mayor o igual a 1024 bits **DSA** con tamaño de clave de 512 bits a 1024 bits **El Gamal** con tamaño de clave comprendida entre los 1024 bits y los 2048 bits

	Ventajas	Desventajas	Garantías de seguridad	Uso	Algoritmos más usados
	permite autenticar a quien utilice la clave privada				

Tabla 2-14. Tabla comparativa entre criptografía simétrica y asimétrica

2.6.6. Criptoanálisis

Es el conjunto de técnicas que se pueden usar para romper los códigos criptográficos, por tanto trata de comprometer la seguridad de un cripto sistema, ya sea simétrico o asimétrico, sin embargo, aunque pueda identificar que el criptoanálisis es el enemigo del cripto sistema ya que trata de romperlo, la realidad es que ayuda a perfeccionar al cripto sistema, el mismo que aplicando técnicas de criptoanálisis se puede ver cuáles son los puntos débiles de un algoritmo, perfeccionarlo y dificultar el posible criptoanálisis invasivo futuro o nuevo.

El perfeccionamiento de los algoritmos ha provocado que para el criptoanálisis suela ser necesaria una computadora ya que en general se lleva a cabo analizando grandes cantidades de pares mensaje-criptograma.

Los principales tipos de análisis son:

- **Texto claro escogido.** Este tipo de ataque se basa en que conocemos algunos mensajes elegidos por nosotros y sus respectivos criptogramas. A partir de ahí se buscan relaciones para averiguar cómo sería el mensaje sin cifrar a partir del cifrado.

- **Fuerza bruta.** El menos elaborado de todos, descifra el criptograma con todas las posibles contraseñas y de las posibles soluciones identifica las que tienen sentido.

- **Análisis diferencial.** Observa cómo afectan al criptograma ligeras codificaciones en el mensaje para deducir el criptograma a descifrar.

- **Análisis Lineal**. Esta técnica consiste en realizar operaciones lógicas a pares mensaje-criptograma de las que se pueden sacar conclusiones sobre la clave de cifrado.Un tipo de ataque que solo se

puede utilizar con los algoritmos asimétricos consiste en tratar de deducir la clave privada a partir de la pública.

- **Ataques de Canal lateral.** Estudio de la potencia consumida por el componente electrónico que realiza elcifrado. Este método se basa en detectar qué operaciones está realizando el microprocesador a partir de su potencia consumida. De esta manera, conociendo el funcionamiento interno del algoritmo, si se observa la potencia que el sistema electrónico consumen el momento de operar con la clave, se puede identificar cual es la clave.

Según el análisis previo para la ejecución e implementación del proyecto en el Municipio de la Ciudad del Este, trabajaremos con el algoritmo AES. Está demostrado que este algoritmo es muy resistente a todos los ataques comentados anteriormente, por tanto en la última parte de este proyecto implementaremos técnicas que hagan el algoritmo más robusto frente a este método de criptoanálisis.

2.6.7. Implementación del algoritmo en encriptación AES

Una de las ventajas del algoritmo Rijndael en relación a otra, se refiere a que es el único que podía trabajar con claves y bloques de cifrado de 128, 192 y

256 bits indistintamente, pudiendo usarse 9 configuraciones distintas fruto de mezclar cualquier longitud de clave con cualquier longitud de bloque.

El algoritmo AES es uno de los utilizados para proteger la información del gobierno de los EE.UU. usados también por el sector privado y se estandarizaría en muchos países (Sobre todo en los europeos).

Si se comprende el funcionamiento del proceso de cifrado, el de descifrado se puede resumir fácilmente. Consiste en sustituir las operaciones del proceso de cifrado por sus inversas y alterar el orden en que estas se aplican. El aplicar este algoritmo permitiría a la Institución Publica mejorar su seguridad en relación a información crítica y confidencial a razón de poder tener a buen recaudo toda la información de la institución una vez aplicada el algoritmo.

2.6.8. Cifrado de Disco para Linux

LUKS[9] es una implementación muy sencilla de utilizar para la gestión de particiones y unidades de almacenamiento cifradas en GNU/Linux. Se recomienda su uso en dispositivos móviles, computadoras portátiles y

[9] Joel Barrios Dueñas, "Cifrado de Particiones Con LUKS. - Alcance Libre" <http://www.alcancelibre.org/staticpages/index.php/ciframiento-particiones-luks>.

dispositivos de almacenamiento cuya información se desee proteger en caso de extravío o robo.

2.6.9. Cifrado de Disco para Windows

BitLocker[10] cifra todos los datos almacenados en el volumen del sistema operativo Windows (y en los volúmenes de datos configurados). Esto incluye el sistema operativo Windows, los archivos de paginación e hibernación, las aplicaciones y los datos usados por las aplicaciones.

BitLocker está configurado para que use de manera predeterminada un Módulo de plataforma segura (TPM) que ayude a garantizar la integridad de los componentes de arranque inicial (los componentes utilizados en las primeras fases del proceso de inicio), y "bloquea" los volúmenes que hayan sido protegidos con BitLocker para que permanezcan protegidos aun en el caso de que se altere el equipo cuando el sistema operativo no se esté ejecutando.

[10] "Cifrado de Unidad BitLocker - Microsoft Windows" <http://windows.microsoft.com/es-419/windows7/products/features/bitlocker> .

2.6.10. Control de Inventario y Monitoreo de PC's

Belarc, Inc.[11] es una empresa de clase mundial dedicada al desarrollo y diseño de productos basados en arquitectura WAN que ayudan a hacer más sencillo el control de inventario y monitoreo de PC's por medio de una sencilla administración, tanto para usuarios pequeños como para los grandes corporativos, dependencias de gobierno, agencias de seguridad, universidades, etc.

La arquitectura en formato portal WEB de Belarc permite a los usuarios simplificar y automatizar la administración de equipos de escritorio, servidores y equipo portátil en cualquier lugar del mundo, utilizando una sola base de datos y un servidor de Intranet. Los productos de Belarc crean automáticamente una base de datos centralizada (CMDB), precisa y actualizada que contiene información detallada de software, hardware y configuraciones en seguridad.

[11] Belarc, “PRODUCTOS DE BELARC” <http://www.belarc.com/es/products.html>.

CAPÍTULO 3

3. EVALUACIÓN DE RIESGOS, AMENAZAS Y VULNERABILIDADES TECNOLÓGICAS.

3.1. Identificación de Riesgos

La siguiente evaluación de riesgo realizada al Municipio de la Ciudad del Este está basada en la Normativa AS/NZS ISO 31000:2009. A continuación en la siguiente tabla se realiza un análisis específico en donde se identifican todos los riegos de tipo interno y externos que podrían afectar directa o indirectamente en la administración del Centro de Procesamiento de Datos Municipal, además incluye la preparación de planes de tratamiento de riesgos.

Nº	Tipos de riesgo	Riesgo	Descripción	Posibles consecuencias
1	Externo /Interno	Cortes de energía	Fallas en red eléctrica, que alimenta al Centro de Datos Municipal	Inoperatividad de los equipos de comunicaciones y servidores de datos.
2	Interno	Fallas de UPS	Falla de equipos de respaldo eléctrico	Inoperatividad de los equipos de comunicaciones y servidores de datos.
3	Interno	Fallas en equipo de ventilación (aires acondicionados)	Temperatura no adecuada para la operatividad de equipos de Comunicación y Servidores	Baja el desempeño de procesamiento y generación de daños por recalentamiento en equipos
4	Externos	Terremotos	Eventos naturales	Daño total del equipamiento de comunicación y servidores de datos

5	Externo	Tsunami	Eventos naturales	Daño total del equipamiento de comunicación y servidores de datos
6	Externo /Interno	Incendios	Fuego en las instalaciones del Centro de Datos Municipal	Daño total del equipamiento de comunicación y servidores de datos
7	Interno	Desconexión de medio físico por interconexión proveedor de Internet	Corte o daños en la fibra óptica de interconexión	Usuarios no tendrán acceso al servicio de internet
8	Interno	Fallas en hardware de equipos del Centro de Datos Municipal	falla en los equipos Informáticos de comunicación y servidores de datos	Interrupción del servicio Tecnológicos parcialmente
9	Interno	Fallas en software de Equipos de Centro de Datos	Servicio no disponible por problemas en el Sistema Operativo o Software de	Interrupción del servicio Tecnológicos parcialmente

		Municipal	Administración	
10	Interno	Falla en los equipos de conmutación de la redes LAN	Desperfecto eléctrico o cualquier problema interno en los equipos de comunicaciones	Interrupción de la red de comunicación
11	Interno	Saturación en los equipos de comunicaciones	Problemas en saturación de paquetes de datos y procesamiento entre otras	Pérdida de desempeño hasta posible desconexión o saturación de la red interna
12	Interno	Falla en los equipos de radio comunicación para la red MAN	Desperfecto eléctrico o cualquier problema interno en los equipos de comunicaciones	Interrupción de la red de comunicación e internet
13	Externo	Interrupción servicio de internet por problemas de ultima milla	Falla en el acceso al servicio de internet	Usuarios no tendrán acceso al servicio de internet

14	Interno /Externo	Interrupción del servicio de Firewall	Falla en el equipo de filtraje	Vulnerabilidad de acceso a Información del Centro de Datos Municipal
15	Interno	Acceso no autorizado a los servidores del Centro de Datos Municipal	Acceso de personas no autorizada a los servidores	Robo de información
16	Interno	Acceso no autorizado a los equipos de comunicaciones	Acceso de personas sin permiso a la configuración del núcleo de comunicaciones	Robo de información
17	Interno /Externo	Actos de ciberataques	El saboteador puede ser un empleado o un sujeto ajeno a la empresa que utiliza herramientas de Craqueo	Interrupción de Servicio Tecnológicos y/o robo de información

18	Interno	Errores humanos	Mantenimiento rutinario que terminan en un apagado no programado de equipos	Interrupción del servicio Tecnológicos parcialmente

Tabla 3-15. Identificación de Riesgos

El proceso de administración de riesgo contempla la identificación de todos los posibles riesgos, los cuales afectan a los estándares. Cabe destacar que estos pueden ser directos o indirectos que inciden en la administración, como por ejemplo el corte de energía se categoriza como un riesgo directo, debido a que por un desperfecto eléctrico se suspende el servicio, entre los riesgos indirectos se puede mencionar la interrupción o reinicio de un Servidor FTP.

3.1.1. Análisis de Riesgos

Es importante identificar los riesgos que afectan directamente a la institución con el fin de que no existan dificultades en mantener una continuidad del negocio y poder tener una clara realidad de los costos que se verían involucrados, esto implica que se debe tener bien identificado las probabilidades de ocurrencia y su impacto, evaluación de controles aplicados a los procesos así como también sus debilidades.

3.1.1.1. Magnitud del Riesgo

La magnitud de un riesgo se determina por la probabilidad de ocurrencia y sus consecuencias o impactos asociados.

Magnitud= probabilidad * Impacto

3.1.1.2. Matriz de Priorización y Probabilidades

Para esto se debe considerar lo siguiente:

Probabilidad: Frecuencia que podría presentar el riesgo.

ALTA: Es muy factible que el riesgo se presente

MEDIA: Es factible que el riesgo se presente

BAJA: Es muy poco factible que el riesgo se presente

Impacto: Forma en la cual el riesgo podría afectar los resultados del proceso.

ALTO: afecta en alto grado la disponibilidad del servicio

MEDIO: afecta en grado medio la disponibilidad del servicio

BAJO: afecta en grado bajo la disponibilidad del servicio

En la siguiente gráfica se presenta la matriz de priorización, con la cual se clasificaran los riesgos de acuerdo a su magnitud:

Magnitud A: Nivel de Alto Riesgo

Magnitud B: Nivel Medio de riesgo

Magnitud C: Nivel Bajo de Riesgo

Probabilidad				
	ALTA	B	A	A
	MEDIA	B	B	A
	BAJA	C	B	B
		BAJO	MEDIA	ALTO
		Impacto		

Tabla 3-16. Matriz de Priorización

Basado en la matriz de priorización antes presentada, se realizará el análisis de la magnitud del riesgo de acuerdo al nivel de probabilidad e impacto, para luego sean clasificados según su grado de importancia.

Nº	Riesgo	Control existente	Probabilidad	Impacto	Magnitud
1	Cortes de energía	UPS exclusivo para el Centro de Datos Municipal	Media	Media	B
2	Fallas de UPS	Mantenimiento anual	Baja	Alto	B
3	Fallas en equipo de ventilación (aires acondicionados)	Mantenimiento Anual	Baja	Bajo	C
4	Terremotos	Plan de Contingencia	Baja	Alto	B
5	Tsunami	Centro de datos el Primer Piso del Edificio Municipal	Baja	Alto	B
6	Incendios	Extintores y detectores de humo	Baja	Media	B

7	Desconexión de medio físico por interconexión proveedor de internet	Monitoreo de la red	Baja	Alto	B
8	fallas en el hardware de Equipos del Centro de Datos Municipal	Mantenimiento Anual	Media	Alto	A
9	Fallas en software de Equipos del Centro de Datos Municipal	Respaldo en contingencia diario	Media	Media	B
10	Falla en los equipos de redes comunicación LAN	Monitoreo de disponibilidad de equipos de comunicación	Media	Alto	A
11	Saturación en los equipos de comunicaciones	Monitoreo de tráfico de red	Media	Alto	A

12	Falla en los equipos de radio comunicación para la red MAN	Monitoreo de disponibilidad de equipos de comunicación	Media	Alto	A
13	Interrupción del Servicio de Internet por problemas de última milla	Monitoreo	Baja	Alto	B
14	Interrupción del servicio de Firewall	Monitoreo	Baja	Alto	B
15	Acceso no autorizado a los servidores del Centro de Datos	Lista de acceso y conexión a través de SSH2	Media	Alto	A
16	Acceso no autorizado a los equipos de comunicaciones	Lista de acceso y conexión a través de protocolos de Seguridad	Baja	Alto	A

		WPA2			
17	Actos de ciberataques	Software de Monitoreo	Media	Alto	A
18	Errores Humanos	-	Baja	Alto	B

Tabla 3-17. Análisis de Riesgo

3.1.2. Evaluación de Riesgo

Luego de realizarse la matriz de priorización de riesgo, es importante evaluar los riesgos principales con el propósito de tomar decisiones en base a los resultados obtenidos previamente.

3.1.2.1. Prioridades o Criterios

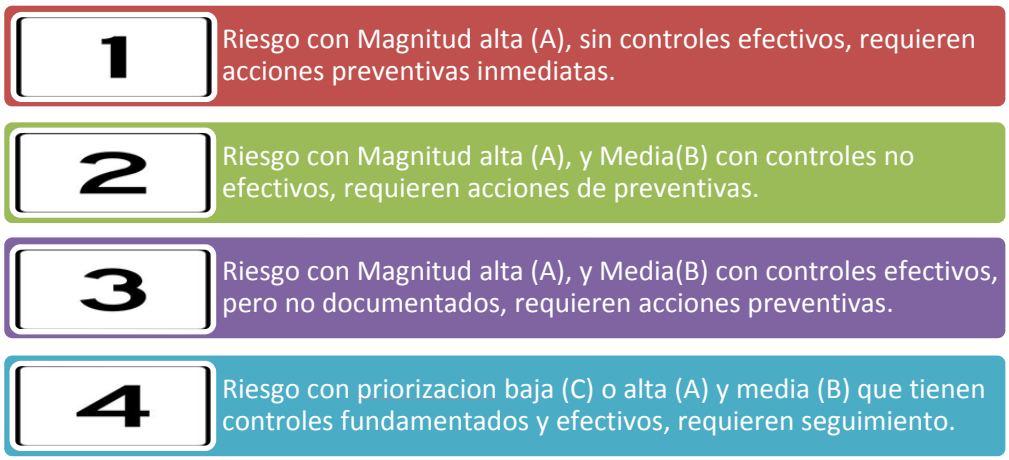


Figura 3-22. Criterios de Evaluación de riesgo

Nº	Riesgo	Criterio	Tratar riesgo
1	Cortes de energía	3	SI
2	Fallas de UPS	3	SI
3	Fallas en equipo de ventilación (aires acondicionados)	4	NO
4	Terremotos	3	NO
5	Tsunami	3	NO
6	Incendios	2	SI
7	Desconexión de medio físico por interconexión proveedor de internet	4	NO
8	fallas en el hardware de Equipos del Centro de Datos Municipal	2	SI
9	Fallas en software de Equipos del Centro de Datos Municipal	3	SI
10	Falla en los equipos de conmutación de la redes LAN	2	SI
11	Saturación en los equipos de comunicaciones	1	SI
12	Falla en los equipos de radio comunicación para la red MAN	2	SI

13	Interrupción del Servicio de Internet por problemas de ultima milla	3	SI
14	Interrupción del servicio de Firewall	2	SI
15	Acceso no autorizado a los servidores del Centro de Datos	1	SI
16	Acceso no autorizado a los equipos de comunicaciones	1	SI
17	Actos de ciberataques	1	SI
18	Errores Humanos	4	NO

Tabla 3-18. Evaluación de Riesgos

3.1.3. Tratamientos de Riesgos

El tratamiento de riesgos permite preparar alternativas y planes que ayuden a mitigar incidentes que afecten a la continuidad del negocio. Cada una de las alternativas identificadas a continuación permitirá combatir los riesgos más evidentes dentro de esta Institución Municipal.

3.1.3.1. Identificación de Alternativas

Alternativas	Descripción
Reducir probabilidad	Bajar la cantidad de veces que se presenta el riesgo en un periodo de tiempo
Reducir impacto	Mitigar las consecuencias negativas cuando se presenta el riesgo
Transferir el riesgo	Traspasar el resigo a otra compañía(contrato de outsourcing, póliza de seguro)
Compartir el riesgo	Consiste en intentar extender el riesgo de un área en concreto, a diferentes secciones, con el fin de impedir la perdida de todo el negocio
Evitar el riesgo	Si prestar de un servicio supone un gran riesgo, el servicio se deja de entregar

Tabla 3.19Alternativas de Manejo de Riesgo

3.1.4. Evaluación de las Alternativas

En el proceso de evaluación de las alternativas se debe apuntar a la mitigación o disminución de incidentes de alto riesgo que tiene la Institución y lograr ejecutar estos procesos en coordinación con las áreas responsables.

Luego del análisis de riesgo se identifican las alternativas a implementar y sus responsables a ejecutar dentro de esta entidad Municipal, esto previa la autorización de la máxima autoridad:

Nº	Riesgo	Alternativas de manejo	Alternativas	Área responsable
1	Cortes de energía	Reducir Impacto	Mantenimiento periódico del generador eléctrico	Dpto. de Servicios Generales
2	Fallas de UPS	Reducir Impacto	Disponibilidad de UPS redundantes en el Centro de Datos Municipal y Mantenimiento Periódicos	Dpto. de Informática
6	Incendios	Reducir probabilidad, impacto y evitar riesgo	Revisión de las Instalaciones Eléctricas periódicamente. Mantenimiento de extintores y sistema de detección de incendio	Dpto. de Servicios Generales
8	Fallas en el hardware de Equipos del Centro de	Reducir probabilidad, impacto y evitar riesgo	Mantenimiento Preventivos periódicos Generar Documentación, para	Dpto. De Servicios Generales e Informática

	Datos Municipal		traspaso de servicio a contingencia Remplazo del Equipo de ser necesario	
9	Fallas en software de Equipos del Centro de Datos Municipal	Reducir probabilidad, impacto y evitar riesgo	Mantenimiento Preventivos periódicos Actualización de Software y Antivirus Implementar un plan efectivo de recuperación y copias de seguridad Generar Documentación, para traspaso de servicio a contingencia	Dpto. de Informática
10	Falla en los equipos de redes comunicación del Centro de Datos Municipal	Reducir Impacto	Revisión de las Instalaciones Eléctricas periódicamente. Mantenimiento Periódico de UPS de los Equipos de Comunicación Remplazo del Equipo de ser necesario	Dpto. De Servicios Generales e Informática

11	Saturación en los equipos de comunicaciones	Reducir Impacto	□ Monitoreo y testeos periódico de la red LAN y MAN de la Institución □ Generación de políticas de Navegación y acceso a la información □Distribución de Carga con otro equipo de comunicación	Dpto. de Informática
12	Falla en los equipos de radio comunicación para la red MAN	Reducir Impacto	□ Revisión de las Instalaciones Eléctricas periódicamente. □Mantenimiento Periódico de UPS de los Equipos de Comunicación □ Remplazo del Equipo de ser necesario	Dpto. De Servicios Generales e Informática
13	Interrupción del Servicio de Internet por problemas de ultima milla	Reducir impacto y probabilidad	□Solicitar al proveedor de Internet un plan de contingencia o respaldo del Servicio	Dpto. de Informática

14	Interrupción del servicio de Firewall y Proxy Server	Reducir impacto y probabilidad	□ Reinicio del Servidor □Revisión de las políticas de acceso □Pentesting del Servidor	Dpto. de Informática
15	Acceso no autorizado a los servidores del Centro de Datos	Reducir Impacto	□ Revisión de las políticas de protección de datos □ Pentesting del Servidor	Dpto. de Informática
16	Acceso no autorizado a los equipos de comunicaciones	Reducir impacto	□ Revisión de las políticas de acceso □ Pentesting del Servidor de Comunicación	Dpto. de Informática
17	Actos de ciberataques	Reducir probabilidad, impacto y evitar riesgo	□ Revisión de las políticas de acceso □ Pentestingde los equipos de Comunicación □Capacitar a los empleados sobre el phishing □Proteger el servidor de correo electrónico.	Dpto. de Informática

			□ Implementar un plan efectivo de recuperación y copias de seguridad □Aplicar plan de contingencia	

Tabla 3-20. Evaluación de Alternativas

3.1.5. Preparación de Planes de Tratamiento

Al preparar el plan de tratamiento se debe identificar las responsabilidades, los resultados esperados de los tratamientos, las medidas de desempeño y el proceso de revisión a establecer.

Se ha considerado para el alcance de este proyecto, que se fundamente en desarrollar medidas de gestión de riesgo específicamente para las áreas de Infraestructura y Comunicación del Municipio y dentro de la implementación de las alternativas establecida para los riesgos más críticos e identificados en la tabla de Evaluación son las siguientes:

Riesgos de prioridad alta:

- Saturación en los equipos de comunicación

- Acceso no autorizado a los servidores del Centro de Procesamiento de Datos
- Acceso no autorizado a los equipos de comunicación
- Actos de ciberataques

Riesgo de prioridad media:

- Fallas en el hardware de Equipos del Centro de Datos Municipal
- Falla en los equipos de conmutación de las redes LAN
- Falla en los equipos de radio comunicación para la red MAN
- Interrupción del servicio de Firewall

Con la información antes destacada se presenta a continuación el índice de magnitud y prioridad cambiante, una vez que se implemente los planes o alternativas de tratamientos.

Riesgo	Sin Tratamiento		Con Tratamiento	
	Magnitud	Prioridad	Magnitud	Prioridad
Saturación en los equipos de comunicaciones	A	1	B	3
Acceso no autorizado a los servidores	A	1	B	3

del Centro de Datos				
Acceso no autorizado a los equipos de comunicaciones	A	1	B	3
Actos de ciberataques	A	1	B	3
Fallas en el hardware de Equipos del Centro de Datos Municipal	A	2	B	4
Falla en los equipos de conmutación de la redes LAN	A	2	B	4
Falla en los equipos de radio comunicación para la red MAN	A	2	B	4
Interrupción del servicio de Firewall	A	2	B	4

Tabla 3-21. Índice de Magnitud y prioridad esperada

Para la verificación de estas alternativas que se adoptaran de forma efectiva dentro de un tiempo específico, se presenta el siguiente plan de pruebas:

- Pruebas de conectividad de toda la redes interconexión.
- Pruebas de conexión red de servidores de forma directa, sin la utilización de filtros, con desconexión del servicio de Internet.
- Pentesting de los servidores de datos Municipales
- Pentesting de conmutadores de red
- Pruebas del plan efectivo de recuperación y copias de seguridad.

- Cumplimiento de Políticas de Seguridad de la Información

3.1.6. Resultados y Ejecución

Para la ejecución de las alternativas de tratamiento del plan de riesgo que permita evitar problemas críticos en lo físico y lógico, es necesario considerar el permiso previo de la máxima autoridad, para que en su posterior se pueda ejecutar paulatinamente todos los procesos con el objetivo primordial de mantener la continuidad del negocio.

Se debe conocer que al ser ejecutada dentro una Institución Pública se debe considerar la optimización de recursos económicos y el presupuesto del área TICs. El ser un ente Municipal no es la excepción, por tal motivo se ha considerado que para la implementación de todo este proceso se necesita el apoyo de todo el personal de la Jefatura de Informática que a su vez cuenta con conocimientos calificados para ejecutar al 100% esta propuesta.

El tiempo que se tomaría la implementación de las alternativas es estimado en tres meses aproximadamente y podría verse afectada de acuerdo a los siguientes factores:

- Proceso de Adquisición de Equipos redundantes (Servidores de Datos, UPS) para el Centro de Procesamiento de Datos.
- Proceso de Contratación de Mantenimientos Periódicos para Servidores y Equipos electicos del Centro de Procesamiento de Datos.
- Capacitación del Personal de la Jefatura incluyendo a líderes de cada Departamento con el fin de replicar políticas y normativas internas.

Las otras alternativas descritas en el Plan de Riesgo se las pueden realizar de forma inmediata una vez autorizado por parte del Departamento de Informática y no demanda costo alguno porque se lo realizaría de forma planificada dentro de las actividades diarias del área.

El espíritu de la gestión de riesgo es que se logre ejecutar en su totalidad cada una de las alternativas de tratamiento y mantener el servicio de los Sistemas Informáticos de forma continua y sin interrupciones.

3.2. Seguridad Física

La importancia de la seguridad física radica en que la institución pública pueda ser una de las más seguras, desde el punto de vista en que se pueda

minimizar las vulnerabilidades de cualquier tipo de ataques sean estos internos o externos, a pesar de que en la actualidad estos aspectos no son tomados en cuenta, se mantiene una lucha por parte de la TI hacia la máxima autoridad de la Institución para que sean priorizados, porque actualmente en el mundo tecnológico en que vivimos estamos propensos a sabotajes , desastres naturales o cyberataque. Al crear formas de detección preventivas a favor de la seguridad física dentro del Centro de Procesamiento de Datos hace que la Institución pueda tener mecanismos de mitigación que permitan la continuidad de las actividades administrativas a pesar del riesgo de ataques Informáticos.

Es indispensable que el entorno en donde se ubican a los Servidores y equipos de conmutación deben estar protegidos por barreras y controles físicos, para evitar de esta manera intrusión física o cualquier otro tipo de amenazas que afecten su normal operación, para esto actualmente la institución cuenta con un área solo para el Centro de Procesamiento de Datos donde están ubicados todos los Servidores y Equipos de comunicación, además de la existencia de una cámara de monitoreo con visión nocturna que captura la imagen del personal que ingresa a este lugar.

Los mecanismos de seguridad física que se puedan implementar en la Institución deben resguardar de amenazas producidas tanto por el hombre como por eventos adversos, y estar basados en un estándar utilizado de forma nacional o internacional tal como se lo está realizando a través de la normativa AS/NZS ISO 31000:2009 orientada a Riesgos.

Los riesgos físicos de altas prioridades detectadas y mencionados en los puntos anteriores son los siguientes:

- Acceso no autorizado a los servidores del Centro de Procesamiento de Datos
- Cortes de Energía que provoquen problemas a los Servidores y Equipos de Comunicación.
- Desperfectos por falta de mantenimiento periódicos a los Equipos Informáticos.

3.3. Seguridad Lógica

Para el tema de seguridad lógica es importante resaltar que en el Centro de Procesamiento de Datos no solo se debe identificar los niveles de daños físicos que puedan sufrir, sino también los daños lógicos que pueda tener la

información crítica almacenada y procesada en los Servidores de Datos ubicados en esa área.

Para la seguridad lógica se necesita de la generación de barreras y procedimientos que resguarden el acceso a los datos y que sólo puedan tener acceso personas autorizadas. El Municipio como Institución contiene información crítica relacionada con el catastro de predios cantonal, así como también el registro de pagos de varios impuestos que se realizan año a año por los contribuyentes, entre otros.

Con el fin de salvaguardar, toda esta información valiosa y de tipo crítica se haplanteado a la máxima autoridad de la Institución los siguientes objetivos:

1. Restringir el acceso a los programas y archivos.
2. Garantizar que la información recibida sea la misma que ha sido transmitida.
3. Garantizar que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro usuario desconocido.
4. Asegurar la integridad, confidencialidad y disponibilidad de la información almacenada.
5. Disponer de sistemas alternativos secundarios de transmisión de datos entre diferentes puntos también conocido como redundancia.

6. Establecer niveles de autenticación en los accesos de datos.
7. Definir un Plan de mantenimiento de software para los servidores de datos existentes.

Se debe considerar que adicional a estos objetivos, al realizar una evaluación y determinación los procedimientos adecuados con respecto a la asignación de permisos, modificaciones de configuración a los equipos de comunicaciones o sistemas operativos, el National Institute for Standars and Tecnology (NIST) plantea los siguientes requisitos mínimos de seguridad que también son considerados para la aplicación en esta Institución Pública:

- Identificación y autenticación
- Asignación de roles
- Limitación de servicios
- Modalidad de acceso
- Controles de acceso interno y externo

3.4. Probabilidades de amenazas y vulnerabilidades críticas

Las amenazas y vulnerabilidades hoy en día pueden producir mucho daño a una institución pública si no se toma las precauciones debidas de seguridad informática, este tipo de amenaza puede ser externo, tales como las

agresiones naturales o humanas, así como también las internas, como negligencia del propio personal, condiciones, procesos operativos internos, entre otros. En lo referente a las amenazas más alarmantes que según la "Encuesta sobre Seguridad y Crimen de Computación – 2008″ del Instituto de Seguridad de Computación (CSI por sus siglas en inglés) encuesta basada en base en 433 respuestas de diferentes entidades privadas y estatales en los EE.UU, se presenta la siguiente gráfica.

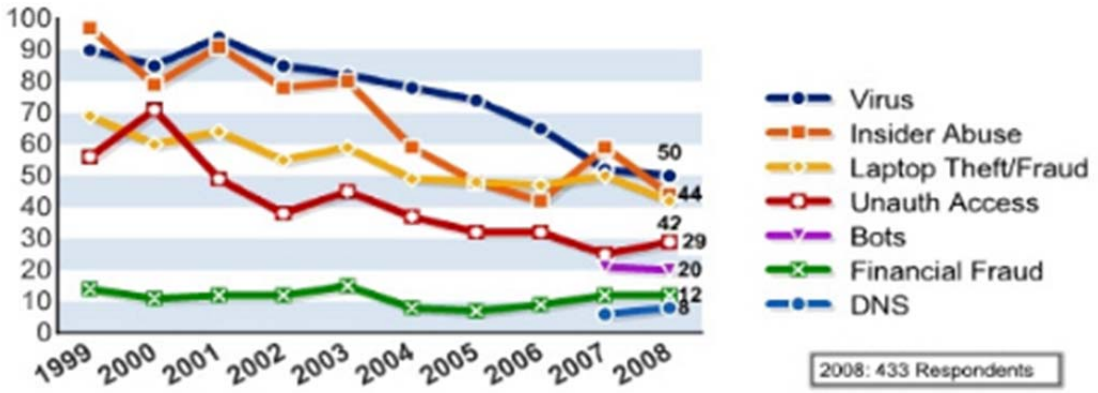


Figura 3-23. Encuestas sobre seguridad y crimen informático.

Por tal motivo se debe tomar con mucha seriedad el tema de seguridad por parte de la máxima autoridad Municipal, porque en caso de existir un ataque severo a la Institución, este puede tener un impacto alto y afectar económicamente. Cabe entender que actualmente existen herramientas de libre descarga en el Internet que han hecho más fácil la identificación y

explotación de los recursos de la red, Sistemas Operativos, servicios, entre otros, causando que los atacantes puedan vulnerar sin necesidad de ser expertos en área.

A continuación se presenta en la siguiente figura los productos más afectados por vulnerabilidades informáticas según INTECO[12] en su informe de Vulnerabilidades del 2011.

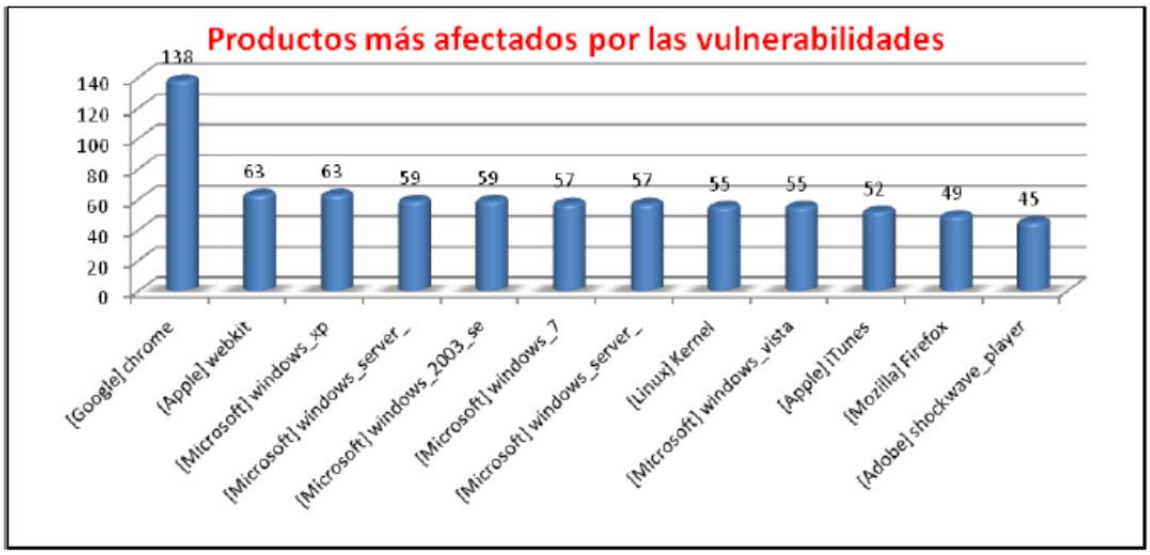


Figura 3-24. Productos más afectados por las vulnerabilidades

Además es importante citar los fabricantes más afectados por las vulnerabilidades según INTECO

[12] INTECO Cert, "Informe de Vulnerabilidades 2011" <http://www.inteco.es//extfrontinteco/img/File/intecocert/Formacion/EstudiosInformes/Vulnerabilidades/cert_inf_vulnerabilidades_semestre_1_2011.pdf>.

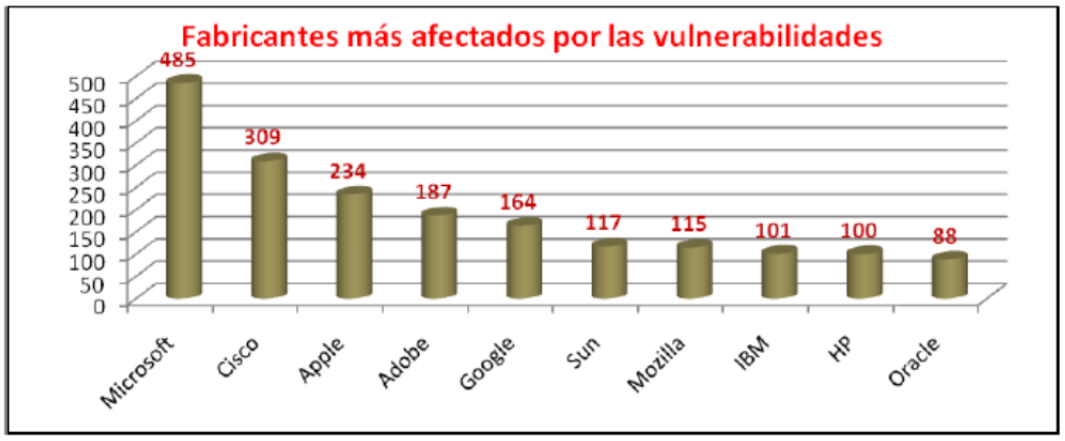


Figura3-25. Fabricantes más afectados por las vulnerabilidades

Estas estadísticas identifican claramente que las aplicaciones de los fabricantes más reconocidos son vulneradas, por tanto se hace necesario realizar una evaluación del tipo de vulnerabilidades que puedan existir en el centro de datos Municipal que arroje resultados reales y basados en los resultados obtenidos de plantear políticas de seguridad que garanticen la integridad de la información y la continuidad de la Institución

3.4.1. Herramientas utilizadas para detección de vulnerabilidades

Para la detección de vulnerabilidades o amenazas se ha utilizado las siguientes herramientas:

Tipo de Herramienta	Descripción
Linux Backtrack 5 r3	Sistema Operativo de distribución GNU/Linux diseñada para la auditoría de seguridad Informática
Metas ploitable	Versión de Ubuntu Linux intencionalmente vulnerable diseñada para probar herramientas de seguridad y demostrar vulnerabilidades comunes.
Wireshark	Analizador de Protocolo utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos
Network Scan	Utilidad gratuita que permite el análisis de la red LAN
Nmap	Programa de código abierto que sirve para efectuar rastreo de puertos y IP especificas
Zenmap	Utilidad grafica de código abierto que facilita el uso del comando nmap en los sistemas operativos Windows
Ubuntu 12.04	sistema operativo basado en Linux y que se distribuye como software libre
Foca	Herramienta de análisis de metadata, utilizada

	para encontrar información oculta en documentos de Microsoft Office, Open Office y documentos PDF/PS/EPS, extraer todos los datos de ellos exprimiendo los ficheros al máximo y una vez extraídos cruzar toda esta información para obtener datos relevantes de una empresa.
NeXpose	Herramienta grafica que permite el análisis y clasificación de vulnerabilidades, aplicación de meta exploit, generación de reportes estadísticos en base a las vulnerabilidades encontradas.
Nesuss	Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos
Maltego	Programa que **recopila información** de internet y la representa de forma gráfica para que sea sencilla de analizar, es una herramienta muy potente, llena de opciones que pueden ser muy útiles para investigar empresas, sitios, personas y mucho más.

Tabla 3-22. Herramientas utilizadas para la detección de vulnerabilidades

3.5. Intento de Intrusión Externa

3.5.1. Identificación de Objetivos y Recolección de Información

Para la identificación de los objetivos con la empresa o Institución se debe tratar el tema de confidencialidad de la información y el alcance del testeo, es decir que hay que identificar cuáles van a ser las reglas del negocio con los encargados de la Institución, de tal forma que se pueda llegar a acuerdos que permitan en horas determinadas realizar todo tipo de análisis sin que la Institución sufra problemas de saturación o incidentes que pueda paralizar las actividades administrativas.

La recolección de información consiste en la aplicación de varias técnicas para el reconocimiento de información del objetivo, previo a la auditoria de tipo hacking ético que se realizará al Municipio. A mayor información recolectada, mayor probabilidad de detección de vulnerabilidades.

La recolección de información, también se puede considerar como la construcción de un perfil básico de la entidad u organización utilizando información que está disponible de forma pública en la Web.

3.5.2. Recolección de Información a través de herramientas de la red

Nuestra primera prueba es básicamente a través del comando ping y la consola de comando CMD de una máquina con Sistema Operativo Windows y así lograr obtener la IP del servidor Web, el mismo que dio como resultado la IP 186.42.198.98, que es la dirección pública en la que se encuentra alojado el portal Web de la institución sin permitirme hacer pruebas ICMP, diagnosticar las condiciones de transmisión, a continuación se ilustra en la siguiente gráfica.

Figura 3-26. Comando Ping

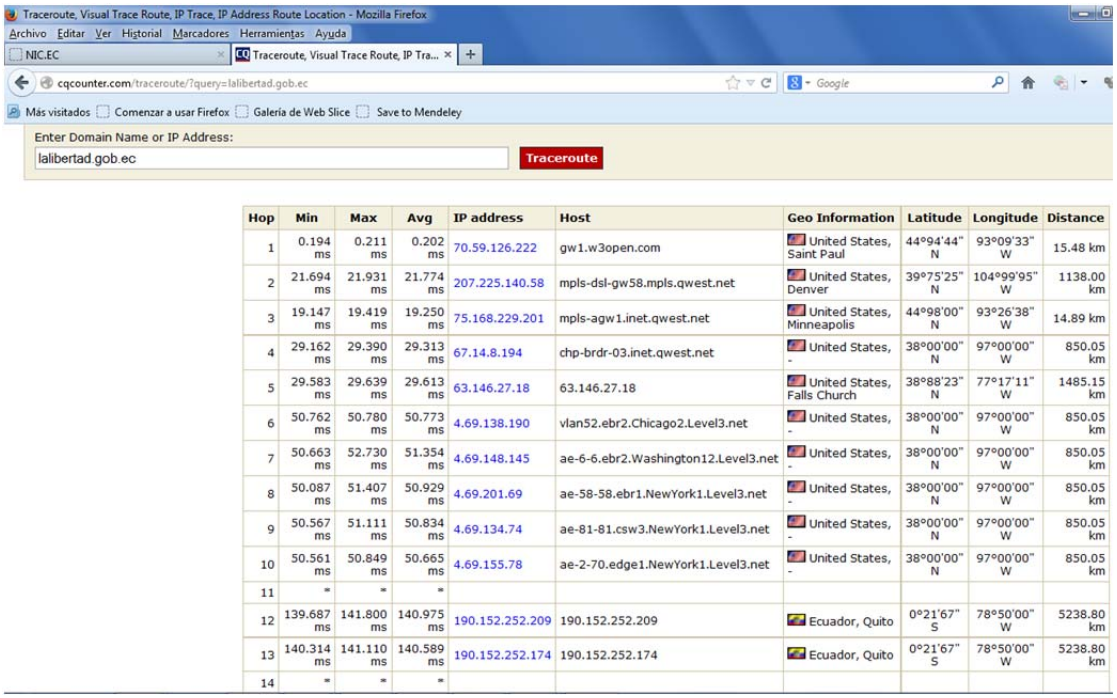
Para la siguiente actividad se utilizó el portal de Registro de Dominio en el Ecuador “NIC.EC”,que consiste en una base de datos de todas las instituciones que existen en Ecuador que tiene Sitio o Portal Web. Este Portal posee una herramienta llamada Whois, el mismo que permite la extracción de información de la institución a través del registro de su dominio, se ilustra en la siguiente gráfica.

Figura 3-27. Portal de Registro de Dominios del Ecuador

Cabe indicar que esta información que aparece en el portal de registro de dominio es pública, la misma que es solicitada mediante formulario por la NIC previo al registro del Portal Web sea esta para entidades públicas o privadas.

En continuación de este proceso de footprinting utilizamos la URL **http://cqcounter.com/traceroute/?query=ciudaddeleste.gob.ec** y escogemos la opción de Traceroute, el mismo que permitirá identificar donde se encuentra configurado el servidor de ruteo al Portal Web Institucional, no su ubicación física.

Mediante la siguiente gráfica se identifica que su ubicación del servicio de ruteo por parte del proveedor de internet está en la Ciudad de Quito.



Hop	Min	Max	Avg	IP address	Host	Geo Information	Latitude	Longitude	Distance
1	0.194 ms	0.211 ms	0.202 ms	70.59.126.222	gw1.w3open.com	United States, Saint Paul	44°94'44" N	93°09'33" W	15.48 km
2	21.694 ms	21.931 ms	21.774 ms	207.225.140.58	mpls-dsl-gw58.mpls.qwest.net	United States, Denver	39°75'25" N	104°99'95" W	1138.00 km
3	19.147 ms	19.419 ms	19.250 ms	75.168.229.201	mpls-agw1.inet.qwest.net	United States, Minneapolis	44°98'00" N	93°26'38" W	14.89 km
4	29.162 ms	29.390 ms	29.313 ms	67.14.8.194	chp-brdr-03.inet.qwest.net	United States, -	38°00'00" N	97°00'00" W	850.05 km
5	29.583 ms	29.639 ms	29.613 ms	63.146.27.18	63.146.27.18	United States, Falls Church	38°88'23" N	77°17'11" W	1485.15 km
6	50.762 ms	50.780 ms	50.773 ms	4.69.138.190	vlan52.ebr2.Chicago2.Level3.net	United States, -	38°00'00" N	97°00'00" W	850.05 km
7	50.663 ms	52.730 ms	51.354 ms	4.69.148.145	ae-6-6.ebr2.Washington12.Level3.net	United States, -	38°00'00" N	97°00'00" W	850.05 km
8	50.087 ms	51.407 ms	50.929 ms	4.69.201.69	ae-58-58.ebr1.NewYork1.Level3.net	United States, -	38°00'00" N	97°00'00" W	850.05 km
9	50.567 ms	51.111 ms	50.834 ms	4.69.134.74	ae-81-81.csw3.NewYork1.Level3.net	United States, -	38°00'00" N	97°00'00" W	850.05 km
10	50.561 ms	50.849 ms	50.665 ms	4.69.155.78	ae-2-70.edge1.NewYork1.Level3.net	United States, -	38°00'00" N	97°00'00" W	850.05 km
11	*	*	*						
12	139.687 ms	141.800 ms	140.975 ms	190.152.252.209	190.152.252.209	Ecuador, Quito	0°21'67" S	78°50'00" W	5238.80 km
13	140.314 ms	141.110 ms	140.589 ms	190.152.252.174	190.152.252.174	Ecuador, Quito	0°21'67" S	78°50'00" W	5238.80 km
14	*	*	*						

Figura 3-28. Traceroute Portal Web "ciudaddeleste.gob.ec"

3.5.3. Reconocimiento Pasivo

Una de las técnicas para el reconocimiento pasivo es utilizar el buscador Google con técnicas de Hacking; esta herramienta ha demostrado ser un potente buscador de información pública. Google Hacking es muy utilizada para la investigación de fuga de información a través de Sitios o Portales Web en especial si estamos realizando recolección de información.

Para esta prueba ingresamos al navegador de google y digitamos en el buscador los siguientes sufijos tal y como se muestra en la Figura 3.15, el resultado de esta prueba dio como resultado que el SitioWeb Institucional tiene un entorno administrativo montado en la Web, así como también que la plataforma de desarrollo es Joomla.

Figura 3.29. Búsqueda con google hacking1

Figura 3-30. Búsqueda con google hacking2

Otra importante herramienta en el proceso de recolección de información es utilizar un Plug-in de Firefox llamado PASSIVERECON, esta herramienta permite a los Analistas de Seguridad realizar proceso de recolección de información automáticamente de varios sitios Web. Para el proceso de instalación solo se debe ingresar a la dirección https://addons.mozilla.org/en-us/firefox/addon/passiverecon/. Y descargar la extensión en el navegador

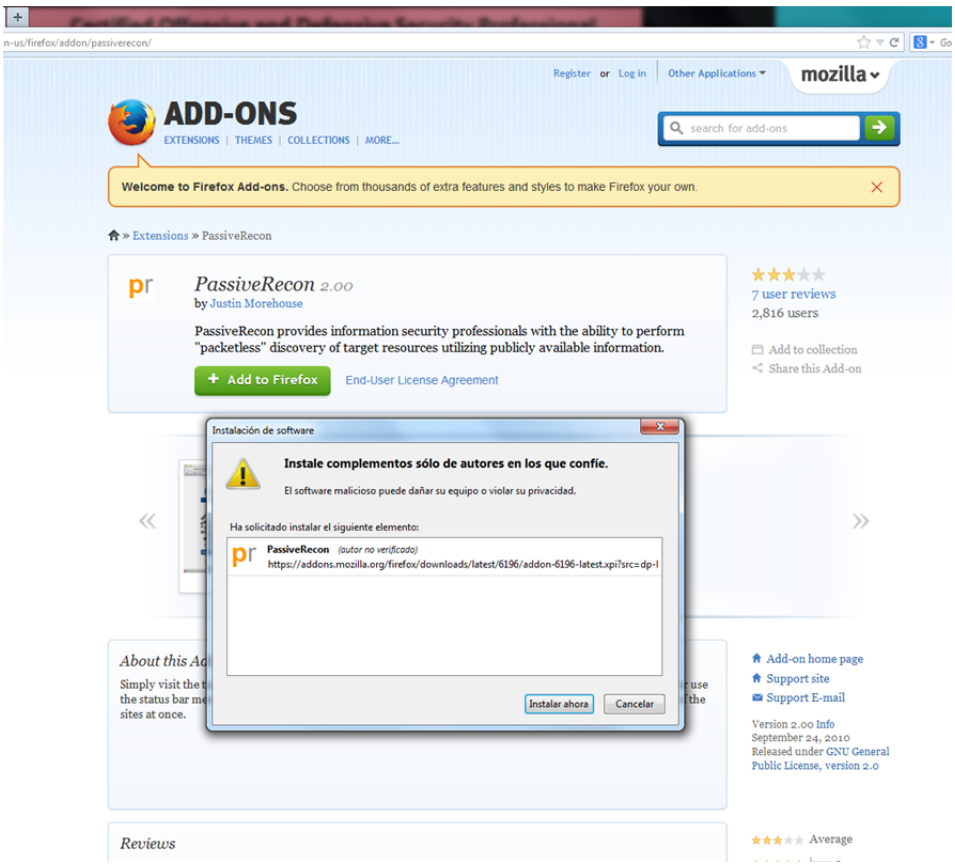


Figura 3-31. Instalación de la Extensión PassiveRecon2.00

Luego de la instalación la extensión Passive Recon 2.00, podemos abrir el navegador de firefox e ingresar en la URL del sitio web que quiera evaluar, posterior a esto dar clic derecho y escoger el aplicativo con la opción “show all”, esto genera veinte y tres operaciones, es decir llama a veinte y tres ventanas en firefox con aplicativos web como netcraft, DNS tool, robtex entre otros.

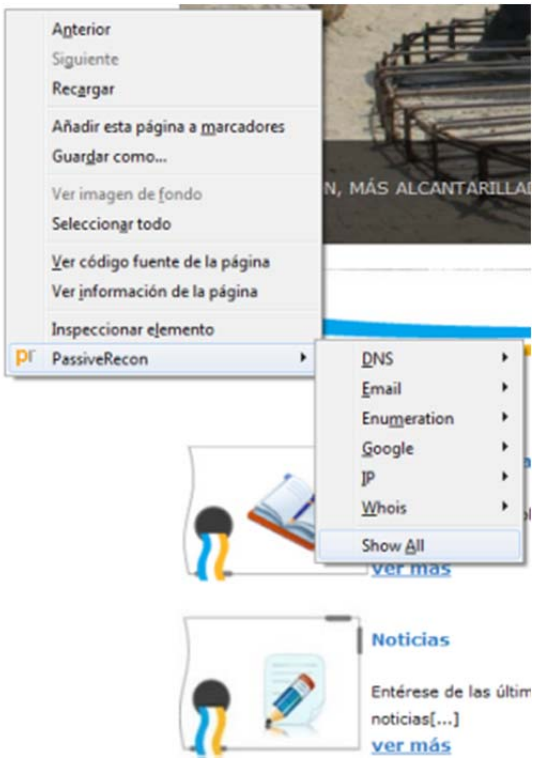


Figura 3-32. Opción del PassiveRecon

NetCraft es una herramienta de análisis de seguridad que permite presentar información relevante de la institución, entre ellas:

- Proveedor ISP de la Institución
- Dirección IP del Servidor que administra el Portal Web
- Si estas en lista negra
- Reverse DNS

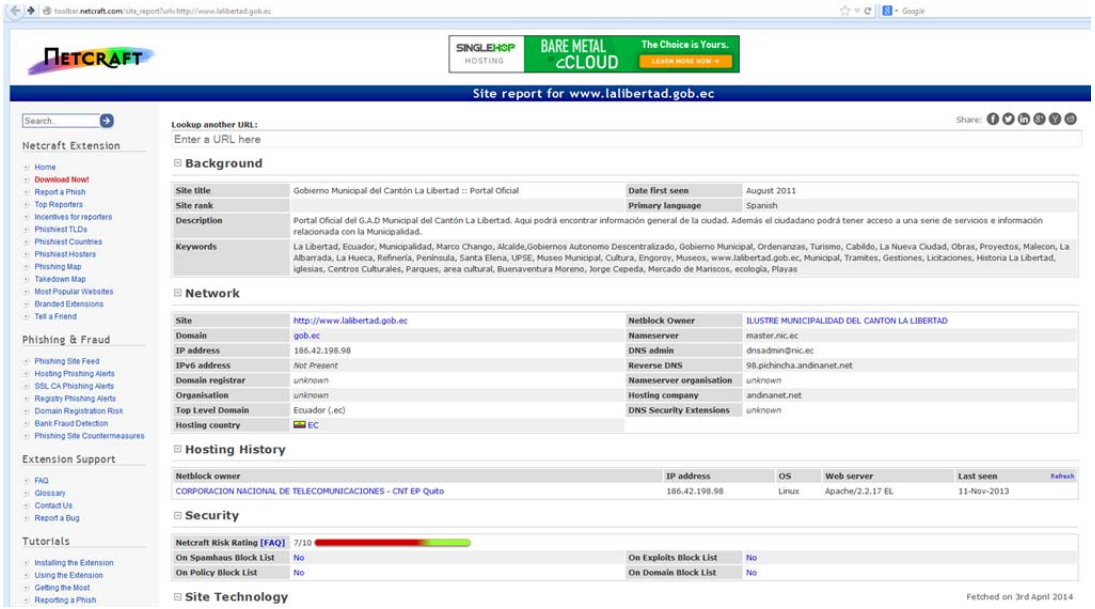


Figura 3-33. Análisis Web, Netcraft

Así también se puede apreciar que la siguiente dirección **http://whois.domaintools.com/ciudaddeleste.gob.ec**, permite realizar un whois del Dominio de la institución extrayendo la siguiente información: representante legal y responsable de áreas administrativas de la Institución, fecha de caducidad del dominio, etc., material que puede servir para posteriormente realizar un proceso de Ingeniería Social.

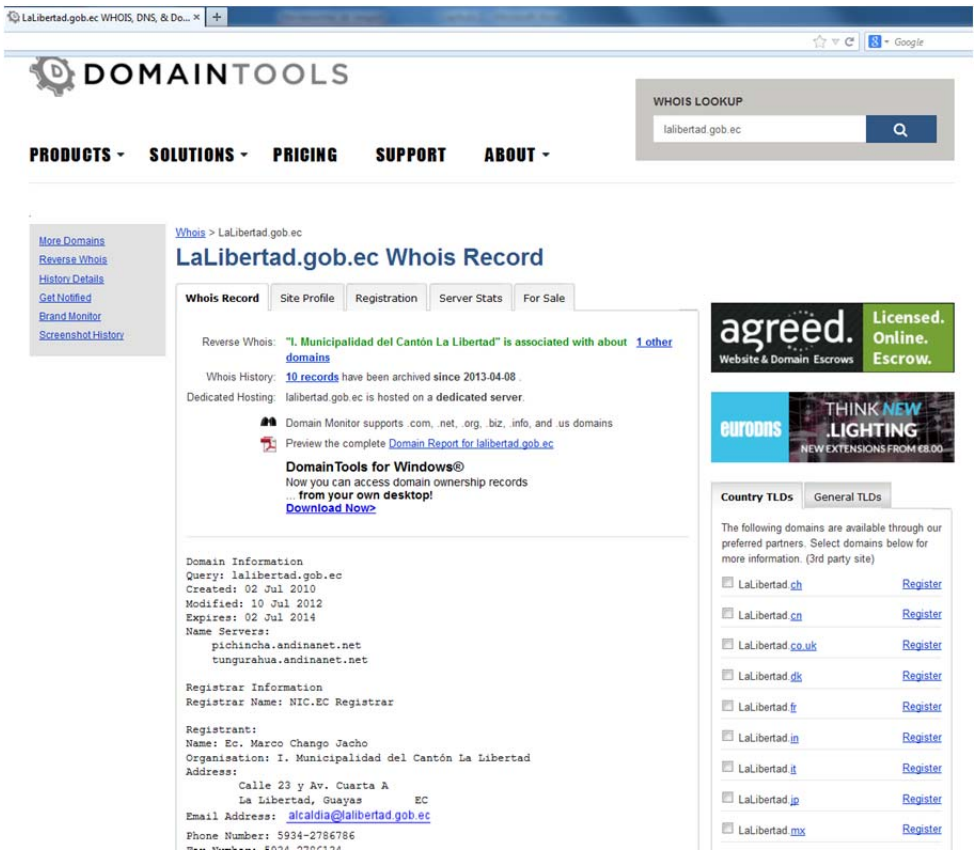
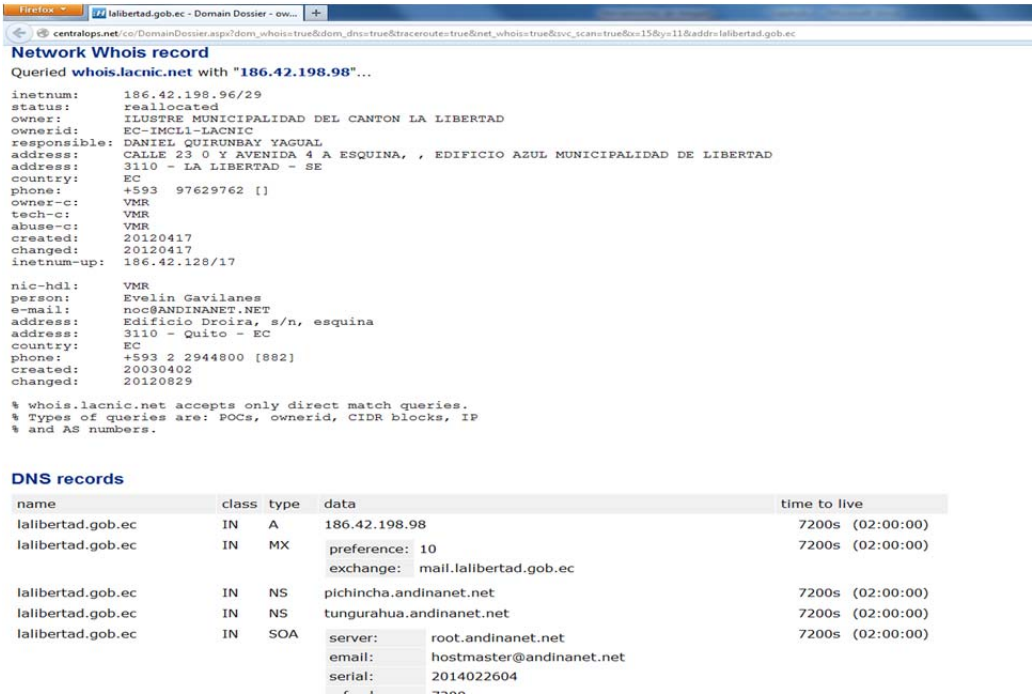


Figura 3-34. Herramienta domaintools

Otra de las herramientas de evaluación Domain Dossier que permite confirmar la información descrita por otras herramientas mencionadas en este documento, el mismo que hace un análisis por IP, extrayendo de esta manera información como son: Network Whois record, DNS records, entre otros.



Network Whois record

Queried whois.lacnic.net with "186.42.198.98"...

```
inetnum:      186.42.198.96/29
status:       reallocated
owner:        ILUSTRE MUNICIPALIDAD DEL CANTON LA LIBERTAD
ownerid:      EC-IMCL1-LACNIC
responsible:  DANIEL QUIRUNBAY YAGUAL
address:      CALLE 23 0 Y AVENIDA 4 A ESQUINA, , EDIFICIO AZUL MUNICIPALIDAD DE LIBERTAD
address:      3110 - LA LIBERTAD - SE
country:      EC
phone:        +593  97629762 []
owner-c:      VMR
tech-c:       VMR
abuse-c:      VMR
created:      20120417
changed:      20120417
inetnum-up:   186.42.128/17

nic-hdl:      VMR
person:       Evelin Gavilanes
e-mail:       noc@ANDINANET.NET
address:      Edificio Droira, s/n, esquina
address:      3110 - Quito - EC
country:      EC
phone:        +593 2 2944800 [882]
created:      20030402
changed:      20120829

% whois.lacnic.net accepts only direct match queries.
% Types of queries are: POCs, ownerid, CIDR blocks, IP
% and AS numbers.
```

DNS records

name	class	type	data	time to live
lalibertad.gob.ec	IN	A	186.42.198.98	7200s (02:00:00)
lalibertad.gob.ec	IN	MX	preference: 10 exchange: mail.lalibertad.gob.ec	7200s (02:00:00)
lalibertad.gob.ec	IN	NS	pichincha.andinanet.net	7200s (02:00:00)
lalibertad.gob.ec	IN	NS	tungurahua.andinanet.net	7200s (02:00:00)
lalibertad.gob.ec	IN	SOA	server: root.andinanet.net email: hostmaster@andinanet.net serial: 2014022604	7200s (02:00:00)

Figura 3-35. Herramienta Domain dossier

Finalmente unas de las herramientas muy utilizada por los Analistas de Seguridad para el levantamiento de información basado en la metodología de numeración es Theharvester.py que está instalado en el BackTrack 5R3 y que permite auditar el dominio de la Institución a partir de correos electrónicos, nombres de dominios, subdominios y listados de IP's

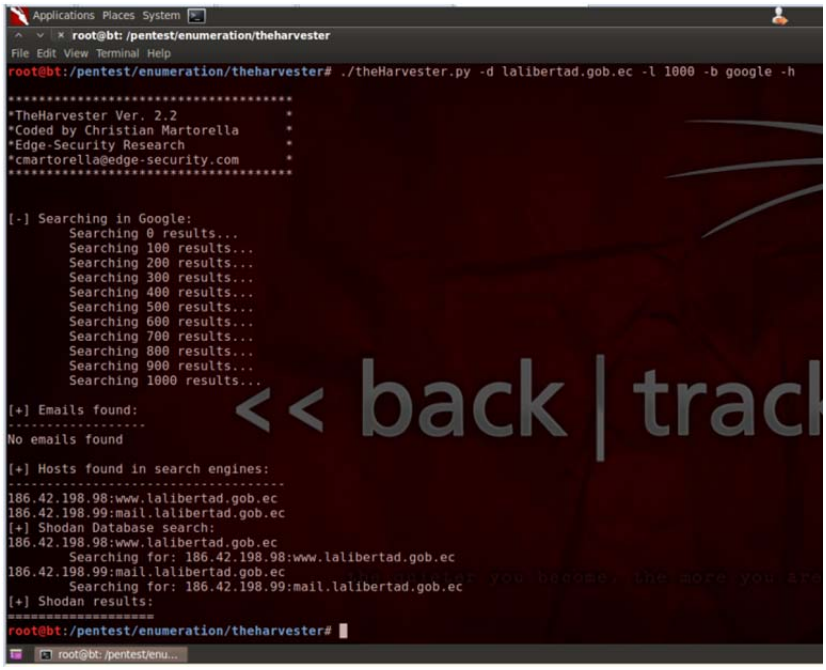


Figura 3-36. Utilidad the harvester en backtrack5r3

Los resultados que presenta esta utilidad son las IP públicas relacionadas al dominio de la institución, de las cuales la IP 186.42.198.99 es identificado por esta herramienta como el servidor de correo electrónico, ambas IP sirve para poder realizar un mapeo de puerto y lograr identificar cuales están abierto y su grado de riesgo.

Para identificar el estado de los puertos, se utilizará el comando “nmap” para cada una de las IP de los equipos encontrados.

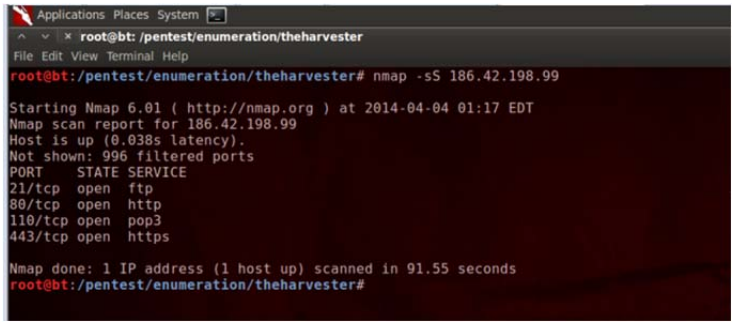


Figura 3-37. Manejo de NMAP

El resultado del comando nmap para la IP 186.42.198.99 ha encontrado 4 puertos abiertos (Servicios FTP, http, pop3, https) que posteriormente serán evaluados y se verificara si es necesario mantenerlos con ese estado o de lo contario serán cerrados.

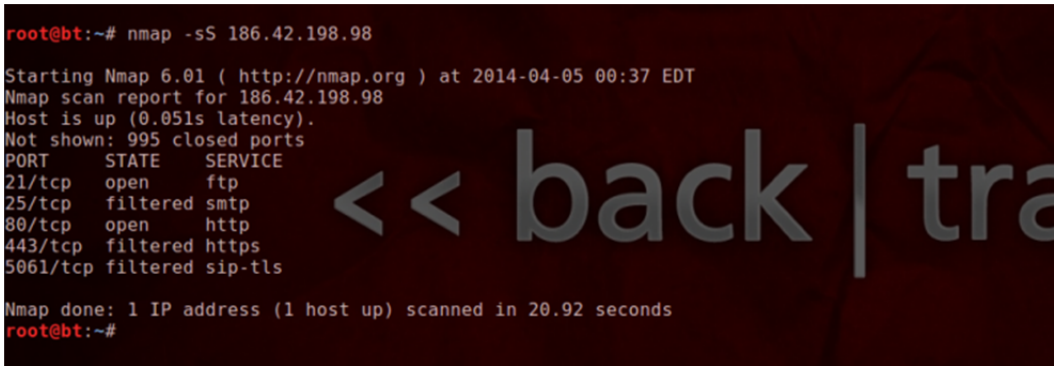


Figura 3-38. Ejecución comando NMAP

El resultado del comando nmap para la IP 186.42.198.98 ha encontrado 2 puertos abiertos (Servicios FTP, http) y tres filtrados (SMTP, HTTPS, SIP-TLS) que al igual que el anterior serán evaluados y se verificara si es necesario mantenerlos con ese estado o de lo contario serán cerrados.

Para confirmar el resultado anterior con el Servicio POP3 que se encontraba abierto para la IP 86.42.198.99 se realizó una prueba de conectividad a través del comando telnet, el cual se logró conectar con el servidor a través del puerto 110, como se demuestra en la siguiente gráfica.

Figura 3-39. Comando Telnet

Para confirmar que el resultado anterior con el servicio FTP se encontraba abierto para la IP 186.42.198.98 se realizó una prueba de conectividad a través del comando ftp, cuyo resultado fue una conexión exitosa y lista para ingresar usuario y contraseña, se observa en la siguiente gráfica.

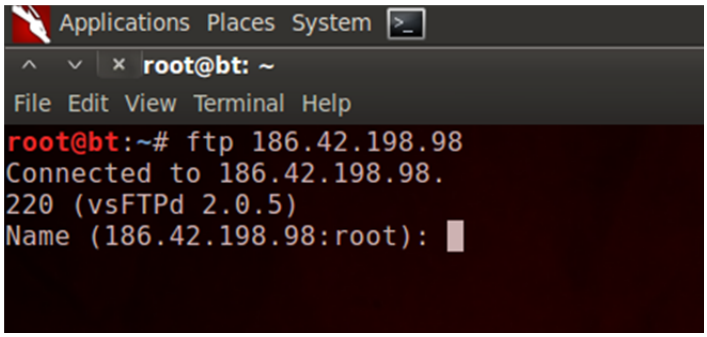


Figura 3-40. Comando FTP

A través del software Maltego versión 3.1.1 que viene incorporado en Backtrack 5 r3, se logró identificar cuáles son los enlaces o links externos

que tiene el Portal Web, como parte de la recopilación de información sobre nuestro target u objetivo de evaluación actual.

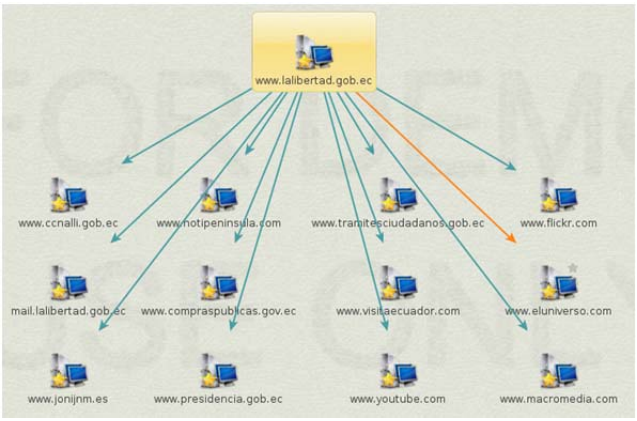


Figura 3-41. Mapa de enlaces externo Sitio Web

Esta evaluación permite identificar vínculos o enlaces externos que puede tener la institución y de esta manera generar algún tipo de ataque de ingeniería social.

Luego se realizó un análisis de vulnerabilidad del Portal Web que fue realizado a través de la herramienta instalada en el Backtrack llamado "WhatWeb" esto en relación a que el portal fue desarrollado en joomla. El comando que se ejecutó es el siguiente:

/pentest/enumeration/web/whatweb# ./whatweb -v www.ciudaddeleste.gob.ec

Los resultados de este análisis identificaron que la plataforma de desarrollo del Porta Web es Joomla, razón por la cual se realizó un análisis más profundo de las vulnerabilidades del Portal Web a través de la herramienta “joomscan” de BackTrack, esto se muestra en la siguiente gráfica:

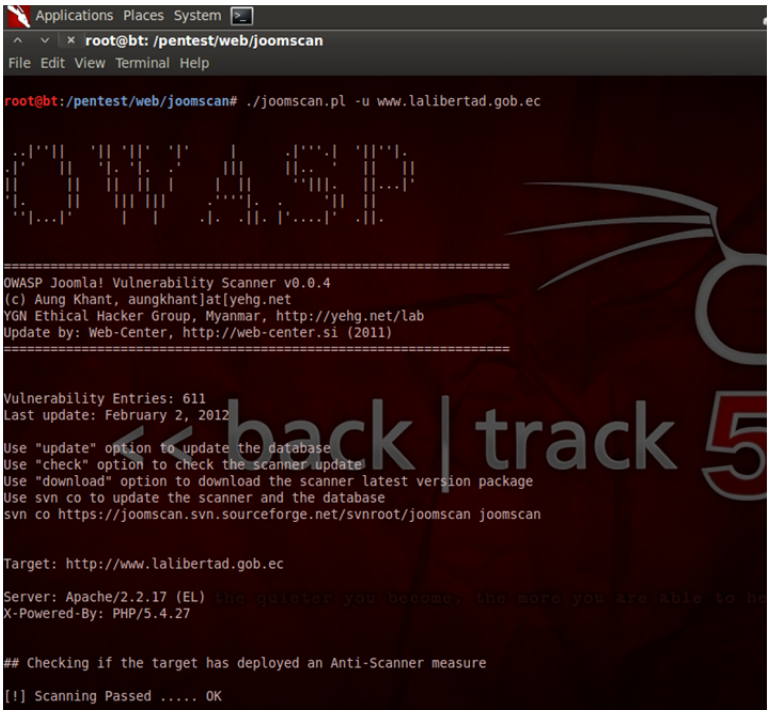


Figura 3-42. Análisis de vulnerabilidades Portal Web Municipal

Los resultados visualizados luego de la ejecución del comando son los siguientes:

Figura 3-43. Vulnerabilidad portal Web # 1

Esta vulnerabilidad identifica que se debe corregir el archivo htaccess.txt con el fin de evitar ataques exitosos desde la nube del internet.

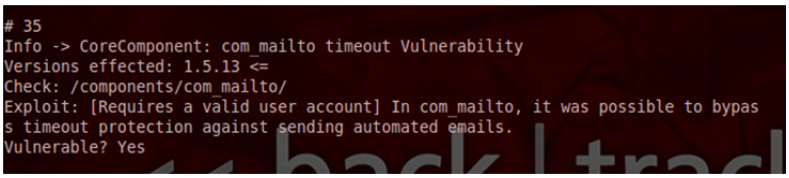


Figura 3-44. Vulnerabilidad portal Web # 2

Este reporte identifica que se debe corregir errores en la configuración del componente de correo electrónico de Joomla con el objetivo de que no se convierta en un bypass por parte de una persona no autorizada.

Luego del testeo externo previo se logra identificar dos IP públicas que están ligadas a la institución, las mismas que son 186.42.198.98/29 y 186.42.198.99/29. A estas IP se les realizó el levantamiento de información

de los puertos abiertos que poseen cada una de ellas, para el siguiente proceso se utilizó la herramienta de mapeo de puertos NMAP

Línea de comando para obtención de información es:

Nmap -sS –sV –O 186.42.198.98Nmap -sS –sV –O 186.42.198.99

Nmap –sV –sU –O 186.42.198.98Nmap –sV –sU –O 186.42.198.99

Una vez ejecutada la instrucción a las direcciones de IP Públicas se logra obtener los siguientes resultados:

Dirección IP: 186.42.198.98/29			
Actividad del Servidor: Servidor Firewall y Proxy			
Sistema Operativo: Linux 2.6.18			
Puerto	**Protocolo**	**Servicio**	**Versión**
21	TCP	FTP	Vsftpd 2.0.5
25	TCP	SMTP	
80	TCP	HTTP	Apache httpd 2.2.17
443	TCP	HTTPS	
5061	TCP	SIP-TLS	
1900	UDP	upnp	

Tabla 3-23. Tabla de IP Pública encontrada Servidor Firewall

Dirección IP: 186.42.198.99/29			
Actividad del Servidor: Servidor de Correo Electrónico			
Sistema Operativo: Microsoft Windows 2003 SP2			
Puerto	**Protocolo**	**Servicio**	**Versión**
21	TCP	FTP	Microsoft Ftpd
80	TCP	HTTP	Microsoft IIS Httpd 6.0
110	TCP	POP3	Mail Max
443	TCP	SSL/HTTP	Kerio Mail Server

Tabla 3-24. Tabla de IP Pública encontrada Servidor de Correo

3.6. Intento de Intrusión Interna

Uno de los primeros pasos que se deben realizar en el levantamiento de información para identificar vulnerabilidades en la red LAN o MAN en una Institución, es realizar un Network Mapping (Mapeo de la Red), que consiste en tratar de identificar la arquitectura de la red a la cual vamos a realizar pruebas de auditoría a nivel intrusivo.

3.6.1. Escaneo de Red LAN

A través de la herramienta “Network Scanner ”instalado en una máquina con Windows ubicado dentro de la red LAN y además conocedores de que la

dirección de red de la Institución es 120.40.64.0 /20, se logra realizar un escaneo a toda la red para identificar las IP vivas, de las cuales específicamente nos interesan extraer las IP de los servidores y equipos de comunicación del Centro de Datos Municipal, de esta manera se está cumpliendo con el objetivo de este proyecto.

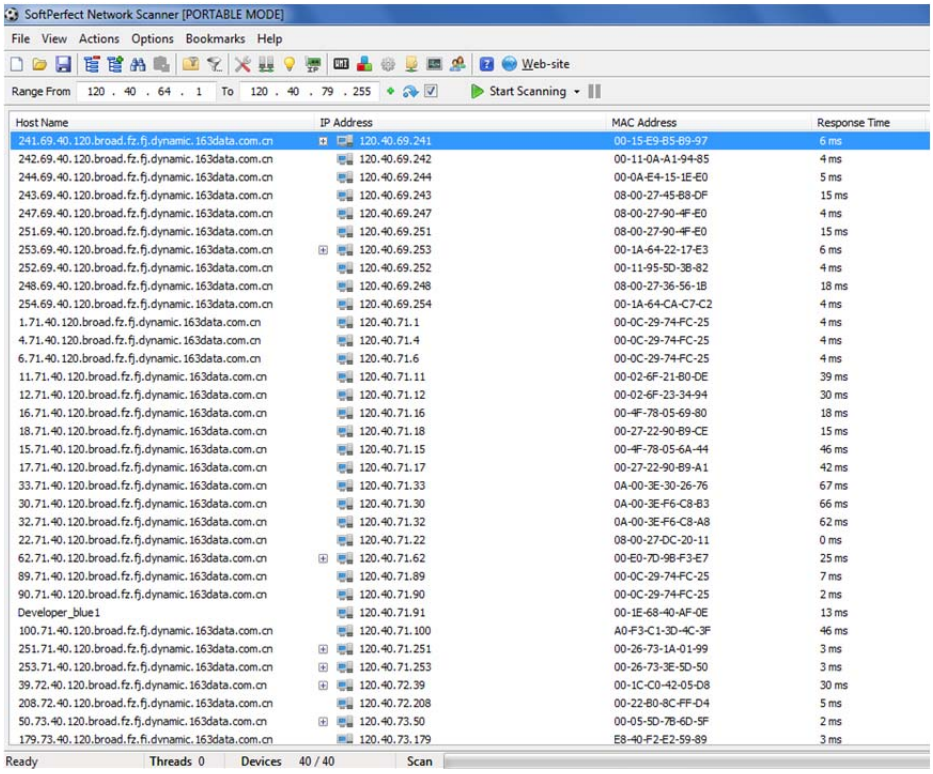


Figura 3-45. Escaneo de puerto con software NetScan

Luego del testeo con la herramienta NetScan, se logró identificar que la mayoría de los equipos que empieza con la dirección de red 120.40.69.XX son Servidores de Datos de la institución que fue constatado por el Jefe del Área, así como también se identificó que los equipos con la dirección de red

120.40.71.XX que en su mayoría son equipos de comunicación, que solo en ciertos casos son IP pertenecen a servidores, luego de haber hecho esta actividad es importante identificar los puertos abiertos, cerrados o filtrados de cada uno de los servidores del target a evaluar.

3.6.2. Scanning de Puertos

Para la exploración de puertos se ha considerado realizar este tipo de actividad con el comando NMAP incluyendo parámetros que no sean ruidosos, es decir que no sean fácil de detectar por Firewall o detectores de intrusos IDS.

Los principales objetivos del escaneo de puerto para la red LAN de la institución son las siguientes:

- Detectar sistemas vivos corriendo o ejecutando procesos en la red
- Descubrir que puertos están abiertos o tienen programas/servicios en ejecución
- Descubrir huellas de sistemas operativos, o lo que se conoce como OS fingerprinter
- Descubrimiento de direcciones IP en la red o sistemas planteados como objetivos

- Identificación de Banners
- Arquitectura del Sistema Evaluado

Una vez identificado los objetivos de un escaneo de puerto, se debe extraer información de todos los equipos del Centro de Datos Municipal a través de comando “nmap”.

La primera prueba la realizaremos utilizando el comando antes mencionado pero con los siguientes parámetros: nmap -v -A 186.42.198.98, a una IP pública de la Institución, el mismo que ilustró los siguientes resultados:

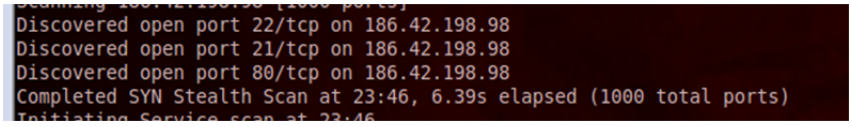


Figura 3-46. Análisis NMAP, Puertos abiertos

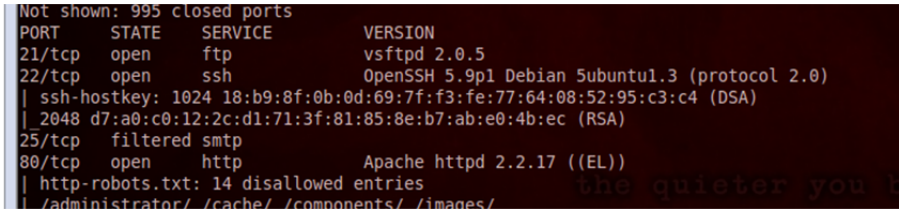


Figura 3-47. Análisis NMAP, Puertos, servicios y versión

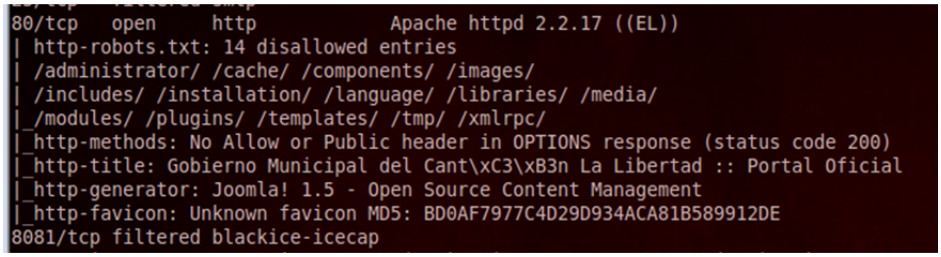


Figura 3-48. Banner con el nombre de la institución y tipo de administrado portal Web

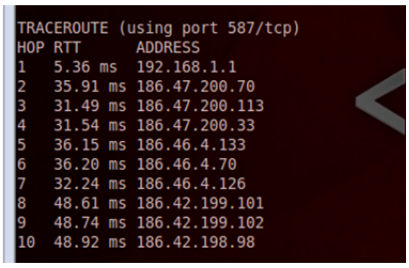


Figura 3-49. Trazado de ruta al momento de hacer ping desde una máquina externa

La Línea de ejemplo utilizado para este levantamiento de información de puertos abiertos para los protocolos TCP /UDP de todos los Servidores del Centro de Datos Municipal en la red LAN son:

Nmap –sV–sS–O 120.40.69.241

Nmap –sV –sU –O 120.40.69.241

Los parámetros del comando indican lo siguiente:

-sV: Busca puertos abiertos para determinar el servicio/versión e información

-sS: escaneo de tipo SYN/Connect

-O: Detección del Sistema Operativo

-sU: escaneo de puertos UDP

Tabla de Servidores del Centro de Datos Municipal

Dirección IP: 120.40.69.241/20			
Actividad de Servidor: Administrador de Virtuales			
Sistema Operativo: Linux 2.6.13 -2.6.32(Open Suse)			
Puerto	Protocolo	Servicio	Versión
22	TCP	SSH	OpenSSH 5.1(protocol 2.0)
111	TCP	rpcbind	Rpc #100000
139	TCP	Netbios-ssn	Samba smbd 3.X
445	TCP	Netbios-ssn	Samba smbd 3.X
873	TCP	rsync	Protocol versión 30
5801	TCP	Vnc-http	TightVNC 1.2.9
5802	TCP	Vnc-http	TightVNC 1.2.9
5901	TCP	vnc	Vnc (protocol 3.7)
5902	TCP	vnc	Vnc (protocol 3.7)
111	UDP	rpcbind	Rpc #100000
137	UDP	Netbios-ns	Microsoft Windows XP
138	UDP	Netbios-dgm	
177	UDP	xdmcp	XDMCP host virtual

			willing
5353	UDP	mdns	Apple mDNSResponder

Tabla 3-25. Tabla de Servidor Administrador de Virtuales

Dirección IP: 120.40.69.242/20			
Actividad de Servidor: Servidor de la Base de Datos Oracle			
Sistema Operativo: Windows 2003 Server (Enterprise Edition)			
Puerto	Protocolo	Servicio	Versión
53	TCP	domain	Microsoft DNS
80	TCP	HTTP	Microsoft IIS Web server 6.0
135	TCP	msrpc	Microsoft Windows RPC
139	TCP	Netbios-ssn	
445	TCP	Microsoft-ds	Microsoft Windows 2003
1025	TCP	msrpc	Microsoft Windows RPC
1026	TCP	msrpc	Microsoft Windows RPC
1029	TCP	msrpc	Microsoft Windows RPC
1043	TCP	Oracle	Oracle Database
1521	TCP	Oracle -tns	Oracle TNSListener
5560	TCP	HTTP	Oracle Aplication
5800	TCP	Vnc-hhtp	RealVNC 4.0

137	UDP	Netbios-ns	Microsoft Windows netbios
445	UDP	Microsoft-ds	
1028	UDP	Domain	Zoom X5 ADSL modem DNS
1645	UDP	radius	
1813	UDP	radacct	
4500	UDP	Nat-t-ike	

Tabla 3-26. Tabla de Servidor de la Base de Datos Oracle

Dirección IP: 120.40.69.243/20			
Actividad de Servidor: Servidor de Cámaras IP			
Sistema Operativo: Microsoft Windows Server 2003			
Puerto	Protocolo	Servicio	Versión
135	TCP	msrpc	Microsoft W
139	TCP	Netbios-ssn	
445	TCP	Microsoft-ds	Microsoft Windows 2003
1025	TCP	msrpc	Microsoft Windows RPC
5800	TCP	VNC-HTTP	VNC(protocol 3.8)
8080	TCP	HTTP	WebCamXPhttpd 5
137	UDP	Netbios-ns	Microsoft Windows NT

445	UDP	Microsoft-ds	
500	UDP	isakmp	
1027	UDP	unknown	
3702	UDP	unknown	
4500	UDP	Nat-t-ike	

Tabla 3-27. Tabla de Servidor de Cámaras IP

Dirección IP: 120.40.69.244/20			
Actividad de Servidor: Servidor de Respaldos			
Sistema Operativo: Linux 2.6.9-2.6.28 (CENTOS 5.3)			
Puerto	Protocolo	Servicio	Versión
21	TCP	FTP	Vsftpd 2.0.5
22	TCP	SSH	OpenSSH 4.3
80	TCP	HTTP	Apache httpd 2.2.3
111	TCP	rpcbind	Rpc #100000
139	TCP	Netbios-ssn	Samba smbd 3.X
443	TCP	ssl/http	Apache httpd 2.2.3
445	TCP	Netbios-ssn	Samba smbd3.X
901	TCP	Tcpwrapped	
5801	TCP	Vnc-http	RealVNC 4.0
5901	TCP	VNC	VNC(protocol 3.8)
6001	TCP	X11	

111	UDP	Rpcbind	Rpc #100000
137	UDP	Netbios-ns	Samba nmbd
5353	UDP	mdns	Apple mdnsResponder

Tabla 3-28. Tabla de Servidor de Respaldos

Dirección IP: 120.40.69.247/20			
Actividad de Servidor: Servidor de Administración Documentación twiki			
Sistema Operativo: Linux 2.6.23-2.6.28 CENTOS			
Puerto	Protocolo	Servicio	Versión
21	TCP	FTP	Vsftpd 2.0.5
22	TCP	SSH	OpenSSH 4.3
80	TCP	HTTP	Apache httpd 2.2.3
111	TCP	rpcbind	Rpc #100000
443	TCP	ssl/http	Apache httpd 2.2.3
3306	TCP	Mysql	MYSQL
10000	TCP	http	MiniServ 0.01 (Webmin)
111	UDP	rpcbind	Rpc #100000
123	UDP	ntp	NTP v4
631	UDP	Ipp	
657	UDP	status	Rpc #100024
5353	UDP	mdns	Apple MdnsResponder

Tabla 3-29. Tabla de Servidor de Documentación twiki

Dirección IP: 120.40.69.248/20			
Actividad de Servidor: Servidor Web Institucional Local			
Sistema Operativo: Linux 2.6.18-2.6.27 CENTOS			
Puerto	Protocolo	Servicio	Versión
22	TCP	SSH	OpenSSH 4.3
80	TCP	http	Apache httpd 2.2.3
443	TCP	Ssl/http	Apache httpd 2.2.3
3306	TCP	Mysql	MySQL

Tabla 3-30. Tabla de Servidor Web Institucional

Dirección IP: 120.40.69.251/20			
Actividad de Servidor: Servidor DNS			
Sistema Operativo: Linux 2.6.9-2.6.28 CENTOS			
Puerto	Protocolo	Servicio	Versión
21	TCP	ftp	Vsftpd 2.0.5
22	TCP	Ssh	OpenSSH 4.3
53	TCP	domain	ISC BIND 9.3.4P1
80	TCP	http	Apache httpd 2.2.3
111	TCP	rpcbind	Rpc #100000
443	TCP	Ssl/http	Apache httpd 2.2.3
3306	TCP	Mysql	MySQL
53	UDP	domain	ISC BIND 9.3.4P1

111	UDP	rpcbind	Rpc #100000
123	UDP	NTP	NTP v4
657	UDP	Status	Rpc # 100024

Tabla 3-31. Tabla de Servidor DNS

Dirección IP: 120.40.69.252/20			
Actividad de Servidor: Servidor Firewall y Proxy			
Sistema Operativo: Linux 2.6.23-2.6.28 CENTOS			
Puerto	Protocolo	Servicio	Versión
22	TCP	SSH	Open SSH 4.3
80	TCP	http-proxy	Squid web proxy 2.6
8080	TCP	http-proxy	Squid web proxy 2.6
3128	TCP	http-proxy	Squid web proxy 2.6
1900	UDP	UPNP	

Tabla 3-32. Tabla de Servidor Firewall y Proxy

Dirección IP: 120.40.69.253/20			
Actividad de Servidor: Servidor de Aplicaciones 1			
Sistema Operativo: Linux 2.6.23-2.6.28 CENTOS			
Puerto	Protocolo	Servicio	Versión
21	TCP	Ftp	Vsftp 2.0.5
22	TCP	SSH	Open SSH 4.3
111	TCP	rpcbind	Rpc #100000

139	TCP	Netbios-ssn	Samba smbd 3.x
445	TCP	Netbios-ssn	Samba smbd 3.x
631	TCP	ipp	CUPS 1.2
2049	TCP	NFS	2-4
5801	TCP	Vnc-http	RealVNC 4.0
5901	TCP	VNC	VNC (protocol 3.8)
7777	TCP	http	Oracle Application Server 10g
7778	TCP	http	Oracle Application Server 10g
1156	TCP	http	Oracle Manager
10000	TCP	http	Miniserv 0.01(Webmin)
20000	TCP	http	Miniserv 0.01(Webmin)
9102	TCP	Jetdirect?	
69	UDP	tftp	
111	UDP	rpcbind	Rpc #100000
137	UDP	Netbios-ns	Samba nmbd
177	UDP	xdmcp	XDMCP host willing
631	UDP	ipp	
2049	UDP	nfs	
10000	UDP	webmin	Httpson TCP port 10000

32768	UDP	nlockmgr	1-4 RPC # 100021

Tabla 3-33. Tabla de Servidor de Aplicaciones 1

Dirección IP: 120.40.69.254/20			
Actividad de Servidor: Servidor de Aplicaciones 2			
Sistema Operativo: Windows 2003 Server SP2			
Puerto	Protocolo	Servicio	Versión
19	TCP	charger	
21	TCP	Ftp	Microsoft Ftpd
25	TCP	smtp	Microsoft ESMTP 6.0.3790
42	TCP	wins	Microsoft Windows Wins
53	TCP	domain	Microsoft DNS
80	TCP	http	Microsoft IIS webserver 6.0
135	TCP	msrpc	Microsoft Windows RPC
139	TCP	Netbios-ssn	
445	TCP	Microsoft-ds	Microsoft Windows 2003
902	TCP	Ssl/vmware-auth	VMwareAuthenticationDaemon1.10
1025	TCP	msrpc	Microsoft Windows RPC
5800	TCP	Vnc-http	RealVNC 4.0
5900	TCP	VNC	VNC(protocol 3.8)
8222	TCP	http	Microsoft IIS webserver 6.0

8333	TCP	Ssl/http	Microsoft IIS webserver 6.0
53	UDP	domain	
123	UDP	NTP	
137	UDP	Netbios-ns	Microsoft Windows netbios
445	UDP	Microsoft-ds	
1645	UDP	Radius	
1646	UDP	radacct	
3456	UDP	IISrcp-or-vat	
4500	UDP	Nat-t-ike	

Tabla 3-34. Tabla de Servidor de Aplicaciones 2

3.6.3. Análisis de Vulnerabilidades

Para el proceso de análisis de vulnerabilidades el objetivo primordial es la identificación y documentación de vulnerabilidades del software y equipos host a utilizar por el cliente. Este tipo de auditoría de Seguridad nos permite identificar fácilmente problemas críticos por la cual un intruso puede vulnerar o extraer información no autorizada de la Institución evaluada.

Este proceso se realiza posterior a la exploración de puertos delos equipos que previamente se ha definido como blanco de ataque, y posteriormente el

siguiente paso será analizar las vulnerabilidades asociadas a los servicios que hay en los puertos abiertos y la búsqueda de solución más óptima a la debilidad presentada según la herramienta a utilizar; para la ejecución de este proceso es necesario utilizar una herramienta que cuente con base de datos de vulnerabilidades previamente identificadas y publicadas en el internet, de las cuales las más conocidas son:

- National Vulnerability Databases
- Security Tech Center de Microsoft
- Simantec Connect

Las vulnerabilidades se pueden categorizar según su criterio en:

- Críticos
- Altos
- Medio
- Bajos
- Información

Para el proceso de análisis de vulnerabilidad utilizaremos la herramienta Nessus Home, versión gratuita de la empresa Tenable Network Security que cuenta con una base de datos de vulnerabilidades ,el mismo que será

instalada en una máquina que servirá de monitor dentro de la red LAN de la Institución como parte del proceso recolección y que permitirá obtener información acerca de las vulnerabilidades más críticas que puedan tener los Servidores del Centro de Procesamiento de Datos Municipal.

3.6.4. La explotación dentro de la Auditoría Técnica

Es necesario mencionar que esta etapa de Auditoría de Seguridad, o del ataque, se considera altamente importante, ya que es aquí donde el auditor de seguridad demuestra al cliente cuales con las vulnerabilidades identificadas y reportadas en la fase anterior, pueden afectar de forma representativa a la integridad, confidenciabilidad y disponibilidad de los Sistemas de Información que utiliza la Institución. Cuando se ejecuta un proceso de explotación, el cliente entenderá que las vulnerabilidades no solo se reportan en un informe técnico, sino también se intenta explotar, logrando así un ataque real pero controlado en el sistema del cliente o usuario.

3.6.4.1. Riesgos en el Proceso de Explotación

Entre los riesgos más frecuente al momento de realizar el proceso de explotación son los siguientes:

- Caída de servicio

- Caída del sistema
- Denegación de servicios
- Perdida de confidencialidad en datos
- Perdida de disponibilidad
- Exposición de información confidencial
- Impacto en la estabilidad del sistema evaluado

Basado en esta recomendación se definió que la explotación de vulnerabilidades se realice en horas de almuerzo y al finalizar la jornada laboral, que a su vez debe ser coordinado con la Administración de la Institución y el Jefe Departamental del área de Informática.

La ejecución de este proceso se realizara en un tipo estimado de un mes y puede ser extendido de acuerdo a los situaciones que se presente en la auditoria a los equipos Informáticos.

A continuación a través de la siguiente gráfica se muestra las vulnerabilidades encontradas en el servidor de datos con la IP 120.40.69.254 las mismas que son visualizadas y documentadas según la base de datos del Software NESSUS

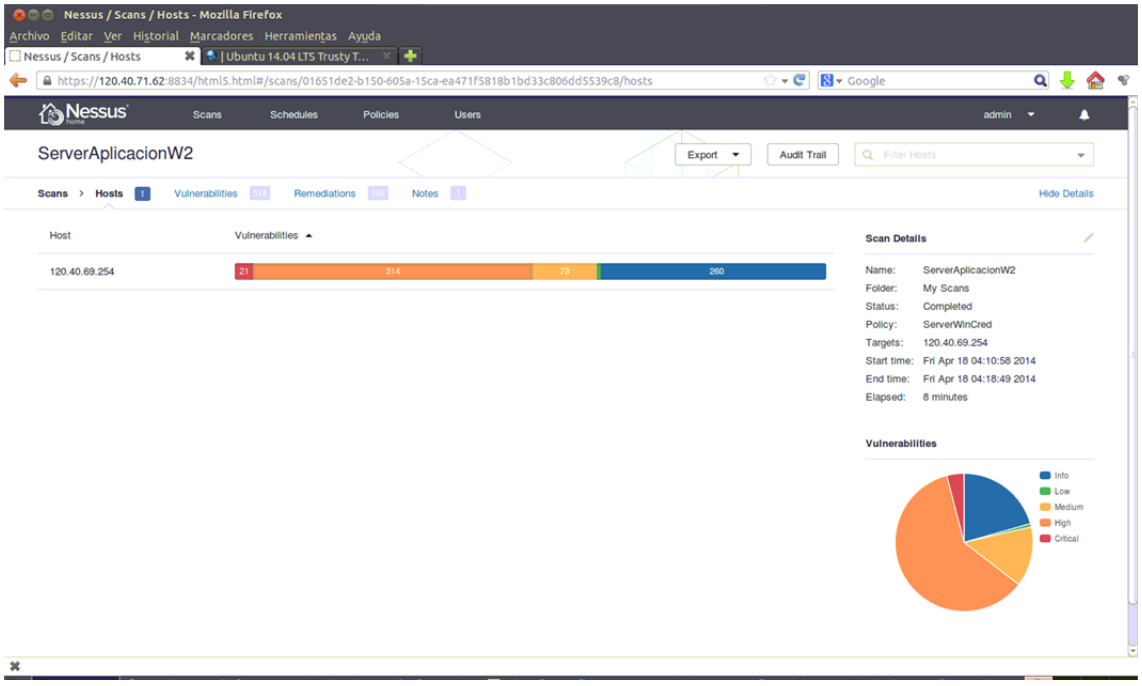


Figura 3-50. Análisis de Vulnerabilidad con Nessus

Luego que se identifican las vulnerabilidades por parte del Software Nessus se compara con la base de datos integrado especificándolas por colores, se procede a examinar los niveles de severidad y complejidad con que son definidas por esta herramienta en relación ala inseguridad informática encontrada.

El análisis al equipo antes mencionado, implica que el Auditor de Seguridad puede realizar el levantamiento de información y extraer del Servidor de Datos un mínimo de cinco vulnerabilidades, que a su vez son categorizados

de alta peligrosidad para el Municipio y de esta manera se mantiene un control de la administración tecnológica con resultados efectivos.

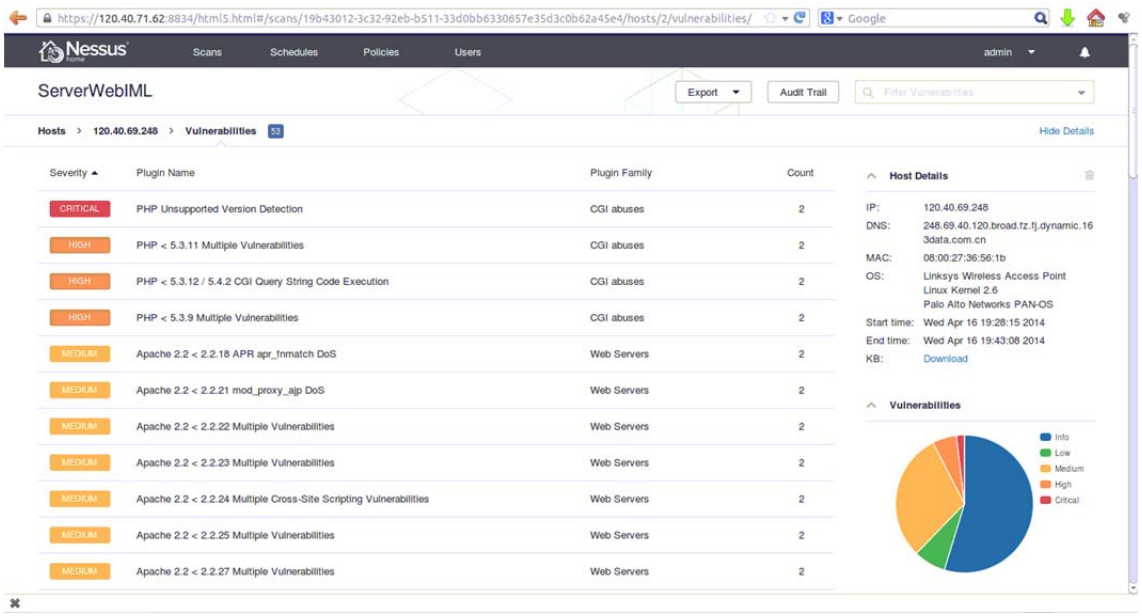


Figura 3-51. Niveles de Vulnerabilidades con Nessus

Mediante la tabla que se muestra a continuación se ha extraído cinco vulnerabilidades comunes y de alta peligrosidad que son considerados armas letales por Crackers que quieran realizar algún tipo de acto ilícito a la Institución para que posteriormente sea parchados o modificados, conservando la integridad de los equipos vulnerados.

Tabla de Identificación de Vulnerabilidades

Nombre del Servidor: Servidor de Pagina Web
Vulnerabilidad # 1: PHP < 5.3.11 MultipleVulnerabilities

IP Equipo analizado: 120.40.69.248
Referencia: CVE-2012-0831, CVE-2012-1172, Bug #60227 / CVE-2011-1398
Servicios-i tem afectados: Servicio Web, Portal Web
Descripción de la vulnerabilidad: De acuerdo a la bandera encontrado por Nessus, la versión de PHP instalada en el host remoto es una versión inferior a la5.3.11, y como tal está potencialmente afectada por múltiples vulnerabilidades.
Detalles de la vulnerabilidad: Las versiones inferiores a 5.3.11 poseen vulnerabilidades de SQL injection que permite ser explotados de manera sencilla.
Riesgo: es de manejo fácil para los atacantes remotos realizar ataques de inyección de SQL a través de una petición manipulada, relacionado con principal / php_variables.c, SAPI / cgi / cgi_main.c y SAPI / FPM / FPM / fpm_main.c.
Impacto: Alto y Critico

Evidencias:
Output
`Version source : X-Powered-By: PHP/5.2.16`
`Installed version : 5.2.16`
`Fixed version : 5.3.11`

Recomendaciones para solucionar esta vulnerabilidad: Instalación versión actualizada del software PHP 5.4.17 o superior

Referencia Web: http://www.nessus.org/u?e81d4026 https://bugs.php.net/bug.php?id=61043 https://bugs.php.net/bug.php?id=54374 https://bugs.php.net/bug.php?id=60227 http://marc.info/?l=oss-security&m=134626481806571&w=2 http://www.php.net/archive/2012.php#id2012-04-26-1 http://www.php.net/ChangeLog-5.php#5.3.11
Observaciones: Mantener actualizado las versiones de PHP, Apache y Mysqlen el Servidor de Web

Tabla 3-35. Tabla de Identificación de Vulnerabilidad # 1

Nombre del Servidor: Servidor de Aplicaciones 2
Vulnerabilidad # 2: MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687)
IP Equipo analizado: 120.40.69.242
Referencia: CVE-2008-4834, CVE-2008-4835, CVE-2008-4114
Servicios-item afectados: Sistema Operativo
Descripción de la vulnerabilidad: SMB en el servicio de servidor de Microsoft Windows 2000 SP4, XP SP2 y SP3, Server 2003 SP1 y SP2, Vista

Gold y SP1 y Server 2008 permite a atacantes remotos ejecutar código arbitrario a través de los valores con formato incorrecto de "campos contienen los paquetes SMB" no especificados en una solicitud de NT Trans2, relacionados con "insuficientemente validar el tamaño del buffer," también conocido como "la validación de SMB Código vulnerabilidad de ejecución remota."
Detalles de la vulnerabilidad: Proporciona acceso de administrador, permite una total confidencialidad, integridad y disponibilidad de violación; Permite la divulgación no autorizada de la información; Permite la interrupción del servicio
Riesgo: Ataques de Denegación de Servicios
Impacto: Critico
Evidencias: ninguna
Recomendaciones para solucionar esta vulnerabilidad: Instalación de parche para Windows 2003 Server
Referencia Web: http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx
Observaciones: Mantener actualizado los parches y paquetes del Servidor de Datos 2003 Server

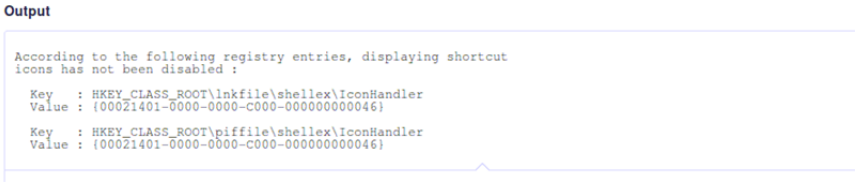
Tabla 3-36. Tabla de Identificación de Vulnerabilidad # 2

Nombre del Servidor: Servidor de Aplicaciones 1
Vulnerabilidad # 3: MS09-026: Vulnerability in RPC Could Allow Elevation of Privilege (970238)
IP Equipo analizado: 120.40.69.254
Referencia: CVE-2009-0568
Servicios-item afectados: Sistema Operativo
Descripción de la vulnerabilidad: El motor de cálculo de referencias de RPC instalada en el host remoto de Windows no se encuentra actualiza en su estado interno apropiada, lo que podría conducirá un puntero se leen en una ubicación incorrecta. Un atacante remoto podría aprovechar este problema para ejecutar código arbitrario en la máquina afectada y tomar el control completo de la misma.
Detalles de la vulnerabilidad: El motor de cálculo de referencias de RPC (NDR) en Microsoft Windows 2000 SP4, XP SP2 y SP3, Server 2003 SP2, Vista Gold, SP1 y SP2 y Server 2008 SP2 no mantiene adecuadamente su estado interno, que permite a atacantes remotos sobrescribir arbitraria posiciones de memoria a través de un mensaje RPC diseñada que provoca la lectura puntero incorrecto, relacionados con "interfaces IDL que contiene una matriz de variables no conformes" y FC_SMVARRAY, FC_LGVARRAY, FC_VARIABLE_REPEAT y FC_VARIABLE_OFFSET, conocido como "Vulnerabilidad RPC Marshalling Engine".

Riesgo: Permisos, privilegios y control de acceso
Impacto: Alto, Critico
Evidencias: 
Recomendaciones para solucionar esta vulnerabilidad: Instalación de los parches respectivos para eliminar la vulnerabilidad del Servidor
Referencia Web: http://technet.microsoft.com/en-us/security/bulletin/MS09-026
Observaciones: Mantener actualizado los parches y paquetes del Servidor de Correo Electrónico

Tabla 3-37. Tabla de Identificación de Vulnerabilidad # 3

Nombre del Servidor: Servidor de Aplicaciones 1
Vulnerabilidad # 4: MS KB2286198: Windows Shell Shortcut Icon Parsing Arbitrary Code Execution
IP Equipo analizado: 120.40.69.254
Referencia: CVE-2010-2568
Servicios-item afectados: Sistema Operativo
Descripción de la vulnerabilidad: Shell de Windows no valida

correctamente los parámetros de un archivo de acceso directo al cargar su icono. El intento de analizar el icono de un archivo de acceso directo especialmente diseñado puede provocarla ejecución de código arbitrario.
Detalles de la vulnerabilidad: Un atacante remoto podría aprovechar engañando a un usuario para que vea un archivo de acceso directo mal intencionado a través del Explorador de Windows, o cualquier otra aplicación que analiza el icono del acceso directo. Esto también puede ser aprovechado por un atacante que engaña a un usuario para insertar un medio extraíble que contiene un acceso directo malicioso(por ejemplo CD, unidad USB), y la reproducción automática está habilitada.
Riesgo: Control del Equipo
Impacto: Alto, Critico
Evidencias: 
Recomendaciones para solucionar esta vulnerabilidad: Instalación de cualquier parcheMS10-046 o desactivar la visualización de los iconos de acceso directo
Referencia Web: http://technet.microsoft.com/en-us/security/advisory/2286198 http://technet.microsoft.com/en-us/security/bulletin/MS10-046

Observaciones: Mantener actualizado los parches y paquetes del Servidor

Tabla 3-38. Tabla de Identificación de Vulnerabilidad # 4

Nombre del Servidor: Servidor de Correo Electrónico
Vulnerabilidad # 5: MTA Open Mail Relaying Allowed
IP Equipo analizado: 120.40.71.1
Referencia: CVE-1999-0512, CVE-2002-1278, CVE-2003-0285
Servicios-item afectados: Correo Electrónico
Descripción de la vulnerabilidad: El servidor SMTP remoto permitirla retransmisión de correo. Esto significa que un usuario no autenticado, remoto podría utilizar el servidor de correo de la Institución para enviar mensajes al mundo, desperdiciando así recursos de ancho de banda de la redy de la computadora. Estos servidores son el blanco de los spammers para enviar correo electrónico masivo no solicitado (UBE).
Detalles de la vulnerabilidad: En algunos casos el número de mensajes colapsara la entrega , podría ser de cientos de miles de personas, haciendo que el servidor de correo se bloquee. Además, los servidores SMTP que permiten la retransmisión de frecuencia se añaden a las listas de bloqueo en tiempo real que mantiene sitios de seguridad y utilizados por las empresas en todo el mundo. Si se añade a una lista de este tipo, la entrega del correo

legítimo podría verse seriamente afectada, causando una forma denegación de servicio.
Riesgo: bloqueo del envió de correo electrónico por presunto spammers
Impacto: Alto, Critico
Evidencias: 
Recomendaciones para solucionar esta vulnerabilidad: Investigue si el servidor debe permitirla retransmisión de correo.
Referencia Web: ninguna
Observaciones: Mantener actualizado los parches y paquetes del Servidor de Correo Electrónico

Tabla 3-39. Tabla de Identificación de Vulnerabilidad # 5

3.7. Evaluación y Valoración de Resultados

Luego de realizar el levantamiento de información de cada uno de las actividades expuestas en este documento se debe realizar el proceso de evaluación y valoración de los resultados sobre estas cinco vulnerabilidades más críticas y dar soluciones efectivas a cada uno de los incidentes,

vulnerabilidades o problemas encontrados en los Servidores del Centro de Datos Municipal.

3.7.1. Eliminación de Vulnerabilidad

Para el caso del Portal Web Municipal se realizó varias pruebas de SQL injection los mismos que en su mayoría se obtuvo resultados de 0% de vulnerabilidades a este tipo de ataques, descartando de esta manera oportunidades de actos ilícitos de entes externos específicamente para este Programa de Gestión de Contenidos Web “Joomla”, aplicativo utilizado por la institución para la administración del Portal Web Municipal.

Específicamente se detectó que el problema esencial de este Servidor Web, es la actualización de los paquetes de administración a nivel de Portales Web, debido a que se detectó una versión de PHP que contiene múltiples vulnerabilidades y errores.

Basado en el problema se procedió a realizar la actualización de los paquetes del PHP y de esta manera dar seguridad al Portal Web antes posibles ataques externos.

Figura 3-52. Vulnerabilidad PHP encontrada por Nessus

El trabajo realizado es la actualización del paquete PHP de la versión 5.2.16 a la versión 5.4.27 a través de consola del Servidor del Portal Web Municipal, versión que no es vulnerable a ataques de SQL injection y cuenta con soporte actualmente por parte de sus autores.

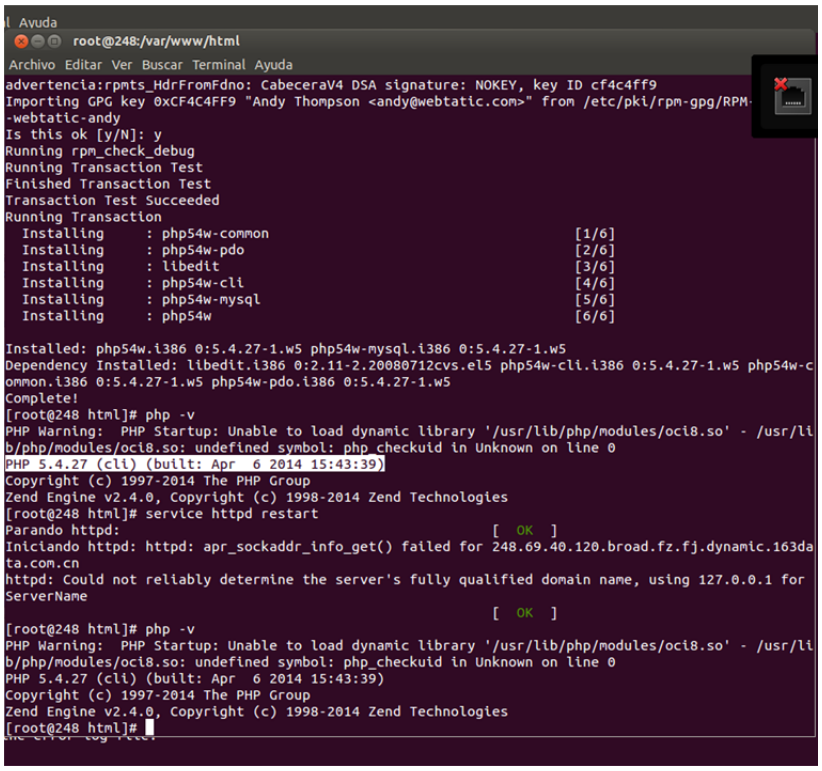


Figura 3-53. Actualización de Paquetes PHP

Para el caso del problema detectado de estar habilitado el archivo htaccess.txt dentro de la estructura instalada por Joomla, se ingresó en el servidor del Portal Web y se procedió a renombrar el archivo antes mencionado por .htaccess para que de esta manera se pueda bloquear el acceso público vía Web a determinados ficheros de Joomla. A continuación se muestra la gráfica.

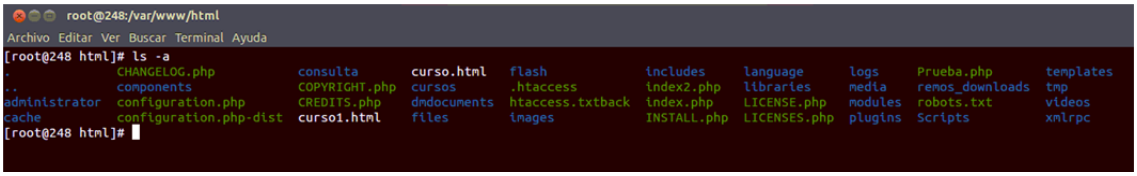


Figura 3-54. Renombrar archivo htaccess.txt

Para el problema encontrado de com_mailto, vulnerabilidad que se detectó en joomla a través de la herramienta “joomscan” de BackTrack, se procedió a realizar el bloqueo respectivo y la realización de otras pruebas de inyección SQL de las cuales la vulnerabilidad resulto negativo, en la siguiente grafica se observa.

Línea de inyección SQL utilizada:

http://www.lalibertad.gob.ec/index.php?option=com_mailto&tmpl=mailto&article=550513+and+1=2+union+select+concat%28username,char%2858%29,password%29KHG+from+jos_users--&Itemid=1

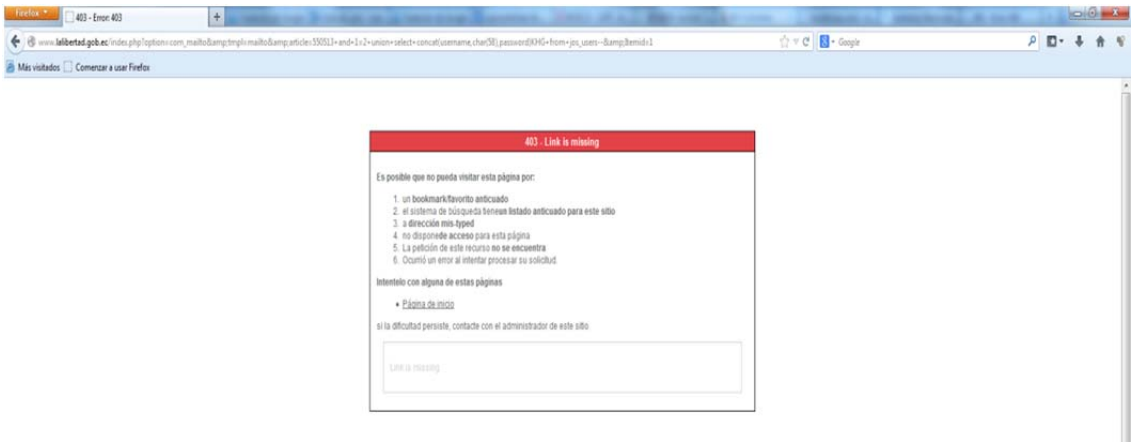


Figura 3-55. Prueba de Vulnerabilidad en Joomla

3.7.2. Filtrado y Bloqueo de Puertos

Para el proceso de Escaneo de Puertos de los Servidores del Centro de Datos Municipal, previamente se procedió a realizar la verificación y análisis de cada uno de los puertos abiertos para identificar cuál de ellos estaba ligado con algún tipo de servicio que requería tenerlos en ese estado, caso contrario se procedía a realizar el cierre de cada uno de los puertos encontrados con el comando NMAP y configuración que se realizó con el firewall del sistema operativo en mucho de los casos.

Luego del bloqueo de los puertos del servidor 120.40.69.242 se procedió a realizar un nuevo escaneo con el objetivo de identificar la existencia de puertos abiertos. Claramente se observa en la siguiente gráfica.

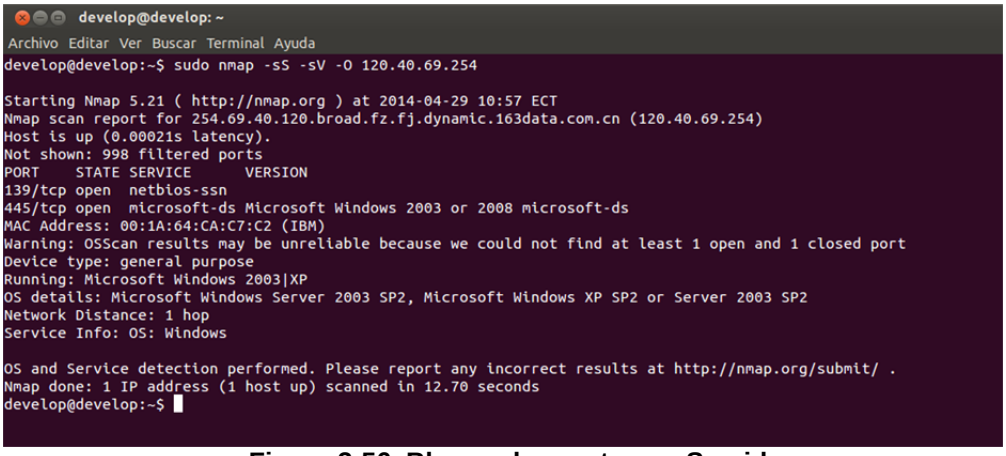


Figura 3-56. Bloque de puertos en Servidor

Como se observa el resultado de la petición realizada a través del comando nmap, el mismo que envía como resultado solo dos puertos abiertos que son necesarios para la actividad del Servidor. Quedando de esta manera seguro ante ataques que podrían realizarse por algún puerto abierto.

Para el caso del servidor con IP 120.40.69.254 cuyo sistema operativo detectado es Windows se procedió a bloquear los puertos a través del firewall y deshabilitar los servicios que no son utilizados por la actividad detectada de estos servidores de Aplicaciones y compartición de recursos Cartográficos.

El bloqueo de los puertos específicamente se la realizo habilitando un firewall para dichos servidores que solo de paso a tráfico por puerto que son necesarios para la actividad diaria de dicho equipo.

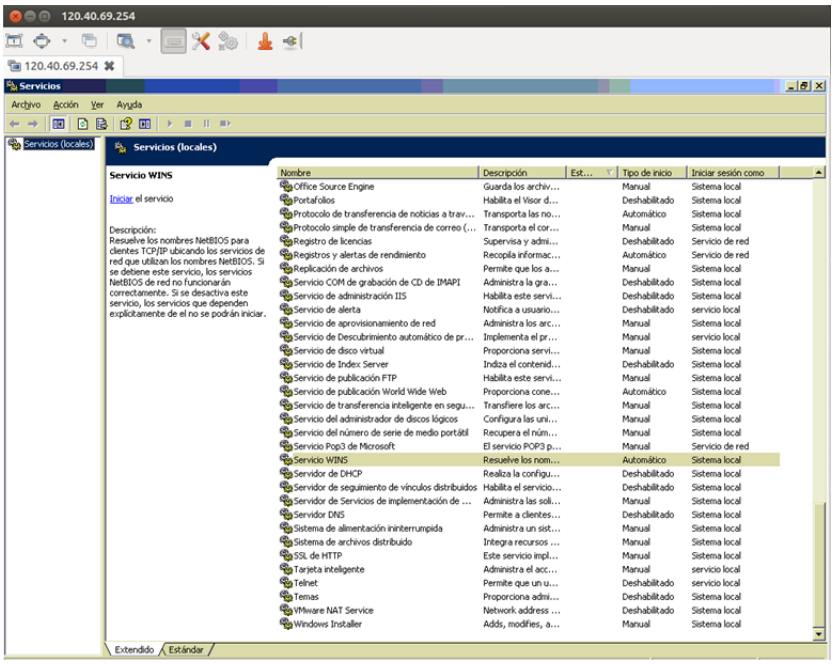


Figura 3-57. Inhabilitar servicios innecesarios en Servidor de Aplicaciones

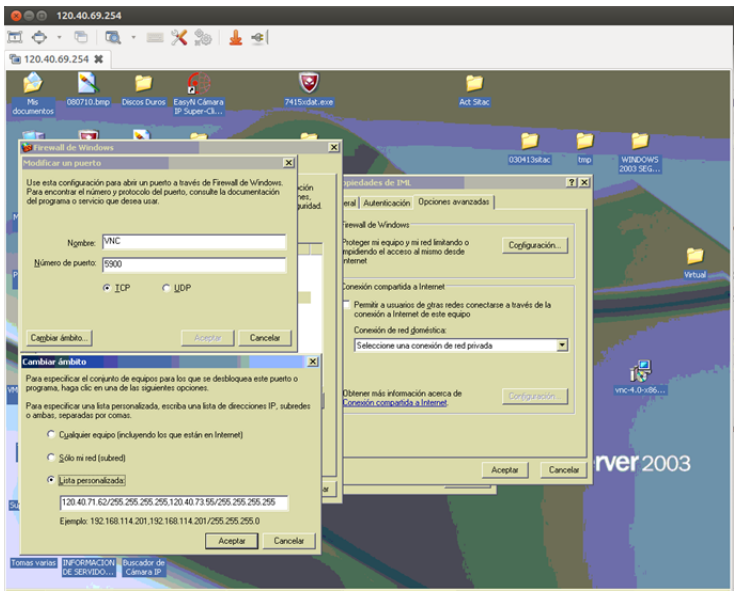


Figura 3-58.Configuración de Puertos específicos para el Servidor de Aplicaciones

Para el caso del servidor DNS cuya IP es 120.40.69.251el mismo que funciona con Sistema Operativo Linux Centos 5.3 se procedió a habilitar el firewall, el mismo que es de vital importancia para el bloqueo de puertos, los cuales no son necesarios que se encuentre abiertos y expuesto a cualquier vulnerabilidad. En la configuración que se realizó se especificó mediante el comando setup que envía a la consola de administración donde se puede habilitar el Cortafuegos de este Sistema Operativo, esto se demuestra en la siguiente gráfica.

Figura 3-59. Habilitar firewall de Centos 5.3

Es necesario dejar habilitado el Servicio Domain de Centos debido a que este sistema operativo hace la función de DNS y permite la ejecución del sistema municipal que está levantado bajo la infraestructura de Oracle 10g.

Figura 3-60. Configuración de Firewall Linux

Luego de haber habilitado el firewall y dar apertura a los puertos necesarios que utilizaran los servicios activos en este Servidor, nuevamente se procede a ejecutar el comando NMAP para identificar si los cambios fueron efectuados satisfactoriamente.

Los resultados como se muestran en la siguiente Figura son satisfactorios y por ende tenemos un servidor asegurado a cualquier ataque

por puertos abiertos.

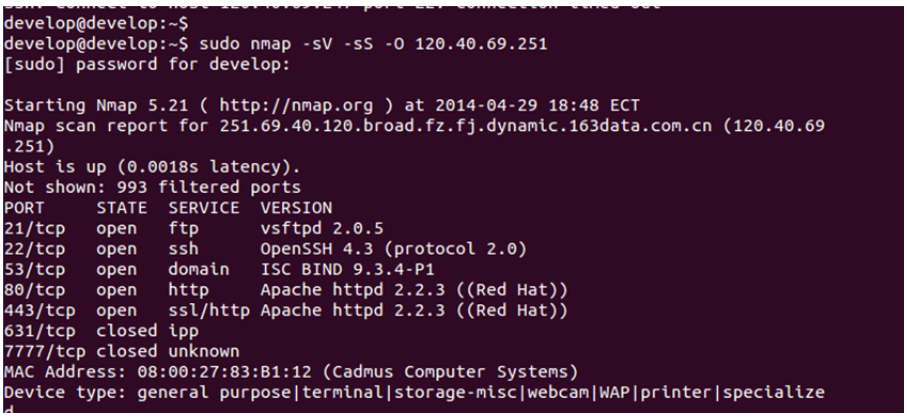


Figura 3-61. Cierre de puertos en Servidor DNS

3.7.3. Evaluación de Vulnerabilidades

En este proceso se procedió a escoger cinco vulnerabilidades más críticas que fueron identificados dentro de los Servidores del Centro de Datos Municipal, las mismas que son las siguientes:

1. PHP < 5.3.11 Multiple Vulnerabilities
2. MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687)
3. MS09-026: Vulnerability in RPC Could Allow Elevation of Privilege (970238)
4. MS KB2286198: Windows Shell Shortcut Icon Parsing Arbitrary Code Execution
5. MTA Open Mail Relaying Allowed

Para cada una de las vulnerabilidades se procedió a realizar los ajustes necesarios para que los Servidores no presenten vulnerabilidades y no existan agentes externos accediendo a la información sin autorización.

En el punto de Resultado de vulnerabilidades de Portal Web Municipal de este documento ya procedió a realizar la actualización del PHP dentro del servidor Web, para las vulnerabilidades del 2 hasta el 4 se procedió a la instalación del parche y Service Pack adecuado para eliminar el problema desde la raíz; y para el caso del Servidor de Correo se procedió a realizar configuraciones en la administración del correo electrónico, cuyo nombre del Software es Kerio Server, bajando de esta manera los índices de vulnerabilidades encontrados en los Equipos del Centro de Procesamiento de Datos y dando apertura a un Plan de acción para mantenerse alerta de nuevas formas de CiberAtaques muy comunes hoy en día.

3.7.4. Plan de Acción

Finalmente se recomienda varias buenas prácticas que se deben seguir para que en el futuro a pesar que se realizó un análisis de vulnerabilidad y se ejecutó los parches necesarios no sean víctimas de Ciberataques, robo de información o accesos no autorizados.

Las recomendaciones y acciones a realizar se detallan a continuación:

- ✓ Mantener una constante capacitación a los usuarios en Ingeniería Social acompañado de recordatorios de las Políticas de uso de Herramientas y Servicios Tecnológicos que día a día utilizan en la institución.
- ✓ Actualización periódica de los antivirus que son utilizado en los servidores Windows.
- ✓ Control de Tráfico a través de software como Wireshark, con el objetivo de evitar ataques de Denegación de Servicios, sean estos internos o externos.
- ✓ Parchar periódicamente todos los servidores sean estos Windows o Linux con nuevas actualización de acuerdo a las nuevas vulnerabilidades que aparezcan en la Internet y reconocidas mundialmente.
- ✓ Recomendar a la institución la adquisición de un equipo firewall y un Servidor IDS y aumentar el nivel de seguridad de la institución.

3.7.5. Implementación de software IDS

En vista de la falta de recursos económicos para el área se instaló en un equipo robusto el Software para Sistema Operativos de tipo Servidores Linux llamado **Snort** que trabaja como un sistema de detección automática de

intrusión ubicada dentro de la Red de la Institución Municipal, también conocido como IDS. El significado de IDS[13] es Intrusion Detection System, es decir, un Sistema de Detección de Intrusos, que básicamente sirve para detectar un comportamiento anómalo dentro de la red LAN es llamado también NIDS (Network Intrusion Detection System), en un host es llamados HIDS (Host Intrusion Detection System) o en una red WiFi llamados WIDS (WiFi Intrusion Detection System).

Este comportamiento extraño dentro del Internet debe de ser detectado por un Server IDS, suele basarse normalmente en patrones que buscara sea esta en la red, host o red Wifi, y en el caso de coincidencia generara una alarma advertencia de un posible ataque que también puede considerarse y ser descartado por un falso positivo.

Snort utiliza un lenguaje flexible basado en reglas para describir el tráfico que debería recolectar o dejar pasar, y un motor de detección modular. La mayor parte de personas en el mundo de la Seguridad Informática sugiere que la Consola de Análisis para Bases de Datos de Intrusiones (Analysis Console for Intrusion Databases, ACID) sea utilizada con Snort.

[13] Wikipedia.org, "Sistema de Detección de Intrusos - Wikipedia, La Enciclopedia Libre" <http://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos>.

Para el caso de la institución la ubicación estratégica del IDS implementado, fue considerada situarlo en el Centro de Datos Municipal, luego de receptar tráfico de red a través del Router modelo 1841, tanto de Datos y Voz IP, esto se debe a que también pueda cubrir la verificación del tráfico de la red a través de las conexiones de Voz sobre IP como también la de Datos.

Diagrama de Ubicación del IDS en el Centro de Datos Municipal

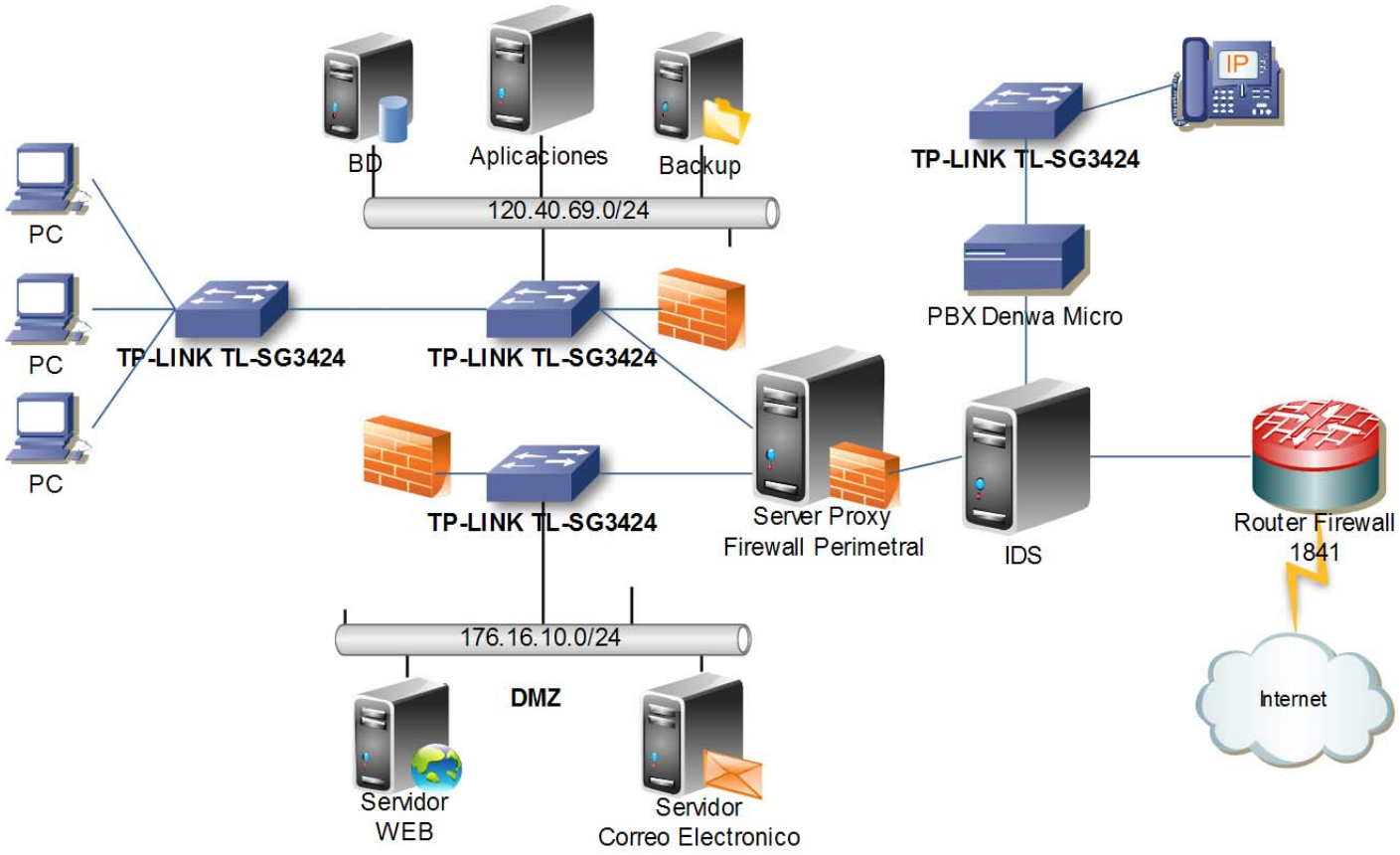


Figura 3-62. Diagrama de Ubicación del IDS en el Centro de Datos Municipal

CAPÍTULO 4

4. DESARROLLO DEL PLAN DE RECUPERACIÓN DE DESASTRES Y RESPALDO DE INFORMACIÓN

4.1. Introducción

El lograr prevenir un desastre a nivel informático para una institución pública como lo es el GAD Municipal, puede significar evitar desde la pérdida de datos muy importantes hasta cualquier interrupción en las operaciones sistemáticas normales de la organización.

Para una institución púbica la acción de prevenir dañossean estos en hardware o software es fundamental si se logra definir e implementarun plan de recuperación ante desastres (del inglés Disaster Recovery Plan- DRP)[14]de forma inmediata con el objetivo de obtener resultados rápidos, eficientes y con el menor costo posible.

En recopilación a lo anunciado anteriormente, se ha diseñado para el Municipio de la Ciudad del Este un Plan de Recuperación de Desastres y Respaldos esencial que permita dar continuidad permanente a la Institución, disminuyendo notablemente los diferentes posibles siniestros que pueden impactar negativamente las operaciones normales de la organización.

Por tal motivo es importante identificar que cada entidad sea esta pública o privada tiene necesidades y visiones distintas de cómo llevar la administración, sin embargo existen tres factores claves para el éxito de un plan de recuperación ante desastres y que puede adaptarse a todo tipo de empresa.A continuación se menciona las siguientes:

[14]Ongei.gob.pe, “INEI - PLAN DE CONTINGENCIAS Y SEGURIDAD DE LA INFORMACION” <http://www.ongei.gob.pe/publica/metodologias/lib5007/0300.HTM>.

- ✓ **Medidas Preventivas:** Se deben identificar las diferente causas de un evento de desastre o siniestro y tomar las medidas necesarias para prevenirlo.

- ✓ **Medidas de Detección:** Se deben implementar mecanismos que permitan detectar eventos de improviso o inesperados.

- ✓ **Medidas de Corrección:** Una vez ocurrido el evento de desastre o siniestro, se deben tomar medidas para reparar los daños causados.

4.2. Objetivo y Alcance del Plan

El objetivo principal de contar con un Plan de Recuperación de Desastres y Respaldo de información, es establecer responsabilidades concretas a los usuarios dueños de los procesos,socializar las acciones y procedimientos esenciales para recuperar la capacidad operacional del Municipio de la Ciudad del Este de forma inmediata ante cualquier evento de interrupción no esperada.

El Plan de Recuperación de Desastres, pretende cubrir los siguientes objetivos específicos:

- ✓ Recuperar la capacidad de gestión operativa en un tiempo determinado y aceptado por la comunidad de usuarios según los recursos disponibles.
- ✓ Socializar y educar periódicamente a todo el personal que labora en la institución para tener capacidad de reacción ante siniestros tecnológicos que puedan suspender o interrumpir la gestión operacional.

4.3. Planificación Estratégica

La estrategia que se aplicará es la de incrementar el factor desatisfacción del servicio al contribuyente, controlando los posibles factores de riesgo operativo, con el fin de proteger, optimizar tiempo y mantener un nivel adecuado de calidad en la entrega de servicios a la comunidad.

4.3.1. Identificación de Procesos Críticos

Se consideran procesos críticos aquellos que en menor o mayor grado pueden impedir el normal funcionamiento de la institución y la consecución de los objetivos planificados.

El tiempo máximo de recuperación con relación a los niveles de criticidad han sido establecidos en función al grado de importancia de las máquinas, equipos, sistemas entre otras herramientas que intervienen directa o indirectamente en el proceso de producción:

Nivel de Criticidad	Descripción	Tiempo máximo de recuperación
Baja	Proceso cuya falla no afecta el funcionamiento a corto plazo	1 hora -2 horas
Media	Proceso cuya falla podría retrasar el normal funcionamiento	45 minutos a 1 hora
Alta	Proceso cuya falla podría impedir el normal funcionamiento	30 minutos a 45 minutos
Extrema	Proceso cuya falla impide el normal funcionamiento	30 minutos máximo

Tabla 4-40.Nivel de Criticidad de los Procesos en caso de eventos de Interrupción

Cuando el problema está plenamente identificado como daños en él hardware delequipo dentro de un proceso correctivo, el tiempo depende de lagestión en importación del repuesto que esta desde 15 días hasta un mes

aproximadamente; teniendo presente el análisis de alternativas secundarias a ejecutar hasta que se solvente el problema principal.

4.4. Plan de Acción

El paso inicial en el desarrollo del plan deprevención de desastres y respaldos, es la identificación de las personas que serán las responsables de crear el plan y coordinar las funciones específicas. Característicamente dentro de esta institución las personas pueden sermiembros del área TIC, Analistas de Seguridad o el personal directamente involucrado en el accionar del proceso.

Las actividades a realizar dentro de este Plan de Recuperación de Desastres y Respaldos se clasifican en tres etapas o Fases:

ANTES	DURANTE	DESPUÉS
▪ Capacitación de personal ejecutivo, administrativo y empleados. ▪ Señalizar las instalaciones de la empresa. ▪ Realización de simulacros. ▪ Implementar las instalaciones con Equipos de Seguridad. ▪ Cumplir las recomendaciones dadas por el personal calificado del área TICs	▪ Aplicar las medidas adoptadas, para la autoprotección en el momento del desastre. ▪ Dar informe veraz a través del Jefe de Informática sobre los hechos sucedidos.	▪ Normalizar las actividades laborales, con una participación programada. ▪ Evaluar la infraestructura Tecnológica. ▪ Rehabilitación de los servicios esenciales y áreas afectadas.

Tabla 4-41. Etapas de Plan de Recuperación de Desastres y Respaldos

4.5. Actividades Previas al Desastre

En esta fase se realizatodas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo tanto de la infraestructura como en software delos Servidores del Centro de procesamiento deDatos Municipalque aseguren un proceso de recuperación ordenado con el menor costo y tiempo posible para la institución.

Para esta actividad es posible detallar las siguientes actividades generales:

- ✓ Establecimiento de Procedimiento de Acción y Prevención.
- ✓ Formación de Equipos Operativos.
- ✓ Formación de Equipos de Evaluación (auditoria de cumplimiento de los procedimientos sobre Seguridad de la Información).

4.5.1. Establecimiento de Procedimientos de Acción y Prevención.

En esta parte de Planeamiento se debe implantar los procedimientos relacionados a los activos de la institución, en este caso se establecerá este accionar dirigido a las siguientes descripciones:

- ✓ Entorno de los Sistemas y Equipos.
- ✓ Sistemas de Información.
- ✓ La información. obtención y almacenamiento de los respaldos de información, backups, políticas, normas y procedimientos de backups.

4.5.1.1. Entorno delos Sistemas y Equipos

El Municipio de la Ciudad del Este dispone para este procesodelos siguientes ítems:

a) Inventario actualizado de los equipos de manejo de información: 5 Servidores de Datos, 8 switches, 1 router, y demás equipos de comunicación.

b) Inventario en contenido especificado: Software que usa y principales archivos que contiene.

c) Ubicación y nivel de uso institucional.Actualmente el Centro de procesamiento de Datos tiene un área exclusiva para los Servidores de datos y equipos de comunicación con la climatización adecuada.

d) El Municipio tiene una póliza de Seguros, como parte de la protección de los activos Organizacionales que fue requerida en las Auditoria Externas, la adquisición de una póliza pero haciendo la salvedad en el contrato, que en caso de siniestros, la restitución de los equipos siniestrados se podrá hacer por una mejor característica para realizar la actualización tecnológica, siempre y cuando esté dentro de los montos asegurados.

e) Se cuenta con la señalización o etiquetado de los computadores y unidades de almacenamiento en relación al inventario y de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación. Por ejemplo se encuentra etiquetado de color rojo a los Servidores, color amarillo a los computadores con Información crítica o estratégica y color verde a aquellos de contenidos normales. Para la ejecución de este proceso se contó con la colaboración del Departamento de Bodega y Activos Fijos.

El Municipio de la Ciudad del Este, a través de la jefatura de Tecnología deberá comprometerse en hacer cumplir y mantener actualizado de forma periódica cada uno de los puntos descritos anteriormente para garantizar el emprendimiento correcto y continuidad de este procedimiento a ejecutar

Otra de las forma de garantizar la ejecución y el correcto desempeño del plan de Acción, es tener presente el manual de funciones Institucional, que establezca la participación de los usuarios del Sistema ysu compromiso con el desarrollo de las responsabilidad asignadas y sus sanciones por parte de Talento Humano en caso de no realizarlo.

4.5.1.2. Sistemas de Información

El Municipio cuenta coninformación disponible y actualizada de los Sistemasde Información con losque cuenta la Institución. Debiendo identificar toda información sistematizada o no, que seanecesaria para la buena marcha Organizacional.

Dentro del Plan de Recuperación de Desastres y Respaldo se realizó el levantamiento de información de los sistemas, basado en lascaracterísticas

dadas de planes ya elaborados tales como se cita en Documento “Información General Acerca de la Recuperación ante Desastres” [15] y que se encuentra elabora en la siguiente tabla.

Sistema de Información	**Lenguaje de Desarrollo**	**Generador Primario de Información**	**Administrador del Sistema**	**Volumen de Transaccionalidad diaria**	**Nivel de Importancia**	**Fecha de Reportes**
Sistema de Gestión Municipal	Oracle 10g	Dpto. De Catastro y Tesorería	Depto. De Informática	10000	ALTA	Fin de Mes
Función: Sistema de Información para la Gestión Administrativa de todo el Municipio, los módulos son los siguientes: Ordenes de Pago, Control de Multas, bodega, Catastro, Coactiva, Seguridad y Control, Terrenos, Contabilidad, Planificación, Presupuesto, Nomina, Rentas, Recaudación, Centro Medico						
SITAC (SISTEMA INTEGRADO DE TRIBUTACION ASESOR CONTABLE)	FOXPRO	Dirección Financiera y Dpto. De Contabilidad	Depto. De Informática	2000	MEDIA ALTA	Fin de Mes

[15]Microsoft.com, “Información General Acerca de La Recuperación Ante Desastres” <http://technet.microsoft.com/es-es/library/bb418909.aspx>.

Función: Software diseñado para exigencias tributarios, con este sistema puedes obtener lo siguiente: - anexos transaccionales y reoc - formularios 103. 104. 107						
Sistema de Información Registral (SIRE)	Visual Studio y Access.	Registrador de la Propiedad	Depto. De Informática	1000	MEDIA	Fin de Mes
Función: Sistema de control de los cambios en la información de dominios que experimenta un bien inmueble registrado dentro del Cantón por el departamento del Registrador de la Propiedad.						

Tabla 4-42.Sistemas de Información Municipal

Actualmente para el correcto funcionamiento de los Sistemas informáticos se cuenta con Servidores un poco antiguos pero robustos de marca IBM y HP, de las cuales se realiza respaldos diarios y se está gestionando la contratación anual de mantenimiento preventivos todo esto con el fin de cubrir con los requerimientos establecidos en el Plan de recuperación de desastres.

Cabe destacar que se ha establecido responsabilidades con el personal involucrado en dar soporte a estos equipos, determinado que diariamente se realicen monitoreo que permitan identificar que los procesos internos de estos equipos funcionen correctamente y en caso de suscitarse alguna incidencia, se

puede activar el proceso de levantamiento de una estructura virtualizada (Sistema operativo y Aplicativo) como gestión de respaldo en caso de la identificación de un problema críticoa nivel de hardware con el equipo original; para la ejecución de este proceso el tiempo establecido en ellevantamiento de esta infraestructurade un Servidor previamente definido es de 3 horas, y de la Base de Datos de forma completa es de 2 horas aproximadamente, todo esto bajo la responsabilidad del Analista de Infraestructura y el DBA de la Institución.

A este proceso se suma los simulacros periódicosque se realizan con el fin de probar todo tipo de falencia de los procedimientos como por ejemplola verificación de respaldosque se encuentre enóptimas condiciones para que en el momento que suceda un siniestro tener la confiabilidad al 100% de estos respaldos.

4.5.1.3. Administración de Respaldos

Toda la información respaldada debe estarubicada en el Departamento de Informática Municipaly estar disponible en todo momento en un lugar seguro sea este de forma local o remota,considerando los parámetros específicos y la disponibilidad de recursos.

Los Servicios Informáticos que funcionan actualmente en el GAD Municipaly administrados por parte del Departamento de Informática son los siguientes:

- ✓ Sistema de comunicación y redes
- ✓ Servicio de correo corporativo
- ✓ Servicios Web: Publicación de Páginas Web, servicios consulta deuda predial en línea, ley de transparencia y Tramite Ciudadanos.
- ✓ Internet, Intranet.
- ✓ Servicios Proxy
- ✓ Servicio Firewall Software.
- ✓ Servicio de Monitoreo de la red: monitorea los equipos de comunicación distribuidos en la red del Municipio de la Ciudad del Este.
- ✓ Servicios de telefonía IP
- ✓ Servicios de enseñanza de manera virtual. (en el caso de existir capacitación)
- ✓ Servicio de Antivirus básico
- ✓ Soporte Técnico
- ✓ Servicio de Consulta en Línea Portal Web sobre “deuda de predios Urbanos y Pagos a través de Entidad Bancaria”.

Cada uno de estos servicios son monitoreados diariamente y respaldados con el objetivo de evitar incidentes o imprevistos, todo este proceso está bajo la responsabilidad del Analista de Infraestructura y el DBA de la institución.

4.5.1.4. La Obtención y Almacenamiento de los Respaldos de Información, Backups, Políticas, Normas y Procedimientos de Backups.

Previo a la administración y manejo de políticas de respaldo se debe identificar que en el caso de ser necesario los sitios o lugares de respaldo con la que cuenta la institución, estos deben serun sitio con climatización fría (Para este caso interno sería Centro de Procesamiento de Datos, y externa del Municipio como el Cerro de Engoroy).

Es necesario un sitio de respaldo frío ubicado en un edificio externo configurado apropiadamente y que de las facilidades necesarias, se debe conseguir todo lo que se necesite para restaurar el servicio a sus usuarios y entregar a este sitio antes de comenzar el proceso de recuperación. [16]

[16] Eumed.net, "PLAN DE RECUPERACIÓN DEL DESASTRE Y RESPALDO DE LA INFORMACION" <http://www.eumed.net/libros-gratis/2009c/605/PLAN DE RECUPERACION DEL DESASTRE Y RESPALDO DE LA INFORMACION.htm>.

Una vez definido la ubicación del lugar físico paralos respaldos, el Municipiodeberá establecer los procedimientos necesarios para la obtención de copias de seguridad de todos los elementos de software o aplicativos necesarios en el Centro de procesamiento de datos Municipal, para lo cual se cuenta con:

1. **Backups del Sistema Operativo:** En caso de tener varios sistemas operativos oversiones, actualmente se cuenta con una copia de los instaladores de cada uno de ellos tanto de software libre, como los licenciados.

2. **Backups del Software Base**: Paquetes y/o Lenguajes de Programación con los cuáles han sido desarrollados o interactúan los aplicativos organizacionales, específicamente todo lo relacionado a las herramienta Cliente/ Servidor de Oracle.

3. **Backups del Software Aplicativo:** Considerando tanto los programas fuentes,como los programas objetos correspondientes, y cualquier otro software oprocedimiento que también trabaje con la data, para producir los resultados con los cuales trabaja el usuario final.

4. **Backups de los Datos:** Bases de Datos, Índices, tablas de validación, passwords, y todo archivo necesario para la correcta ejecución del Software Aplicativo utilizados en el Municipio de la Ciudad del Este.

5. **Backups del Sitio Web:** Aplicativo y Bases de Datos, índices, ficheros dedescarga,herramientas multimedia, contraseñas del portal Web y ambiente administrativo.

6. **Backups de Sistemas Virtualizados:** de respaldos semanal de los aplicativos virtualizados.

7. **Backups de Información de Equipos de Escritorios:** Aplicación instalada en Servidor de Respaldo cuyo Backups la realiza diariamente mediante el método diferencial con la información de cada una las máquinas activas en la red de la Institución.

4.5.1.5. Modalidad de Respaldo y Tiempo de Ejecución

Debido a que no se cuenta con la infraestructura y presupuesto necesaria, la forma implementada para la extracción de respaldo de información se la

realizamediante la generación y configuración de archivos CRON en los Servidores cuyo Sistema Operativo sonLinux y un archivo de tareas programadas dentro de la Familia de Servidores Windows, procesos que todos los días a partir de las 19H00 ejecuta instrucciones en batch, respaldando cada uno de componentes registrado por el administrador de tareas programadas.

La información es procesada en las noches de tal forma que no genera tráfico o saturación de la red optimizando tiempo y recursos de la institución, todos los respaldos son almacenados en un servidor de Aplicaciones que posee, instalando 3 discos duros de 1 tera cada uno para el uso exclusivo de esta actividad.

El Analista de Infraestructura del Municipio como parte de sus responsabilidades al término de la semana laboral extrae esta información en dispositivos magnéticos que son enviados a centro de Comunicación de Datos ubicado en una dependencia externa del municipio llamado “Cerro de Engoroy”.

Es importante insistir que en vista de la falta de recursos económicos destinadas para el áreatecnológica, se ha tenido que implementar esta modalidad no sin

antes haber presentado propuestas ante la máxima autoridad de la Institución que no son los procedimientos adecuados y que para la buena gestión del Plan se requiere de servidores redundantes y sistemas de respaldo con brazos mecánicos que realicen metódicamente los respaldos.

Los métodos utilizados por el Departamento de Informática en la actualidad son considerando como valido dentro del Plan de recuperación de Desastres y Respaldo hasta que se pueda obtener el presupuesto necesario para la adquisición de los equipos adecuados para esta actividad.

4.5.1.6. Tipos de Respaldo a Utilizar

Es importe identificar que para este tipo de actividades es necesario utilizar los siguientes tipos de respaldo:

Respaldo Completo ("Full"): Guarda todos los archivos que sean especificados al tiempo de ejecutarse el respaldo. El archive bit es eliminado (o bloques), indicando que todos los archivos ya han sido respaldados.

Respaldo Diferencial ("Differential"): es muy similar al "Respaldo de Incremento", la diferenciaconsiste en que el archive bit permanece intacto y para la aplicación de este Plan de recuperación de Desastres y Respaldos ambos tipos son considerados.

4.5.1.7. Secuencia de Respaldo GFS (Grandfather-Father-Son)

Domingo (1)	Lunes (2)	Martes (3)	Miércoles (4)	Jueves (5)	Viernes (6)	Sábado (7)
Respaldo Diferencial	Respaldo Diferencial	Respaldo Diferencial	Respaldo Diferencial	Respaldo Diferencial	Respaldo Full	Respaldo Diferencial
Domingo (8)	Lunes (9)	Martes (10)	Miércoles (11)	Jueves (12)	Viernes (13)	Sábado (14)
Respaldo Diferencial	Respaldo Diferencial	Respaldo Diferencial	Respaldo Diferencial	Respaldo Diferencial	Respaldo Full	Respaldo Diferencial

Tabla 4-43. Secuencia de Respaldo GFS (Grandfather-Father-Son)

Una vez que se revisa la tabla de Secuencia de Respaldo GFS, utilizando este tipo de metodología de respaldos de información,para el caso de tener problemas con el sistema en el día 8 se puede utilizar el diferencial del día 7 o el Respaldo a full de día 6.

Por tal situación, es importante realizar el respaldo diferencial todos los días y el Tipo Full solo los viernes, opción recomendada para este tipo de Instituciones que tiene una carga de información de tipo media y que hoy en día se la está realizando así, de tal forma se optimizaría de una mejor forma la cantidad espacio en los discos de almacenamiento disponibles en la institución, garantizando la integridaddel respaldo de la información.

4.5.1.8. Políticas, Normas y Procedimientos de Backups

Para la aplicación de este proceso se establecen políticas, normas, y determinación de responsabilidades en la obtención de los respaldos cuyos procedimientos de ejecución fueron mencionados anteriormente, para la cual se debe implementar en la Institución la siguiente Política:

1. Mantener y garantizar la periodicidad de Backup por parte del Analista de Infraestructura y el DBA de la Institución.

2. Mantener Respaldo de Información de movimiento entre los períodos que no se obtienen Backups (backups diferenciales). Responsabilidad por parte del Analista de Infraestructura.

3. Uso obligatorio de un formulario estándar para el registro y control de los Backups por parte del responsable del proceso dentro del Departamento de Informática.

4. Almacenamiento de los Backups en condiciones óptimas y adecuados equipos, esto dependiendo delmedio de almacenamiento empleado y disponible

5. Reemplazo de los Backups, en forma periódica, antes que el medio dealmacenamiento de soporte se pueda deteriorar.

6. Mantener el almacenamiento de los respaldos en locales diferentes de donde reside la información primaria, evitando de esta manera la pérdida, en caso de que el desastre alcanzara todo el edificio administrativo.

7. Realizar Pruebas periódicas de los Respaldos por parte de los responsables del proceso, verificando su funcionalidad, a través delos Sistemas, comparando contra resultados anteriores confiables.

Basado en estas política e implementadodentro del Plan de Recuperación de desastres y respaldos, losSistemas Municipalesdesarrollados en Oracleson el activo primario considerado en este proceso, los mismos que actualmente están siendo respaldados según la disponibilidad de los recursos tecnológicos y existentes, siendo de la siguiente manera:

Aplicativo	**Prioridad**	**Respaldo**	**Responsable**
Sistema Municipal	Alta	diario	Oficial de Seguridad Informática o Analista de Infraestructura
Sistema SITAC	Alta	diario	Oficial de Seguridad Informática o Analista de Infraestructura
Respaldo de Servidores DNS, Firewall	alta	diario	Oficial de Seguridad Informática o Analista de Infraestructura
Respaldo de Servidor de Correo Electrónico	alta	diario	Oficial de Seguridad Informática o Analista de Infraestructura

Portal Web	Media	Semanal	Oficial de Seguridad Informática o Analista de Infraestructura
Cartografía	Media	diaria	Oficial de Seguridad Informática o Analista de Infraestructura
Inspecciones Municipales	Media	diaria	Oficial de Seguridad Informática o Analista de Infraestructura
Respaldo de Información de Usuarios	media	diaria	Oficial de Seguridad Informática o Analista de Infraestructura

Tabla 4-44.Tabla de Prioridad de Respaldo de Aplicativos

4.5.2. Formación de Equipos Operativos

Para la formación de equipos operativos, se deberá designar un responsable de la Seguridad de la Información; pudiendo ser el jefe de dicha Área Operativa para lo cualsus labores y responsabilidades serán las siguientes:

1. Proporcionar soporte técnico necesario para las copias de respaldo de las aplicaciones.
2. Planificar y establecer los requerimientos de los Sistemas Operativos en cuanto aarchivos, bibliotecas, utilitarios, etc., para los principales sistemas y subsistemas de la Institución.
3. Supervisar procedimientos de respaldo y restauración.
4. Supervisar la carga de archivos de datos de las aplicaciones, y la creación de los respaldos diferenciales.
5. Coordinar, administrar y monitorear periódicamente redes, líneas, terminales, equipos inalámbricos, otros aditamentos para las Comunicaciones.
6. Establecer procedimientos de seguridad en los sitios de recuperaciónexternao lugares remotos a la institución donde se almacena la información.

4.5.3. Formación de Equipos Operativos y de Evaluación

4.5.3.1. Auditoria de Cumplimiento de los Procedimientos Sobre Seguridad

Esta función será realizada de preferencia por personal de Auditoria del Municipio, en caso de no serposible, la realizará el personal del área de Informática, debiendoestablecerse claramente sus funciones, responsabilidades y objetivos en los siguientes puntos:

1. Revisar que las normas y procedimientos con respecto a Respaldos y Seguridad deequipos establecidos en el Municipio se cumpla con el fin de dar la seguridad adecuada de la información.
2. Supervisar la realización periódica de los Respaldos, por parte de los equiposoperativos, comprobando físicamente su realización, adecuado registro, conservación de integridad y almacenamiento.
3. Revisar la correlación entre la relación de Sistemas de Información necesariospara la buena marcha de la Organización, y los Backups realizados.

4. Informar de los cumplimientos e incumplimientos de las Normas, así como los correctivos a ejecutar en caso de incumplimiento, esto ante el Departamento de Talento Humano.

4.6. Actividades Durante el Desastre

Es importante para la ejecución de este proceso y una vez presentada la contingencia o el siniestro, se deberá ejecutar las siguientes actividades, planificadas previamente:

- ✓ Plan de Emergencias.
- ✓ Formación de Equipos.
- ✓ Entrenamiento.

4.6.1. Plan de Emergencias

En este plan se establecerán las acciones quedeberán realizar cuando se presente un siniestro, así como la difusión de las mismas. Es conveniente prever los posibles escenarios de ocurrencia del siniestro, estos pueden ser específicamente:

- ✓ Durante el día de labores.
- ✓ Durante la noche o madrugada.

Este plan deberá incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro para los dos Edificios Administrativos Municipales, debiendo realizar el siguiente levantamiento de información que permita la efectividad de ejecución del Plan:

1. Al no contar con un Plan de Evacuación para el Edificio, se ha solicitado al Analista Administrativo, la creación de la misma.
2. Actualmente se encuentra identificada solo las vías de salida o escape dentro de los dos edificios de la Institución Municipal.
3. Organizar capacitaciones al Personal Municipal para que puedan actuar inmediatamente y ubicar a buen recaudo los activos, incluyendo los deInformación de la Organización, siempre y cuando las circunstancias del siniestro loposibiliten.
4. Familiarizar y Socializar con la ubicación y señalización de los elementos contra el siniestro: extinguidores,cobertores contra agua, herramientas entre otros.

5. Ejecución de la cadena de llamadas en caso de siniestro, para esto debe tener a la mano: elementos de iluminación, lista de teléfonos de bomberos, ambulancia, Jefatura de policía o Seguridad o del personal responsable del proceso de la Gestión de riesgo Institucional.

4.6.2. Formación de Equipos

Es importante que a través del personal que labora en la Institución se logre adaptar una cultura de conocimiento constante para que cuando sucedan los siniestros puedan actuar rápida y directamente durante el mismos, protegiendo de esta manera la integridad personal y en lo posible el salvamento de los activos del sistema informático que a su vez este accionar deben de estar de acuerdo a los lineamiento o clasificación de prioridades con las que cuenta la Institución siendo un punto crítico la Base de Datos Municipal.

4.6.3. Entrenamiento

Este punto se centra con simulacros que apliquenen la prácticalas responsabilidades y roles establecido para cada responsable de un determinado proceso. Es importante que para este tipo de entrenamiento se debe

considerarse siempre minimizar costos aprovechando fechas de recarga de extinguidores de incendio, exposiciones de los proveedores, capacitación del manejo del sistema de información y charlas del uso correcto de los equipos de comunicación, facilitados por el personal del área de Informática.

Otro aspecto importante es que el personal del Departamento de Informática, tome en consideración todos los posibles siniestros (incendios, inundaciones, terremotos, apagones, daños maliciosos, accidentes a la infraestructura) que puedan ocurrir, y se actúe con seriedad y responsabilidad en estos entrenamientos. Para llevar a cabo esto y lograr un impacto visible, es conveniente que participen los directivos y líderes de procesos, para que sirva de ejemplo y permitan crear una cultura de Seguridad Organizacional.

4.7. Actividad Después del Desastre

Después de suscitado el siniestro o desastre es necesario realizar las actividades que se detallan, las cuales deben estar especificadas en el Plan de Acción.

- ✓ Evaluación de Daños.

- ✓ Priorización de Actividades del Plan de Acción.
- ✓ Ejecución de Actividades.
- ✓ Evaluación de Resultados.
- ✓ Retroalimentación del Plan de Acción.

4.7.1. Evaluación de Daños

Después que el siniestro seha consumado, se deberá evaluar la magnitud del daño que se ha producido, que sistemasInformáticos se encuentranafectados, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo.

Para el caso del Municipio de la Ciudad del Este es prioritario el enfoque a problemas que puedan suceder en los Servidores donde está alojado el Sistema Municipal que permitenrealizar la recaudación diaria de los impuestos municipales, ingreso que se obtienen a diario dentro de esta Institución.

Es importante para esta evaluación informar a la máxima autoridad y los responsables de cada proceso el tiempo estimado de restablecimiento de los servicios.

4.7.2. Priorización de Actividades del Plan de Acción

En este Plan de acción se está contemplando como punto primariola pérdida total de la información, la evaluación de daños reales y su comparación contra el Plan. Esta revisión nos dará la lista de las actividades que debemos realizar, siempre priorizándola en vista a las acciones estratégicas y urgentes de nuestra Institución.

Antes de la ejecución de todo accionar se debe dar a conocer a la máxima autoridad el percance sucedido, para ejecutar el plan de acción de forma inmediata controlando los tiempos que lleva el poner en marcha el sistema operativo o equipo defectuoso.

Aplicativo	Prioridad	Tiempo de Ejecución	Responsable	Observación
Sistema Operativo	ALTA	2 horas	Analista de Infraestructura	Se levanta estructura Virtualizada
Base de Datos	ALTA	2 horas	DBA	Se ejecuta Instalación o restauración
Levantamiento de Respaldo Full	ALTA	2 horas	DBA	

Tabla 4-45.Tabla de Ejecución de Procedimiento

4.7.3. Ejecución de Actividades

Se debe realizar actividades previamente planificadas en el plan de acción, mediante la creación de un único equipo de trabajo debido a que la Institución pública es pequeña.

Este equipocontará con un coordinador que deberá reportar diariamente el avance de los trabajos de recuperación y, en caso de producirse algún

problema, reportarlo de inmediato a la jefatura a cargo del Plan de Contingencias para proceder de la mejor manera y con el consentimiento de la máxima autoridad.

Los trabajos de recuperación tendrán dos etapas, la primera la restauración del servicio usando los recursos de la Institución o local de respaldo disponibles, y la segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta última etapa lo suficientemente rápida y eficiente, contando con el presupuesto adecuadoen caso del siniestro sinperjudicar el buen servicio de nuestro Sistema e imagen Institucional.

4.7.4. Evaluación de Resultados

Una vez concluidas las labores de Recuperación del Sistema que fue afectado por el siniestro, se debe evaluar en forma efectiva, todas las actividades realizadas, la calidad con la que fue hecha, el tiempo utilizado, las circunstancias que aceleraron o entorpecieron las actividades del plan de acción, comportamientodel equipo de trabajo, etc.

De la evaluación de resultados y del siniestro en sí, se puede determinar que son necesarios realizar previamentesimulacros en la Institución que sirvan como retroalimentación, antecedentes y que permita el cálculo de presupuesto presuntivo ante el Plan de Contingencia, teniendo como ejemplo que al ejecutar este tipo de actividades se pueda identificar o detectar si se encuentra en óptima condiciones la información respaldada, la Operatividad de los Servidores entre otros, de tal forma que certifique la integridad y confiabilidad de los datos.

Al ejecutar estas actividades sin que suceda un siniestro real, permite identificar cuáles son las falencias y debilidades ante el equipo de trabajo al momento de actuar en un contingente, planificándose de mejor manera para su próxima simulación, debiendoobligatoriamente documentar todos los sucesoscomo soporte de apoyo y control tiempo por la paralización del servicio.

4.7.5. Retroalimentación del Plan de Acción

Con la evaluación de resultados, debemos de optimizar el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente.

Uno de los puntos evaluados previamente es la pérdida económica que involucra el no tener un plan de acción en el caso de surgir un percance, esta parte fue evaluada por el área Financiera en la que se enfatiza el caso de no tener operativo el Servidor de Datos Municipal, afectará directamente a las recaudaciones con un ingreso promedio por día de $10.000 que multiplicado por los 20 días laborables del mes, daría el gran total de $200.000 en perdida por recaudación de impuesto, siendo este un problema muy relevante para la Institución que depende mucho de la recaudación diaria para la gestión y crédito de nuevas obras Municipales.

4.7.6. Acciones Frente a los Tipos de Riesgo

Importante tener siempre presente las acciones frente a los tipos de riesgos existentes conaltas posibilidades de ocurrir.

Clase de Riesgo: Robo común de equipos Informáticos y archivos.
Análisis realizado: La institución se encuentra ubicada estratégicamente cerca de un área comercial y de fácil acceso, muy cercano a la vía principal, de tal forma que siendo una Entidad Pública se dé el libre acceso al área, creando una preocupación por este riesgo, a pesar de que el Municipio cuenta con personal de Seguridad Privada ubicada estratégicamente alrededor de los dos edificios es importante considerar lo mencionado. Las computadoras no son pueden ser observadas desde la calle, debido a que la Institución cuenta con vidrios oscurecidos que dificulta ser observado desde la parte exterior, descartando el riesgo. La Base de Datos Municipal tiene un valor incalculable, debido a que se encuentra registrado el catastro de alrededor de 27000 Predios Urbanos de todos los ciudadanos del Cantón, siendo la principal razón de mantener activo este Plan de Acción. Actualmente Talento Humano realiza los contratos eventuales con cláusula de Confidencialidad, que garantice la confianza y honestidad del personal al momento de trabajar en área críticas.

Tabla 4-46.Acciones frente a Riesgo # 1

Clase de Riesgo: Equivocaciones.
Análisis realizado: Para evitar esta clase de riesgo, periódicamente se está realizando evaluaciones al personal sobre los procedimientos que deben conocer y ejecutar en un Plan de contingencia, además se está constantemente solicitando a la máxima autoridad de la Institución la priorización de capacitación para el Área de Tecnología. Se realiza la difusión de políticas y procedimiento en relación a la Seguridad de la Información de forma periódica a través de correo electrónico y talleres relámpagos realizados dentro del área de Tecnología con una duración máxima de 2 horas en especial para el personal nuevo. Durante el periodo de vacaciones el personal que tiene a cargo un proceso debe de capacitar previamente con una semana de anticipación al encargado del proceso, quien a su vez debe de ser monitoreado por el jefe Departamental evitando de esta manera algún tipo de equivocación o falla humana. Actualmente la Jefatura de Tecnología está dividido en 3 áreas específicas: Soporte Técnico, Sistemas y Desarrollo, Infraestructura y Tecnología. Cada una de estas áreas cuenta con personal calificado y con experiencia para el buen desenvolvimiento de las actividades Departamentales.

Tabla 4-47.Acciones frente a Riesgo # 2

Clase de Riesgo: Fallas en los equipos.
Análisis realizado: Las fallas del sistema de red o Servidores de Datos pueden deberse al mal funcionamiento de los equipos ó la pérdida de configuración de los mismos, por lo que se deben monitorear y evaluar para determinar si esto ha ocurrido por variaciones de voltajes o desperfectos en el hardware.

Tabla 4-48.Acciones frente a Riesgo # 3

Clase de Riesgo: Vandalismo
Análisis realizado: Para evitar todo tipo de vandalismo interno o externo el Municipio se procedió a la instalación de 15 cámaras de video vigilancia con visión nocturna, ubicadas en sitios estratégicos, que permita registrar todos los movimientos de entrada del personal y sus alrededores. Actualmente se está gestionando la adquisición por parte las áreas Administrativa para la instalación de identificadores biométricas o tarjetas de acceso para ingreso a ciertas áreas de la institución

Tabla 4-49.Acciones frente a Riesgo# 4

CAPÍTULO 5

5. IMPLEMENTACION DE POLITICAS DE SEGURIDAD APLICABLES A LA TIC's.

5.1. NORMAS Y ESTÁNDARES DE SEGURIDAD DE LA TI

5.1.1. INTRODUCCIÓN

El Municipio de la Ciudad del Este actualmente provee a todos los funcionarios y empleados los recursos informáticos y servicios de comunicación necesarios

para que sean utilizados en las actividades laborales diarias, así como también para el desarrollo, innovación y manejo óptimo de la gestión administrativa.

Todos los recursos y servicios informáticos con los que cuenta la Institución son ampliamente utilizados a través de la red de comunicación de datos que se integra incluso con otras dependencias ubicadas fuera del Edificio Principal, evidenciándose de esta manera su amplia infraestructura tecnológica y la necesidad urgente de implementar Políticas de Seguridad que se adapte a la normativa vigente y garanticen la seguridad física y lógica de todos los servicios que se ofrece a la comunidad, así como también de la infraestructura del Centro de Procesamiento de Información.

En base a estos antecedentes el Municipio establecerá a través de este documento los mecanismos para la implementación, difusión, actualización y consolidación tanto de la política como también los componentes del Sistema de Gestión de la Seguridad de la Información y alinearlos de forma efectiva al tipo de servicio que ofrece esta Institución Pública a la comunidad, este proceso se basa en la aplicación de políticas construidas y alineadas al **estándar Británico**

ISO/IEC 27002:2013, el mismo que fue tomado como una guía base para el desarrollo de este capítulo.

5.1.2. Políticas Generales de Seguridad

La Política de Seguridad Informática requeridas para el Municipio permitirán mostrar a cada uno de los usuarios la forma de cómo debe actuar frente a los recursos y servicios informáticos de la Institución, sin pensar que la Política a implementar es un conjunto de sanciones o disposiciones molestosas, sino más bien identificarlas como un conjunto de normativas y reglas que permitan salvaguardar la información crítica y no critica de la Entidad para la cual se está trabajando.

5.1.3. Consideraciones Generales

Las políticas referidas en este documento están enfocadas para ser implementadas específicamente dentro del Centro de Procesamiento de Datos Municipal, además de estar orientada a la propiedad de la información creada y usada por los usuarios del Municipio de la Ciudad del Este, con el ánimo de evitar la inadecuada e improcedente utilización de los recursos informáticos que

se pone a disposición de los funcionarios y empleados para el cumplimiento de sus labores diarias.

Es importante conocer que se cuenta con el apoyo de Talento Humano, quien deberá cumplir con la función de notificar a todo el personal que se vincula contractualmente con el Municipio de las obligaciones con respecto al cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas y guías que surjan de la implementación de la política a través de la **norma ISO 27002:2013**.

De igual forma, el área TIC's Municipal será responsable de la notificación y socialización de la presente Política a implementarse **en un lapso no mayor a tres meses** y reportar los cambios que en ella se produzcan, además de firmar los compromisos de confidencialidad y la obligación de capacitación continua en materia de seguridad.

5.1.4. Objetivos Generales

Aplicar y difundir las políticas y Estándares de Seguridad Informática a todo el personal de la Municipalidad de la Ciudad del Este, para que sea de su conocimiento el cumplimiento en el buen manejo de los recursos informáticos asignados.

5.1.5. Beneficios de la Implementación de Políticas de Seguridad Informática

La implementación de Políticas de Seguridad basada en la **ISO 27002:2013**, constituyen la base a partir de la cual el Municipio de la Ciudad del Este diseñará sus propios procedimientos de seguridad, con el fin de garantizar que la información, productos y soluciones adquiridos cumplan con los objetivos de la institución y que éstos sean utilizados correctamente sin que sean expuestos deliberadamente en la red del Internet.

Por lo tanto, los beneficios derivados de la buena gestión de Políticas de Seguridad informática son los siguientes:

- Permitir Aplicar procedimientos de seguridad informática regulados, uniformes y coherentes en toda la Institución.
- Fomentar a través de la capacitación constante la cultura organizacional en materia de seguridad informática.
- Minimizar a través de su aplicación, la pérdida o fuga de la información y recursos.
- Proporcionar la confianza necesaria a todos los usuarios, demostrando que la seguridad de la información es un factor importante y necesario dentro de la Institución debiéndose abordar de forma correcta.

5.2. Diseño de Controles de Seguridad Informática

El diseño de controles para la Seguridad Informática dentro del Municipio se aplicara mediante la normativa ISO 27002:2013 (Iso27000.es 2013), de las cuales se ha extraído tres dominios idóneos que permitan cumplir con el objetivo de aplicación de esta política, tal como se presenta en la siguiente tabla.

Control	Como se Implementará	Métricas a Seguir
Políticas de Seguridad - Directrices de la dirección en Seguridad de la Información	Se habilitara un Wiki en la Web que pueda ser observado por todos, en la que se plasme el conjunto de políticas a aplicar en la Institución	Buscar Grado de despliegue y adopción de la política en la organización (medido por auditoría, gerencia o auto-evaluación).
Control de Acceso - Control de Acceso a sistemas y Aplicaciones	Documente procedimientos, normas y directrices de seguridad de la información, además de roles y responsabilidades, identificadas en el manual de política de seguridad de la organización	Métricas de madurez de procesos TI relativos a seguridad, tales como el periodo de aplicación de parches de seguridad (tiempo que ha llevado parchear al menos la mitad de los sistemas vulnerables -esta medida evita la cola variable provocada por los pocos sistemas inevitables que permanecen sin parchear por no ser de uso diario, estar normalmente fuera de la

		oficina o cualquier otra razón
Cumplimiento – Revisiones de la Seguridad de la Información	Alinee los procesos de auto-evaluación de controles de seguridad con las auto-evaluaciones de gobierno corporativo, cumplimiento legal y regulador, etc., complementados por revisiones de la dirección y verificaciones externas de buen funcionamiento	Porcentaje de revisiones de cumplimiento de seguridad de la información sin incumplimientos sustanciales.

Tabla 5-50. Tabla de Dominios a implementar

Esta guía es extraída de la ISO 27002:2013 las mismas debe tomarse con mayor relevancia porque es el apoyo fundamental para el desarrollo de este capítulo. El implementar y mantener esta normativa, está asegurando el cumplimiento de la legislación vigente, con el que se evitara riesgos y costos innecesarios, esto siempre sobre un marco legal que permita proteger al Municipio de aspectos probablemente no considerados y que permitan hacer de este una Institución Pública más confiable incrementando su prestigio ante la comunidad.

Cada una de las políticas desarrolladas en base a estándares ya establecidos debe ser expuesta a la máxima autoridad de la Institución para que este a su vez autorice su cumplimiento, previa revisión del Departamento de Asesoría Jurídica para su posterior publicación en Gaceta Oficial y socializada a todos los funcionarios y empleados que laboran en la Institución.

Finalmente cabe destacar que el objetivo principal de este capítulo es lograr la implementación de al menos 3 dominios de la Políticas de Seguridad Informática aplicada para el alcance de este documento.

5.2.1. Alcance de las Políticas a Diseñar

Las Políticas de Seguridad es elaborado de acuerdo al análisis de riesgos y de vulnerabilidades encontradas en las dependencias del Municipio de la Ciudad del Este y revisadas en los capítulos anteriores, por consiguiente el alcance de estas políticas se encuentra orientado a la actividad de la Organización y a los tres dominios seleccionados.

5.2.2. Etapas para el Desarrollo de una Política

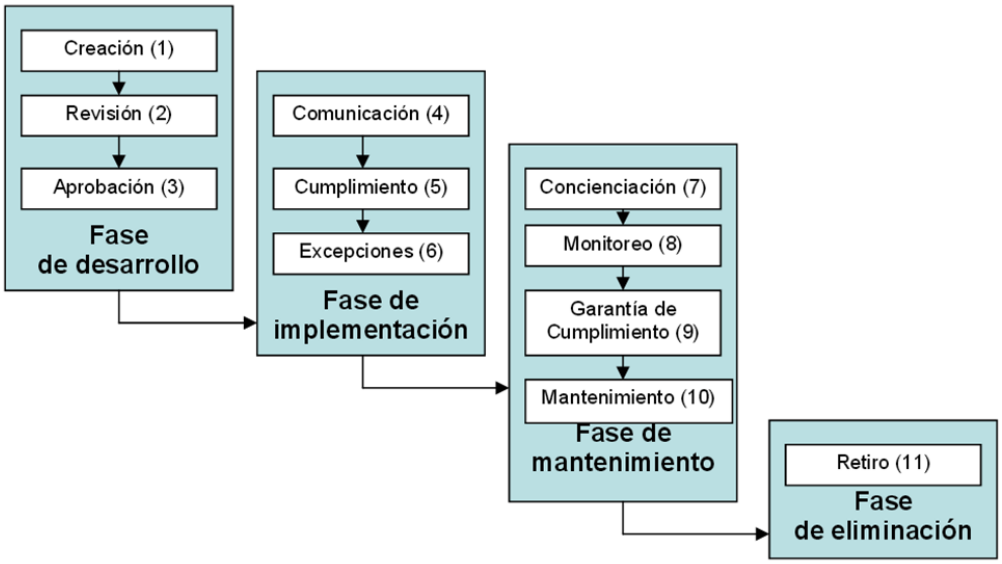


Figura 5-63. Desarrollo de Políticas de Seguridad

5.3. Plan de Implementación de las Políticas de Seguridad Informática

5.3.1. Responsabilidad y Tiempo de Ejecución

Plan de Ejecución					
Etapa	**Política**	**Estándares y buenas practicas**	**Recurso Humano**	**Ejecución**	**Tiempo**
Generación	Seguridad Informática	Función de seguridad	Auditor informático, Oficial	Dependencias que los proponen	**15 días**

		informática y profesionales con conocimientos en el área	de Seguridad Informática		
Revisión	Comité de evaluación de políticas	Comité de evaluación de políticas	Auditor Informático	Función de seguridad informática y director de área comprometida	**5 días**
Aprobación	Consejo Municipal	Consejo Municipal	Máxima Autoridad Municipal	Máximas autoridades de la Institución	**5 días**
Difusión o Comunicación	Secretaria General	Secretaria General	Oficial de Seguridad Informática	Dependencias que los proponen	**4 días**
Cumplimiento	Todo el Personal de la Institución	Todo el Personal de la Institución	Oficial de Seguridad Informática	Todo el Personal de la Institución	**Periódica**
Excepciones	Comité de evaluación de políticas	Comité de evaluación de políticas	Oficial de Seguridad Informática	Directivos del Área	**No aplica**
Capacitación	Función de Seguridad Informática y función de capacitación	Función de Seguridad Informática y función de capacitación	Oficial de Seguridad Informática	Jefe del Área	**5 días**

Monitoreo	Funcionarios responsables de la Supervisión, Auditoria	Funcionarios responsables de la Supervisión, Auditoría	Oficial de Seguridad Informática	Funcionarios responsables de la Supervisión, Auditoría	**3 días**
Garantizar Cumplimiento	Funcionarios, responsables de la Supervisión	Funcionarios, responsables de la Supervisión	Oficial de Seguridad Informática	Función de seguridad informática y director de áreas comprometida	**Periódica**
Mantenimiento	Seguridad Informática	Seguridad Informática	Oficial de Seguridad Informática	Seguridad Informática	**Semestral**
Retiro	Seguridad Informática	Seguridad Informática	Máxima Autoridad Municipal y Oficial de Seguridad Informática	Dependencia que lo propone	**Cuando sea necesario**

Tabla 5-51. Tabla de responsabilidades y tiempo de ejecución

5.3.2. Diagrama de Planificación para la Implementación de Políticas de Seguridad

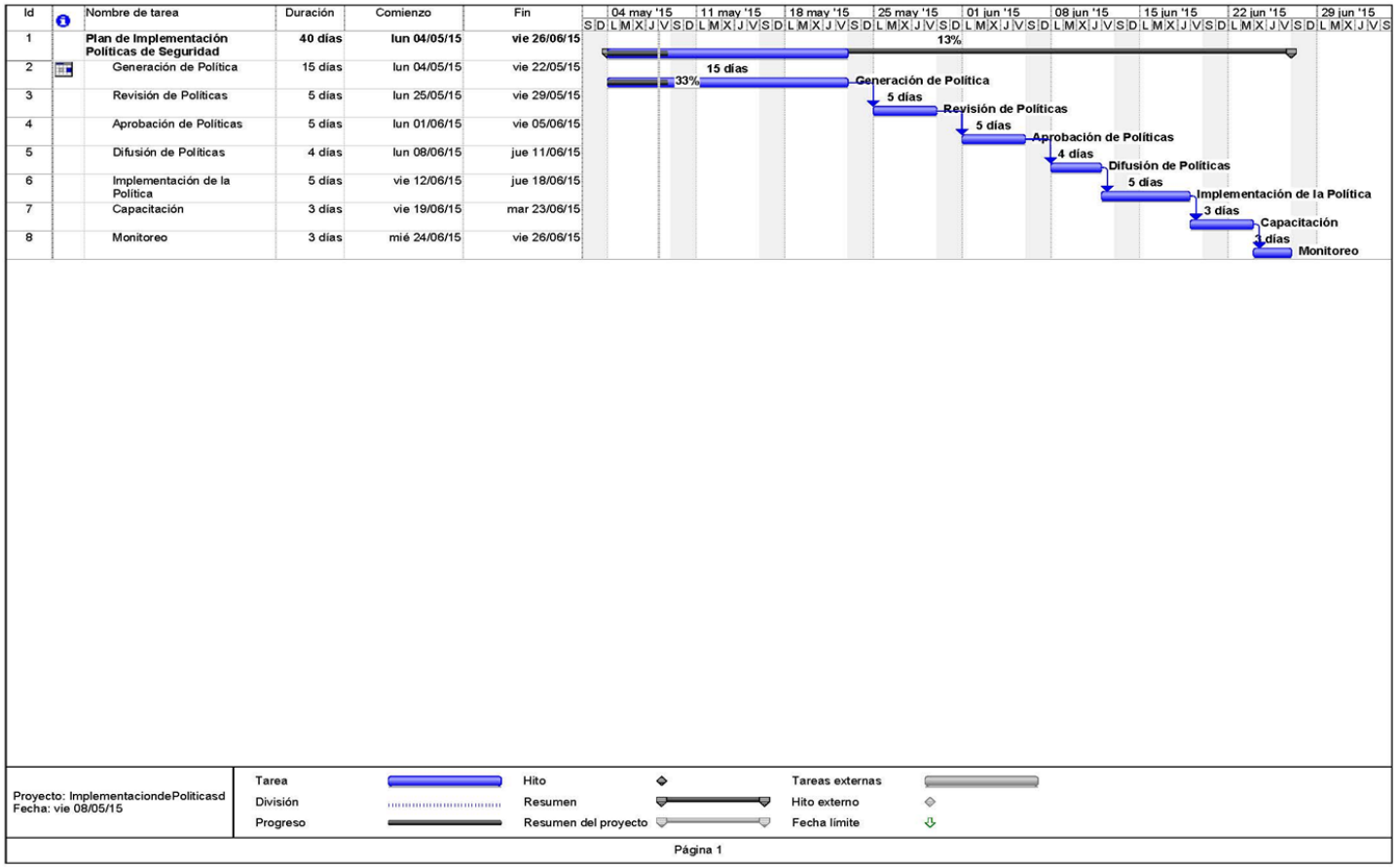


Figura 5-64. Diagrama GANTT

Este plan de ejecución está basado en un tiempo de 40 días, **no mayor a tres meses** para que sea implementado como plan piloto dentro de la Institución de forma inmediata una vez aprobada por el Consejo Cantonal y la máxima autoridad Municipal.

5.3.3. Recursos Tecnológicos y Talento Humano

Para implementación de esta política se procedió a identificar que el recurso primario es la documentación de la norma ISO 27002, para este caso **no existirá contratación de personal** debido a que el recurso Humano (6 empleados públicos) del Departamento de Informática se encuentra comprometido con ejecución de la misma.

El software administrativo como parte de ayuda a la gestión de esta política **no tiene costo** ya que se implementara una herramienta con licencia de Software libre. Todas estas consideraciones serán colocadas en observación ante la máxima Autoridad Municipal de primera instancia debido a que la Institución Pública debe sujetarse al ahorro y optimización de recursos.

Por tal motivo se siguiere además que el Jefe Departamental considere dentro del Plan Operativo Anual para el siguiente año los equipos de seguridad informática necesarios para la seguridad de la información sin que estas afecten a la implementación de la Política, lo que se detalla a continuación:

- Cerradura biométrica para acceso al Centro de Procesamientos de Datos
- Firewall de última generación y robusto
- IDS/IPS
- Cámaras de Monitoreo con visión nocturna, incluya Equipo de Grabación

5.3.4. Costos de Implementación

Los costos estimativos del diseño de la política son:

Costos de Diseño	**Valor**
Norma ISO 27002	$ 35
Costo de Diseño (2 meses)	$1500
Cursos de Seguridad de la Información	$ 300
Otros Gastos	$200
Subtotal	**$ 2035**

Tabla 5-52. Tabla de Costo de Diseño

Los costos de Implementación de la Política son

Costos de Implementación	**Valor**
Costo de Software de Administración	$ 0
Medio de Almacenamiento Externo para Respaldos	$ 250
Póliza de Seguro	$ 500
Otros Gastos	$ 100
Subtotal	**$ 850**

Tabla 5-53. Tabla de Costo de Implementación

Costos de Totales	**Valor**
Diseño	$ 2035
Implementación	$ 850
Total Inversión	**$ 2885**

Tabla 5-54. Tabla de Costo Total Inversión

El software a utilizar como soporte para la Administración y monitoreo de equipos de Escritorio, Servidores de Datos, portátiles entre otros se llama "**Belarc**", producto utilizado por múltiples empresas a nivel mundial y que no

tiene costo, permite obtener beneficios de una administración desde la nube del Internet que permita al Oficial de Seguridad Informática tener el facilismo de monitorear incluso desde lugares remotos.

5.3.5. Análisis de la Política de Seguridad para el Área Tics Municipal

El análisis de la Política de Seguridad Informática a implementar es aquella que tiene como objetivo evaluar los controles de la función informática, determinar la eficiencia de los sistemas, verificar el cumplimiento de las políticas y procedimientos de la Institución para que los recursos materiales y humanos de esta área se utilicen eficientemente.

Este análisis surge basado en que la información es uno de los activos más importantes del Municipio, así como el uso de la tecnología y sistemas computarizados para el procesamiento de la información. A continuación se observa la siguiente tabla en la que se presenta el proceso de recolección y evaluación de evidencia para determinar sistema Informáticos.

Salvaguarda Activos	Daño
	Destrucción
	Uso no autorizado
	robo
Mantiene la Integridad de los Datos	Oportunidad
	Preciso
	Confiable
	Completa
Alcance y Metas Organizacionales	Contribución de los Sistemas Informáticos
Consume recursos Eficientemente	Utiliza recursos con mesura para procesar la información

Tabla 5-55. Proceso de la Auditoria Informática

5.4. Guía para el Establecimiento del Plan de Políticas de Seguridad

5.4.1. Políticas de Seguridad para Instalaciones Físicas

Con el objetivo de disminuir problemas de seguridad aplicables a los recursos físicos utilizados en el procesamiento de la información de la Institución y

considerando como responsable de la ejecución de este proceso al oficial de Seguridad de la Información o al Analista de Infraestructura de la Jefatura de Informática, quien deberá garantizar el cumplimiento de las políticas y requerimientos de seguridad pertinentes, a través de la generación de un compromiso con el área de Tecnología que permita aplicar y mantener las siguientes políticas:

a) Todos los sistemas de comunicación se encontraran debidamente protegidos con infraestructura apropiada de manera que el usuario común no tenga acceso físico directo.
b) Cumplir con los niveles de aprobación vigentes en la organización, incluyendo al responsable de Seguridad de la Información, asegurando de esta manera el cumplimiento de las políticas y requerimientos.
c) Las visitas internas o externas podrán acceder a las áreas restringidas siempre y cuando se encuentren acompañado por un responsable del área con permiso de la autoridad correspondiente.
d) Establecer horarios de acceso a las instalaciones físicas (Centro de Procesamiento de Datos Municipal), especificando los procedimientos y excepciones.

e) Definir y socializar internamente qué personal está autorizado para mover, cambiar o extraer equipo del Centro de Datos a través de identificaciones y formularios de E/S; debiendo informar de estas disposiciones al personal de seguridad del Edificio Municipal.

f) Se verificará periódicamente el hardware y software para garantizar su compatibilidad, operatividad y ejecución correcta de los procesos, este debe realizarse de forma periódica y es responsabilidad del oficial de Seguridad de la Información.

g) El acceso al Centro Procesamiento de Datos y Redes de comunicación, es exclusivo e intransferible para los funcionarios del Área de Informática que tenga los conocimientos y la autorización respectiva de quien dirige la Dirección o Departamento.

5.4.1.1. Robo de Equipo

- El área de bodega en conjunto con el Departamento de Informática deberá definir procedimientos para mantener actualizado el inventario físico, firmas de resguardo para préstamos y usos dedicados de equipos de tecnología de información.

- El resguardo de los equipos de comunicaciones deberá quedar bajo la Dirección, Jefatura o responsable del área, permitiendo conocer siempre la ubicación física de los equipos.
- El centro de operaciones o área de procesamiento de datos, así como las áreas que cuenten con equipos de misión crítica deberán contar con vigilancia y/o algún tipo de sistema de video cámaras que ayude a recabar evidencia de accesos físicos a las instalaciones.

5.4.1.2. Mantenimiento y Protección Física

El Centro de Procesamiento de Datos del Municipio de la Ciudad del Este debe considerar para el mantenimiento y protección de equipos los siguientes puntos:

- Contar con un personal del área de limpieza al menos una vez cada dos semana y así mantener libre de polvo.
- Ser un área restringida y protegida.
- Estar libre de contactos e instalaciones eléctricas en mal estado
- Estar libre de líneas de agua o reservorios cercanos
- Contar por lo menos con un extinguidor de incendio adecuado y cercano al Centro de Procesamiento de Datos.

- Cada vez que se requiera conectar equipo de cómputo, se deberá comprobar la carga de las tomas de corriente.
- Contar con algún esquema o plan de contingencia que asegure la continuidad del servicio

Actualmente el área está recibiendo el mantenimiento periódico y posee la señalética adecuada para que el encargado de la limpieza pueda realizar su trabajo sin problemas. El acondicionamiento de la habitación de primera instancia fue diseñado por los arquitectos para que las líneas de agua y ducterias primarias eléctricas no paseen por la parte superior de esta, logrando además reubicar el panel principal de energía eléctrica en un lugar más seguro, trabajo que fue revisado por técnicos que certifican que no existirá problema alguno para los equipos electrónicos.

5.4.2. Políticas de Control de Acceso a la Información

Uno de los activos de mayor cuidado y crítico de una Institución es la información que se genera a través de la transacción diaria, por tanto es importante considerar dentro de las políticas de una institución pública el control de acceso a la misma.

El Mantener la integridad de la Información Municipal es responsabilidad del Departamento de Informática y del oficial de Seguridad de la Información quienes deben aplicar las siguientes políticas:

a) Las claves de acceso a los Servidores de Datos estarán bajo la custodia y de responsabilidad exclusiva del Jefe de Departamento de Informática y solo se entregarán a tercera personas previa autorización por escrito de la máxima autoridad del Municipio.
b) La Gestión de claves de acceso es estrictamente responsabilidad del Jefe Departamental o a quien delegue la responsabilidad en el área correspondiente.
c) La configuración de los servicios tecnológicos en los ambientes de pruebas y producción, así como el paso a producción de las aplicaciones desarrolladas o adquiridas, son de responsabilidad del Departamento de Informática.
d) Es responsabilidad de la Jefatura de Informática, monitorear los enlaces de comunicaciones, los servicios tecnológicos de esta Institución Pública, además de garantizar la continuidad de los servicios y comunicaciones instalados en el Centro de Datos Municipal.

e) Al presentarse problemas o modificaciones en los Servicios Tecnológicos o Servidores de datos que afecten el normal funcionamiento de los Sistemas Municipales, deberán comunicarse inmediatamente de las fallas y el tiempo de retorno del Servicio, con las áreas pertinentes dentro de la Institución Pública.

f) Asignar a los usuarios un rol o permiso dentro de los perfiles que tiene definido cada sistema, que les habilite las posibilidades de realizar acciones en el mismo, solicitando la asignación de roles o permisos a los nuevos usuarios, los Directores de Departamento, División o Servicio, los que deberán indicar para cuál de éstos se solicita acceso. Es responsabilidad del jefe de área informar cuando un funcionario ya no puede tener más acceso a la red o un rol en particular, quien a su vez será certificado por el Departamento de Talento Humano en caso de que el usuario deje de laborar para la Institución.

5.4.2.1. Políticas de Contraseñas

Para el buen manejo de los Sistemas Informáticos Municipales se implementaran las siguientes políticas de contraseñas:

a) Todo funcionario y empleados del Municipio de la Ciudad del Este, es responsable de velar por la seguridad de las contraseñas a su cargo que utiliza para el acceso a los distintos servicios y recursos ofrecidos por la Institución.
b) Toda contraseña es de uso exclusivo, y por lo tanto es personal e intransferible.
c) Todas las contraseñas de los Sistema de Información (cuentas de administrador, cuentas de administración de aplicaciones, etc.), se cambiarán con una periodicidad de al menos una vez cada tres meses.
d) Todas las contraseñas de usuario (cuentas de correo electrónico, cuentas de servicios Web, etc.), se cambiarán al menos una vez cada seis meses.
e) Ante la sospecha de que una contraseña haya sido revelada a terceros, se cambiará la misma de forma inmediata, y se procederá a notificar del incidente de seguridad, al Departamento de Informática o al oficial de seguridad responsable.
f) Las cuentas de usuario que tengan privilegios de sistema, a través de su pertenencia a grupos o por cualquier otro medio, tendrán contraseñas distintas a otras cuentas mantenidas por dicho usuario en los servicios y recursos.

g) Las contraseñas de los funcionarios que ingresan al Municipio de la Ciudad del Este, por primera vez serán proporcionadas por el Departamento de Informática, luego de recibir el listado respectivo por parte de Talento Humano.

h) Las contraseñas de los funcionarios que se desvinculan de la Institución, se desactivarán una vez que el Departamento de informática, reciba el listado o Informe respectivo por parte del Departamento de Talento Humano.

5.4.2.2. Prohibición en Política de Contraseña

- Revelar o compartir su contraseña de cualquier forma.
- Escribir la contraseña o almacenarla en archivos sin que sean encriptados, comunicarla en el texto de mensajes de correo electrónico, o en cualquier otro medio de comunicación electrónica.
- Evitar que el usuario registre las contraseñas en papel o archivos físicos de forma no segura.
- Evitar facilitar la contraseña a terceras personas por motivo de vacaciones.

5.4.2.3. Perfiles de Acceso en la Red

Uno de los aspectos más importantes a la hora de implementar un acceso remoto hacia los servicios de la institución es definir las políticas de seguridad y el tipo de perfil de acceso.

Para el Acceso al Sistema Municipal dentro del Administrador de Oracle se encuentra creado los siguientes perfiles que se agregan según las funciones y responsabilidades del personal plasmado en el orgánico Funcional de la Institución vigente.

Perfil	**Áreas de Acceso**	**Tipos de Vigencia**
Adm_Tesoreria	Sistema de Recaudación, y Coactiva	Indefinido o Temporal
Adm_Contabilidad	Sistema Contable	Indefinido o Temporal
Adm_Financiera	Sistema de Resoluciones y Autorizaciones Financieras Municipales	Indefinido o Temporal
Adm_Catastro	Sistema de Catastro	Indefinido o Temporal

Adm_Rentas	Sistema de Rentas	Indefinido o Temporal
Adm_Terrenos	Sistema de Inspecciones	Indefinido o Temporal
Adm_Planificacion	Sistema de Catastro y Planificación Urbana	Indefinido o Temporal
Adm_TH	Sistema de Roles , Faltas y atrasos	Indefinido o Temporal
Adm_Juridico	Sistema de Minuta	Indefinido o Temporal

Tabla 5-56. Perfil del Sistema Municipal

La administración de perfiles es controlado a través del módulo de Seguridad del Sistema Municipal donde se puede crear al usuario y asignarle de forma inmediata su perfil de acceso según los parámetros especificados por parte del Departamento de Talento Humano.

5.4.2.4. Asegurando el Acceso

El método de acceso más común para conectarse remotamente a los recursos de una Institución se realiza a través de un Navegador Web. Se introduce la dirección URL o IP y se envía al usuario a un formulario donde ha de introducir sus credenciales (usuario y contraseña) de acceso remoto. Una vez validado en el sistema y creada la conexión remota con la oficina debe validarse con sus

credenciales de acceso la red local de la organización, otra forma de seguridad que se está implementando como piloto es adoptar franjas horarias para acceder al sistema, de esa manera se establecen periodos de tiempo donde se autoriza el acceso a los recursos.

5.4.3. Políticas de Seguridad para Cuentas de Usuario del Sistema Institucional

La implementación de esta política es dar a conocer el manejo de las cuentas (usuario - contraseña) de acceso a los Sistemas Institucionales, a continuación se definen las siguientes políticas para el manejo correcto de cuentas de usuario de los Sistemas Institucionales:

a) El uso de la cuenta de usuario es responsabilidad de la persona a la que está asignada. La cuenta es para uso personal e intransferible.
b) La cuenta de usuario se protegerá mediante una contraseña. La contraseña asociada a la cuenta de usuario, deberá seguir los criterios para la construcción de contraseñas seguras descrito en el siguiente punto de este capítulo.

c) Las cuentas de usuario (usuario y contraseña) son sensibles a mayúsculas y minúsculas, es decir que estas deben ser tecleadas como tal como fueron escritas.
d) No compartir la cuenta de usuario con otras personas: compañeros de trabajo, amigos, familiares, etc.
e) Si otra persona demanda hacer uso de la cuenta de usuario, hacer referencia a estas políticas. De ser necesaria la divulgación de la cuenta de usuario y su contraseña asociada, deberá solicitarlo por escrito o medio digital y dirigido al DBA Municipal.
f) Si se detecta o sospecha que las actividades de una cuenta de usuario puede comprometer la integridad y seguridad de la información, el acceso a dicha cuenta será suspendido temporalmente e informado a Talento Humano, esta cuenta será reactivada sólo después de haber tomado las medidas necesarias a consideración del Administrador del Sistema.

5.4.3.1. Tipos de Cuentas de Usuario

Para ejecución de las presentes políticas, se definen dos tipos de cuentas de usuario:

Cuenta de Usuario de Sistema de Información: todas aquellas cuentas que sean utilizadas por los usuarios para acceder a los diferentes sistemas de información. Estas cuentas permiten el acceso para consulta, modificación, actualización o eliminación de información, y se encuentran reguladas por los roles o Perfiles de usuario del Sistema.

Cuenta de Administración de Sistema de Información: Corresponde a la cuenta de usuario que permite al administrador del sistema realizar tareas específicas de usuario a nivel directivo, como por ejemplo: agregar/modificar/eliminar cuentas de usuario del sistema.

Para llegar al cumplimiento de esta política son necesarios implementar las siguientes:

a) Todas las contraseñas para acceso al Sistema con carácter administrativo deberán ser cambiadas al menos cada 6 meses.
b) Todas las contraseñas para acceso al Sistema de nivel usuario deberán ser cambiadas al menos cada 12 meses.
c) Todas las contraseñas deberán ser tratadas con carácter confidencial.

d) Las contraseñas de ninguna manera podrán ser transmitidas mediante servicios de mensajería electrónica, instantánea, redes sociales, ni vía telefónica.
e) Si es necesario el uso de mensajes de correo electrónico para la divulgación de contraseñas, estas deberán transmitirse de forma cifrada.
f) Se evitará mencionar y en la medida de lo posible, teclear contraseñas en frente de otros.
g) Se prohíbe revelar contraseñas en cuestionarios, reportes o formularios.
h) Se evitará el utilizar la misma contraseña para acceso a los sistemas operativos y/o a las bases de datos u otras aplicaciones.
i) Se evitará el activar o hacer uso de la utilidad de Recordar Contraseña o Recordar Password.
g) No se almacenarán las contraseñas en libretas, agendas, post-it, hojas sueltas, etc. Si se requiere el respaldo de las contraseñas en medio impreso, el documento generado deberá ser único y bajo resguardo personal.
h) No se almacenarán las contraseñas sin encriptación, en sistemas electrónicos personales (asistentes electrónicos personales, memorias USB, teléfonos celulares, agendas electrónicas, etc.).

i) Si alguna contraseña es detectada y catalogada como no segura, deberá darse aviso al(los) usuario(s) para efectuar un cambio inmediato en dicha contraseña.

5.4.3.2. Criterios en la Construcción de Contraseñas Seguras

Una contraseña aplicada de forma segura deberá cumplir con las siguientes características:

- La longitud debe ser al menos 8 caracteres.
- Contener caracteres tanto en mayúsculas como en minúsculas.
- Puede tener dígitos y caracteres especiales como _, -, /, *, $, ¡, ¿, =, +, etc.
- No debe ser una palabra por sí sola, en ningún lenguaje, dialecto, jerga, etc.
- No debe ser un palíndromo (ejemplo: oso)
- No debe ser basada en información personal, nombres de familia, etc.
- Procurar construir contraseñas que sean fáciles de recordar o deducir.

5.4.4. Políticas de Seguridad para el uso de Equipos Informáticos

El Municipio de la Ciudad del Este, cuenta actualmente con una amplia inventario de equipos informáticos, por tal razón a través de esta política se requiere socializar al funcionario administrativo del correcto uso de los equipos dentro de la institución así como la implementación de buenas prácticas de seguridad informática.

El Departamento de Informática implementará las siguientes políticas:

a) Los equipos informáticos propiedad del Municipio de la Ciudad del Este, se utilizarán únicamente para actividades laborales que permitan alcanzar las metas y objetivos planteados por la Institución.

b) Para el correcto funcionamiento de los equipos informáticos de la Municipalidad, se planificaran mantenimientos necesarios tanto preventivos como correctivos una vez al año, los términos de contratación de ser necesarios serán elaborados y considerados en el POA del Departamento de Informática.

c) La compra de equipos informáticos será responsabilidad del Departamento de Informática en conjunto con la Dirección Administrativa, previa aprobación de la máxima autoridad del Municipio, enmarcadas en la Ley Orgánica del Sistema Nacional de Contratación Pública y su Reglamento.

d) La compra de accesorios y reparaciones será solicitada por el Departamento de Informática y gestionada a través de la Dirección Administrativa, si un área requiere algún tipo de accesorio especifico, deberá contar con el respetivo informe técnico y la debida aprobación de la máxima autoridad de la Institución, enmarcadas en la Ley Orgánica del Sistema Nacional de Contratación Pública y su Reglamento.

e) Para poder conectar un equipo informático que no sea propiedad de la Institución, se solicitará el permiso correspondiente al Departamento de Informática, para que inspeccione el equipo, con el fin de comprobar que dicho activo no constituya en una amenaza para la seguridad de los servicios, red y recursos informáticos de la Institución, se evalué la necesidad de conexión a la red y se concede la autorización correspondiente si es el caso.

f) En caso de robo, hurto o extravío del equipo informático del Municipio de la Ciudad del Este, se notificará inmediatamente a la Dirección Administrativa, para empezar los trámites legales correspondientes.

g) Para el caso de daño de cualquier equipo informático, se informará inmediatamente al Departamento de Informática, para realizar las correcciones necesarias o el informe técnico de ser necesario.

h) Solo el personal autorizado por el Departamento de Informática, será el encargado de abrir los equipos informáticos propiedad de la Institución.

i) Todos los equipos informáticos pertenecientes al Municipio de la Ciudad del este, contarán con un Sistema Operativo con licencia de tipo GLP (Software Libre Linux Ubuntu), los cuales serán administrados por el Departamento de Informática.

j) Todos los equipos informáticos serán actualizados de manera periódica con los últimos parches de seguridad del Sistema Operativo y aplicaciones instaladas en el equipo.

k) Solo en los caso de no existir Paquetes Informáticos que no son compatibles o de optima operativas para Linux se procederá a instalar Sistema Operativo Licenciado (Microsoft) con sus respectivos aplicativos.

5.4.5. Políticas de Seguridad para el Uso del Internet

La política de navegación y buen uso del Servicio de Internet proporciona a los empleados reglas e indicaciones sobre el uso apropiado de la red y el acceso a este servicio. Esta directiva ayuda a proteger tanto a la administración del Municipio como al empleado; quien deberá ser consciente y con el pleno conocimiento de que navegar por ciertos sitios o descargar archivos está prohibido y que la directiva debe cumplirse o podría haber serias repercusiones, y aplicar esta política llevará a menores riesgos de seguridad para el Municipio como resultado de empleados negligentes.

Entre las principales políticas para el uso del servicio de Internet tenemos:

a) Los empleados que laboran en la Institución Pública se comprometerán a utilizar internet de forma responsable y productiva. El acceso a internet se limita a actividades relacionadas solo con el trabajo y no se permite su uso personal.
b) Los usuarios pueden acceder a la red local (Intranet) del servicio y cualquier otro sitio de Internet que tenga relación con el quehacer Institucional y quedará estrictamente prohibido las redes: de tipo social

(tales como Facebook, Hi5, youtube etc.), sitios de contenido sexual, terrorismo, descarga de piratería, media on-demand (tales como videos, tv, radios, streaming en general).

c) Toda la información de internet redactada, transmitida y/o recibida por los sistemas informáticos del Municipio de la Ciudad del Este, se considera propiedad de Institución y se reconoce como parte de sus datos oficiales, por lo tanto, podrá revelarse por exigencias legales o a terceros autorizados por la máxima autoridad del Municipio.

d) El equipamiento, los servicios y la tecnología utilizados para acceder a internet que pertenecen a Institución, se reserva el derecho a supervisar el tráfico de internet y a acceder a los datos redactados, enviados o recibidos a través de sus conexiones en línea

e) Todos los sitios y descargas serán susceptibles de supervisión y/o bloqueo por parte del Departamento de Informática o el oficial de Seguridad de la Información si se consideran perjudiciales y/o improductivos para el ejercicio.

f) Queda estrictamente prohibida la instalación de software del tipo tecnología de mensajería instantánea

g) Los usuarios tienen prohibido instalar y usar programas para “bajar” información desde INTERNET hacia sus computadores, como también el

uso de programas tales como Emule, Ares, Kazaa y cualquier otro programa P2P (Peer to Peer).

h) Los usuarios deben acceder a INTERNET usando el navegador que se provee en sus respectivos computadores. El navegador por defecto y autorizado para su uso es el Firefox o Chrome.

i) Las configuraciones del PC y su navegador es de exclusiva responsabilidad del Departamento de Informática y siempre orientado a asegurar el ancho de banda para las aplicaciones y uso de interés de la TIC's.

j) Para evitar algún problema de contagio masivo por el uso de programas NO autorizados por el área de Informática, se prohíbe la instalación de software NO licenciado por la Institución, asimismo, serán auditados los programas instalados en cada computador, entregando la información recogida a la autoridad competente que pueda evaluar las consecuencias de cada situación.

k) El Departamento de Informática a través de su oficial de Seguridad de la Información, realizará monitoreo permanente, mediante las herramientas con las que cuenta o bien solicitando reportes al proveedor de Internet (ISP), para determinar el cumplimiento de estas políticas.

5.4.5.1. Difusión

Se mantendrá publicada dentro de la intranet de la Institución, las normas de uso y políticas de seguridad establecidas en el presente reglamento.

5.4.6. Políticas de Seguridad Inalámbrica

El correcto manejo y utilización de los recursos de la red inalámbrica en la Institución se ejecutan a través de la implementación de una política perfilada a la situación actual de la Institución.

Entre las responsabilidades a ejecutar por parte del Departamento de informática están:

a) Toda instalación de equipo inalámbrico que tenga como propósito tener acceso a la red de comunicaciones de la Institución, debe ser aprobada por el Departamento de Informática.

b) Proveer asistencia, orientación y recomendaciones a usuarios sobre el manejo correcto de equipo de comunicaciones inalámbricas que utilizan en la Institución.
c) Mantener un registro MAC de todas las tarjetas de comunicación inalámbrica y puntos de acceso en la Institución.
d) Aprobar la instalación de equipo y programado para la red inalámbrica utilizado en la Institución.
e) Informar a los usuarios de la red inalámbrica sobre la seguridad, las políticas y procedimientos relacionados al uso de las comunicaciones inalámbricas en la Institución.
f) Monitorear el rendimiento y seguridad de todo el equipo de comunicaciones inalámbricas para prevenir acceso no autorizado a la red.
g) Monitorear el desarrollo de las tecnologías de redes inalámbricas, evaluar mejoras a la red inalámbrica y si es apropiado, incorporar nuevas tecnologías para mejorar el rendimiento, capacidad, disponibilidad, seguridad y confiabilidad de la red.

5.4.6.1. Asignación del Servicio

El servicio de acceso a la Red Inalámbrica será proporcionado a los usuarios de la Institución de manera segura a través de una petición formal al Departamento de Informática.

El Departamento de Informática activará los accesos a la Red Inalámbrica a partir de que el usuario haya registrado su equipo llenando la solicitud del servicio.

5.4.6.2. Disponibilidad del servicio.

El servicio de conexión a la Red Inalámbrica estará disponible las 24 horas del día, todos los días del año, salvo en situaciones de fuerza mayor, fallas de energía o interrupciones relativas al mantenimiento preventivo o correctivo de los equipos y elementos relacionados con la prestación del servicio de Internet.

El área de cobertura de la red inalámbrica dependerá del equipo instalado para el área o piso, por lo general será de un radio de 100 mts. aproximadamente y ubicado en la Alcaldía.

5.4.6.3. Suspensión del Servicio

El Departamento de Informática podrá suspender o desactivar temporalmente el servicio o cancelarlo de manera definitiva para determinado equipo, cuando detecte que el usuario haya hecho uso indebido del servicio. La reactivación deberá ser autorizada por Responsable del área Administrativa a través de una petición escrita o correo electrónico.

De la misma manera, el servicio será restringido para ciertos equipos en caso de que se detecte tráfico excesivo de los mismos o condiciones que indiquen que están interfiriendo con el funcionamiento normal de la red.

5.4.7. Política de Seguridad para el manejo de Correo Electrónico

Dentro de una empresa o institución púbica hoy en día se hace necesario el uso continuo del correo electrónico para la respectiva comunicación interna y

externa de la institución, pero debido a los varios tipos de ataques informáticos de las que puede ser víctima el servidor de correo electrónico se ha considerado las siguientes políticas, siendo responsable el Departamento de Informática y el oficial de Seguridad de la Información.:

- El dominio establecido para el Municipio es “**cuidadeleste.gob.ec**”, todos los subdominio requeridos para el uso de la institución se engancharan al dominio principal. El acceso a este servicio, se lo realizará por medio de la página web institucional (www.ciudaddeleste.gob.ec), link Webmail, o directamente desde la URL https://mail. ciudaddeleste.gob.ec.
- El correo electrónico institucional se utilizará solamente como una herramienta de comunicación e intercambio de información oficial y no debe utilizarse como una herramienta de difusión indiscriminada de información.
- El usuario es responsable del contenido que envié usando el correo electrónico institucional. Los correos enviados a través del sistema de correo electrónico de la organización no podrán incluir contenidos ofensivos. Se incluyen, sin límite, el uso de lenguaje/imágenes vulgares u ofensivas

- El correo electrónico no se utilizará para él envió de información confidencial, para esta situación existen otros medios de transmisión de información confidencial o institucional.
- Los usuarios estarán sujetos a una auditoria por parte del comité de Seguridad de la información en cuanto a tráfico y manejo seguro de la información enviada, cuando se estime estrictamente necesario.
- El Municipio de la Ciudad del Este, en caso de uso indebido de correo electrónico, podrá suministrar la evidencia a la entidad que lo requiera para su investigación.
- Se prohíben expresamente, para todo usuario autorizado, el uso de técnicas de ataque a sistema de correo electrónico como mail SPAM, mail Bombing, mail Spoofing o mail Relay no autorizado,
- Los usuarios son los únicos responsables de todas las actividades realizadas, desde sus cuentas de acceso y buzones.
- La cuenta de correo es intransferible, por lo que no debe proporcionarse a otras personas.
- Los correos deberán ser marcados como urgentes únicamente cuando realmente lo sean.

- La información que se recibe de manera personal y confidencial por correo electrónico, no se puede reenviar a otra persona, sin la autorización del remitente.
- En forma general un correo electrónico, deberá ser impreso únicamente cuando sea necesario, ya que esta herramienta fue creada para tener un archivo electrónico, agilizar las comunicaciones, descartar en la medida de lo posible el archivo tradicional y lograr un ahorro de papel para la Institución.

5.4.7.1. Restricciones para el Servicio de Correo Electrónico

1. Mensajes: El servicio de correo permite enviar archivos anexados (attachments) de hasta **20MB** usando un cliente de correo (Thunderbird y Outook) y de hasta **2 MB** usando la interface Web en: http://mail.ciudaddeleste.gob.ec/
2. Mensajes Enviados, Eliminados y Buzones**:** Se les informa a los usuarios que el servicio de correo permitirá almacenar mensajes eliminados en la carpeta **Trash (Basurero)** hasta **1 semana,** es decir, cada semana se eliminarán automáticamente todos los mensajes en el Trash de los usuarios; para lo cual se les pide que tomen las medidas del caso. Los

mensajes enviados son guardados automáticamente en el servidor (sólo en el caso de usar IMAP).

3. Cuota: Los buzones administrativos tienen cuota definida de 2 Megas.

   Nota: Si el Usuario hace caso omiso al mensaje de advertencia, el administrador bloqueará la cuenta del usuario y únicamente podrá ser reactivada al liberar el espacio excedente.

4. Cadenas y Múltiples Usuarios: Está PROHIBIDO el fomentar el envío de cadenas de mensajes a múltiples usuarios, ya sea enviando o reenviando esta clase de mensajes.

   Se puede enviar mensajes a múltiples usuarios siempre que no sobrepasen el número de **20**. El incumplimiento de esta norma, tendrá como consecuencia un mensaje de advertencia y de persistir, el bloqueo de la cuenta del Usuario

   Si por razones de necesidad laboral o en casos especiales, necesite enviar mensajes masivos a grupos de usuarios, debe contactar al Personal de Soporte Técnico para que le proporcione acceso a otro tipo de servicio (Servidor de Listas de Interés), esto con el objetivo de evitar problemas de registros de Spam a través del dominio de la institución que

bloquee de manera general el envió de correos masivos. Para esto se debe considerar las siguientes indicaciones:

- Utilizar el correo electrónico para actividades comerciales ajenas a la institución.
- Participar en la propagación de cadenas, esquemas piramidales y otros similares de envío con el correo institucional.
- Enviar o reenviar mensajes con contenido difamatorio, ofensivo, racista u obsceno.
- Enviar mensajes anónimos, así como aquellos que consignen títulos, cargos o funciones no oficiales.
- Utilizar mecanismos y sistemas, que intenten ocultar o suplantar la identidad del emisor del correo electrónico.
- Distribuir mensajes con contenidos inapropiados.
- Ofrecer su cuenta de correo electrónico a personas no autorizadas.
- Atentar contra la seguridad del servidor de correo de la institución.

5.4.7.2. Privacidad en los Servicios de Correo:

El Administrador del Servicio de Correo no podrá interceptar, editar, monitorear o eliminar ningún mensaje de correo de ningún usuario, salvo autorización expresa de este o su superior, o en los siguientes casos:

- El usuario haya incurrido en actos ilegales
- Requerimiento expreso de Autoridades Policiales o Judiciales.
- Para identificar o resolver problemas técnicos
- El mensaje comprometa el normal funcionamiento del servicio.

El Administrador del Sistema es la única persona que eventualmente podría tener acceso a los mensajes de los usuarios y únicamente en los casos referidos de los puntos de la política mencionados en el párrafo anterior.

5.4.8. Políticas de Seguridad de Respaldo y Recuperación

Dada la importancia de la información que maneja la Institución y la obligatoria necesidad de resguardar los datos, surge la necesidad de complementar el capítulo cinco a través de la normativa para regular el uso de cualquier tipo de unidades de respaldo sean estas internas o externas, entre las que podemos

mencionar los quemadores de discos compactos, DVD, cintas magnéticas, entre otros; con el objeto de que su uso sea para labores propias de la institución. Por lo antepuesto, toda unidad que cuente con dispositivos para la realización de respaldos (computadoras de escritorio, portátiles, servidores y equipos médicos) debe velar porque se haga un uso adecuado de esos recursos, utilizándolos únicamente para cumplir con los intereses de la institución, y tomando en cuenta las funcionalidades operativas del equipo.

La realización periódica de respaldos de la información generada en los sistemas, bases de datos, así como la información residente en los equipos de los funcionarios del Municipio de la Ciudad del Este, es de gran importancia para brindar continuidad de los servicios. Por lo tanto todas las unidades Operativas de la institución deben elaborar un plan de recuperación y respaldo de información, donde los respaldos deberán realizarse periódicamente conforme las características de los equipos, las aplicaciones y los datos asociados. El plan de recuperación y respaldo de la información debe contemplar la realización de pruebas continuas para asegurarse que los respaldos estén correctamente ejecutados y deben almacenarse en un lugar seguro y lejano de la fuente de información original.

5.4.8.1. Consideraciones Generales

Todo sistema deberá contar con la documentación de los procedimientos de respaldo y recuperación antes de entrar en producción. La misma será controlada por el Administrador de la aplicación, para verificar que es clara y completa, deberá de contemplar como mínimo la recuperación de los siguientes elementos:

- El remplazo de los servidores críticos.
- El sistema operativo y su configuración (parámetros, file Systems, particiones, usuarios y grupos, etc.)
- Los parches y paquetes de software de base necesarios para que la aplicación se ejecute.
- Los programas que componen la aplicación
- Los archivos y/o bases de datos del sistema.
- Horario de ejecución de la copia de respaldo.

No se pondrá en producción ningún sistema que no cumpla este requerimiento.

Todas las copias de respaldo deberán estar claramente identificadas, con etiquetas que indiquen como mínimo:

- Equipo al que pertenece
- Fecha y hora de ejecución
- Frecuencia: anual, mensual, semanal, diario
- Número de secuencia
- Tipo de Backup
- Nombre del sistema o aplicativo y otros datos necesarios para su fácil reconocimiento.

Se llevará un registro diario de las cintas en uso indicado al menos.

- Fecha de ejecución del respaldo
- Que cintas o discos que integran el Backup de los equipos.
- Cantidad de veces que se use cinta. Una cinta tiene un máximo de 25 veces (Vida útil).
- Luego de lo cual se procederá a remplazarlas.
- Lugar es asignados para su almacenamiento

El administrador de servidores revisara periódicamente que se cumpla con este registro en tiempo y forma. En el caso de base de datos se debe llevar bitácora de respaldos bajo la responsabilidad del DBA.

a) Todos los procedimientos de respaldo deberán generar un registro en el equipo que permita la revisión del resultado de la ejecución y dentro de lo posible, se realizaran con la opción de verificación de integridad (lectura posterior a la escritura.)
b) Los sitios donde se almacena las copias de respaldo deberán ser físicamente seguros, con los controles físicos y ambientales según normas estándares; las cintas deben guardarse dentro de la caja fuerte.
c) Se realizaran copias del respaldo del sistema completo de acuerdo a lo indicado por el administrador de la aplicación, en la frecuencia asignada a cada aplicación o sistema, previendo la conservación de estos backups por el periodo de tiempo también estipulado previamente conforme a la criticidad de la información.

Los periodos de retención de la información histórica son los siguientes:

- Lotes de transacción: perpetuo

- Actividades de los usuarios y pistas de auditoría: 3 años.

El respaldo de la información histórica se realizara utilizando soportes magnéticos de preferencia no reutilizables (DVDs, discos ópticos, etc.), los procedimientos de generación y grabación de estos archivos serán automáticos, a fin de evitar su modificación.

5.5. Responsabilidades del Usuario

- ✓ **Uso adecuado de los mecanismos de seguridad:** Dado que el usuario conoce las graves implicaciones que podría ocasionar el uso indebido o no autorizado de los mecanismos de seguridad y sus componentes, se obligan a limitar el acceso a estos únicamente a las personas señaladas en las respectivas “Actas de entrega” y a mantener los componentes de los mecanismos de seguridad bajo estrictas medidas de seguridad.

- ✓ **Respecto a los reglamentos y circulares:** Los usuarios se obligan a dar estricto cumplimiento a los reglamentos y circulares que establezca la Municipalidad de la Ciudad del Este, en relación con los dispositivos de

seguridad y con el manejo y utilización de los mecanismos de seguridad y sus componentes.

- ✓ Los usuarios se comprometen a mantener estricta confidencialidad frente a terceros, respecto a los detalles de los mecanismos de seguridad ofrecidos por la Institución.

5.6. Responsabilidad del Administrador de la TI

- ✓ Es responsabilidad del Administrador de TICs o del oficial de Seguridad de la Informática, el desarrollar, someter a revisión y divulgar en adición a los demás medios de difusión (intranet, email, Sitio Web oficial, revistas internas) de los Procedimientos de Seguridad. De esta forma se identifica claramente la responsabilidad del Administrador de TI de capacitar a los empleados de la Institución en lo relacionado con los procedimientos de Seguridad.

- ✓ El Administrador de la Seguridad de TI se ocupa de salvaguardar la confidencialidad, integridad y disponibilidad de los activos, información, datos y servicios de TI de una organización.

5.7. Implementación, Administración y Configuración de Servicios, procedimientos y protocolos de seguridad

Para la implementación de procedimientos y protocolos es necesario que la gestión de la Municipalidad de la “Ciudad del Este” reconozca la autoridad de la Gestión de la Seguridad respecto a todas estas cuestiones y que incluso permita que ésta proponga medidas disciplinarias vinculantes cuando los empleados u otro personal relacionado con la seguridad de los servicios y sistemas incumpla con sus responsabilidades de tal forma que logre un exitosa implementación.

Es responsabilidad de toda Gestión de Seguridad coordinar la implementación de los protocolos y medidas de seguridad establecida en la Política y el Plan de Seguridad de la Institución que esté acorde a estándares y que sea aplicable a la misma.

Para todos los procesos TI es necesario realizar un riguroso control del proceso para asegurar que la Gestión de la Seguridad cumple sus objetivos. Además es recomendable realizar evaluaciones que se complementen con auditorías de seguridad externas y/o internas que sean realizadas por personal independiente de la Gestión de la Seguridad.

5.8. Aplicación de Métodos de Encriptación y Protección de la Información

El método de encriptación utilizado por el Gestor de Base de Datos Oracle a través de la Herramienta Oracle Key Manager es el encapsulado de claves de AES (RFC 3994) con claves de cifrado de clave de 256 bits que permite proteger las claves simétricas cuando se crean, almacenándolas en el dispositivo de gestión de claves y que pueden ser utilizada cuando se transmiten a agentes o entre archivos de transferencia de claves.

Para el caso de los Servidores Linux CentOS se ha procedo a cifrar los discos duros mediante LUKS (Linux Unified Key Setup-on-disk-format) de tal forma que en caso de robo o pérdida del disco duro este no permita descifrar la información por falta de llaves de acceso.

En el manejo de Sistema Operativos Windows se utiliza BitLocker, herramienta que permite cifrar todos los datos almacenados en el volumen del sistema operativo Windows, siendo este de fácil manejo para los Administradores de servidores el trabajar con equipos de tipo servidor.

CONCLUSIONES Y RECOMENDACIONES

Como se ha observado en el desarrollo de los cinco capítulos se concluye que luego de haber realizado una evaluación de riesgos y análisis de vulnerabilidades al Centro de Procesamiento de Datos Municipal, se puede identificar de forma clara y precisa la situación actual y el tipo de infraestructura Tecnológica que posee la Institución, para que luego de todo este análisis se pueda aplicar normativas y estándares que sirvan de guía en la identificación de amenazas logrando prevenir cualquier tipo de ataque informático.

Es aconsejable para este tipo de Instituciones Gubernamentales dar prioridad a la gestión de inversión Tecnológica que permita brindar la seguridad y las garantías necesarias, y de esta forma conservar la integridad de la información siendo este el activo más preciado de la institución.

Por tal razón se realiza recomendaciones alineadas a los servicios que son otorgadas por el Municipio considerando el equipamiento tecnológico actual:

- Aplicar análisis de vulnerabilidades periódicas a la infraestructura Tecnológica del Centro de Procesamiento de Datos Municipal, principalmente a los servicios que se encuentran expuestas al Internet.

- Gestionar la pronta adquisición de Servidores de Datos más robustos, que permitan agilitar los servicios brindados por el Municipio, mejorando la atención al contribuyente y usuario en común.

- Monitorear de forma continua a través de analizadores de tráfico o sistemas de detección de intrusos (IDS), para que sirva de alerta ante cualquier intrusión o problemas de ataque que se quiera ejecutar en los servidores de datos de la Institución.

- Segmentación Física y Lógica de la Red LAN, con el objetivo de aislar el tráfico en fragmentos optimizando de manera eficiente los recursos de la institución.

Además se logra identificar que luego de realizar el proceso de Ethical Hacking a cada uno de los Servidores de Datos de la Institución, este permitió identificar muchas deficiencias y debilidades que poseían estos

equipos, logrando de esta manera la eliminación de vulnerabilidades a través de la correcta configuración y actualización de software.

Finalmente se ha considerando la implementación de estándares que permitan desarrollar el plan de recuperación ante desastres y respaldos, basados en las necesidades y servicios que brinda el Municipio, para lograr de esta manera mantener siempre la continuidad operativa de la Institución evitando posibles problemas al momento de ocurrir algún percance o incidente Tecnológico; así como también la aplicación y socialización de la política de seguridad que este acorde a las necesidades de las Entidades Públicas actuales permitiendo penalizar al empleado por el mal uso de los recursos Municipales.

BIBLIOGRAFÍA

[1] Alfonso Bilbao and De Cuevavaliente Ingenieros, “La Necesaria Normativa ISO Sobre Seguridad Artículo Técnico,” 2010 http://www.cuevavaliente.com/es/documentos. fecha de consulta Marzo 2015

[2] ISO, Consejos de implantación y métricas de ISO/IEC 27001 y 27002, http://www.iso27000.es/download/ISO_27000_implementation_guidance_v1_Spanish.pdf, fecha de consulta Marzo del 2015.

[3] ISOTOOLS, Norma ISO 31000:2009. Gestión de Riesgos. Principios y directrices, http://www.isotools.com.co/norma-iso-310002009-gestion-de-riesgos-principios-y-directrices/, fecha de consulta Octubre del 2014

[4] Elio Ríos Serrano, “Los Desastres - Por: Elio Ríos Serrano” <http://www.aporrea.org/actualidad/a13255.html>. fecha de consulta febrero del 2015

[5] ISO, ISO/IEC 27002:2013, http://iso27000.es/download/ControlesISO27002-2013.pdf, fecha de consulta Mayo 2015

[6] Iso/iec 27002:2005., “Iso/iec 27002:2005.”, 2011, 27002 <http://www.iso27000.es/download/ControlesISO27002-2005.pdf>. fecha de consulta Febrero 2015

[7] Wikipedia, “Criptografía - Wikipedia, La Enciclopedia Libre” ,http://es.wikipedia.org/wiki/Criptografía, fecha de consulta Septiembre 2014.

[8] Textoscientificos.com, “Encriptación” <http://www.textoscientificos.com/redes/redes-virtuales/tuneles/encriptacion> , fecha de consulta Septiembre 2014.

[9] Joel Barrios Dueñas, “Cifrado de Particiones Con LUKS. - Alcance Libre” <http://www.alcancelibre.org/staticpages/index.php/ciframiento-particiones-luks> , fecha de consulta Abril 2015

[10] Windows.microsoft.com, “Cifrado de Unidad BitLocker - Microsoft Windows” <http://windows.microsoft.com/es-419/windows7/products/features/bitlocker> , fecha de consulta Abril 2015.

[11] Belarc, “PRODUCTOS DE BELARC” <http://www.belarc.com/es/products.html>, fecha de consulta Abril 2015.

[12] INTECO Cert, Informe de Vulnerabilidades 2011, http://www.inteco.es//extfrontinteco/img/File/intecocert/Formacion/EstudiosInformes/Vulnerabilidades/cert_inf_vulnerabilidades_semestre_1_2011.pdf, fecha de consulta Marzo 2014.

[13] Wikipedia.org, “Sistema de Detección de Intrusos - Wikipedia, La Enciclopedia Libre” <http://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos> , fecha de consulta Abril 2015.

[14] INEI “INEI - PLAN DE CONTINGENCIAS Y SEGURIDAD DE LA INFORMACION”,http://www.ongei.gob.pe/publica/metodologias/lib5007/0300.HTM , fecha de consulta 30 May 2014.

[15] Microsoft.com, “Información General Acerca de La Recuperación Ante Desastres” <http://technet.microsoft.com/es-es/library/bb418909.aspx>,. fecha de consulta Junio 2014

[16] Fernando Enrique Montero Gonzalez, Gestión del Riesgo en infraestructura y Comunicaciones TI, Proyecto final, abril 2011.

[17] Leonardo Sena and Mario Tenzer, “Introducción a Riesgo Informático,” . PDF Personal, Agosto del 2014

[18] EUMED, “Plan de Recuperación del Desastre y Respaldo de la Informacion” http://www.eumed.net/libros-gratis/2009c/605/PLAN DE RECUPERACION DEL DESASTRE Y RESPALDO DE LA INFORMACION.htm, fecha de consulta 10 June 2014.

[19] PTES Technical Guidelines ,“PTES Technical Guidelines - The Penetration Testing Execution Standard” ,http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines, Fecha de consulta Abril 2014.

GLOSARIO

Amenaza: Es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir daño (material o inmaterial) sobre los elementos (activos, recursos) de un sistema.

Ataque: Es una amenaza que se convirtió en realidad, es decir cuando un evento se realizo. No dice nada si o no el evento fue exitoso.

Autenticidad: La legitimidad y credibilidad de una persona, servicio o elemento debe ser comprobable.

Confidencialidad: Datos solo pueden ser legibles y modificados por personas autorizados, tanto en el acceso a datos almacenados como también durante la transferencia de ellos.

Disponibilidad: Acceso a los datos debe ser garantizado en el momento necesario. Hay que evitar fallas del sistema y proveer el acceso adecuado a los datos.

Elementos de Información: También “Activos” o “Recursos” de una institución que requieren protección, para evitar su perdida, modificación o el uso inadecuado de su contenido, para impedir daños para la institución y las personas que salen en la información. Se distingue y divide tres grupos, a) Datos e Información, b) Sistemas e Infraestructura y c) Personal.

Gestión de Riesgo: Método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo. Está compuesta por cuatro fases: 1) Análisis, 2) Clasificación, 3) Reducción y 4) Control de Riesgo.

Integridad: Datos son completos, non-modificados y todos los cambios son reproducibles (se conoce el autor y el momento del cambio).

Seguridad Informática: Procesos, actividades, mecanismos que consideran las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad.

Vulnerabilidad: Son la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño.

Análisis de vulnerabilidades: Análisis del estado de la seguridad de un sistema o sus componentes mediante el envío de pruebas y recogida de resultados en intervalos.

Denegación de servicio (DoS): Estrategia de ataque que consiste en saturar de información a la víctima con información inútil para detener los servicios que ofrece. Véase también ("Denegación de servicio distribuida").

Denegación de servicio distribuida (DDoS): Estrategia de ataque que coordina la acción de múltiples sistemas para saturar a la víctima con información inútil para detener los servicios que ofrece. Los sistemas utilizados para el ataque suelen haber sido previamente comprometidos, pasando a ser controlados por el atacante mediante un cliente DDoS. Véase también ("Denegación de servicio").

Interfaz de comandos segura (SSH): También conocida como "Secure Socket Shell", es una interfaz de comandos basada en UNIX y un protocolo para acceder de forma segura a una máquina remota. Es ampliamente utilizada por administradores de red para realizar tareas de gestión y control. SSH es un conjunto de tres utilidades: slogin, ssh y scp; versiones seguras de las anteriores utilidades de UNIX: rlogin, rsh y rcp.

Gestión de riesgos: Selección de implementación de medidas de seguridad para conocer, prevenir, impedir, reducir o controlar los riesgos identificados. La gestión de riesgos se basa en resultados obtenidos en el análisis de riesgos.

Acceso Físico: Es la actividad de ingresar a un área.

Acceso Lógico: Es la habilidad de comunicarse y conectarse a un activo tecnológico para utilizarlo.

Herramientas de Seguridad: Son mecanismos de seguridad automatizados que sirven para proteger o salvaguardar a la infraestructura tecnológica de una Comisión.

Respaldos: Archivos, equipo, datos y procedimientos disponibles para el uso en caso de una falla o pérdida, si los originales se destruyen o quedan fuera de servicio.

Falso Positivo: Son los hallazgos o evidencias que se consideran verdaderas pero que luego demuestran falsas, la certeza o falsedad dependen de la capacidad del observador de evaluar las pruebas