ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"IMPLEMENTACIÓN DE UNA METODOLOGÍA PARA LA EVALUACIÓN DE RIESGOS EN LA DIVISIÓN DE REDES DE UNA ENTIDAD PÚBLICA"

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del grado de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

MAYRA ALEJANDRA ESPÍN GALLARDO

GUAYAQUIL – ECUADOR

AÑO: 2016

AGRADECIMIENTO

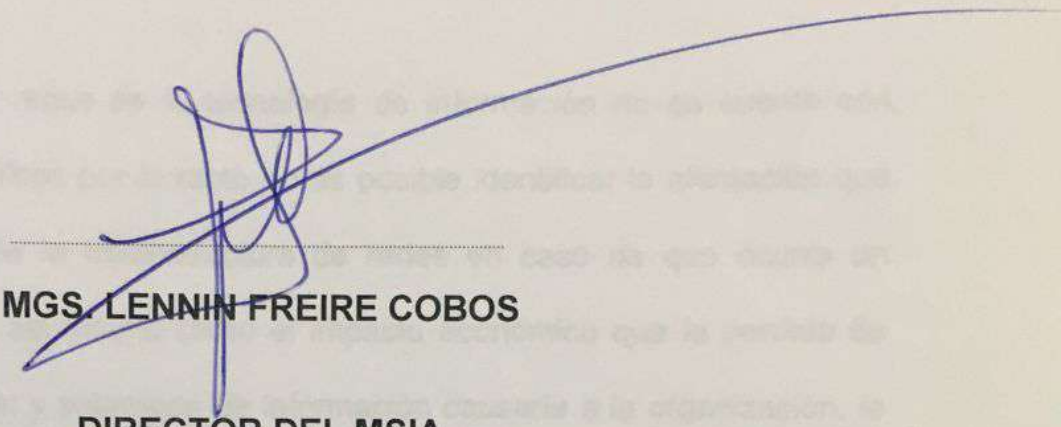
Agradezco a Dios por darme salud e iluminarme para poder continuar con mi carrera, a mis padres, a mi enamorado por el apoyo así como la motivación brindada durante esta etapa; a los consejos de mi querido primo e incondicional amigo Geovani, a mis profesores quienes aportaron con todo su conocimiento y al ingeniero Lennin Freire quien me dijo: “ya termina esa vaina” y me dio el último empujón para decidirme terminar.

DEDICATORIA

El presente proyecto lo dedico a Dios, mi familia y en especial a mi ángel que me cuida desde el cielo, mi abuelo; que aunque no logré terminar mi tesis a tiempo para que la vea, sé que va a estar orgulloso y feliz, ya que él me dio todo su apoyo y amor incondicional hasta el final.

ING. MAYRA ESPÍN

TRIBUNAL DE SUSTENTACIÓN

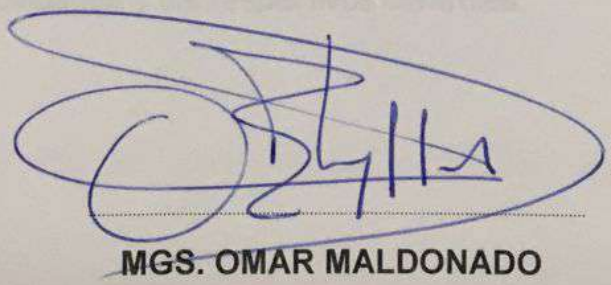


MGS. LENNIN FREIRE COBOS

DIRECTOR DEL MSIA

MGS. ROKY BARBOSA

PROFESOR DELEGADO POR LA FIEC



MGS. OMAR MALDONADO

PROFESOR DELEGADO POR LA FIEC

RESUMEN

En el departamento de redes de la tecnología de información no se cuenta con inventario de activos críticos por lo tanto no es posible identificar la afectación que tendrían los servicios de la infraestructura de redes en caso de que ocurra un incidente de seguridad, así mismo como el impacto económico que la perdida de equipos de comunicación y sobretodo de información causaría a la organización, lo cual dificulta al momento de planificar que activo debemos proteger

El objetivo general de esta tesis es Implementar una metodología para la evaluación de riesgo en la cual se pueda medir, proteger y reducir el riesgo de los activos críticos de la división de Administración de Redes de una entidad Pública.

El resultado de esta implementación es contar con un listado de activos críticos, sus amenazas, vulnerabilidades y los respectivos controles.

ÍNDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

ABREVIATURAS Y SIMBOLOGÍA

AMENAZAS	PELIGRO INMINENTE
CORE	NUCLEO
CRACKER	CREA Y MODIFICA SOFTWARE
HACKER	DESCUBRE DEBILIDADES DE UN SOFTWARE
INTEGRIDAD	TOTALIDAD
LAN	LAN AREA NETWORK
NIST	NATIONAL INSTITUTE OF STANDARS AND TECHNOLOGY
ROUTER	DISPOSITIVO DE RED QUE PERMITE ENRUTAMIENTO
SWITCH	CONMUTADOR
TI	TECNOLOGIA DE LA INFORMACIÓN
WAN	WIDE AREA NETWORK
WIFI	COMUNICACIÓN INALÁMBRICA

INTRODUCCIÓN

Existen varias metodologías para la identificación del riesgo, dependiendo la necesidad y la que más se adapte a la organización pueden ser utilizadas; estas metodologías deberán tener en cuenta los tres elementos básicos para la identificación del riego dentro de la organización como son: Activos, Amenazas y Vulnerabilidades las cuales están relacionadas unas con otras; ya que de este modo podemos realizar un análisis de riesgo [1].

Dado que al implementar una evaluación de riesgo a través de la metodología NIST SP 800-30 se pueden poner en práctica los conceptos de los pilares fundamentales de la seguridad de la información se toma como estudio esta metodología para su análisis [3].

CAPÍTULO 1

1. GENERALIDADES

1.1 Descripción del problema.

La entidad pública es una institución encargada de la seguridad a nivel de estado contribuyendo a la defensa de soberanía territorial.

La División de Administración de Redes es la encargada de mantener las comunicaciones y enlaces a nivel nacional apuntando al direccionamiento estratégico de esta entidad pública.

Esta división cuenta con varios servicios en la ciudad de Guayaquil dentro de los que podemos destacar:

-Internet Institucional

-Red de Datos LAN

-Red de Datos WAN

En el año 2008 esta división era un departamento del centro de datos de tercer nivel es decir se dedicaba al control local y monitoreo de un nodo del sector sur de Guayaquil.

En el año 2012 el departamento de redes cambia de nombre y pasa a ser una gran división llamada División de Administración de redes y comunicaciones pasando a formar parte de la Dirección de tecnologías de información haciéndose cargo de la conexión y monitoreo de los principales nodos de Guayaquil en cuanto a red LAN y red WAN ocupa los nodos SALINAS, MANTA, MACHALA

Producto del cambio y crecimiento organizacional esta dirección no cuenta con un manual organizacional actualizado provocando que las competencias del personal que labora en esta División no estén bien definidas, el tener que monitorear mayor cantidad de enlaces así como el soporte, hizo que se solicitara más personal técnico para soporte mas no para administración de los enlaces y equipos de comunicación con los que cuenta esta división por lo que provoco un descontrol y manipulación total de los equipos de comunicación a personal técnico sin experiencia en el manejo de los mismos asignándoles accesos a los equipos de comunicación.

Debido a que esta dirección de tecnologías de información no cuenta con procedimientos, ni inventarios de sus activos críticos no es posible identificar la afectación que tendrían los servicios de la infraestructura de redes de la división de administración de redes y comunicaciones en caso de que ocurra un incidente de seguridad, así mismo como el impacto económico que la perdida de equipos de comunicación y sobretodo de información causaría a la organización, lo cual dificulta al momento de planificar que activo debemos proteger en cuanto a confidencialidad, integridad y disponibilidad de la información.

1.2 Solución propuesta.

Debido a que esta institución maneja información sensible ya que brinda seguridad a nivel de estado contribuyendo a la defensa de soberanía territorial, debe contar con una metodología que le ayude a realizar una evaluación de riesgo y así poder identificar los activos más críticos dentro de la infraestructura de redes, ofreciendo diferentes beneficios tales como:

- Identificación y valoración de activos críticos de la división de administración de redes y comunicaciones de la Dirección de Tecnología de Información.
- Identificar amenazas y vulnerabilidades de los activos [4].
- Mitigar el riesgo para proteger activos y asegurar la confidencialidad, disponibilidad e integridad de los servicios.

- Evitar incurrir en costos innecesarios al realizar adquisición de equipamiento activo.
- Aseguramiento de los sistemas de información que transmiten y almacenan información.

Es por esto que se va a realizar análisis de riesgo utilizando una metodología denominada NIST [4] la cual tiene publicaciones relacionadas a la seguridad de la información en la cual consta la metodología para el análisis de riesgo y gestión de riesgo de seguridad de la información.

CAPÍTULO 2

2. METODOLOGÍA DEL DESARROLLO DE LA SOLUCIÓN

2.1 Levantamiento de información de activos del departamento de redes y comunicaciones

Con la finalidad de analizar los riesgos que existen en el departamento de redes y comunicaciones de la dirección de tecnologías de información es necesario realizar el levantamiento de información de una de las variables para el análisis de riego como son los activos.

Activos son todos aquellos componentes que permiten el funcionamiento de los servicios del departamento de redes y comunicaciones, estos pueden ser equipos, cables, información, etc.

Tabla 1. Tipo de activos departamento de redes

ACTIVOS DEL DEPARTAMENTO DE REDES DE LA DIRECCIÓN DE TECNOLOGÍAS	
TIPOS DE ACTIVOS	**DESCRIPCIÓN**
1. Activos de información	Documentación (manuales de usuario, contratos, etc.)
2.Hardware	Equipos de oficina (pc de escritorio, laptops)
3. Red	Dispositivos de conectividad de redes (routers, switch, concentradores, etc.)
4.Instalación	Cableado estructurado
5.Servicios	Conectividad a internet, Conectividad LAN, Conectividad Wan

2.2 Caracterización del Sistema

Para la evaluación de riesgo lo primero que se debe definir es el alcance que va a tener dentro de la organización, en este caso vamos a evaluar el alcance dentro del departamento de redes; los limites lo definen con la información del sistema y los recursos tales como hardware, software, conectividad, etc. [2]

2.2.1 Identificación de información relacionada con el sistema

Se debe escribir información relacionada al ambiente de la organización para poder identificar el sistema de información, para la identificación del sistema se requiere de un análisis a fondo de los componentes del mismo,

por lo que en primera instancia se realizará la recolección de información que concierne al sistema la cual se la clasifica de la siguiente manera:

-Hardware

-Acoplamiento del sistema (Conectividad interna y Conectividad externa)

-Los datos y la información

-Los usuarios del sistema que brindan apoyo técnico de TI.

- Topología de red actual

Tabla 2. Identificación de Activos

LISTADO DE ACTIVOS DEL DEPARTAMENTO DE REDES DE LA DIRECCIÓN DE TECNOLOGÍAS		
NOMBRE DE ACTIVOS	**UBICACIÓN**	**DESCRIPCIÓN**
Hardware		
-Estación fija de trabajo -Laptop	Departamento de Redes	-Equipo de escritorio LENOVO para monitoreo de enlaces de red. -Laptop hp para configuración de equipos activos de red.
Acoplamiento de sistemas		
-Servicio de Internet -Servicio de red LAN -Servicio de red WAN	Departamento de Redes	-Proveedor externo de internet. -Red interna de la organización -Red externa, interconexión con las demás provincias que forman parte de la organización y que reciben

		servicios desde el nodo principal.
RED		
-Switch Core -Switch de Acceso -Switch de Distribución -Router -Wireless -Controladora Wireless	Departamento de Redes	-CISCO 4500, 02 tarjetas controladoras, 02 fuentes, velocidad de transmisión 10/100/1000 Mbps, Full-Duplex, vlan 4094. -CISCO 2960, 48 Puertos UTP 10/100/1000, 255 Vlan, protocolo IPV6, Full-Duplex, Capa 2. -CISCO 3750 24 puertos Fibra Óptica, Full-Duplex, velocidad de transmisión 1Giga -CISCO 3800, protocolo de enrutamiento (RIP V1, RIP V2), EIGRP,OSPF, enrutamiento estático, protocolo IPV4, IPV6 -CISCO Puertos Ethernet 10/100/1000 RJ-45 autosensing, puerto consola, Velocidades Soportadas 802.11a: hasta 54 Mbps; 802.11g: hasta 54 Mbps; 802.11n: hasta 1.3 Gbps - Puertos de red Gigabit Ethernet estándares WiFi Soportados 802.11a/b/g/n, estándares Cableados 802.3, 802.3u, 802.1q
Los datos e información		
--Documentos Microsoft -Informe de red de datos	Departamento de Redes	-Documentos de claves equipos de red. -Levantamiento de información de red.
Los usuarios		
-Personal	Departamento de	Responsables de soporte técnico

técnico de TI	Redes	Responsables de la administración
Topología de red		
-Cableado estructurado	Departamento de Redes	Transmite y recibe información a través de la red.

2.2.2 Técnicas de recopilación de información

Para la recopilación de información se pueden usar varias técnicas, tales como: cuestionarios, entrevistas en las instalaciones, revisión de documentos, el uso de herramientas de escaneo automatizado, estas técnicas pueden ser combinadas o utilizadas de forma individual siempre y cuando este dentro de su límite operativo.

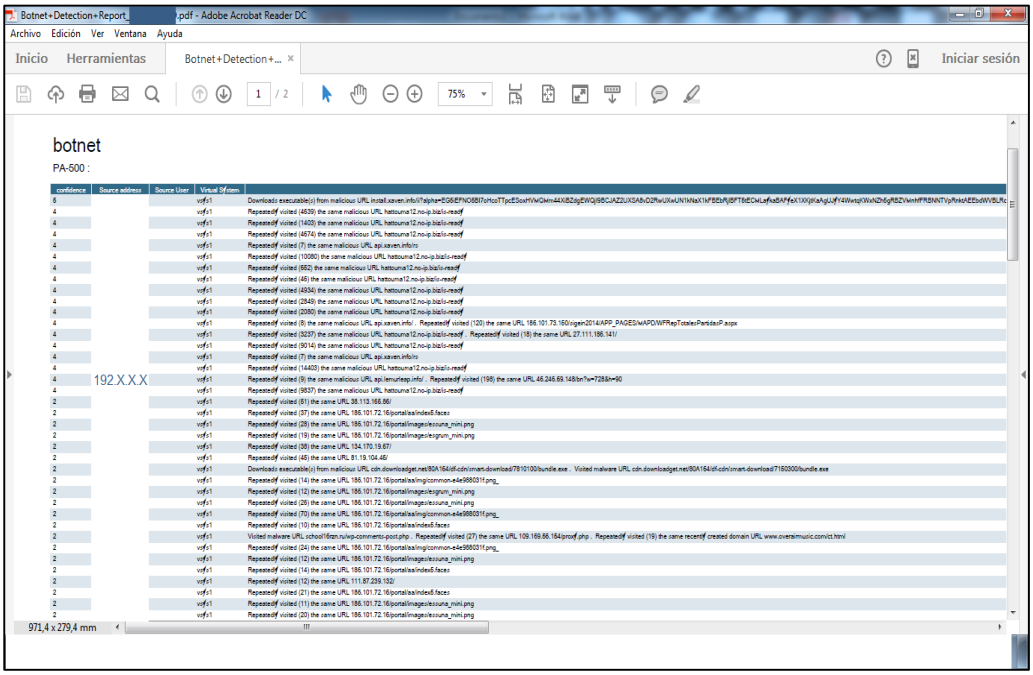


Figura 2.1 Escaneo de Red

2.3 Identificación de Amenazas

Una amenaza es aquella que ocurre cuando una vulnerabilidad se materializa, las amenazas pueden existir en mayor o menor grado y no causar efectos dentro de la organización a menos que existe una vulnerabilidad que pueda ser explotada por dicha amenaza, una amenaza no representa peligro si no hay una vulnerabilidad.

Una amenaza es cualquier suceso o incidente con un potencial de poder causar daño a un sistema de tecnología de información.

2.3.1 Fuente de identificación

Dentro de las amenazas más comunes tenemos las siguientes: humanas, naturales, Ambientales [5].

- Amenazas Humanas: Las personas son uno de los principales motivos de amenaza ya que pueden generar actos voluntarios o involuntarios de amenazas; un acto involuntario puede darse por desconocimiento, negligencia, errores; en cambio un acto voluntario se da por personas mal intencionadas o empleados descontentos dentro de la organización.

- Amenazas Naturales: Las amenazas de esta índole tienen que ver con factores externos y que no son predecibles tales como los fenómenos naturales: terremotos, inundaciones, derrumbes, tormentas eléctricas, etc.

Amenazas Ambientales: Tienen que ver con fallos de fugas de líquidos, alimentación eléctrica, la contaminación, productos químicos, etc.

En este paso a través de un listado identificaremos las amenazas potenciales ya sean accidentales o no.

Tabla 3. Identificación de Amenazas

Identificación de Amenazas		
Fuente de amenaza	**Motivación**	**Acción de la Amenaza**
Humanas		
-Hacker, -Cracker -Espionaje -Empleados	Robo de información Espionaje económico Curiosidad, Ego, omisiones, errores por desconocimiento, inconformidad laboral	-Ingeniería Social, hackeo -Robo de información, violación a la privacidad -Espionaje de información confidencial, acceso a los sistemas no autorizados, eliminación o daño de la información y equipos activos.
Naturales		
-Inundaciones -Terremotos -Descargas eléctricas	Desastres Naturales	Daño o pérdida en las instalaciones donde se encuentra el departamento de redes. -Daño en los equipos activos de red

Ambientales		
-Fallos en la alimentación eléctrica	-Variación de Voltaje	-Corto circuito en los equipos del departamento de redes, acceso físico a instalaciones.
-Fuga líquida	-Condensación de Aire Acondicionado	-Daño en los equipos activos de red.

2.4 Identificación de vulnerabilidades

Una vulnerabilidad es una debilidad o un hueco de seguridad que puede ser usada para causar daño en los sistemas, ya sea esto en hardware, software, sistemas operativos, etc., violando la integridad, disponibilidad, confidencialidad de los datos. Las vulnerabilidades se dan por errores o fallos, muchos de ellos son el resultado de limitaciones tecnológicas, debilidad dentro de los procedimientos y controles estas vulnerabilidades pueden ser intencionales o accidentalmente provocados.

Una vulnerabilidad representa la posibilidad de que una amenaza se efectúe sobre cualquier activo de la organización.

La metodología y los tipos de vulnerabilidades van a depender de cada organización, en la selección de técnicas de vulnerabilidades ya sean estas técnicas o no técnicas, una revisión de otras fuentes así como el internet es otro

medio de información sobre el sistema, los documentos que pueden ir en el análisis de vulnerabilidades son: informes de auditoría, informes de anomalías del sistema, lista de vulnerabilidades.

En los host de una red se pueden explorar las vulnerabilidades a través de herramientas automatizadas, sin embargo se debe tomar en cuenta que esta herramienta puede arrojar falsos positivos, debido a que dependiendo la organización lo encontrado puedo ser considerado normal.

En esta etapa se identifica las debilidades que pueden ser aprovechadas por las amenazas.

Dentro de las posibles vulnerabilidades tenemos:

-Contraseñas no encriptadas o en texto plano

-Configuración básica en los equipos de comunicación

-Falta de seguridad física donde se encuentran los equipos de comunicación

-Falta de documentación técnica (levantamiento de información)

2.4.1 Desarrollo de requisitos de seguridad listas de control

Los requisitos de seguridad estipulados para el sistema de TI se detallan en esta etapa; estos se presentan en una tabla, en la cual constan los requisitos del diseño y si este cumple o no cumple el requisito de control de seguridad, las normas básicas de seguridad están contenidas dentro de los requisitos de seguridad para metódicamente evaluar las

vulnerabilidades de los activos en las siguientes zonas de seguridad: Gestión, Operativo y Técnico.

Tabla 4. Lista de Controles

Lista de Controles	
Área de Seguridad	**Controles de Seguridad**
Gestión	
Administración de la Seguridad	-Asignación de responsabilidades -Designación de responsabilidades -Capacitación técnica -Separación de Funciones
Operativo	
Seguridad Operacional	-Acceso a los medios de datos y eliminación. -Fondo para la protección(salas informáticas, centro de datos) -Contaminantes que viajan a través del aire (polvo, productos químicos, aire) -Estaciones de trabajo, laptops -Control de Humedad -Control de Temperatura -Controles que aseguren el suministro de energía eléctrica
Técnico	
	-Comunicaciones (interconexión de routers)

Seguridad Técnica	-Control de acceso -Identificación y autenticación

2.5 Análisis de Controles

En este paso se analizan los controles puestos por la organización con la finalidad de eliminar o disminuir la probabilidad de que una amenaza ejerza sobra una vulnerabilidad del sistema.

Método de Control:

Este control se clasifica en dos métodos técnicos como son: hardware, software y firmware y los no técnicos: políticas de seguridad, seguridad física y ambientales.

Control de Categoría:

La categoría de control para los dos métodos de control se las conoce como: preventivo y detectivo. Los controles preventivos inhabilitan los intentos de violar la política de seguridad y utilizan controles de acceso, autenticación y cifrado.

Los controles detectivos advierten las violaciones e intento de violación de las políticas de control incluye controles de auditoría.

Análisis de Control técnico:

Las listas de comprobación control y de requisitos de seguridad sirven para el análisis de los controles y validar el cumplimiento e incumplimiento.

2.6 Determinación de Probabilidades

Para obtener una clasificación global se debe considerar los siguientes factores: capacidad y motivación de la fuente de amenaza, naturaleza de la vulnerabilidad, existencia y eficacia de los controles actuales.

La probabilidad de que una vulnerabilidad sea ejercida por una amenaza se define en tres niveles:

Alto: La amenaza es altamente capaz de ser ejecutada, los controles se ejecutan pero no son eficientes, en este caso la ponderación que daremos a este nivel será 3.

Medio: La amenaza puede ser capaz de ejecutarse, pero los controles realizados dificultan la ejecución exitosa de la vulnerabilidad, para el nivel medio la ponderación será 2.

Bajo: La amenaza tiene poca capacidad para ejecutarse o los controles que existen previenen o impiden de manera significativa la ejecución de la vulnerabilidad, para el nivel medio la ponderación será 1.

CAPÍTULO 3

3 ANÁLISIS DE RESULTADOS

3.1 Análisis de Impacto

En esta fase se determinará el nivel de impacto de que una amenaza se materialice sobre una vulnerabilidad; para el análisis de impacto se utiliza información extraída de la organización así como el análisis de criticidad de los activos; en esta etapa a través de una valoración cuantitativa y cualitativa se prioriza el nivel de impacto con los activos de la organización, determinando así los activos críticos y sensibles para la organización (hardware, software, servicios, etc.) los cuales apoyan a la misión de la organización.

En el caso de que no exista información sobre la criticidad de los activos o no se cuente con dicha información, independiente de los métodos que se utilice para la valoración del grado de sensibilidad, se debe consultar con el responsable del

área de redes o dueño del sistema quien será el encargado de dar una valoración y medir el nivel de impacto teniendo en cuenta la integridad, disponibilidad y confidencialidad de la información.

Perdida de integridad: Se refiere a la protección de la información contra modificaciones sin aviso o modificaciones no autorizadas, la pérdida de integridad provoca que se tomen malas decisiones y existan fraudes, esta es una ventana para un ataque con éxito.

Perdida de la disponibilidad: Si los sistemas y servicios de una organización no están disponibles para los usuarios de la misma, esta puede verse afectada en el normal funcionamiento de sus actividades afectando la misión de la organización.

Pérdida de la confidencialidad: Se refiere a la pérdida del resguardo de todo tipo de información ya sea de gobierno o privada con intensión, sin intensión, el impacto puede ser medido de forma cuantitativamente en algunos casos, para esta evaluación lo mediremos de manera cualitativa es decir Alto, Medio, Bajo.

Tabla 5. Magnitud de Impacto

Magnitud de Impacto	
Alto	Ejercicio de la Vulnerabilidad, cuando la pérdida representa valores económicos muy altos ya sea sobre activos tangibles (pérdida total de equipos, daño, intromisión, etc) o tenga que ver con personas (muerte o luxaciones graves)
Medio	Ejercicio de la Vulnerabilidad, cuando la pérdida representa valores económicos, este aplica a los mismos casos del impacto alto.
Bajo	Ejercicio de la Vulnerabilidad, cuando la pérdida representa de algunos activos, causando daño afectando la credibilidad, misión o funcionamiento normal de la organización.

También se pueden realizar evaluaciones cuantitativas y cualitativas pero si queremos tener una apreciación costo beneficio debemos realizar una medida de magnitud de impacto cuantitativa pero interpretada de manera cualitativa [4].

3.2 Matriz el Nivel de Riesgo

En esta etapa para el análisis del nivel de riesgo se puede utilizar una matriz de 3 por 3, dependiendo el nivel de detalle la misma puede ser de 4 por 4, esta matriz analizará la probabilidad de amenazas y la probabilidad de impacto (alto, medio, bajo). La ponderación para los activos del departamento de redes va a ser del 1 al 10 tal como se muestra en la tabla 7 [4].

Tabla 6. Descripción del riesgo

Descripción del riesgo y sus acciones	
Alto	Si en la evaluación se detecta un riesgo como alto, es necesario tener una medida correctiva, un sistema puede seguir funcionando pero se debe ejecutar un plan de acción lo antes posible
Medio	Si en la evaluación se detecta un riesgo como medio, es necesario tener una medida correctiva y hacer un plan de acción para ponerlo en práctica dentro de un periodo de tiempo adecuado.
Bajo	Si en la evaluación se detecta un riesgo como bajo, el sistema puede aceptar el riesgo o indicar si debe implementar acciones correctivas.

3.3 Controles Recomendados

En esta etapa lo que se quiere es disminuir el nivel de riesgo implementando controles, cabe indicar que no todos los controles van a ser implementados estos dependerán de cada organización.

En la tabla 8. se puede observar los controles implementados para los activos de la organización.

3.4 Documentación de Resultados

En esta etapa se muestra el producto de la evaluación de vulnerabilidades, amenazas, riesgos, etc., los resultados de este informe no se realizan con la finalidad de acusar sino de informar para que la dirección puedan tomar decisiones acertadas y realizar la asignación de recursos necesarios.

En la tabla 7 podemos observar los resultados de la evaluación de riesgo.

Tabla 7. Evaluación de Riesgo

Activo	**Evaluación de Riesgo**			
Hardware				
Estaciones fija trabajo	**Evaluación de Vulnerabilidades**			**Evaluación de Amenazas**
	Vulnerabilidad	Nivel	Valor	
Riesgo total 4/10	1. Equipos sin clave	Alto	3	**Amenaza**
				Ocurrencia medio — Robo de información 2
				Impacto
				Confidencialidad medio 3
				Integridad medio 2
	2. Contraseñas débiles	Medio	2	**Amenaza**
				Ocurrencia medio — Hackeo 2
				Impacto
				Confidencialidad medio 3
				Integridad medio 2

Activo	**Evaluación de Riesgo**			
Laptop	**Evaluación de Vulnerabilidades**			**Evaluación de Amenazas**
	Vulnerabilidad	Nivel	Valor	
Riesgo total 3/10	1. Equipos sin clave	Alto	2	**Amenaza**
				Ocurrencia medio — Robo de información 2
				Impacto
				Confidencialidad medio 3
				Integridad medio 2
	2. Contraseñas	Medio	2	**Amenaza**

	débiles			
				Ocurrencia Hackeo medio 2
				Impacto
				Confidencialidad medio 2
				Integridad medio 2

Activo	**Evaluación de Riesgo**			
Acoplamiento de Sistemas				
Servicio Internet	**Evaluación de Vulnerabilidades**			**Evaluación de Amenazas**
	Vulnerabilidad	Nivel	Valor	
Riesgo total 7/10	1. Falta de soporte técnico	Alto	3	**Amenaza**
				Ocurrencia Falta de documentación técnica medio 2
				Impacto
				Disponibilidad alto 3
	2. Falta de seguridad física	Medio	2	**Amenaza**
				Ocurrencia Fallos en alimentación eléctrica medio 2
				Impacto
				Confidencialidad medio 2
				Disponibilidad alto 3

Activo	**Evaluación de Riesgo**			
Red				
Switch CORE	**Evaluación de Vulnerabilidades**			**Evaluación de Amenazas**
	Vulnerabilidad	Nivel	Valor	
Riesgo total	1.Configuracion básica	Alto	3	**Amenaza**

9/10				Saturación del canal de datos Ocurrencia Alto 3 **Impacto** Disponibilidad alto 3 Integridad medio 3
	2. Falta de seguridad física	Medio	2	**Amenaza** Fallo en alimentación eléctrica Ocurrencia Alto 3 **Impacto** Confidencialidad medio 2 Disponibilidad alto 3
	3. Contraseñas débiles	Medio	2	**Amenaza** Empleados Ocurrencia medio 2 **Impacto** Confidencialidad alto 3 Integridad alto 3 Disponibilidad alto 3
	4. Falta de mantenimiento en Sistema de tierras	Medio	2	**Amenaza** Descargas eléctricas Ocurrencia medio 2 **Impacto** Integridad alto 3 Disponibilidad alto 3

Activo	**Evaluación de Riesgo**			
Red				
Switch Distribución	**Evaluación de Vulnerabilidades**			**Evaluación de Amenazas**
	Vulnerabilidad	Nivel	Valor	
Riesgo total 9/10	1.Configuracion básica	Alto	3	**Amenaza** Ocurrencia: Saturación del canal de datos Alto 3 **Impacto** Disponibilidad: alto 3 Integridad: medio 3
	2. Falta de seguridad física	Medio	2	**Amenaza** Ocurrencia: Fallo en alimentación eléctrica Alto 3 **Impacto** Confidencialidad: medio 2 Disponibilidad: alto 3
	3. Contraseñas débiles	Medio	2	**Amenaza** Ocurrencia: Empleados medio 2 **Impacto** Confidencialidad: alto 3 Integridad: alto 3 Disponibilidad: alto 3
	4. Falta de mantenimiento en Sistema de tierras	Medio	2	**Amenaza** Ocurrencia: Descargas eléctricas

				medio	2
				Impacto	
				Integridad	alto 3
				Disponibilidad	alto 3

Activo	**Evaluación de Riesgo**			
Red				
Switch Acceso	**Evaluación de Vulnerabilidades**			**Evaluación de Amenazas**
	Vulnerabilidad	Nivel	Valor	
Riesgo total 9/10	1.Configuracion básica	Alto	3	**Amenaza**
				Ocurrencia Saturación del canal de datos
				Alto 3
				Impacto
				Disponibilidad alto 3
				Integridad medio 3
	2. Falta de seguridad física	Medio	2	**Amenaza**
				Ocurrencia Fallo en alimentación eléctrica
				Alto 3
				Impacto
				Confidencialidad medio 2
				Disponibilidad alto 3
	3. Contraseñas débiles	Medio	2	**Amenaza**
				Ocurrencia Empleados
				medio 2
				Impacto
				Confidencialidad alto 3

				Integridad	alto 3
				Disponibilidad	alto 3
	4. Falta de mantenimiento en Sistema de tierras	Medio	2	**Amenaza**	
				Ocurrencia medio	Descargas eléctricas 2
				Impacto	
				Integridad	alto 3
				Disponibilidad	alto 3

Activo	**Evaluación de Riesgo**				
Red					
Router	**Evaluación de Vulnerabilidades**			**Evaluación de Amenazas**	
	Vulnerabilidad	Nivel	Valor		
Riesgo total 9/10	1.Configuracion básica	Alto	3	**Amenaza**	
				Ocurrencia Alto	Saturación del canal de datos 3
				Impacto	
				Disponibilidad	alto 3
				Integridad	medio 3
	2. Falta de seguridad física	Medio	2	**Amenaza**	
				Ocurrencia Alto	Fallo en alimentación eléctrica 3
				Impacto	
				Confidencialidad	medio 2
				Disponibilidad	alto 3
	3. Contraseñas	Alto	3	**Amenaza**	

	débiles			
				Ocurrencia Empleados medio 2
				Impacto
				Confidencialidad alto 3 Integridad alto 3 Disponibilidad alto 3
	4. Falta de mantenimiento en Sistema de tierras	Alto	3	**Amenaza**
				Ocurrencia Descargas eléctricas medio 2
				Impacto
				Integridad alto 3 Disponibilidad alto 3
	5. Falta de mantenimiento en sistema de climatización	Medio	2	**Amenaza**
				Ocurrencia Condensación de aire acondicionado medio 2
				Impacto
				Integridad alto 3 Disponibilidad alto 3

Activo	**Evaluación de Riesgo**			
Red				
Wireless	**Evaluación de Vulnerabilidades**			**Evaluación de Amenazas**
	Vulnerabilidad	Nivel	Valor	
Riesgo total	1.Configuracion	Alto	3	**Amenaza**

9/10	básica			
				Ocurrencia Empleados Alto 3
				Impacto
				Disponibilidad alto 3 Integridad medio 3
	2. Falta de conciencia de seguridad	Medio	2	**Amenaza**
				Ocurrencia Hackeo Alto 2
				Impacto
				Confidencialidad alto 3 Integridad alto 3 Disponibilidad alto 3
	3. Contraseñas débiles	Alto	3	**Amenaza**
				Ocurrencia Empleados medio 2
				Impacto
				Confidencialidad alto 3 Integridad alto 3 Disponibilidad alto 3
	4. Falta de mantenimiento en Sistema de tierras	Alto	3	**Amenaza**
				Ocurrencia Descargas eléctricas medio 2
				Impacto
				Integridad alto 3 Disponibilidad alto 3

Activo	Evaluación de Riesgo			
Red				
Controladora Wireless	**Evaluación de Vulnerabilidades**			**Evaluación de Amenazas**
	Vulnerabilidad	Nivel	Valor	
Riesgo Total 6/10	1. Falta de conciencia de seguridad	Medio	2	**Amenaza** Ocurrencia Hackeo Alto 2 **Impacto** Confidencialidad alto 3 Integridad alto 3 Disponibilidad alto 3
	2. Contraseñas débiles	Alto	3	**Amenaza** Ocurrencia Empleados medio 2 **Impacto** Confidencialidad alto 3 Integridad alto 3 Disponibilidad alto 3
	Falta de mantenimiento en sistemas de tierras	Alto	3	**Amenaza** Ocurrencia Descargas eléctricas medio 2 **Impacto** Integridad alto 3 Disponibilidad alto 3

Activo	Evaluación de Riesgo			
Datos e Información				
Documentos de Microsoft	**Evaluación de Vulnerabilidades**			**Evaluación de Amenazas**
	Vulnerabilidad	Nivel	Valor	
Riesgo total 8/10	1. Manejo inadecuado de documentos	Alto	2	**Amenaza** Ocurrencia medio — Robo de información 2 **Impacto** Confidencialidad medio 3 Integridad medio 2
	2. Documentos sin Contraseñas	Medio	2	**Amenaza** Ocurrencia medio — Espionaje 2 **Impacto** Confidencialidad alto 3 Integridad alto 3

Activo	Evaluación de Riesgo			
Usuarios				
Personal técnico de TI	**Evaluación de Vulnerabilidades**			**Evaluación de Amenazas**
	Vulnerabilidad	Nivel	Valor	
Riesgo total 8/10	1. Falta de definición de roles	Alto	2	**Amenaza** Ocurrencia medio — Acceso a los sistemas no autorizados 3 **Impacto** Confidencialidad alto 3 Integridad alto 3
	2. Personal	Medio	2	**Amenaza**

	técnico sin experiencia			
				Ocurrencia: Errores por desconocimiento — medio: 2
				Impacto
				Disponibilidad: alto 3
				Integridad: alto 3
	3. Falta de cultura organizacional	Medio	2	**Amenaza**
				Ocurrencia: Personal técnico inconforme — alto: 3
				Impacto
				Disponibilidad: alto 3
				Confidencialidad: alto 3
				Integridad: alto 3

Activo	**Evaluación de Riesgo**			
Topología de red				
Cableado estructurado	**Evaluación de Vulnerabilidades**			**Evaluación de Amenazas**
	Vulnerabilidad	Nivel	Valor	
	1.Falta de mantenimiento del cableado	Alto	3	**Amenaza**
Riesgo total 8/10				Ocurrencia: Daño de puntos de red — medio: 2
				Impacto
				Disponibilidad: alto 3
				Integridad: medio 3
	2. Falta de seguridad física	Medio	2	**Amenaza**
				Ocurrencia: Acceso de personal no autorizado

				Alto 3
				Impacto
				Confidencialidad medio 2
				Disponibilidad alto 3
	3. Ubicado en un lugar propenso a inundaciones	Alto	3	**Amenaza**
				Ocurrencia Inundaciones medio 2
				Impacto
				Integridad alto 3
				Disponibilidad alto 3
	4. Falta de mantenimiento en Sistema de tierras	Alto	3	**Amenaza**
				Ocurrencia Descargas eléctricas medio 2
				Impacto
				Integridad alto 3
				Disponibilidad alto 3
	5. Falta de mantenimiento en sistema de climatización	Medio	2	**Amenaza**
				Ocurrencia Condensación de aire acondicionado medio 2
				Impacto
				Integridad alto 3
				Disponibilidad alto 3

Documentación de Resultados de Activos Críticos

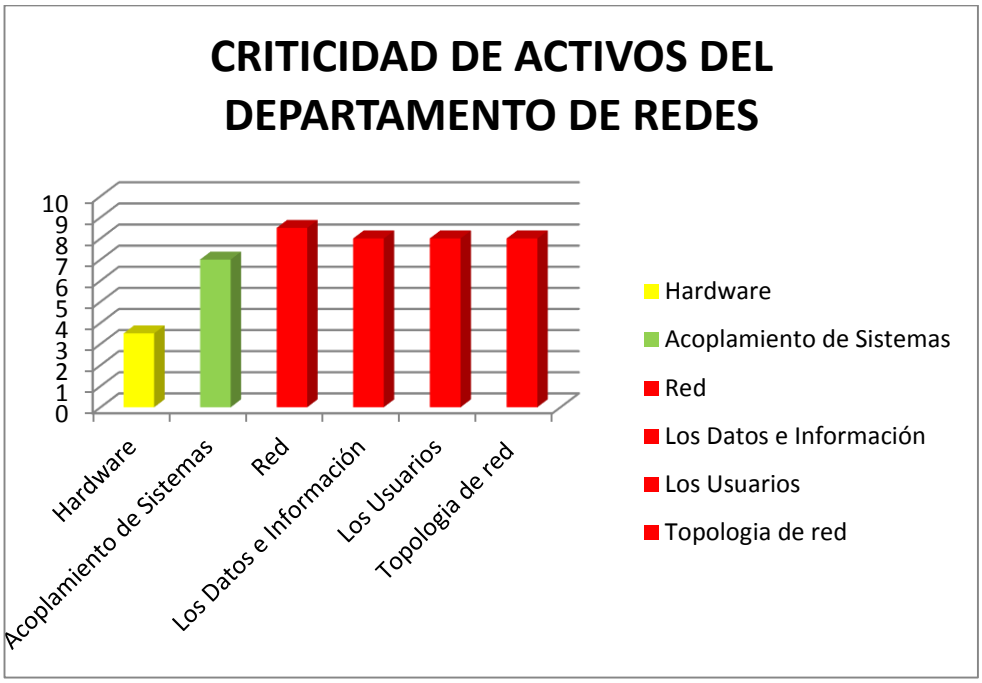


Figura 3.1 Criticidad de Activos

Listado de Controles

Activo: Estación fija de Trabajo	
Control:	Autenticación
Prioridad:	medio
Estado:	En ejecución
Responsable:	Analista de soporte técnico
Recursos:	Directorio Activo
Control:	Gestión de claves de cifrado
Prioridad:	medio
Estado:	En ejecución
Responsable:	Analista de seguridad
Recursos:	Políticas de seguridad

Activo: Laptop	
Control:	Autenticación
Prioridad:	medio
Estado:	En ejecución
Responsable:	Analista de soporte técnico
Recursos:	Directorio Activo
Control:	Gestión de claves de cifrado
Prioridad:	medio
Estado:	En ejecución
Responsable:	Analista de seguridad y Admin de redes
Recursos:	Políticas de seguridad

Activo: Servicio de internet	
Control:	Manual de Procedimientos
Prioridad:	medio
Estado:	En ejecución
Responsable:	Analista de Seguridad
Recursos:	Manual de Procedimientos
Control:	Mantenimiento preventivo
Prioridad:	medio
Estado:	En ejecución
Responsable:	Analista de Seguridad
Recursos:	Políticas de seguridad

Activo: Switch Core	
Control:	Capacitación sobre seguridad informática
Prioridad:	medio
Estado:	En ejecución
Responsable:	Administrador de red
Recursos:	Personal capacitado
Control:	Mantenimiento preventivo
Prioridad:	medio

Estado:	En ejecución
Responsable:	Analista de Seguridad y Admin de redes
Recursos:	Políticas de seguridad
Control:	Gestión de claves de cifrado
Prioridad:	medio
Estado:	En ejecución
Responsable:	Analista de seguridad y Admin de redes
Recursos:	Políticas de seguridad
Control:	Supresor de picos de voltaje
Prioridad:	media
Estado:	inicial
Responsable:	Analista de Seguridad
Recursos:	Seguridad en el cuarto eléctrico

Activo: Switch de Distribución	
Control:	Capacitación sobre seguridad informática
Prioridad:	medio
Estado:	En ejecución
Responsable:	Administrador de red
Recursos:	Personal capacitado
Control:	Mantenimiento preventivo
Prioridad:	medio
Estado:	En ejecución

Responsable:	Analista de Seguridad y Admin de redes
Recursos:	Políticas de seguridad
Control:	Gestión de claves de cifrado
Prioridad:	medio
Estado:	En ejecución
Responsable:	Analista de seguridad y Admin de redes
Recursos:	Políticas de seguridad
Control:	Supresor de picos de voltaje
Prioridad:	media
Estado:	inicial
Responsable:	Analista de Seguridad
Recursos:	Seguridad en el cuarto eléctrico

Activo: Switch de Acceso	
Control:	Capacitación sobre seguridad informática
Prioridad:	medio
Estado:	En ejecución
Responsable:	Administrador de red
Recursos:	Personal capacitado
Control:	Mantenimiento preventivo
Prioridad:	medio
Estado:	En ejecución
Responsable:	Analista de Seguridad y Admin de redes

Recursos:	Políticas de seguridad
Control:	Gestión de claves de cifrado
Prioridad:	medio
Estado:	En ejecución
Responsable:	Analista de seguridad y Admin de redes
Recursos:	Políticas de seguridad
Control:	Supresor de picos de voltaje
Prioridad:	media
Estado:	inicial
Responsable:	Analista de Seguridad
Recursos:	Seguridad en el cuarto eléctrico

Activo: Router	
Control:	Capacitación sobre seguridad informática
Prioridad:	medio
Estado:	En ejecución
Responsable:	Administrador de red
Recursos:	Personal capacitado
Control:	Mantenimiento preventivo
Prioridad:	medio
Estado:	En ejecución
Responsable:	Analista de Seguridad Admin de redes
Recursos:	Políticas de seguridad

Control:	Gestión de claves de cifrado
Prioridad:	medio
Estado:	En ejecución
Responsable:	Analista de seguridad Admin de redes
Recursos:	Políticas de seguridad
Control:	Supresor de picos de voltaje
Prioridad:	media
Estado:	inicial
Responsable:	Analista de Seguridad
Recursos:	Seguridad en el cuarto eléctrico
Control:	Control de humedad y temperatura
Prioridad:	Media
Estado:	En ejecución
Responsable:	Analista de Seguridad

Activo: Wireless	
Control:	Capacitación sobre seguridad informática
Prioridad:	Medio
Estado:	
Responsable:	Administrador de red
Recursos:	Personal capacitado
Control:	Gestión de claves de cifrado
Prioridad:	Medio
Estado:	En ejecución
Responsable:	Analista de seguridad y Admin de redes
Recursos:	Políticas de seguridad
Control:	Charlas informativas de seguridad
Prioridad:	Alto
Estado:	

Responsable:	Analista de Seguridad Admin de redes
Recursos:	Personal capacitado
Control:	Supresor de picos de voltaje
Prioridad:	media
Estado:	inicial
Responsable:	Analista de Seguridad
Recursos:	Seguridad en el cuarto eléctrico

Activo: Controladora wireless	
Control:	Charlas informativas de seguridad
Prioridad:	Alto
Estado:	
Responsable:	Analista de Seguridad
Recursos:	Personal capacitado
Control:	Gestión de claves de cifrado
Prioridad:	Medio
Estado:	En ejecución
Responsable:	Analista de seguridad
Recursos:	Políticas de seguridad
Control:	Supresor de picos de voltaje
Prioridad:	media
Estado:	inicial
Responsable:	Analista de Seguridad y Admin de redes
Recursos:	Seguridad en el cuarto eléctrico

Activo: Documentos de Microsoft	
Control:	Acuerdos de confidencialidad
Prioridad:	Alta
Estado:	
Responsable:	Coordinador de sistemas
Recursos:	Actas de confidencialidad
Control:	Gestión de claves de cifrado
Prioridad:	medio
Estado:	En ejecución
Responsable:	Analista de seguridad y Admin de redes
Recursos:	Políticas de seguridad

Activo: Personal de TI	
Control:	Implementación de controles de seguridad incluyendo separación de funciones y privilegios.
Prioridad:	Alto
Estado:	
Responsable:	Dirección
Recursos:	Humano
Control:	Asignación de responsabilidades
Prioridad:	Alta
Estado:	
Responsable:	Dirección
Recursos:	Humano
Control:	Charlas informativas sobre comportamiento organizacional
Prioridad:	Media
Estado:	
Responsable:	Analista de Seguridad
Recursos:	Humano

Activo: Cableado Estructurado	
Control:	Mantenimiento preventivo
Prioridad:	Alto
Estado:	
Responsable:	Personal técnico de soporte en redes
Recursos:	Humano
Control:	Acceso a las instalaciones
Prioridad:	Alta
Estado:	
Responsable:	Dirección
Recursos:	Humano
Control:	
Prioridad:	Alta
Estado:	
Responsable:	Analista de Seguridad
Recursos:	Reportes del INHAMI

Tabla 8. Implementación de controles

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. La aplicación de la metodología NIST SP 800-30 permite tener un panorama claro de cuales son activos críticos que la organización debe proteger.

2. La implementación presenta resultados no con la finalidad de acusar, sino más bien de informar que recursos son críticos dentro de la organización, permitiendo a la dirección tomar medidas sobre ellos.

3. Al implementar esta metodología podemos evitar incurrir en costos innecesarios al realizar adquisiciones de recursos o activos para la organización.

Recomendaciones

1. Tomar acciones proactivas en cuanto a la seguridad de la información antes que ocurran incidentes de seguridad que afecte el normal funcionamiento de las organizaciones.

2. Que la dirección en base a los resultados de la implementación de evaluación de riesgo puedan tomar decisiones acorde a las necesidades reales de la organización

3. Realizar un proceso continuo de la evaluación de riesgo con la finalidad de contar con información real y actualizada.

BIBLIOGRAFÍA

[1] Jackson Ariel Urrutia Chalá, METODOLOGÍAS DE EVALUACIÓN DE RIESGOS INFORMÁTICOS – UNAD 2014

http://metodologia-y-evaluacion-de-riesgos.blogspot.com/

Fecha de consulta marzo 2014

[2] Ing. Elvis Cárdenas, METODOLOGÍAS PARA EL ANÁLISIS DE RIESGO DE SEGURIDAD INFORMÁTICA

http://msnseguridad.blogspot.com/2012/08/seguridad-informatica-la-seguridad.html

Fecha de consulta agosto del 2012

[3] Elizabeth Mayora, METODOLOGÍA DE GESTIÓN DE RIESGO NIST 800-30

https://prezi.com/p8moufe0ikyl/metodologia-de-gestion-de-riesgo-nist-800-30/

Fecha de consulta mayo del 2014

[4] NIS ESPECIAL PUBLICATION 800-30 GUIA DE GESTIÓN DE RIESGO DE LOS SISTEMA DE TECNOLOGÍA DE LA INFORMACIÓN

Fecha de consulta junio 2002

[5] INSTITUTO NACIONAL DE CIBERSEGURIDAD

https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/analisis_riesgos_pasos_sencillo

Fecha de consulta abril 2014