ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DEFINICIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA RED CONVERGENTE DE LA PRESIDENCIA DE LA REPÚBLICA DEL ECUADOR BASADO EN LAS NORMAS ISO 27000

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

DARWIN PAUL SANGOLUISA CHAMORRO

DIRECTOR: ING. DAVID MERA

CODIRECTOR: MSc. XAVIER CALDERÓN

Quito, Septiembre 2015

DECLARACIÓN

Yo, Darwin Paul Sangoluisa Chamorro, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Darwin Sangoluisa

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Darwin Paul Sangoluisa Chamorro, bajo mi supervisión.

_____

Ing. David Mera
DIRECTOR DEL PROYECTO

AGRADECIMIENTOS

A Dios por haberme dado la fuerza y la entereza para no bajar los brazos durante la realización de este proyecto.

A mi familia, en especial a mi tío y a mi tía, por estar ahí apoyándome a pesar de todo.

A mis amigos, casi hermanos, de toda la vida gracias por los momentos vividos durante estos años.

A los verdaderos educadores que tuve durante la carrea, los cuales no solo les importo lo académico sino lo humano y que gracias a sus consejos permanezco en constante lucha por tratar de ser una mejor persona.

A mis amigos de trabajo de quienes he aprendido a ser un mejor profesional, además un agradecimiento especial a David Mera quien me brindó la oportunidad de formar parte del equipo de Redes.

DEDICATORIA

A mi Madre, mi gran amiga, Martha Chamorro que con su amor, sus consejos y su gran paciencia supo apoyarme durante este sueño a pesar de tantos tropiezos durante este andar

A mi pequeño amor, Alisson, con quien estoy aprendiendo la hermosa labor de ser amigo y padre.

A Bryan Chamorro por estar ahí siempre que necesito un abrazo y una sonrisa.

Los amo, gracias por todo.

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Las políticas de seguridad de la información fueron desarrolladas en base a la norma ISO 27002 y la metodología de análisis de riesgo Octave-Allegro la cual consta de 8 fases. La metodología fue aplicada a dos servicios críticos de la Presidencia, estos servicios son críticos por el tipo de usuarios.

La metodología inicia con el criterio para medir el riesgo en las áreas de impacto más relevantes en una organización. Luego se definió los perfiles de los activos de información basándonos en la descripción de los contenedores de forman parte del activo. Una vez definido el perfil del activo se procedió a identificar las amenazas en base a las áreas de relevancia y los posibles escenarios de amenazas. Finalmente se realizó el análisis de riesgo para identificar los escenarios de amenazas en los cuales el riesgo es alto y proceder con la selección de controles sobre los cuales se definirán las políticas de seguridad de información de dos servicio críticos de la Presidencia de la República.

El presente trabajo está conformado de 4 capítulos.

En el capítulo 1 se define un marco teórico con las principales definiciones de seguridad de la información y las redes de información, además de contener un análisis de los controles de la norma ISO 27002 usados en el proyecto.

En el capítulo 2 se definen cuatro principales metodología para la gestión de riesgo de la seguridad de la información.

En el capítulo 3 se realizar el proceso de análisis de gestión de riesgo basado en la metodología de Octave-Allegro, el cual consta de 8 fases. Consecuentemente se realizan las políticas de seguridad de la información.

En el capítulo 4 se definen las conclusiones y recomendaciones del presente proyecto, así como anexos.

PRESENTACIÓN

El Presente proyecto tiene como objetivo realizar las políticas de seguridad de la información para la red de la Presidencia de la República basados en los controles de la norma ISO 27002. Además pretende ser un aporte para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI)

Por ser la Presidencia de la República la primera institución del estado, el acceso a la información debe estar orientado al cumplimiento de los tres principios fundamentales de la seguridad de la información confidencialidad, integridad, disponibilidad.

Tomando en cuenta estos principios fundamentales de la seguridad de la información se puede desarrollar una correcta gestión de riesgos identificando las áreas críticas donde las posibles amenazas pueden llegar a tener un nivel de impacto alto, así poderlas mitigar y llevarlas a un nivel de riesgo aceptable.

El análisis de riesgo se realizó sobre dos servicios críticos de Presidencia; como es el servicio de correo y el servicio de videoconferencia, este último tiene alcance gubernamental ya que la mayoría de las instituciones lo usan constantemente tanto para reuniones entre autoridades de la misma institución con entre autoridades de varias instituciones.

Al momento existe un acuerdo a nivel gubernamental para la implementación de controles de seguridad, el acuerdo 166 emitido por la Secretaria de la Administración Pública (SNAP), pero este acuerdo no menciona sobre cómo realizar la selección de controles, es decir no indica que hay que realizar un análisis de riesgo.

CAPÍTULO I

1.1.MARCO TEÓRICO

1.1.1. INTRODUCCIÓN

Con la evolución de las TI en aplicaciones web, visualización, cloud computing, BYOD y el incremento de dispositivos móviles y sus aplicaciones entre otras, los desafíos TI y en especial de los oficiales de seguridad de la información se han vuelto más complejos al momento de tratar de asegurar la información la cual en el mundo actual acceder a ella es primordial para el desarrollo del trabajo cotidiano.

La productividad y continuidad del negocio depende de la disponibilidad, integridad y confidencialidad de la información, la cual se encuentra en diferentes medios. La seguridad de la información no hace solo referencia a la información digital, sino también a la información que se encuera impresa.

Hoy en día entidades gubernamentales son amenazadas por grupos de personas que luchan “por la libertad de la información” que se autodenominan Hacktivistas. Estos grupos, en mucho de los casos, atacan a entidades gubernamentales solo con el objetivo de causar pánico más no de enviar un mensaje o propuesta de cambio.

En el mundo digital las herramientas tecnológicas provistas por TI que apoyan a conseguir los objetivos estratégicos de una organización están expuestas a amenazas que pueden tener un impacto sobre dichos objetivos y una manera adecuada de asegurar la información es el uso de estándares, normas, protocolos.

Cualquier procedimiento que se adopte para asegurar la información de una organización, debe contar con el apoyo de todas las partes involucradas para que el objetivo estratégico se cumpla.

1.1.2. SEGURIDAD Y LAS REDES DE LA INFORMACIÓN

1.1.2.1. ¿Qué es la seguridad de la información?

Antes de dar una definición formal de lo que es la seguridad de la información, en primera instancia se debe indicar que la información es uno de los activos/recursos más importantes en una organización.

Una vez establecido que la información es el activo/recurso más importante del negocio se puede introducir la definición de seguridad de la información el cual es proteger la información y los sistemas que están envueltos en el giro del negocio de tal manera que la integridad, disponibilidad y confidencialidad de dicha información no sea afectada.

La seguridad de la información se logra implementando un conjunto adecuado de controles, incluidas las políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Estos controles se deben establecer, implementar, supervisar, revisar y mejorar, cuando sea necesario, para asegurar que la seguridad y los objetivos específicos de negocio de la organización se cumplan. Esto debe hacerse en conjunción con otros procesos de gestión empresarial.[1]

La necesidad de la seguridad de la información inicia cuando los activos/recursos más importantes del negocio tienen un alto grado de riesgo, es decir que si el impacto de una o varias amenazas sobre un activo/recurso (sus vulnerabilidades) es alto, entonces el riesgo también lo es, en resumen se tiene la necesidad de asegurar el activo/recurso que permite minimizar el riesgo y el impacto sobre el giro del negocio.

[1] Párrafo tomado de lo norma ISO 27002, Código para la práctica de la gestión de seguridad de la información, pág. 14.

1.1.2.2. Tipos de seguridad

1.1.2.2.1. Seguridad de la Información

Como se había visto la seguridad de la información es asegurar los activos/recursos/procesos involucrados en el giro del negocio, es decir implementar políticas, procesos, procedimientos, estructuras organizacionales y funciones de hardware y software para minimizar el riesgo.

Figura 1.1.1 Seguridad de la Información

Fuente: www.recursostic.educacion.es/observatorio

1.1.2.2.2. Seguridad Informática

La seguridad informática se enfoca a los activos/recursos de TI y el aseguramiento de los mismos de posibles amenazas que puedan afectar el adecuado funcionamiento, cabe indicar que en la seguridad informática no está involucrado el giro negocio.

1.1.3. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

Hay tres principales objetivos que hay que tomar en cuenta al momento de asegurar la información, estos pilares fundamentales son conocidos como CIA o CID (CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD).

1.1.3.1. Confidencialidad

Es el principio en el cual solo individuos, procesos o sistemas autorizados pueden acceder a la información en función de sus necesidades (need-to-Know basis).

El principio de la confidencialidad se debe aplicar en los tres estados de la información es decir en almacenamiento, en procesamiento y en tránsito.

La información debe ser clasificada es decir puede ser (pública, solamente uso interno, o confidencial) con el fin de determinar un nivel de confidencialidad.

Para aplicar el principio de confidencialidad se puede usar identificación, autenticación, autorización a través de controles de acceso, pero esto no garantiza 100% de confidencialidad porque usuarios autorizados también son un riesgo ya que pueden acceder a la información con fines maliciosos.

1.1.3.2. Integridad

Es el principio en el cual la información que se encuentra en almacenamiento, procesamiento y en tránsito solo debe ser alterada de una manera específica(procedimiento) y por sujetos autorizados, cabe señalar que un sujeto autorizado también puede alterar la información debido a errores humanos, algunos ejemplos serian, ingreso de datos inválidos, alteración de configuraciones, borrado de archivos, etc.

Para mantener el principio de integridad no solo se necesita prevenir alteraciones en la información sino tener la habilidad de deshacer cambios autorizados.[2]

El principio de integridad depende del principio de confidencialidad ya que sin confidencialidad la integridad no puede ser mantenida.

---

[2] Párrafo traducido textualmente de: Jasson Andress, The basics of information security.

1.1.3.3. Disponibilidad

Es el principio en el cual la información que se encuentra en almacenamiento, procesamiento y en tránsito debe estar accesible en cualquier momento y en cualquier lugar solo para los sujetos autorizados.

El principio de disponibilidad podría haberse afectado por DoS (Deny of Service) el cual puede darse por la alteración de información sensible en cualquier elemento que compone la cadena de acceso a dicha información, en su mayor parte estas alteraciones son causadas por errores humanos y no solo por sujetos que no están autorizados. También el principio de disponibilidad puede verse afectado por cualquier tipo de desastre natural o incidente totalmente externo.

Para mantener el principio de disponibilidad es necesario implementar adecuados controles de seguridad de la información como:

- Mantener el principio de confidencialidad.
- BCP (Plan de continuidad del Negocio).
- Implementar redundancia.
- Implementar respaldos.

1.1.4. GESTIÓN DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN

La gestión de riesgo de la seguridad de la información es un proceso de la organización el cual está enfocado a la toma de decisiones a nivel de gerencia de acuerdo a un análisis de riesgo que se realiza sobre los activos de información.

Todo tipo de organización debería realizar la gestión de riesgo de sus activos de información antes de realizar la gestión de seguridad de los mismos, ya que con el análisis de riesgo se definirá de mejor manera los controles de seguridad para disminuir los riesgos. Definir los controles antes de realizar un análisis de riesgo no sería lo adecuado ya que se pueden seleccionar algunos o varios que no cubran la verdadera necesidad de seguridad de la Organización.

Hay varias metodologías de gestión de riesgos las cuales nos facilitan realizar todo el proceso de gestión, análisis y tratamiento de riesgos, este tema se profundizará en el capítulo II, algunos de estos métodos son:

- Magerit v3
- NIST 800-39, Managin Information Security Risk
- Octave-Allegro
- ISO 2705 Information technology- security techniques- information security risk management

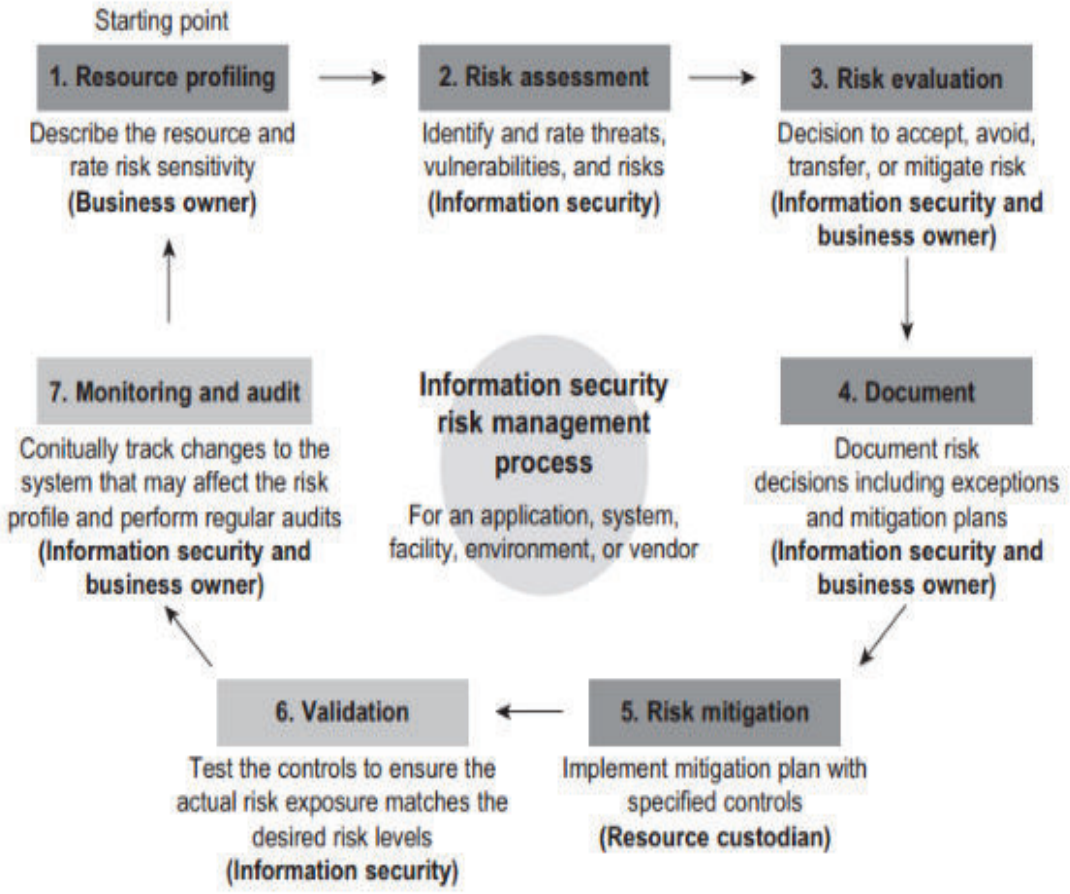

Figura 1.1.2. Ejemplo Proceso de la Gestión de riesgo de la Seguridad

Fuente: Evan Wheeler, Security Risk Management

1.1.5. LA ORGANIZACION Y SUS NORMAS

Las organizaciones humanas se clasifican en; comerciales, residenciales, gubernamentales en las cuales se debe cumplir normas, leyes, regulaciones, etc.

En el ámbito Gubernamental Ecuatoriano está vigente el acuerdo 166[3] el cual es de estricto cumplimiento para todas las instituciones públicas, fue desarrollada por el la Secretaria de la Administración Publica en el año 2013 y publicada a inicios del año 2014 enfocada a la seguridad de la información.

El acuerdo 166 determina los lineamientos para la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI). El EGSI está basado en la NTE INEN-ISO/IEC 27002 publicada en el registro oficial el 22 de Mayo del 2009.

Como tal, el EGSI fue desarrollado para aplicarlo a nivel gubernamental, consta de los 11 dominios de la ISO/IEC 27002 con la diferencia que el documento del EGSI establece lineamientos para específicos para las entidades de la Administración Publica Central. Además el EGSI establece los controles prioritarios que deben aplicarse a nivel gubernamental.

1.1.6. LAS TICS COMO UN EJE PRINCIPAL DE UNA ORGANIZACIÓN

Es muy importante entender como la interrelación entre el proceso del negocio y las TICs facilitan el cumplimiento de las de las metas (misión-visión) de cada organización.

Las TICs son un elemento estratégico que optimizan los recursos de tal manera que los procesos que pertenecen a la organización sean llevados a cabo eficientemente.

---

[3] Acuerdo Gubernamental que conforman el EGSI, Registro Oficial Suplemento 88, vigente.

Las organizaciones con mayor probabilidad de éxito serán las que implementen las TICs como uno de los ejes principales de su negocio, de tal manera que la inversión que se realice, se transforme en valor agregado de la organización.

Las TICs son un factor crítico para alcanzar las metas que cada año se proponen las organizaciones y para que una organización obtenga la meta planteada; toda organización debe considerar un plan relacionada con el área de TICs que contenga actuaciones en cada uno de los siguientes aspectos[4]:

1.1.6.1. Dirigir

Alineamiento con los objetivos del negocio para poder construir los mecanismos necesarios para entregar valor.

1.1.6.2. Crear

Retorno de valor de la inversión realizada en TIC.

1.1.6.3. Proteger

Gestión de riesgos para preservar el valor de los activos.

1.1.6.4. Actuar

Gestión de recursos y desarrollo del plan TIC

1.1.6.5. Monitorizar

Evaluación de la ejecución y desempeño del plan establecido para realinear el gobierno de las TIC con el del negocio si es necesario.

---

[4] Artículo, El papel de las TIC en el siglo XXI, Jose R Vilar, www.Infonova.com

Es importare que las organizaciones donde se quiera implementar las TICS se defina lo que se quiere alcanzar con su implementación y además que se capacite a las personas que van a hacer uso de esta implementación.

La implementación de la TICS podría tener grandes beneficios para las organizaciones haciéndolas más competitivas en el mercado donde se enfoquen, pero si la implementación no contempla un plan de gestión de riesgos, los riesgos que acompañan a las TICS tendrían consecuencias graves para los objetivos estratégicos de las organizaciones.

1.1.7. PRINCIPIOS FUNDAMENTALES DE LAS REDES DE INFORMACIÓN

Una vez que se ha indicado que la Tecnología es parte fundamental para alcanzar los objetivos del negocio se procede a revisar la que son las redes de comunicación.

Para que la una comunicación exista debe haber un emisor y un receptor además de la información que se desea compartir entre ellos, también debe existir un medio de trasmisión por el cual se realice la compartición, y además las reglas para comunicarse que no son más que los protocolos de comunicación

1.1.7.1. Definición de redes de comunicaciones

Es un conjunto de elementos necesarios para que los dispositivos finales a más de intercambiar información entre si también puedan acceder a recursos y servicios, de tal manera que la productividad de las personas se incremente.

Algunos de los componentes de describen en la Tabla 1.1 y Fig.1.3.

1.1.7.2. Clasificación de la redes por el área geográfica que cubre

Una vez definido lo que es una red de comunicaciones se define la clasificación por el área geográfica que cubre.

Los elementos esenciales para el intercambio de información	HARWARE DE RED	SWTICHES
		ROUTERS
		ACCESS POINTS
	MEDIO DE TRANSMISIÓN	WIRE
		WIRELESS
	SOFTWARE DE CONECCIÓN	SISTEMAS OPERATIVOS DE LOS DISPOSITIVOS FINALES Y DE SWITCHES Y ROUTERS

Tabla 1.11. Principales elementos para el intercambio de información

1.1.7.2.1. WAN

Es una red que cubre largas distancias y es usada para conectar redes LAN que se encuentran separadas largas distancias.

1.1.7.2.2. MAN

El concepto de red de área metropolitana representa una evolución del concepto de red de área local a un ámbito más amplio, es decir puede cubrir parte de una ciudad.

1.1.7.2.3. LAN

Consiste en un medio de transmisión compartido y un conjunto de software y hardware para servir de interface entre los dispositivos y el medio, y regular el orden del acceso al mismo.

1.1.7.3. Características de las redes LAN[5]

1.1.7.3.1. Costo

Es el que incluye el costo de los componentes de Red, la instalación y el mantenimiento.

1.1.7.3.2. Seguridad

Incluye la protección de los componentes de red y de la información que ellos contienen, así como la información que cursa entre ellos.

1.1.7.3.3. Disponibilidad

Mide la probabilidad que una red esté disponible a los usuarios, la disponibilidad es típicamente medida en porcentaje basado en el número de minutos que existe en el año, por lo tanto el uptime podría ser el número de minutos que la red está disponible dividido para el numero de minuto en un año.

1.1.7.3.4. Velocidad

Es cuán rápido la información es transmitida entre dispositivos finales que forman parte de la red.

1.1.7.3.5. Topología

Describe la distribución de cableado físico y la manera lógica en la cual se mueve la información entre los componentes de red.

---

[5] Netacat, cisco CCNA módulo 4

1.1.7.3.6. Escalabilidad

De fine que tan bien la red de adapta a nuevos crecimientos, incluyendo nuevos usuarios, componentes y aplicaciones.

1.1.7.3.7. Confiabilidad

Define la confiabilidad de los componentes de red y la conectividad que hay entre ellos. MTBF (Medium Time Between Failure) es la medida comúnmente usada para indicar la probabilidad de que un componente falle.

1.1.7.4.Topologías

1.1.7.4.1. Topología física

Se describe como el arreglo de los componentes de red están físicamente cableados junto.

Las topologías físicas pueden ser Bus con un medio de comunicación en común, Estrella donde los dispositivos se conectan a un nodo central y Anillo donde la comunicación es enviada en modo secuencial.

1.1.7.4.2. Topología lógica

Describe como el arreglo de los componentes se comunican entre sí a través de la Topología física.

En una topología lógica se requiere que un nodo esté disponible por el protocolo de comunicación usado, que esté disponible quiere decir que se puede identificar en el red por su dirección MAC.

1.1.7.5.Medios de transmisión y dispositivos de conectividad

Los medios de transmisión y los dispositivos de conectividad juegan un papel muy importante en el rendimiento de la red, además determina la capacidad de tráfico que puede cursar a través de la red. Los medios de trasmisión pueden ser alámbricos o inalámbricos.

Dentro de los medios de trasmisión alámbricos están los cables de cobre, par trenzado, cable coaxial, fibra óptica.

Dentro de los medios de transmisión inalámbricos está el infrarrojo, microondas y laser. En la Fig.1.3 se describe los medios de transmisión y dispositivos de conectividad.

1.1.8. MODELOS DE REFERENCIA

Los modelos de referencia nacen por la necesidad de buscar que las comunicaciones entre sistemas de computadoras sean establecidas de manera eficiente por medio de protocolos de comunicación[6].

1.1.8.1. Modelo OSI

Desarrollado por la ISO en 1984 está constituido de siete capas, además es un Framework para la red el cual asegura la compatibilidad del hardware y software en la comunicación.

En la Fig. 1.4. Se muestra las capas del modelo de referencia OSI y la denominación de su unidad de paquete.

[6] TanenBaum-Wetherall, Computer Networks, quinta edición.

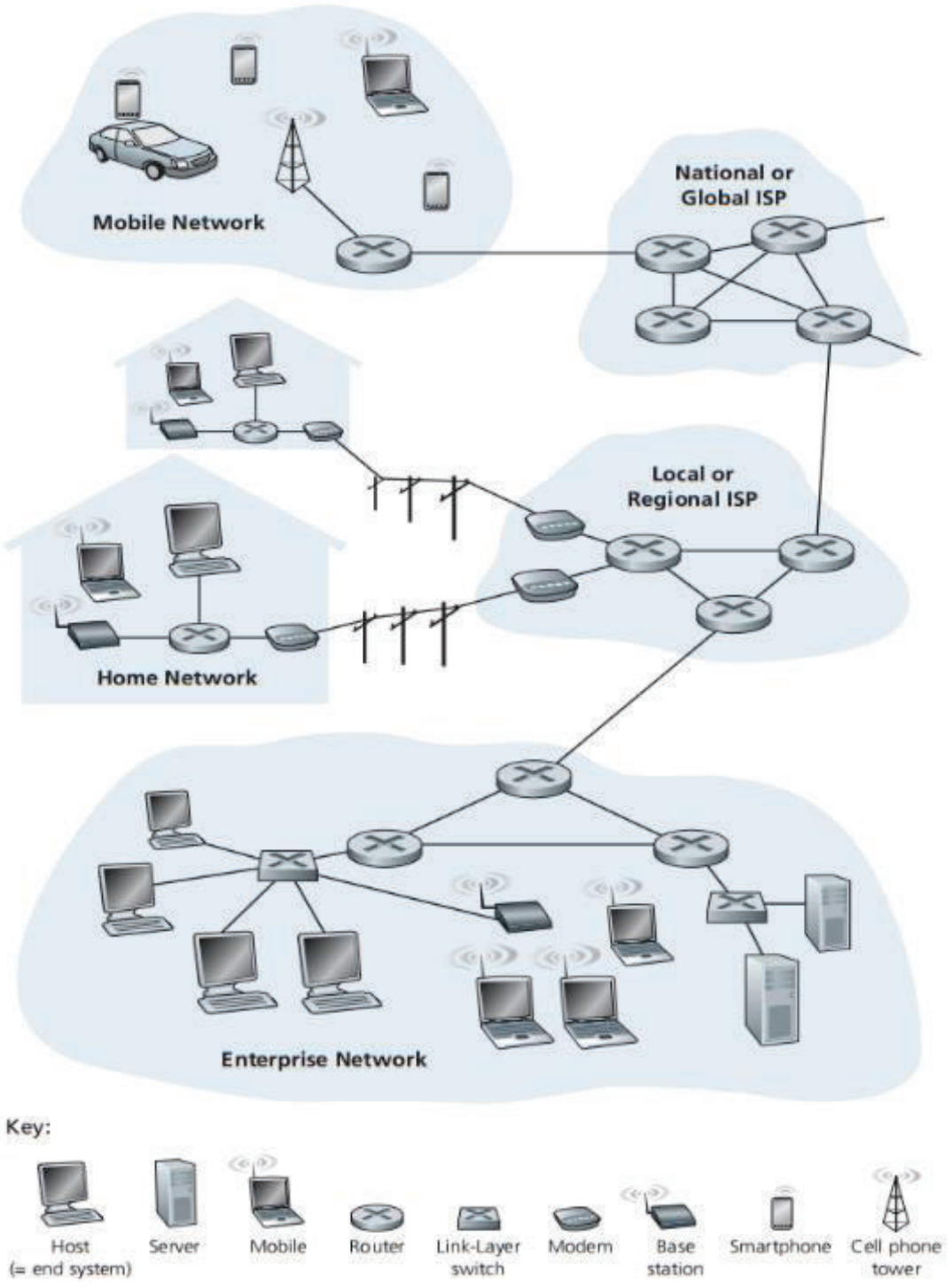

Figura 1.1.3. Resumen de medios de transmisión y dispositivos de conectividad

Fuente: Kurose-Ross, Computer Networking

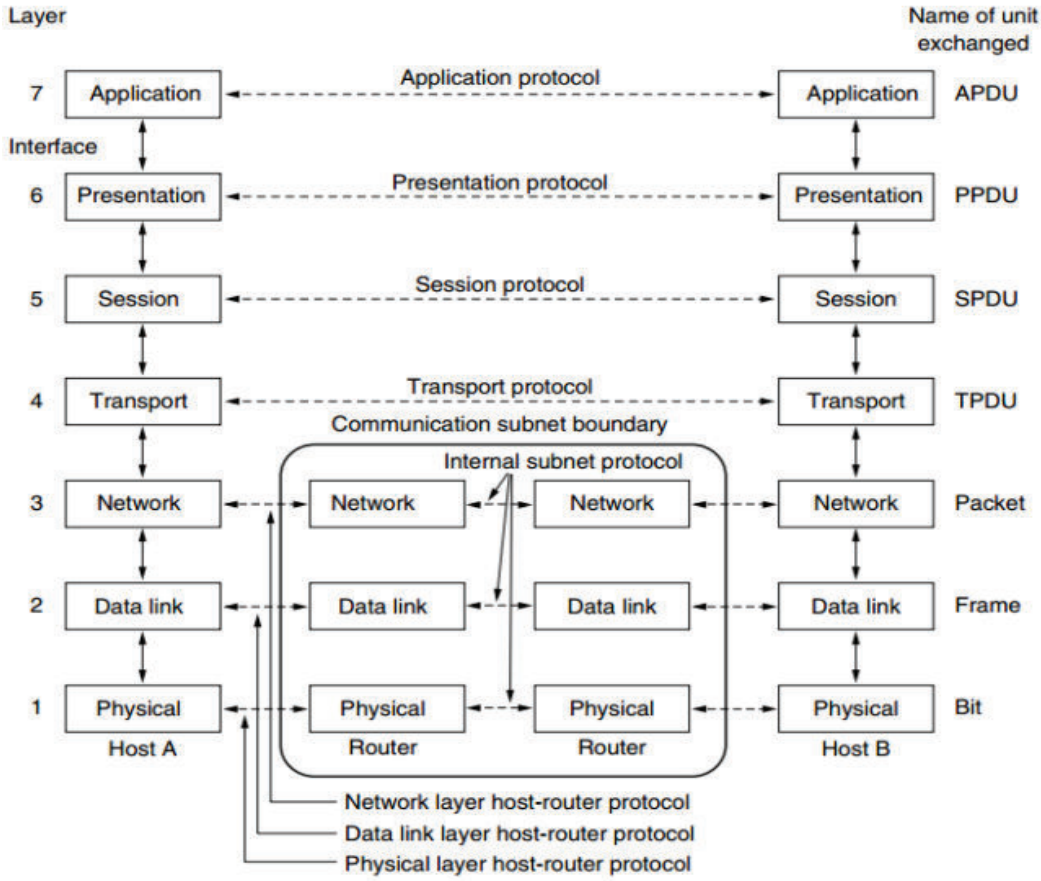

Figura 1.1.4. Modelo de referencia OSI

Fuente: Tanembaum-Wetherall, Computer Networks 5th Edition

El modelo OSI en sí mismo no es una arquitectura de red porque no especifica los servicios exactos y protocolos a ser usados en cada capa, el modelo OSI solo indica la función que cada capa debe hacer.

- Una capa fue desarrollada de acuerdo a la necesidad de abstracción
- Cada capa debe realizar una función bien definida
- Cada función debe estar enfocada a la estandarización de protocolos
- Los límites de cada capa deben estar definidos para minimizar el flujo en las interfaces.
- El número de capas debe ser lo suficientemente largo como para que distintas funciones no estén en la misma capa.

1.1.8.1.1. Capa física

Se encarga de la transmisión de bits entre diferentes locaciones y provee las siguientes características:

Eléctricas

Especifican como se representan los bits 1 y 0, es decir los niveles de voltaje así como también la velocidad de transmisión.

Mecánicas

Relacionada con las propiedades físicas de la interfaz y del medio de transmisión como por ejemplo cable par trenzado, fibra óptica, radio frecuencia

1.1.8.1.2. Capa de enlace

Intenta que el enlace físico sea seguro, proporciona los medios para activar, mantener y terminar el enlace. El principal servicio brindado a las capas superiores es el de detección y control de errores.

Las funciones de esta capa es la segmentación en tramas, el control de flujo mediante la regulación de tráfico, resuelve problemas de daño, perdida, duplicidad de tramas así como el direccionamiento y secuencia de las mimas, además proporciona una conexión lógica entre nodos adyacentes

1.1.8.1.3. Capa de red

Su función es realizar el control de operación de la subred y garantiza que el la información llegue desde el nodo origen al nodo destino. Realiza el enrutamiento, conmutación, control de flujo y recuperación de fallas en la capa de enlace. La unidad de información es el paquete.

1.1.8.1.4. Capa trasporte

Conocida como la capa host to host, esta capa aísla de la capa de sesión los cambios inevitables a los que está sujeta la tecnología del hardware. Se ocupa del establecimiento y liberación de conexiones a través de la subred, también realiza control de flujo entre host.

1.1.8.1.5. Capa de sesión

Permite que usuarios de diferentes maquinas establezcan sesiones entre ellos, la sesión ofrece varios servicios entre otros control de dialogo (indicar quien tiene el turno de transmitir), administración de token (evitar que las dos partes realicen la misma operación simultáneamente) y sincronización (reanudar alguna operación que por alguna razón se interrumpió).

1.1.8.1.6. Capa de presentación

Maneja la sintaxis de los datos es decir sus formatos, códigos, también del formato de los datos pero no de su significado.

1.1.8.1.7. Capa de aplicación

Contiene una variedad de protocolos que son usado comúnmente, también proporciona una interface final entre el usuario y la red así como cualquier proceso de aplicación. Algunos ejemplos de las funciones son:

- Acceso a archivos remotos.
- Administración de la red.
- Mensajería electrónica.

1.1.8.2.Arquitectura TCP/IP

Creado originalmente por ARPA (AGENCIA DE INVESTIGACION DE PROYECTOS AVANZADOS ASOCIADA AL DEPARTAMENTE DE DEFENSA DE USA)[7].

El modelo define 4 capas las cuales se describen a continuación.

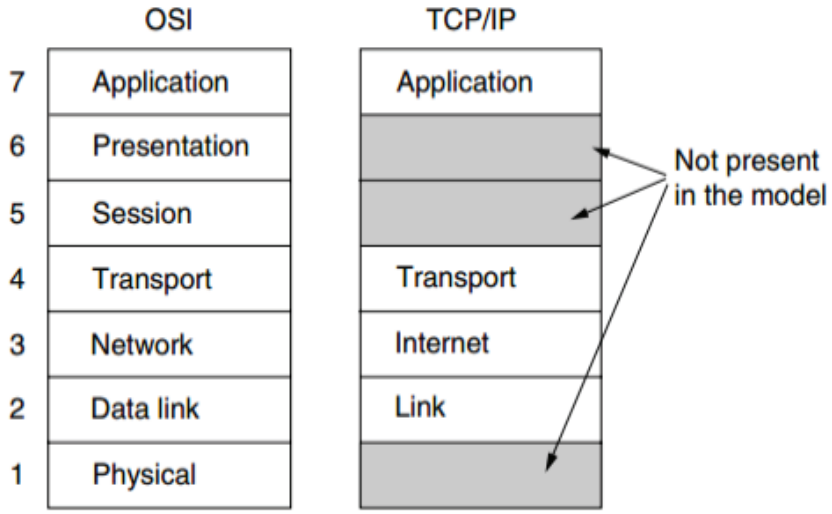

Figura 1.1.5. Arquitectura TCP/IP

Fuente: Tanembaum-Wetherall, Computer Networks 5th Edition

1.1.8.2.1. Capa enlace

Describe lo que los enlaces como líneas seriales y Ethernet deben hacer para satisfacer las necesidades de la capa de Internet.

No es realmente una capa del todo en todo el sentido de la palabra, sino es más bien una interface entre host y enlaces de transmisión.

1.1.8.2.2. Capa internet

[7] TanenBaum-Wetherall, Computer Networks, quinta edición.

Esta capa es el eje que sostiene toda la arquitectura junta, permite entregar paquetes a cualquier red independientemente del destino.

Define un formato de paquete y un protocolo llamado IP el cual es un protocolo no orientado a la conexión.

1.1.8.2.3. Capa de transporte

Permite a entidades de igual nivel en el origen y en el destino llevar una conversación, en esta capa se definen dos protocolos, TCP (protocolo orientado a la conexión) y UDP (no orientado a la conexión).

1.1.8.2.4. Capa de aplicación

Define las aplicaciones usadas para procesar peticiones, puertos y que sockets son usados.

1.1.8.2.5. Resumen del stack de protocolos en la arquitectura TCP/IP

En la siguiente Tabla se resumen algunos protocolos que pertenecen a la arquitectura TCP/IP.

CAPA DE APLICACIÓN	HTTP, SMTP, DNS, DHCP, ECT.	NTP, RTP, SNMP
CAPA DE TRASPORTE	TCP	UDP
CAPA INTERNET	IP, ICMP, ARP	
CAPA DE ENLACE	ETHERNET, ATM, 802.11, SONET, ADSL	

Tabla 1.12. Stack de protocolos en TCP/IP

1.1.9. PROTOCOLOS DE SEGURIDAD DE RED

Los mecanismos o protocolos de seguridad ayudan a proteger la información que se encuentra en almacenamiento, tránsito o en procesamiento, además estos protocolos ayudan a conservar los principios fundamentales de la seguridad de la información.

Se realizará un revisión de los principales protocolos de seguridad que se encuentran en las diferentes capas de la arquitectura TCP/IP.

Los protocolos que se revisaran son los que de alguna manera tienen relación con los servicios analizados como parte del presente proyecto. En el caso del servicio de correo electrónico PGP, S/MIME, SSL, TLS, y en el caso del servicio de videoconferencia HTTS.

1.1.9.1.Capa aplicación

Protocolos usados para proveer seguridad en la comunicación entre programas de cliente final y los servidores de aplicaciones.

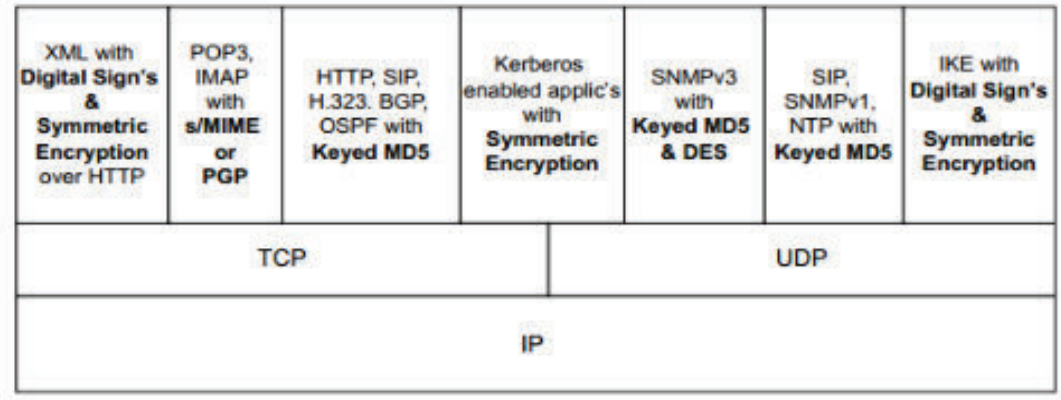

Figura 1.1.6. Protocolos de seguridad en la capa de aplicación

Fuente: Stuart Jacobs, engineering information Security

1.1.9.1.1. PGP

Es un software que provee encriptación, autenticación y privacidad, usado principalmente para encriptar el contenido de correo electrónico (mensajes y adjuntos) desde un cliente de escritorio.

Costa de cuatro procesos, hashing, compresión de datos, cifrado de clave simétrica y cifrada de llave pública. Generalmente se utiliza clientes de correo para realizar el cifrado.

Además cubre los objetivos de confidencialidad e integridad de la información que se encuentra en tránsito y almacenada ya que la información es encriptada antes de ser enviada. Cabe señalar que este proceso es realizado por el cliente de correo.

1.1.9.1.2. S/MIME

Es un protocolo usado principalmente en la trasmisión de correo electrónico que proporciona dos servicios de seguridad como:

- Las firmas digitales, las cuales sirven para validar la identidad del remitente, además de que el mensaje no fue alterado.
- El cifrado de los datos, que provee confidencialidad e integridad de la información contenida en el mensaje enviado.

S/MIME cubre los principios de confidencialidad e integridad ya que el servidor de correo realiza el cifrado de la información antes de ser trasmitida, además no requiere de un cliente de correo para realizar el cifrado.

1.1.9.1.3. HTTP- SEGURO (S-http)

En s-http la información en si es encriptada, es decir conserva el principio de confidencialidad e integridad entre el cliente y el servidor web. La diferencia con

HTTP sobre SSL es que con SSL se encripta el canal de comunicación y no los datos y es independiente de HTTP. Algunas técnicas usadas por S-HTTP para la encripción son: PEM (Privacy Enhanced Mail), PGP, PKGS-7.

1.1.9.1.4. HTTPS

Es un protocolo web, trabaja con la subcapa SSL para proveer un camino encriptado entre el cliente web y el servidor.

Proporciona los principios de confidencialidad e integridad únicamente en tránsito ya que si se realiza una captura de trafico https será complicado poder descifrar su contenido, además de poder modificarlo.

1.1.9.2.Capa transporte

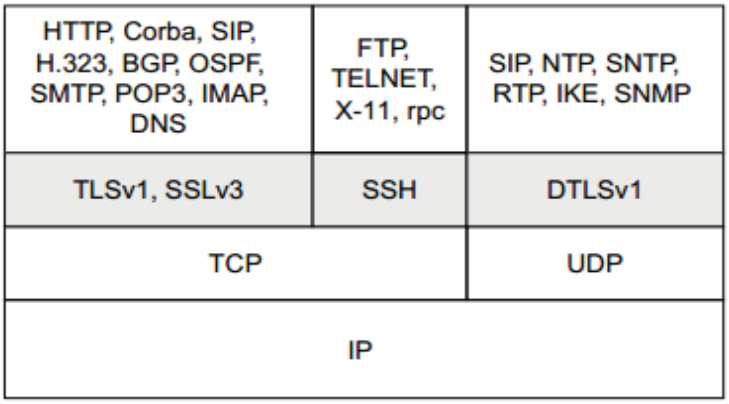

Figura 1.1.7. Protocolos de seguridad en la capa de trasporte

Fuente: Stuart Jacobs, Engineering information security

1.1.9.2.1. SSL (Secure Socket Layer)

Diseñado para proveer un camino encriptado entre cliente y servidor, a más de proveer encripción también provee autenticación entre cliente y servidor cumpliendo con los principios de confidencialidad e integridad del mensaje.

1.1.9.2.2. LS (Transport Layer Security)

Provee seguridad e integridad entre dos aplicaciones, es la evolución del SSL v3.0. Provee dos características interoperatividad de intercambio de parámetros con terceros y la expansibilidad para trabajar con nuevos protocolos. TLS provee integridad de los datos haciendo uso de un Código de Autenticación de Mensaje (MAC), también provee confidencialidad usando algoritmos de cifrado simétrico.

1.1.9.3.Capa de red

1.1.9.3.1. IPSEC (Internet Protocol Security)

Es un conjunto de protocolos de autenticación y encripción que provee los siguientes servicios a nivel de capa de red, control de acceso, integridad de la conexión, confidencialidad, autenticación y protección contra duplicación de paquetes entre dos partes diferentes.

La confidencialidad e integridad esta basa en el cifrado del datagrama ip original dentro de un nuevo datagrama ip.

1.1.9.3.2. VPN (Virtual Private Network)

Una VPN puede ser usada en una infraestructura de comunicaciones pública proveyendo procedimientos seguros en canales de comunicaciones inseguros. Los procedimientos involucran encripción sobre protocolos de túnel.

Existen dos tipos de VPN, acceso remoto para conectar a un usuario itinerante o remoto a la red corporativa y la VPN sitio a sitio la cual une dos redes corporativas. VPN provee confidencialidad e integridad con el encapsulamiento IP de paquetes TCP/IP, encripción únicamente en la parte de los datos y autenticación usando un dominio de encriptación.

1.1.9.4.Seguridad en la capa de enlace de datos

1.1.9.4.1. PPP (Point-to-Point Protocol)

Uno de los primeros protocolos usado para la conexión a Internet usando un módem. Provee 3 métodos de autenticación PAP, CHAP, EAP.

1.1.9.4.2. Radius (remote authentication dial-in user service)

Es un servidor de autenticación remota y auditoria, provee protocolos de autenticación como PAP y CHAP.

Como método de autenticación se recomendaría CHAP, ya que éste trabaja con una clave compartida y un algoritmo de hash, donde el servidor envía al cliente un desafío y espera la respuesta, y si la respuesta procesada en el servidor coincide, el cliente se autenticará. Con PAP no existe seguridad ya que envía el usuario y clave en texto plano y sería muy fácil de realizar una captura de tráfico e identificar las credenciales utilizadas en el método de autenticación.

1.1.9.5.Relación existente entre las TICs y los objetivos estratégicos de la Presidencia.

Una vez revisados los protocolos de seguridad se procede a realizar una relación de cómo estos protocolos pueden ayudar a mantener los objetivos estratégicos vigentes de la Presidencia de la República del Ecuador. Para ello se define en primera instancia dichos objetivos[8].

- Proporcionar productos y servicios de carácter jurídico para asesoramiento y patrocinio jurídico del Presidente/a de la República, de las máximas autoridades de la Presidencia de la República y la institución.

[8] Objetivos tomados del: Estatuto Orgánico vigente de la Presidencia de la República del Ecuador, registro oficial N° 296, 24 Julio 2014.

- Diseñar e implementar un modelo de gestión para el levantamiento de escenarios que permitan emitir un adecuado y oportuno asesoramiento para la toma de decisiones.

- Alcanzar y mantener un alto nivel de gestión operativa financiera, para apoyar eficiente y eficazmente las actividades y proyectos de la Presidencia de la República.

Como antecedente, el primer objetivo estratégico enfocado a un área específica en la cual se genera y procesa información de carácter jurídico tanto en formato físico (papel) como digital (PC, Repositorios) debe cumplir con el objetivo de confidencialidad ya que ninguna persona a más del área Jurídica de la institución debe tener acceso a leyes o propuestas de leyes que aún no son debatidas para su aprobación. La falta de confidencialidad en estos temas podría ocasionar conflictos a nivel político.

La confidencialidad y la disponibilidad son los principios que apoyan los objetivos estratégicos restantes, ya que procedimientos y procesos desarrollados para agilitar la toma de decisiones a nivel presidencial deben estar disponibles y deben ser accedidos de una manera responsable.

TICs definido dentro de un proceso adjetivo en la cadena de valor tiene por misión "Gestionar y administrar los productos y servicios relacionados con las tecnologías de la información y comunicaciones para la integridad y la confiabilidad del software, hardware e información institucional, así como el desarrollo, mantenimiento y disponibilidad de los servicios y equipamiento tecnológico, contribuyendo a que la institución provea una gestión eficiente, transparente y oportuna"[9].De acuerdo a su misión, TICs es un apoyo importante a los procesos gobernantes como gestión jurídica y gestión general y a los procesos sustantivos que son los encargados de hacer que la misión de presidencia de cumpla.

[9] Misión tomada del: Estatuto Orgánico vigente de la Presidencia de la República del Ecuador, registro oficial N° 296, 24 Julio 2014.

Como ejemplo práctico se puede identificar el proceso sustantivo de la gestión de la seguridad de la información el cual está encargado de mantener la disponibilidad, integridad y confidencialidad de la información de los procesos gobernantes, es decir tiene como objetivo principal realizar la gestión de la seguridad de la información por medio de la gestión de riesgo y aplicación de los controles en donde se podría incluir la aplicación de los protocolos de seguridad.

1.1.10. ANÁLISIS DE LA NORMA 27002 (TÉCNICAS DE SEGURIDAD-CÓDIGO DE PRÁCTICAS PARA LA ADMINISTRACIÓN DE SEGURIDAD DE LA INFORMACIÓN)

Se procederá a realizar el análisis de la norma 27002:2005 ya que es la norma propuesta en el plan de titulación y de la cual únicamente se analizarán los controles que hacen referencia al usuario final y a la red. Cabe indicar que la norma 27002:2013 se publicó meses después de la aprobación del plan.

En la actualidad muchas de la instituciones gubernamentales no poseen procesos, procedimientos, etc., descritos en documentos formales es decir todo descrito como un proceso, por esta razón aplicar políticas de la seguridad de la información se vuelva una tarea complicada.

La necesidad puede venir desde cualquier ámbito, lo importante es que la gerencia esté involucrada y se cuente con todo su apoyo para el aseguramiento de la información. Además, la gerencia es la que define el o los procesos que se deben asegurar con el fin de cumplir los objetivos estratégicos de las organizaciones.

La información en cualquiera de sus estados (almacenamiento, procesamiento, transmisión) es el activo más importante para toda organización pública y privada, por tal razón se la debe proteger de los riesgos a los cuales se ve expuesta.

En la Fig. 1.8 se muestra la evolución de norma ISO 27000

En el ámbito gubernamental el impacto de las amenazas no siempre son pérdidas económicas, sino más bien, el impacto recae en la imagen de la institución de gobierno de tal manera que la confianza disminuye.

Lograr que la información tenga adecuados niveles de seguridad no solo se logra aplicando controles, procedimientos, procesos e implementando software y hardware que minimicen los riesgos, sino que también se debe generar campañas educativas con el fin de que el usuario tenga conciencia sobre la información que maneja y de las amenazas a la que está expuesto. Es decir minimizar los riesgos a través del conocimiento.

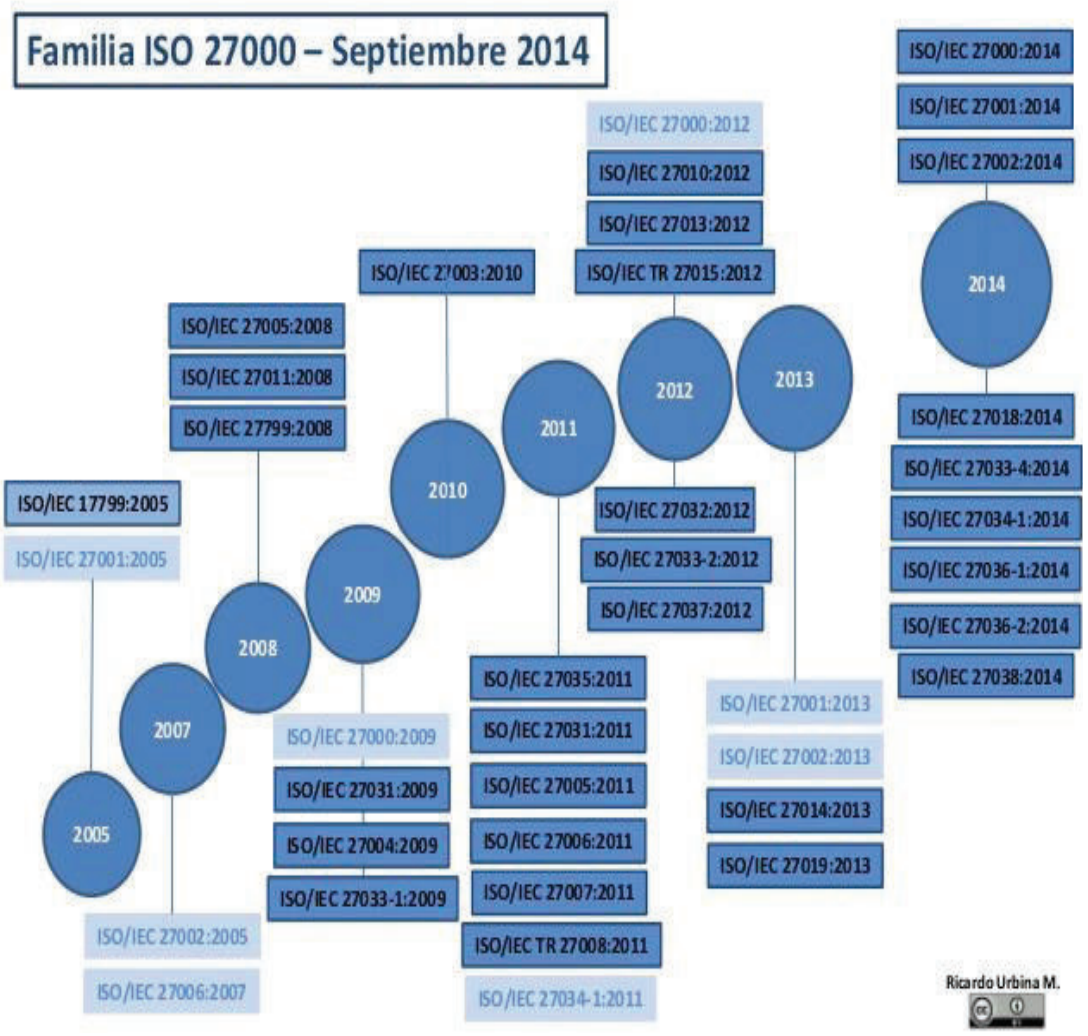

Figura 1.1.8. Evolución de la norma ISO 27000

Fuente: www.es.slideshare.net/Ricardo

La norma se enmarca en 3 tipos de requerimientos de la seguridad de la información, siendo el último el que depende de las particularidades de la organización.[10]

- Evaluar los riesgos tomando en cuenta los objetivos estratégicos de la organización.
- Requerimientos legales, reguladores, estatutarios, contractuales que las organizaciones deben cumplir.
- Principios propios del manejo de la seguridad de la información en la entidad y así poder mantener sus operaciones.

La gestión de riesgo debe ser aplicada previo a la selección de controles que aplicaran para el aseguramiento de los activos, para la gestión de riesgo se utiliza la norma ISO 27005 parte de la familia 27000.

La norma se la puede usar como guía para definir lineamientos propios en los cuales se puede incluir controles que no son propios de la norma, pero siempre tomando en cuenta la realidad de la organización.

El objetivo principal del estándar 27002 es mejorar la gestión de la seguridad de la información en las organizaciones, así como el desarrollo de lineamientos de seguridad propios.

La norma ISO 27002 consta de 11 dominios, 39 objetivos de control (categorías de seguridad) y 133 controles, la norma puede ser aplicada a las organizaciones tanto públicas como privadas, cabe indicar que algunos de los controles dentro de las organizaciones no podrán ser aplicables dependiendo de lo que se requiere proteger.

Cada objetivo de control establece lo que se requiere lograr, además se puede aplicar uno o más controles para lograr los objetivos de control. [11]

---

[10] Tomado de: La norma ISO 27002, Código para la práctica de la gestión de seguridad de la información 2005.

[11] Párrafo tomado de: Norma ISO 27002, Código para la práctica de la gestión de la seguridad de la información 2005.

Los controles están estructurados de la siguiente manera[12]:

- El control define el enunciado específico para el cumplimiento del objetivo de control.
- El lineamiento de implementación proporciona información más detallada para apoyar la implementación y cumplir con el objetivo de control, algunas de estas guías no pueden ser aplicadas en todos los casos y por lo tanto otras maneras de implementar el control sería más adecuado.
- Otra información es proporciona que tal vez se deba considerar, por ejemplo consideraciones legales y referencias a otros estándares.

1.1.10.1. Términos relevantes del estándar

A continuación de muestran las principales definiciones de la ISO 27002.

Activo	Cualquier cosa que tenga valor para la organización.
Control	Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.
Lineamiento	Una descripción que aclara que se debería hacer y como para lograr los objetivos establecidos en las políticas.
Política	Intención y dirección general expresada formalmente por la gerencia.

[12] Ítems tomados de: Norma ISO 27002, Código para la práctica de la gestión de la seguridad de la información 2005.

Riesgo	Combinación de la probabilidad de un evento y su ocurrencia.
Análisis de Riesgo	Uso sistemático de la información para identificar las fuentes y calcular el riesgo.
Evaluación de Riesgo	Proceso para comparar el riesgo estimado con un criterio de riesgo dado para determinar la importancia del riesgo.
Gestión de Riesgo	Actividades para dirigir y controlar el riesgo en una organización.
Tratamiento del Riesgo	Proceso de selección e implementación de medidas para modificar el riesgo.
Amenaza	Una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización.
Vulnerabilidad	La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.
Evento de seguridad de la información	Es una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible falla de seguridad.
Incidente de la seguridad de la información	Es indicado por un solo evento o una serie de eventos inesperados de seguridad de la información que tiene una probabilidad significativa de comprometer las operaciones y amenaza la seguridad de la información.

Tabla 1.13. Definición de términos relevantes del estándar.

1.1.10.2. Protección contra código malicioso y móvil

Objetivo

Proteger la integridad del software y la información.[13]

El código malicioso y código móvil no autorizado como virus, gusanos, caballos de Troya, bombas lógicas entre otras amenazan los activos de las organizaciones, por tal razón el usuario debe tener conocimiento sobre las amenazas que pueden afectar su dispositivo de trabajo y corromper la integridad de la información que maneja.

1.1.10.2.1. Controles contra código malicioso

Controles de detección, prevención y recuperación para proteger contra códigos maliciosos y

Se debieran implementar procedimientos para el apropiado conocimiento del usuario. [14]

Los lineamientos principalmente enfocados a detectar código malicioso, reparación de software y concienciación de la seguridad. Generar políticas que eviten el uso de software no autorizado así como la obtención de archivos o software a través de fuentes externas e internas.

Realizar actualizaciones programadas con el fin de evitar el contagio de código malicioso, revisión de archivos almacenados en los distintos medios antes de ser usados, esto incluye archivos en servidores como por ejemplo correo electrónico y páginas web, estas revisiones y actualizaciones se las debe realizar bajo procedimientos que se deben establecer.

---

[13] Objetivo tomado de: Norma ISO 27002, Código para la práctica de la gestión de la seguridad de la información 2005, pág.71.
[14] Párrafo tomado de: Norma ISO 27002, Código para la práctica de la gestión de la seguridad de la información 2005, pág. 71

1.1.10.2.2. Controles contra el código móvil

Cabe indicar que código móvil hace referencia a cualquier middleware y que es transferido a través de la red o por un medio de almacenamiento y no es ejecutado explícitamente localmente por el usuario.

Para una ejecución segura y controlada de código móvil autorizado se debe tener una política clara en la cual se involucre tanto al hardware y software donde se ejecutará el mismo, además la red que es el principal medio por el cual se realizara el intercambio de dicho código.

1.1.10.3. Gestión de la seguridad de redes

Objetivo

Garantizar la protección de la información en las redes y la protección de la infraestructura de apoyo. [15]

Para la gestión de la seguridad de la información se requiere que la información que está siendo procesada, almacenada y transmitida sea protegida, esto implica tener apoyo de la máxima autoridad de la organización con el fin de determinar el o los requerimiento de aseguramiento de la información.

1.1.10.3.1. Controles de red

Hace referencia a la administración, monitoreo de los elementos de red excluyendo a los computadores, ya que el control para estas consta dentro de otro dominio de la norma.

[15] Objetivo tomado de: Norma ISO 27002, Código para la práctica de la gestión de la seguridad de la información 2005, pág.75.

Establecer controles para asegurar la confidencialidad, integridad y disponibilidad de la información tanto sobre la red sobre la cual se transmite la información como sobre la infraestructura en la cual están incluidos servidores, servicios e información almacenada

Establecer controles para proteger la información cursada sobre redes públicas como por ejemplo Internet, así como también controles sobre las redes inalámbricas las cuales actualmente son las más usadas.

1.1.10.3.2. Seguridad de los servicios de red

Identificar requerimientos que debe cumplir el proveedor (interno o externo) del servicio es fundamental en las organizaciones ya que a partir de este se realizan acuerdos o contratos.

Los requerimientos para los servicios pueden ser, características de seguridad, niveles de servicio, administración de los requerimientos, entre otros. De igual manera poder acordar auditarías con el fin de constatar que los acuerdos o contratos estén cumpliéndose.

1.1.10.4. Intercambio de información

Objetivo

Mantener la seguridad de la información y del software intercambiado dentro de una organización y con cualquier entidad externa. [16]

1.1.10.4.1. Políticas y procedimientos de intercambio de información

[16] Objetivo tomado de: Norma ISO 27002, Código para la práctica de la gestión de la seguridad de la información 2005, pág. 79.

Generar políticas y procedimientos en esencia para proteger la confidencialidad e integridad de la información (voz, datos, video) extremo-extremo haciendo uso de métodos de encriptación, además determinará el uso de las redes inalámbricas en el sentido de su uso, para transmitir/recibir información o software, además se puede usar el Control Contra Código Malicioso como complemento para el aseguramiento.

Campaña informativa al usuario para informarle las posibles amenazas a las que está expuesto sino sigue los procedimientos, políticas al momento del intercambio de información, aún más si ésta tiene algún tipo de clasificación.

La creación de estas políticas se debe apoyarse en reglamentos, decretos u otro instrumento legal vigente.

1.1.10.4.2. Mensajería electrónica

Toda información transportada que hace uso de servicios internos como por ejemplo correo electrónico corporativo y que puede ser accesible desde redes públicas (Internet), se debe proteger la Confidencialidad, Integridad, Disponibilidad, además debe ser confiable par evita que se use otro tipo de servicio de mensajera público.

Los sitios de comparación de archivos como dropbox, box, yousendit, etc, por ser servicios en redes públicas se debe regular su uso.

Se debería hacer uso de herramientas corporativas para el intercambio de información.

1.1.10.5. Requerimiento de la organización para el control de acceso

Objetivo[17]

[17] Objetivo tomado de: Norma ISO 27002, Código para la práctica de la gestión de la seguridad de la información 2005, pág.94.

Controlar el acceso a la información.

1.1.10.5.1. Política de control de acceso

La política debe cubrir los requerimientos de seguridad de la organización, es decir que se debe definir quién o quienes tienen acceso a que, a donde y que nivel de acceso.

Para definir la política se debe tener claro qué aplicaciones, servicios, etc. brinda la organización.

1.1.10.6. Administración del acceso del usuario

Objetivo[18]

Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información.

Definir un procedimiento para designar los derechos de acceso a los servicios y sistemas de información.

1.1.10.6.1. Administración de Privilegios

Controlar y restringir el uso de privilegios de los usuarios (Usuario Final y Administradores de Sistemas). Se deber asignar los niveles de privilegios solo en la premisa de “solo lo que necesita conocer”

La asignación de privilegios debe estar acompañado de un proceso de autorización formal de dichos privilegios.

---

[18] Objetivo tomado de: Norma ISO 27002, Código para la práctica de la gestión de la seguridad de la información 2005, pág.96.

1.1.10.7. Responsabilidades de usuario

Objetivo

Prevenir el acceso a usuarios no autorizados para evitar comprometer la información incluso de los sistemas de procesamiento.[19]

El usuario que juega un papel muy importante en el aseguramiento de la información debe tener clara sus responsabilidades; de tal manera que los riesgos en la confidencialidad, integridad, disponibilidad de la información disminuyan.

Cabe indicar que el termino usuario hace referencia al usuario final como a los usuarios administradores.

1.1.10.7.1. Uso de contraseñas

Establecer un estándar de la composición de contraseñas, es decir en longitud, frase fácil de recordar, tipo de caracteres a usarse, además determinar procedimientos para el mantenimiento de contraseña es decir, cambio y restablecimiento. Sobre todo mantener el principio de confidencialidad.

1.1.10.7.2. Equipo de usuario desatendido

Definir procedimientos con el fin de indicar al usuario sobre el aseguramiento del dispositivo o los dispositivos a su cargo, al momento de terminar una tarea, terminar la jornada laboral o dejar su puesto de trabajo por cualquier motivo.

1.1.10.7.3. Política de puesto de trabajo despejado y pantalla limpia

[19] Objetivo tomado de: Norma ISO 27002, Código para la práctica de la gestión de la seguridad de la información 2005, pág.100.

Aunque no se ha tocado el dominio en el que se hace referencia a la clasificación de información y a pesar que este control sea un complemento de dicho dominio, se podría crear lineamientos enfocados a áreas específicas donde se maneja documentación sensible.

1.1.10.8. Control de acceso a la red

Objetivo

Prevenir el acceso no autorizado a los servicios de red.[20]

Garantizar el principio de confidencialidad hacia las redes y servicios interno desde redes privadas o públicas en función de las necesidades de las otras organizaciones.

1.1.10.8.1. Política de uso de los servicios de red

Identificar redes, servicios de red usadas en la organización debería ser lo primordial.

Tanto para las redes y servicios se deben generar procedimientos de autorización para el acceso a estos, dependiendo de las necesidades de los usuarios.

Se debe definir procedimientos para la conexión a la red y acceso servicios corporativos desde redes públicas como por ejemplo Internet o desde otras redes privadas, para evitar

1.1.10.8.2. Autenticación de usuario para conexiones externas

[20] Objetivo tomado de: Norma ISO 27002, Código para la práctica de la gestión de la seguridad de la información 2005, pág.103.

Usar VPN para el acceso desde redes externas ya que este mecanismo brinda varios métodos de autenticación que conjuntamente con un sistema de autenticación baso en usuario y contraseña brindará seguridad sobre redes externas.

La política se debe extender a las páginas web publicadas que brindar algún tipo de servicio y que requiere autenticación para su uso.

Definir controles de autenticación para las redes inalámbricas tanto para usuarios internos como externos.

1.1.10.8.3. Identificación de los equipos en las redes

Es primordial identificar la conexión del equipo para poder determinar ubicación del mismo dentro de la red LAN o WLAN.

Para lograr aquello habría que definir algún método de identificación de dispositivos y complementar con el monitoreo, con el fin de proteger redes de alta sensibilidad. Se debe tomar en cuenta la diversas de marcas comerciales y tipo de dispositivo.

Hay que tomar en cuenta que el termino equipo no solo se refiere a dispositivos de usuarios finales sino que también a otros equipos que pertenecen un Data Center.

1.1.10.8.4. Protección del puerto de diagnóstico y configuración remota

Generar una política que proteja los puertos lógicos de acceso a consolas de administración de sistemas o servicios que forman parte de la infraestructura de red de la organización, proteger el acceso desde redes internas y/o externas.

Definir el manejo de puertos físicos de los dispositivos que forman parte de infraestructura de red de la organización para evitar accesos no autorizados.

1.1.10.8.5. Segregación de las redes.

La segregación se la debe realizar a nivel macro como micro, a nivel macro segregar la red en varios dominios como Intranet, Extranet, Internet, DMZ y a nivel micro usar las funcionalidad de los dispositivos de conectividad como Switches para segregar la red en VLANs (LAN Virtuales) y ACLs (Listas de acceso). Cabe indicar que realizar la segregación depende de los requerimientos de seguridad de la información o definir qué tipo de información se requiere proteger y en qué áreas.

Para que asegurar la información que fluye entre dominios se requiere de un dispositivo que los interconecte, de tal manera se proteja el principio de confidencialidad.

De igual mera definir un tipo de segregación para la red WLAN ya que esta puede tener más vulnerabilidades al memento del acceso a ella.

1.1.10.8.6. Control de la conexión a la red

El acceso a redes compartidas, entendiendo como red compartida a la Internet, se debe restringir el acceso a los usuarios basando en sus derechos de acceso los cuales se deben revisar de manera continua.

Se debe definir a qué tipo de aplicaciones en redes compartidas el usuario está permitido acceder, y para dar cumplimiento se debe implementar un gateway de seguridad para determinar las conexiones que sí están permitidas.

1.1.10.8.7. Control de ruteo de red

Determinar controles de enrutamiento para evitar que el flujo de información generada desde un origen autorizado llegue a su destino.

Dispositivos par seguridad de perímetro se debe implementar para el control el flujo de tráfico, es decir controlar su origen y destino.

1.1.10.9. Control de acceso al sistema operativo

Objetivo

Evitar el acceso no autorizado al sistema operativo.[21]

1.1.10.9.1. Procedimiento seguro de inicio de sesión

Definir procedimientos seguros de inicio de sesión en los dispositivos de usuario y de los administradores de los sistemas, haciendo uso de los sistemas de seguridad existentes.

Los sistemas de seguridad de inicio de sesión deberían realizar auditoria, monitoreo en tiempo real, contención en caso de violación de políticas y una configuración granular para determinar numero intentos de inicio, tiempos para el inicio de sesión, permitir la transmisión de la clave de inicio de sesión de manera encriptada.

A continuación se define la relación cruzada entre CIA y los controles que serán utilizados.

Controles ISO 27002	Confidencialidad	Integridad	Disponibilidad
Protección contra código malicioso		✓	
Protección contra código móvil		✓	
Controles de red	✓	✓	✓

[21] Objetivo tomado de: Norma ISO 27002, Código para la práctica de la gestión de la seguridad de la información 2005, pág.109.

Seguridad de los servicios de red	✓		✓
Mensajería electrónica	✓	✓	
Política de control de acceso	✓		
Gestión de Privilegios	✓	✓	
Uso de contraseñas	✓		
Equipo de usuario desatendido	✓	✓	
Política de puesto de trabajo despejado y pantalla limpia	✓	✓	
Política del uso de los servicios de red	✓		✓
Autenticación del usuario para conexiones externas	✓	✓	
Identificación de los equipos en la red			✓
Protección del acceso remoto	✓		
Segregación de redes	✓		✓
Control de conexión a la red	✓	✓	

Control de ruteo	✓	✓	✓
Procedimiento seguros de inicio de sesión	✓		

Tabla 1.14. Referencia cruzada entre CID y controles ISO 27002

CAPÍTULO II

2.1. INTRODUCCIÓN A LA GESTIÓN Y ANÁLISIS DE RIESGO Y SUS METODOGIAS

En la actualidad, la tecnología está avanzado rápidamente y con ello la aparición de nuevas amenazas y sofisticados ataques que hacen que la seguridad de la información sea una prioridad en las organizaciones en especial las gubernamentales.

Las regulaciones y leyes acerca de la seguridad de la información hacen que la gestión de riesgos se convierta en un proceso indispensable en una organización. Uno de los objetivos de la gestión de riesgo es poder tomar las mejores decisiones al momento de proteger los activos de información y mantener los riesgos a un nivel aceptable.

En el campo de la seguridad de la información las mejores prácticas podrían ser un problema para la toma de decisiones, ya que no todas las organizaciones tienen la misma misión o los mismos objetivos estratégicos, por tal razón con la gestión de riesgos de seguridad de la información se tomarían decisiones más adecuadas.

Además, con la gestión de riesgo también se evita que en la equivocación de únicamente enfocarse en el aseguramiento el perímetro.

Previo al estudio de la gestión y análisis de riesgo es importante conocer varias definiciones importantes en el campo de la gestión del riesgo de la seguridad de la información.

2.1.1. DESAFÍOS DE LA SEGURIDAD DE LA INFORMACIÓN

2.1.1.1. Mezcla de vidas personales y corporativas

El desafió inicia cuando la diferencia entre la vida personal y corporativa es difícil distinguirla. En ocasiones servicios, PC, teléfonos, o cualquier otro dispositivo corporativos son usados para fines personales. Como ejemplo el uso de un teléfono celular asignado por la institución para realizar llamadas personales.

2.1.1.2. Aplicación incoherente de políticas

En algunas organizaciones la política no se aplica o se aplica de manera incorrecta en función de la posición del empleado, es decir la política se mueve al rededor del empleado. Por ejemplo limitar el acceso a redes sociales a un área de comunicación.

2.1.1.3. El área de TI no posee y controla todos los dispositivos

Este desafío hace referencia al uso de dispositivos personales en ambientes corporativos, ya que si un empleado requiere un dispositivo móvil corporativo y no lo tiene este opta por usar su dispositivo personal para desarrollar sus actividades normales. Además, dependiendo de las leyes, reglamentos, etc., será complicado realizar auditorías sobre estos dispositivos. Un ejemplo es aplicar BYOD (Bring Your Own Device).

2.1.1.4. Accesos internos versus remotos

Anteriormente el acceso dentro o hacia la red era controlado de la manera más estricta, pero ahora el perímetro es compartido con socios “estratégicos” los cuales proveen servicios de hosting, etc. Además el acceso remoto haciendo uso de una VPN en una PC personal. El crecimiento de la Cloud sería un buen ejemplo.

2.1.1.5. Ataques encubiertos ya no son evidentes

Ahora los atacantes son silenciosos y cautelosos, y así poder robar información o tener el control de los dispositivos para atacar a alguien más. El cibercrimen como ejemplo.

2.1.1.6. Blanco móvil

Se refiere a los ataques sofisticados que se crean para evitar los controles, esto siempre se dará.

2.1.2. DEFINICIONES FUNDAMENTALES

2.1.2.1. ¿Qué es el riesgo?

Es la combinación de la probabilidad de un evento y sus consecuencias.[22]

2.1.2.2. La definición de riesgo enfocada a la seguridad de la información

Una vez tratado los pilares se la Seguridad de la Información en el capítulo I, y dada la definición de riesgo, se puede obtener una definición sobre el riesgo enfocada de la seguridad de la información.

Hay que tener presente que la seguridad de la información es la vía para mantener en un nivel aceptable el riesgo expuesto de la organización, sin restringir indebidamente el crecimiento del negocio.

[22] Tomado de: Noma ISO 27002, Código de práctica para de la gestión de la seguridad de la información 2005, pág. 2.

Por lo tanto la seguridad de la información es todo acerca de la gestión de riesgos de la información sensible y recursos críticos.[23]

La seguridad de la información mantiene en niveles aceptables el riesgo que contribuye a la perdida de Confidencialidad, Integridad y Disponibilidad de la información sensible y de los recursos críticos de la organización.

El riesgo es la probabilidad de que una amenaza explote la vulnerabilidad de un activo causando perdida de confidencialidad, integridad o disponibilidad del activo.

2.1.2.3. Gestión de riesgo

Es el costo de identificar, controlar y minimizar el impacto de eventos inciertos, de tal manera que los riesgos lleguen niveles aceptables. Además la gestión de riesgo por ser un proceso del negocio debe ser continuo.

2.1.2.4. Evaluación de riego

Es la estimación del riesgo en base a un análisis de riesgo.

2.1.2.5. Análisis de riesgo

Es un proceso que involucra varias actividades sobre los activos de información para disminuir los niveles de riesgo.

Se definen dos tipos de análisis de riesgo cualitativo y cuantitativo, pero en definitiva el objetivo del análisis es dar un valor al riesgo para poder disminuirlo, entendiendo como riesgo a la probabilidad de que una amenaza explote la vulnerabilidad de un activo causando perdida de confidencialidad, integridad o disponibilidad del activo.

[23] Traducción textual de: Evan Wheeler, Security Risk Managment, pag.22.

2.1.2.6. Tratamiento de riesgos

El tratamiento del riesgo se lo realiza como parte final del análisis de riesgo, es decir una vez identificado los niveles de riesgo de los activos de información se define qué hacer con esos niveles. Hay cuatro opciones para tratar el riesgo.

2.1.2.6.1. Aceptar

La decisión de aceptar los niveles de riesgo y convivir con ellos.

2.1.2.6.2. Evitar

Dejar de realizar la actividad que produce los niveles de alto riesgo.

2.1.2.6.3. Transferir

Desplazar la responsabilidad del riesgo a un tercero

2.1.2.6.4. Mitigar

Disminuir el riesgo a un nivel aceptable, implementado controles y definiendo políticas.

2.1.2.7. Amenazas

Como se revisó anteriormente las amenazas en el contexto de los riesgos de seguridad de la información describe la fuente de un ataque tomando en cuenta que un ataque también son acciones no intencionadas.

La fuente de amenaza es diferente a las consecuencias, por tal razón al momento de describir una fuente de amenaza hay que hacerlo no pensando en las

consecuencias. Además hay que tener en cuenta que en cualquier organización la misma fuente de amenaza puede contener varias consecuencias.

Las amenazas se componen de tres factores localización, agente, motivación[24].

2.1.2.7.1. Localización

Determina el origen de una amenaza es decir si es interna o externa a la organización.

2.1.2.7.2. Agente

Es que o quien causa la amenaza, y se lo ha clasificado en agentes humanos, agentes ambientales, agentes tecnológicos, estos últimos son producidos por procesos físicos o químicos en el material tecnológico.[25]

- **Cibercriminales**

  Son grupos altamente organizados con el objetivo de obtener ganancia de actividades ilegales en el ciberespacio, para ello cuentan con gran equipamiento y conocimiento tecnológico, la motivación es realizar inteligencia y monetización.

  Al contar con una gran infraestructura tecnología, los cibercriminales venden sus actividades ilegales como servicio, además sus actividades se enfocan en los sectores de financias electrónicas, comercio electrónico, pago electrónico, desarrollo y entrega herramientas maliciosas.

  Estos grupos tienen gran recurso financiero por las actividades ilegales a las que se dedican y para poder mover el recurso financiero utilizan las monedas virtuales, anonimato y cifrado, todo esto en el mercado negro.

---

[24] ENISA Threat Landscape 2014, www.enisa.europa.eu
[25] Definición traducida textualmente de: Information Security Society Switzerland, Threat Modeling in Security Architecture. Pág 3.

- **Online Social Hackers**

Este tipo de agentes despliegan las amenazas, son expertos con conocimiento de ingeniería social y están en capacidad de analizar y entender la psicología del objetivo.

Además son expertos en el análisis de la información de la ingeniería social realizada tratando de violar la privacidad del objetivo. Estos grupos sin tener una gran infraestructura pueden ocasionar un gran impacto en la privacidad al suplantar la identidad de la víctima.

- **Hacktivistas**

Son grupos que los mueve los motivos políticos, su objetivo es influir en la toma de decisiones políticas. La motivación es la justicia social, No tienen una estructura definida ya que dependiendo de su ideología pueden formar grupos o subgrupos.

La manera de mostrar su ideología política es cuando hay una actividad que atrae la atención mundial. Los ataque delegados son DDoS, defacement, hacking y los principales objetivos son sitios de gobierno, grandes compañía, infraestructura pública y privada. Además lo hacen la llamar la atención de los medio de comunicación.

- **Estados-nación**

Grupos de inteligencia y contra inteligencia que realizan actividades hostiles particionados por países donde se encuentran estos grupos. Estos grupos han participado en ataques cibernéticos con el fin de extraer información confidencial de algún país.

La motivación de este grupo es obtener secretos de estado, secretos militares, información de inteligencia y amenazar la disponibilidad de las infraestructuras críticas.

- **Corporaciones**

Grupos de enfocados al ciberespionaje industrial, Su objetivo es sustraer resultados de investigaciones, análisis, ideas de innovación entre otras, en algunos casos este ciberespionaje es particionado por países. Las consecuencias es el robo de propiedad intelectual y altos costos para la industria.

- **Empleados (internos, externos, actuales y ex)**

Pertenecen a este grupo empleados, contratistas y exempleados, estos pueden materializar las amenazas como la violación de datos. La materialización de estas amenazas pude ser intencionales o no intencionales. La motivación la extorción, el sabotaje, la venganza, o el beneficio.

- **Ciberluchadores**

Son grupos de ciudadanos que tiene un gran sentimiento por sus valores políticos, nacionales o religiosos, que si son amenazados pueden lanzar algún tipo de ataque, similares a los Hacktivistas, pero la diferencia es que los Ciberluchadores son partidarios de ciertos regímenes políticos en tanto que a los Hactivistas los mueve la justicia social.

- **Ciberterroristas**

Grupos que sus objetivos son los sabotajes a gran escala para dañar a un Estado o sociedad afectando su infraestructura critica, los caracteriza el uso indiscriminado de la violencia para influir en decisiones.

- **Script Kiddies**

Individuos jóvenes fanáticos en especial de los hacktivistas, son considerados como un agente de amenaza ya que tienen fácil acceso a herramientas

maliciosas y no tienen el conocimiento técnico, esta combinación podría causar un gran impacto en algún tipo de ataque de prueba.

2.1.2.7.3. Motivación

Identifica por qué la amenaza es creada, en decir accidental o deliberado.

2.1.2.7.4. Consecuencias

Dependiendo del agente y motivación puede existir una o varias consecuencias.

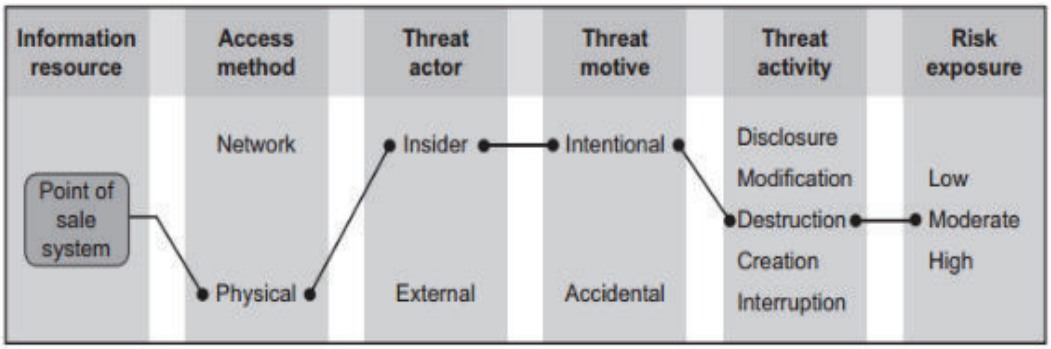

Figura 2.1.1. Flujo de análisis de amenazas

Fuente: Evan Wheeler, Security Risk Management

El análisis de la amenaza comienza identificando el activo de información, su método de acceso, el tipo de agente, la motivación, la consecuencia y al final se define el nivel de exposición de riesgo.

En la Fig. 2.2 se resumen los tipos de agentes de amenazas.

Las empresas proveedores de equipos de seguridad y organizaciones sin fines de lucro al menos cada semestre publican informes sobre la tendencia de las amenazas a nivel mundial, como por ejemplo los que se muestran en la Tabla 2.1.

EMPRESAS DE SOLUCIONES DE SEGURIDAD INFORMÁTICA	ENTIDADES SIN FINES DE LUCRO
CHECKPOINT	CERT
WEBSENSE	NIST
SYMANTEC	ENISA

Tabla 2.11. Resumen de entidades que ofrecen seguridad informática.

2.1.2.7.5. Código Malicioso

El código malicioso se ha incrementado gracias a la distribución de paquetes de software gratuitos llamados PUPs (Potentially Unwanted Programs). Además debido a su sofisticación, complejidad al menos el 50 % del malware no es detectado por un producto de antivirus.

Ambientes libres son el paraíso de las infecciones por malware, es decir que no hay al menos una protección perimetral o de punto final.

- **Gusanos**

  Son programas maliciosos que tienen la capacidad o habilidad de repicarse y redistribuirse por ellos mismo mediante explotación de vulnerabilidades.

  El gusano más común detectado en las redes corporativas es Confiker, a pesar de que son 6 años de su aparición.

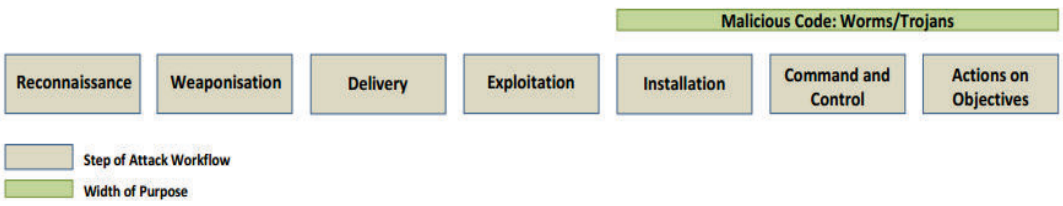

Figura 2.1.2. Pasos de ataque de código malicioso

Fuente: ENISA, Threat Landscape 2013, 2014.

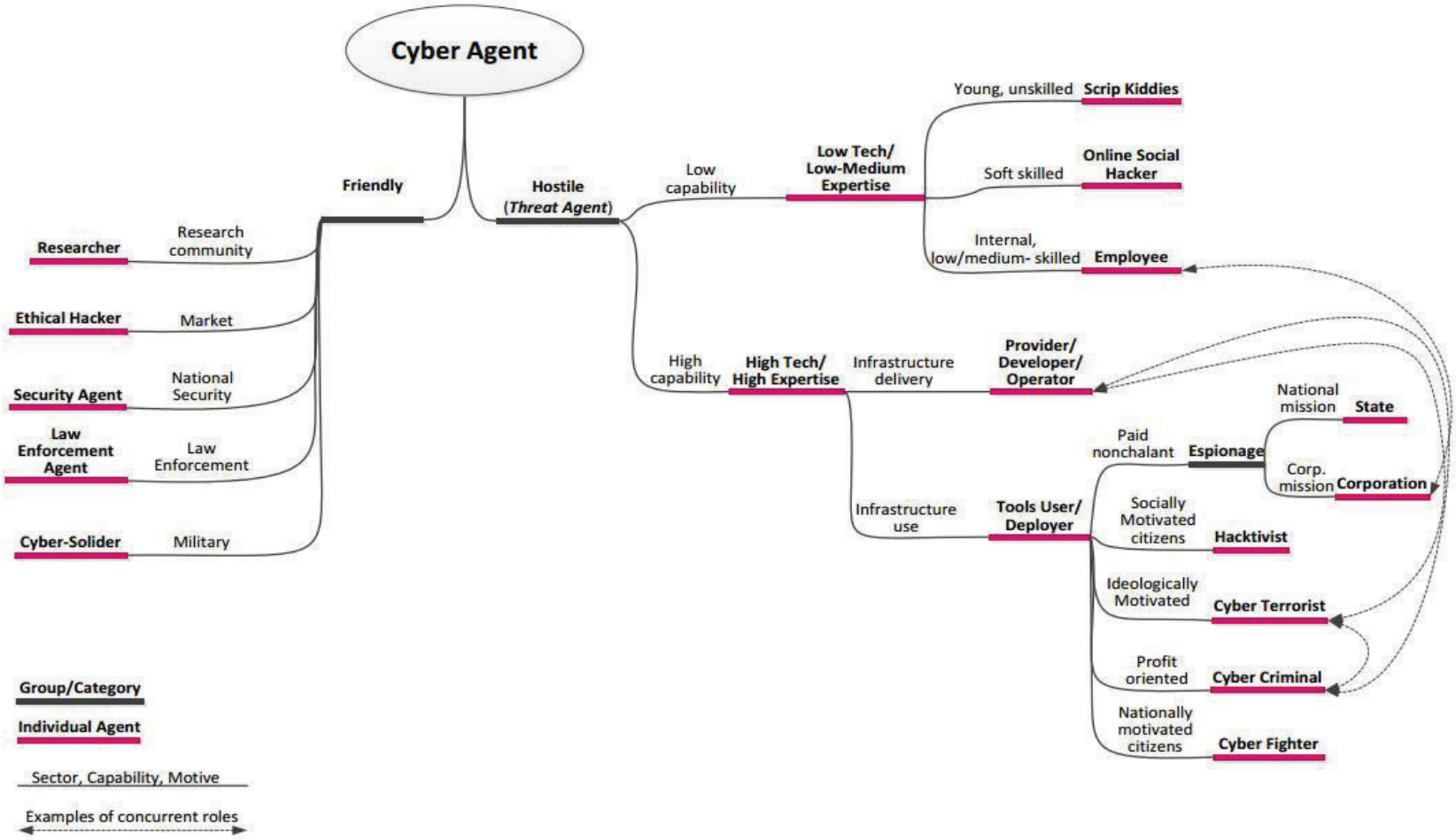

Figura 2.1.3. Agentes de amenazas de tipo humano

Fuente: ENISA, Threat Landscape 2014

- **Troyanos**

  Son programas maliciosos que son sigilosamente inyectados en los sistemas y/o dispositivos de usuarios, tiene la habilidad de actuar como puerta trasera para tomar el control remoto del sistema o dispositivo de usuario, otra habilidad es sustraer información del usuario y sus credenciales. Ejemplo RATs (Remote Acces Trojans). A continuación se representa el flujo de ataque que realiza esta amenaza.

La Fig. 2.3 define el flujo de ataque que inicia con la instalación y luego la ejecución de comandos de control para una tarea específica.

2.1.2.7.6. Ataques basados en WEB

Esta amenaza hace uso de técnicas de redirección de navegadores web a sitios maliciosos para explotar sus vulnerabilidades, cabe indicar que esta amenaza en primera instancia compromete a un sitio web verdadero para realizar dicha redirección. Los usuarios del sitio web comprometido son redireccionados al sitio malicioso para que algún tipo de malware sea instalado. A continuación se representa el flujo de ataque que realiza esta amenaza.

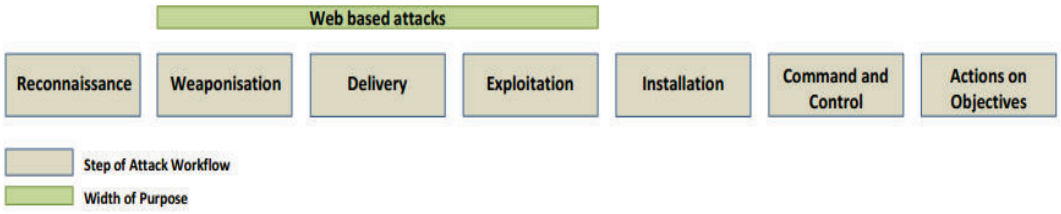

Figura 2.1.4. Flujo de ataques web

Fuente: ENISA, Threat Landscape 2013, 2014.

Su flujo de ataque inicia adquiriendo el malware, luego la entrega y termina aprovechándose de las vulnerabilidades.

2.1.2.7.7. Ataque a aplicaciones web

Consiste principalmente en alimentar servidores vulnerables con entradas maliciosas o secuencias de eventos inesperados con el objetivo de inyectar código malicioso, algunos ejemplos son[26]:

- **SQLi (SQL injection)**

  Consiste en inyectar una consulta SQL en la entrada de usuario de una aplicación web, una inyección de SQL exitosa podría tener acceso al DBMS y realizar comandos como insert, update o delete.

- **XSS (Cross Site Scripting)**

  Es un tipo de ataque a la aplicación web, en la cual se inyecta scripts mal intencionados en sitios web de confianza.

- **SSI (Server Site includes)**

  SSI son directivas presentes en aplicaciones web usadas para alimentar una página en HTML con contendido dinámico. SSI es usado para ejecutar acciones antes de que la página se cargue o mientras la página es visualizada.

A continuación se representa el flujo de ataque que realiza esta amenaza.

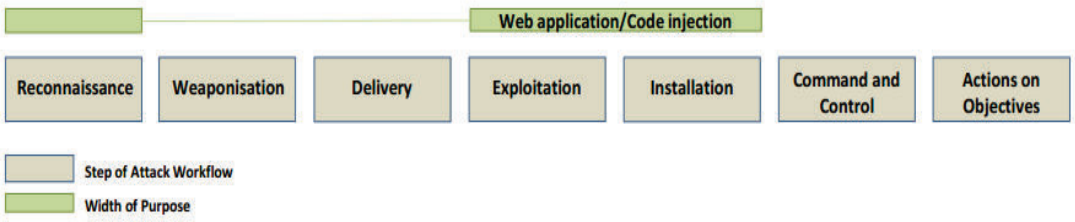

Figura 2.1.5. Flujo de ataque a aplicaciones web e inyección de código

Fuente: ENISA, Threat Landscape 2013, 2014.

[26] OWASP, www.owasp.org

Este tipo de amenazas inician con el reconocimiento de la aplicación web, como un escaneo de puertos, continúa con la instalación de código malicioso para poder explotarlo.

2.1.2.7.8. Bonets

Es un conjunto de computadores comprometidos los cuales están bajo el control del atacante, cada computador comprometido es llamado zombie. Bots tienen múltiples usos, uno de es ser usado como spamming, distribuidor de malware, DoS, etc.

Actualmente los Bots an evolucionado ya que no se usa PCs sino servidores web ya que tiene mejor performance que varios de PCs, este es llamado Botnet-Web-Based. A continuación se representa el flujo de ataque que realiza esta amenaza.

Figura 2.1.6. Flujo de ataque de Botnets

Fuente: ENISA, Threat Landscape 2013, 2014.

Los bots ejecutan rutinas de comandos y control sobre el dispositivo vulnerado.

2.1.2.7.9. DoS/DDoS

La denegación de servicio es intentar hacer que un recurso o servicio no esté disponible para el usuario.

La denegación de servicio distribuido es la denegación de servicio realizado desde varios puntos simultáneamente, usualmente es realizada desde una botnet. Principalmente objetivo de ataques son HTTP, DNS, SMTP.

Los método como la inundación por ICMP, UDP o SYNC floods están desapareciendo y dando paso a métodos enfocados a las capas 3, 4 y 7. A continuación se representa el flujo de ataque que realiza esta amenaza.

Figura 2.1.7. Flujo de ataque de DoS

Fuente: ENISA, Threat Landscape 2013, 2014.

El flujo de ataque inicia con el reconocimiento, adquisición de software malicioso, para poder ejecutar sentencias de comando y control al objetivo identificado.

Este tipo de amenaza realiza un reconocimiento sobre un objetivo específico y poder ejecutar rutinas de comandos y control.

2.1.2.7.10. SPAM

Es el uso abusivo de la tecnología de correo electrónico al inundar los buzones de usuarios con mensajes no solicitados.

Los temas usados en él envió de spam son; depósito bancario, notificaciones de pago, compra de productos vía online, foto adjunta, noticias de viajes, citas online, impuestos, Facebook, gift card, PayPal, etc. A continuación se representa el flujo de ataque que realiza esta amenaza.

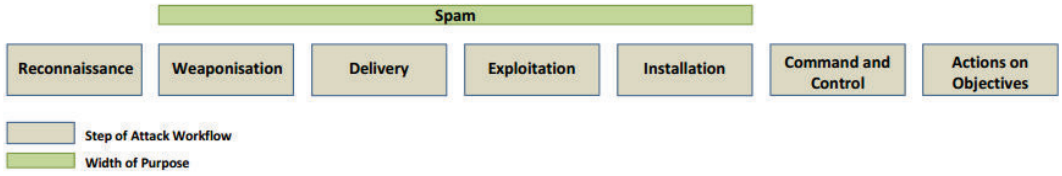

Figura 2.1.8. Flujo de SPAM

Fuente: ENISA, Threat Landscape 2013, 2014.

El flujo de este ataque inicia con adquisición de software malicioso entrega de este software continua con la explotación y la instalación de este software.

2.1.2.7.11. Phishing

Es la combinación de correos electrónicos falsificados y sitios web no legítimos, el objetivo es obtener de manera engañosa credenciales de usuarios. Se ha uso de ingeniería social para engañar y poder obtener dichas credenciales. A continuación se representa el flujo de ataque que realiza esta amenaza.

Figura 2.1.9. Flujo de Pishing

Fuente: ENISA, Threat Landscape 2013, 2014.

Inicia con el reconocimiento del objetivo, conseguir el software malicioso y termina con la entrega. La mayor parte de las ocasiones la entrega se realiza a través del ataque de spam.

2.1.2.7.12. Exploit kits

Es una herramienta importante de fuente de amenaza, que contiene un paquete programas maliciosos para automatizar el cibercrimen, usado primicialmente para explotar la amenaza de ataques basados en web.

No se requiere poseer conocimientos técnicos para poder utilizarlo, en algunos casos se puede contratar a través de internet convirtiéndolo en MaaS (Malware as a Service). Algúnos ejemplos de exploit kits Neutrino, Redkit, SweetOrange, Styx,

Galzunov/Sibhost, Nuclear, Blackhole/Cool y Angler. A continuación se representa el flujo de ataque que realiza esta amenaza.

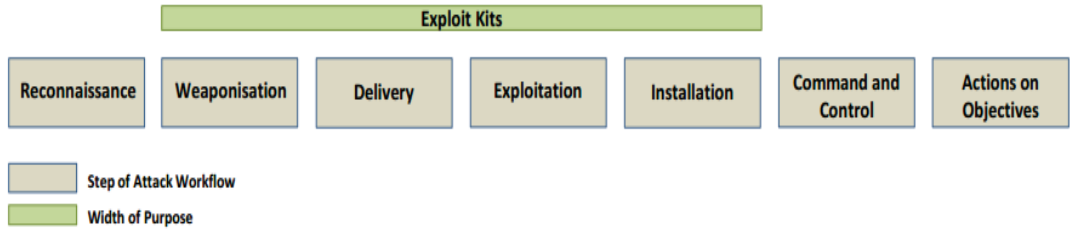

Figura 2.1.10. Flujo de los exploits kits

Fuente: ENISA, Threat Landscape 2013, 2014.

Inicia con la adquisición de software malicioso, luego se realiza la entrega para la explotación y termina con la instalación.

2.1.2.7.13. Violaciones de datos

Es la consecuencia de un ataque exitoso materializando algún tipo de amenaza o de error humano en el manejo de la información. El robo y divulgación de información personal no es el único objetivo sino también en sectores de gobierno, multimedia financiero, etc. A continuación se representa el flujo de ataque que realiza esta amenaza.

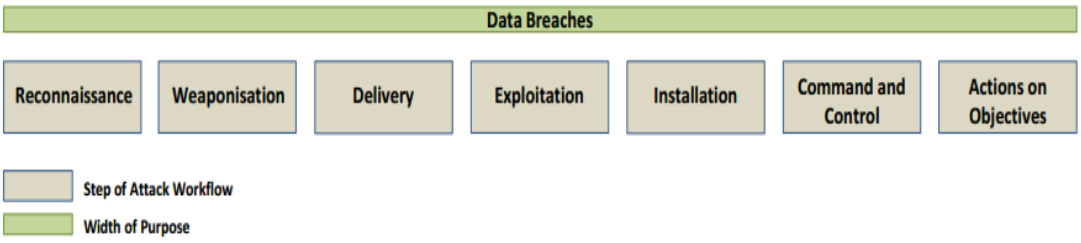

Figura 2.1.11. Flujo de Violaciones de datos

Fuente: ENISA, Threat Landscape 2013, 2014.

El flujo de ataque involucra a todas las fases ya que el mismo se ha materializado.

2.1.2.7.14. Daño físico, robo o pérdida

Hace referencia al daño, robo o pérdida de un dispositivo del usuario final o activo de información, aunque como tal el dispositivo se pierde, la información que contiene es mucha más importante que dicho dispositivo. A continuación se representa el flujo de ataque que realiza esta amenaza.

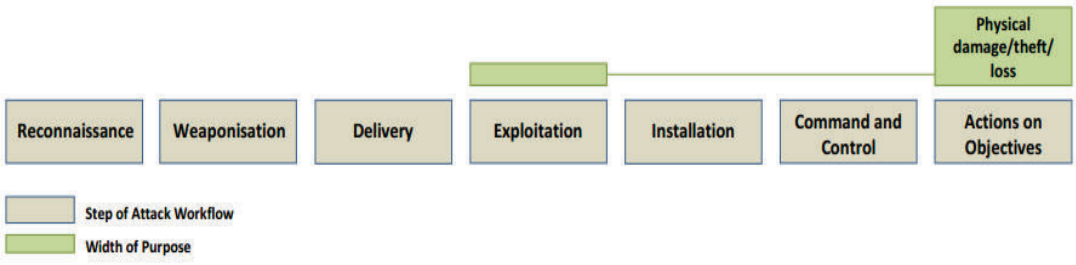

Figura 2.1.12. Flujo de daño físico

Fuente: ENISA, Threat Landscape 2013, 2014.

El flujo de ataque involucra la explotación de vulnerabilidades de objetivos específicos para acusar daño robo o pérdida de la información.

2.1.2.7.15. Amenazas internas

Pueden ser actividades maliciosas de un usuario interno, errores no intencionales, pérdida o robo involuntario de la información.

Este tipo de amenazas son principalmente enfocadas a entidades gubernamentales y militares. A continuación se representa el flujo de ataque que realiza esta amenaza.

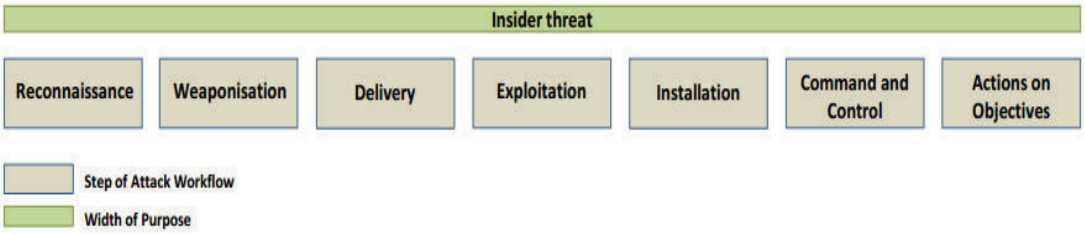

Figura 2.1.13. Flujo de las amenazas internas

Fuente: ENISA, Threat Landscape 2013, 2014.

En este tipo de ataque se puede identificar que todos los pasos están involucrados, esto quiere decir que la amenaza fue materializada generando un tipo de impacto.

2.1.2.7.16. Fuga de Información

Es la explotación de las debilidades técnicas y corporativas con el objetivo de obtener información que será usada en otros tipos de ataques. Un ejemplo es Heartbleed. A continuación se representa el flujo de ataque que realiza esta amenaza.

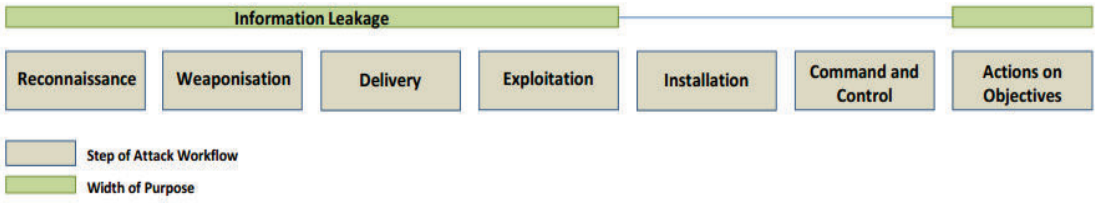

Figura 2.1.14. Flujo de fuga de información

Fuente: ENISA, Threat Landscape 2013, 2014.

El flujo de ataques inicia con el reconocimiento y adquisición de software malicioso, realizar la entrega para la explotación sobre el objetivo identificado.

2.1.2.7.17. Robo de identidad

Principalmente está enfocada a la recolección de PII (Información de Identificación Personal) como numero de CI, numero de cuentas, claves de acceso, etc. Para obtener PII se utilizan herramientas específicas.

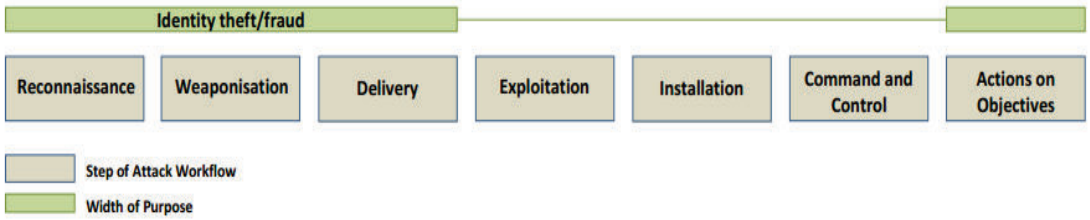

Figura 2.1.15. Flujo de robo de identidad y fraude

Fuente: ENISA, Threat Landscape 2013, 2014.

Inicia con el reconocimiento, adquisición de software, entrega del mismo y generar acciones sobre el objetivo u objetivos identificados.

2.1.2.7.18. Ciberespionaje

Es la combinación de amenazas revisadas anteriormente, la característica de esta amenaza es que tiene un enfoque táctico y técnico, además el agente utiliza métodos sofisticados de ataque. Esta amenaza afecta más a entidades gubernamentales y a cooperaciones, un ejemplo es el APT (Amenaza Persistente Avanzada) y los ataques dirigidos.

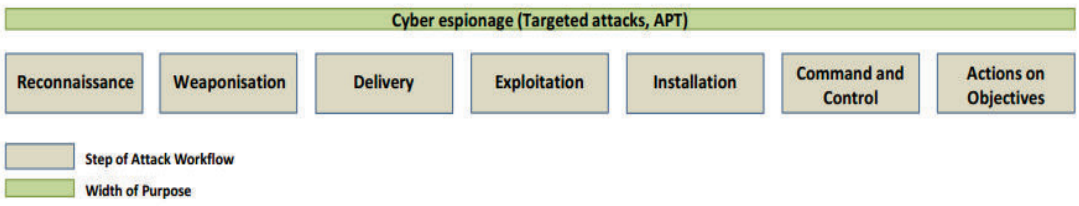

Figura 2.1.16. Flujo del espionaje

Fuente: ENISA, Threat Landscape 2013, 2014

El ciberespionage involucra todos los pasos ya que combina todas las amenazas.

2.1.2.7.19. Otros tipos de malware

- R**asomeware**

Es un tipo de malware que pero por su importancia se lo ha tratado como una amenaza individual, este restringe el acceso al dispositivo y luego pide un rescate para desbloquearlo, ciertos rasomeware cifran la información como por ejemplo CryptoLocker.

- **Rogueware**

Son tipos de malware que se hacen pasar por software de protección para dispositivos de usuario final, con la finalidad de obtener dinero con su venta, información del usuario, etc.

- **Scareware**

Es una técnica empleada en complemento a rogueware, ya que utiliza métodos como ingeniería social para asustar y poder persuadir al usuario que compre el rogueware.

A continuación se representa el flujo de ataque que realiza esta amenaza.

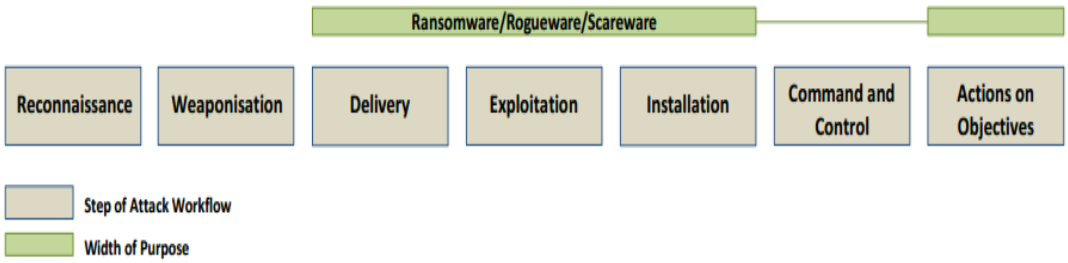

Figura 2.1.17. Flujo de otros tipos de malware

Fuente: ENISA, Threat Landscape 2013, 2014.

Este tipo de ataque inicia con la entrega de software malicioso, luego la explotación e instalación de dicho software.

A continuación se muestra la tendencia de las amenazas entre el 2013 y 2014, donde se puede observar que algunas amenazas han escalado posiciones y otras han disminuido.

La Fig. 2.18 es una estadística de un estudio a nivel mundial realizada por ENISA (European Union Agency for Network and Information Security).

Top Threats 2013	Assessed Trends 2013	Top Threats 2014	Assessed Trends 2014	Change in ranking
1. Drive-by downloads (renamed to Web-based attacks)	↑	1. Malicious code: Worms/Trojans	↑	↑
2. Worms/Trojans	↑	2. Web-based attacks	↑	↓
3. Code Injection	↑	3. Web application /Injection attacks	↑	→
4. Exploit Kits	↑	4. Botnets	↓	↑
5. Botnets	⊃	5. Denial of service	↑	↑
6. Physical Damage/Theft/Loss	↑	6. Spam	↓	↑
7. Identify Theft/Fraud	↑	7. Phishing	↑	↑
8. Denial of Service	↑	8. Exploit kits	↓	↓
9. Phishing	↑	9. Data breaches	↑	↑
10. Spam	⊃	10. Physical damage/theft /loss	↑	↓
11. Rogueware/Ransomware / Scareware	↑	11. Insider threat	⊃	(NA. new threat)
12. Data Breaches	↑	12. Information leakage	↑	↑
13. Information Leakage	↑	13. Identity theft/fraud	↑	↓
14. Targeted Attacks (renamed to Cyber espionage, merged with Watering Hole)	↑	14. Cyber espionage	↑	→
15. Watering Hole (threat consolidated with other threats/attack vector)	↑	15. Ransomware/Rogueware/ Scareware	↓	↓

Legend: Trends: ↓ Declining, ⊃ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Figura 2.1.18. Resumen de amenazas y su tendencia

Fuente: ENISA, Threat Landscape 2014.

2.1.2.8. Vulnerabilidades

A menudo se confunde la evaluación de riesgo con la evaluación de vulnerabilidades. La evaluación de vulnerabilidades es una actividad donde se pretende encontrar o identificar las debilidades o defectos, ésta actividad puede realizarse por medio de un escaneo o a través de ciertas configuraciones.

Con la evaluación de vulnerabilidades se detecta la vulnerabilidad en sí, pero una vulnerabilidad puede estar compuesta de varias amenazas y dando como resultado varios tipos de niveles de riesgo.

La evaluación de vulnerabilidades podría ser incluida como parte de la evaluación de riesgos, ya que al realizar un escaneo sobre el o los activos de información se determinaría de mejor manera los controles para minimizar el riesgo.

Para la evaluación de vulnerabilidades existen varios tipos de herramientas tanto open source como licenciadas, dependiendo del alcance que se la quiera dar, se pude definir cuál es la más conveniente. Algunas de las herramientas se muestran en la Tabla 2.2.

OPEN SOURCE	LICENCIADAS
OSSIM	QUALYSGUARD
OPEN VAS	NESSUS
VEGA(PARA SITIOS WEB)	NEXPOSE
SECURIA(A NIVEL DE USUARIO)	RETINA
NAMP(A NIEVEL DE PUERTOS)	GFI LAN GUARD
SARA	CORE IMPACT
	SAINT

Tabla 2.12. Herramientas para evaluación de vulnerabilidades

2.1.3. TIPOS DE ANÁLISIS DE RIESGO

2.1.3.1. Análisis Cualitativo

Usado más comúnmente por los profesionales de la seguridad, esto porque no hay suficientes datos históricos de ocurrencias para calcular las probabilidades y magnitudes del riesgo. El análisis cualitativo usa escalas aproximadas como por ejemplo (bajo, alto, medio) en base de criterios predefinidos en cada nivel.

El análisis cualitativo provee un examen sistemático de las amenazas y riesgos, y una revisión de contra-medidas y salvaguardas propuestas y determinara el mejor costo-beneficio de la implementación.[27]

En general, un análisis de riesgo debe contener los siguientes pasos.

2.1.3.1.1. Desarrollo del alcance

Determinar la aplicación, el sistema, los datos o el proceso a ser analizada, además identificar al propietario de la aplicación, el sistema, los datos o el proceso, el cual se define como una persona responsable de la gestión para la protección del activo. El alcance debe enfocarse en los procesos que pueden lograrse un cambio.

Desarrollar los objetivos generales del análisis de riesgo, para la seguridad de la información los objetivos normalmente es el impacto de las amenazas en la Confidencialidad, Integridad, Disponibilidad en un proceso determinado. Además definir los objetivos de acuerdo los desafíos que enfrenta la Institución con respecto a la seguridad de la información.

2.1.3.1.2. Determinar el activo de información

[27] Párrafo tomado de: Thomas Peltier, Information security risk analysis, pág. 96.

Un activo es algo que tiene valor para la organización, en el ámbito de la seguridad de la información el llamado activo de información, es la información en forma digital o impresa, y en el caso de la forma digital de la información que se encuentra en almacenamiento, transmisión y procesamiento que tiene valor para la organización.

Un activo de información puede ser un proceso, servicio, aplicación o sistema. El activo de definirá en el alcance del análisis de riesgo.

2.1.3.1.3. Identificación de amenazas

La amenaza generalmente describe la fuente del ataque, entiendo que también puede ser no intencional. Hay que diferenciar entre la fuente de amenaza que potencialmente quien puede dañar al recurso y actividad de amenaza es como el recurso será dañado.

Un origen de amenaza se define como cualquier circunstancia o evento con el potencial de causar daño al activo en revisión. Para la identificación de amenazas se pueden analizar los posibles actores (agentes), motivos y consecuencias como se estudió en la sección de definiciones fundamentales.

2.1.3.1.4. Priorización de amenazas

Una vez que se han identificado las amenazas que pueden afectar a los activos de información, se procede a valorar cuál de estas amenazas tiene mayor probabilidad de ocurrir, por ejemplo se puede utilizar un escala de 1 a 5 donde uno es bajo y 5 alto. A continuación se presenta un ejemplo de niveles de priorización de amenazas.

Bajo	Bajo a Medio	Medio	Medio a Alto	Alto
1	2	3	4	5

Tabla 2.13. Ejemplos de niveles de priorización en el análisis cualitativo del riesgo.

2.1.3.1.5. Impacto de la amenaza

Se estima que impacto tendrán las amenazas con mayor probabilidad de ocurrencia, para ello se define una escala como por ejemplo.

Bajo	Bajo a Medio	Medio	Medio a Alto	Alto
1	2	3	4	5

Tabla 2.14. Ejemplo de niveles de impacto en el análisis cualitativo del riesgo.

2.1.3.1.6. Medidas cualitativas de riesgo

En primer lugar hay que definir escalas de riesgo tanto para la probabilidad de que una vulnerabilidad sea explotada con éxito y la severidad de dicha explotación. Cada par amenaza-vulnerabilidad debe evaluarse por separado ya que cada una va a tener diferente probabilidad y severidad.

En la mayor parte de los casos, los detalles de las amenazas afectaran la tasa de probabilidad y los detalles de la vulnerabilidad afectaran a la tasa de la severidad.

El enfoque cualitativo usa una escala relativa para definir la exposición al riesgo que depende de los criterios predefinidos de cada nivel y además depende de la experiencia y conocimiento del evaluador para aplicar dichos niveles.

2.1.3.1.7. Factores de la exposición al riesgo

Severidad

La severidad es la magnitud de la vulnerabilidad, independiente de la fuente de amenaza y de la sensibilidad del recurso. El nivel de severidad pretende determinar el alcance de la exposición, no una lista de todas las consecuencias.[28]

Se puede definir varios niveles de severidad, ya que mientras más niveles existen más granular se hace la evaluación. Los niveles predefinidos son: bajo, moderado, alto y crítico.

Probabilidad

Puede definirse como el índice tanto de la probabilidad de que una amenaza explotara con éxito una vulnerabilidad, así como la frecuencia con la que se puede producir.[29]

El criterio para los niveles de la probabilidad depende varios factores entre ellos se encuentran, tamaño del universo de la amenaza, motivación, sofisticación del ataque, conocimiento de la organización, nivel de controles implementados para disminuir o detener la explotación.

El universo de la amenaza, describe el alcance de la comunidad de usuarios que pueden acceder a una vulnerabilidad, es decir, definir el universo de que o quienes podrían ser afectados de la explotación de una vulnerabilidad por una amenaza.

Se utiliza cinco niveles los cuales son: Despreciable, Bajo, Moderado, Alto, Muy Alto, los niveles de los extremos ayudan a cubrir la mayor parte del universo de amenazas (muy alto) e identificar las explotaciones teóricamente posibles pero nada probables.

2.1.3.1.8. Exposición al riesgo

La vía para determinar el nivel de la exposición al riesgo es realizar un mapeo de las dos variables estudiadas de tal manera que la probabilidad se encuentre en el

[28] Párrafo traducido textualmente de: Evan Wheeler, Security risk Analysis, pág. 106.
[29] Párrafo traducido textualmente de: Evan Wheeler, Security risk Analysis, pág. 111.

eje de las “Y” y la severidad en el eje de las “X”, se obtiene una matriz llamada matriz de riesgo.

Hay muchos beneficios de terne una matriz de riesgo cualitativo, uno de ellos es que minimizan los tiempos de análisis, dirigir las acciones más fácilmente sobre el recurso, identificar más rápidamente la exposición al riesgo de una nueva vulnerabilidad y poder tomar acciones para mitigarla.

A continuación se presenta un ejemplo de la matriz de riesgo.

	Severidad(Impacto)		
Probabilidad	Alto	Moderado	Bajo
Alto			
Moderado			
Bajo			
Matriz de riesgo			

Tabla 2.15. Ejemplo de la matriz de riesgo.

2.1.3.1.9. Selección de controles

Una vez identificado el nivel de exposición al riesgo, los controles serán una de las maneras para la reducción de estos niveles considerando que:

- Se minimizan los riesgos causados por amenazas accidentales o deliberadas.
- Deben implementarse controles de acuerdo a los objetivos estratégicos de la organización, es decir priorizar que controles aplicar inmediatamente y cuales paulatinamente.

De ser necesario se puede incluir un análisis de costo-beneficio de los controles a aplicarse, de tal manera que la gerencia tenga una referencia de cuánto va a costar la implementación.

2.1.3.2. Análisis cuantitativo

El análisis cuantitativo se enfoca en números específicos y cálculos estadísticos para determinar la exposición al riesgo. Además el cálculo del costo-beneficio es más preciso ya que se obtienen valores de niveles de riesgo, perdida potencial, costo de contramedidas y valor de salvaguardas, los cuales se pueden expresar en un valor monetario.

Los números o métricas específicas que requiere este método, son por ejemplo los históricos de las ocurrencias de un evento para poder calcular la exposición al riesgo de un activo.

Algunos modelos basados en estadísticas y probabilidades han sido desarrollados, además de fórmulas con las que se obtiene la exposición al riesgo tales como:

Sensibilidad*Severidad*Probabilidad = Exposición al riesgo

Índice de Exposición = (Severidad*Severidad)*Amenaza

2.1.3.2.1. Proceso del análisis de riesgo cuantitativo[30]

1. Inventario de activos y asignación de un valor a cada uno de ellos (AV).

2. Investigar cada activo y realizar una lista de todas las posibles amenazas para cada activo, para cada amenaza listada calcular el factor de exposición (EF), la expectativa de perdida (SLE).

[30] Pasos tomados de: CISSP pág. 270.

3. Realizar un análisis de las amenazas para el cálculo de la probabilidad de cada amenaza que tiene lugar dentro de un solo año, es decir, la tasa analizada de ocurrencia (ARO).

4. Deducir el total de la perdida potencial por amenaza mediante el cálculo de expectativa de perdida anualizada (ALE).

5. Investigar contramedidas para cada una de las amenazas, y entonces calcular los cambios de ARO y ALE basados en las contramedidas aplicadas.

6. Realizar un análisis de costo-beneficio de cada contramedida para cada amenaza por cada activo.

2.1.3.2.2. Variables de costo para el análisis de riesgo cuantitativo[31]

Factor de Exposición (EF)

Representa el porcentaje de perdida que una organización podría experimentar si un activo es vulnerado por una amenaza determinada. También es llamado perdida potencial.

Además, EF es bajo cuando se trata de un activo que se puede reemplazar, pero es alto cuando se trata de un activo que es irreemplazable o prioritario.

Expectativa de perdida (SLE)

Es el costo asociado a un único riesgo sobre un activo determinado, indica la cantidad exacta de perdida que una organización podría experimentar si un activo fuera perjudicado por una amenaza determinada.

SLE=AV*FE donde AV es el valor del activo en dólares.

Tasa anualizada de ocurrencia (ARO)

[31] Definiciones tomadas de: Libro de conocimiento común CISSP.

Es la frecuencia esperada con la cual una amenaza o riesgo puede ocurrir, es decir llego a realizarse, dentro de un año. La escala de ARO va desde 0.0 que indica que la amenaza o riesgo nunca será realizado, hasta valores muy altos que indican que la amenaza o riesgo ocurre siempre.

El cálculo de ARO depende de registros históricos, análisis estadísticos o conjeturas. El cálculo de ARO también es conocido como determinación de probabilidad, en algunos casos se calcula multiplicando la probabilidad de una ocurrencia por el número de usuarios que podrían iniciar la amenaza.

Expectativa de perdida anualizada (ALE)

Es el posible costo anual de todas las instancias de una amenaza específica contra de un activo específico.

ALE=SLE*ARO

2.2. METODOLOGÍAS DEL ANÁLISIS DE RIESGOS DE LA INFORMACIÓN

Una vez que se ha realizado el estudio del análisis cualitativo y cuantitativo de riesgos de manera general y definiendo algunas de las variables para la obtención del nivel de exposición al riesgo, se procede al estudio de las diferentes metodologías del análisis de riesgo de tal manera que se obtenga un mejor visión sobre que método se puede aplicar a nivel gubernamental. En la siguiente sección se estudiaran las metodologías cualitativas como:

- Octave-Allegro
- MAGERIT
- ISO 27005
- FRAAP

En la Tabla 2.6 se resume las ventajas y desventajas de realizar un análisis cualitativo y cuantitativo.

ANALISIS CUANTITATIVO	ANALISIS CUALITATIVO
Ventajas	Ventajas
Los resultados se basan sustancialmente en los procesos y métricas objetivas de forma independiente.	El cálculo es simple.
Un gran esfuerzo es puesto en la valoración del activo y la mitigación del riesgo.	No es necesario determinar el valor económico del activo.
Valoran del costo-beneficio es esencial.	No es necesario cuantificar la frecuencia de la amenaza.
Los resultados se pueden expresados en un lenguaje de gestión específica.	Es fácil involucrar a personal que no sea técnico o que no tenga conocimientos de seguridad.
	Provee flexibilidad en procesos y reportes.
Desventajas	Desventajas
El cálculo es complejo.	Es subjetiva.
El cálculo se realiza mejor con herramientas automatizadas (software) y asociada a una base de conocimiento.	Esfuerzo limitado para determinar el valor económico de activos determinados.
El trabajo preliminar es largo	No hoy bases para el análisis del costo-beneficio y mitigación de los riesgos.
Es complicado para cambiar de objetivos.	
Es difícil tratar temas fuera del alcance.	
El personal no puede ser entrenado a través del proceso.	

Tabla 2.26. Ventajas y desventajas del análisis cuantitativo y cualitativo

2.2.1. OCTAVE ALLEGRO (OPERATIONALLY CRITICAL THREAT, ASSET, AND VULNERABILITY EVALUATION)[32]

Metodología creada por el CERT, para ayudar a las organizaciones a mejora el análisis de riesgo de la seguridad de la información en el contexto operacional y de estrategia de tal manera que se cumpla con su misión.

La metodología de OCTAVE fue desarrollada para identificar y evaluar el riesgo de la seguridad de la información y está enfocada a:

- Realizar una metodología de análisis de riesgo cualitativo.
- Identificar los activos que son importantes en la misión de la organización.
- Identificar para cada activo las amenazas y vulnerabilidades.
- Determinar y evaluar las posibles consecuencias si las amenazas son realizadas

El método ha ido evolucionando como se describe a continuación.

2.2.1.1. Método OCTAVE

El enfoque está definido por una guía de implementación del método (procedimientos, guías, catálogos de información, hojas de cálculo) y entrenamiento.

Diseñada para organizaciones que tienen varios niveles de jerarquía, mantienen la infraestructura de computación, realizan evaluación de vulnerabilidades y análisis de las evaluaciones.

[32] Introducing Octve Allegro, Richar A. Caralli, James F. Stevens, Lisa R. Young, William R.Wilson.

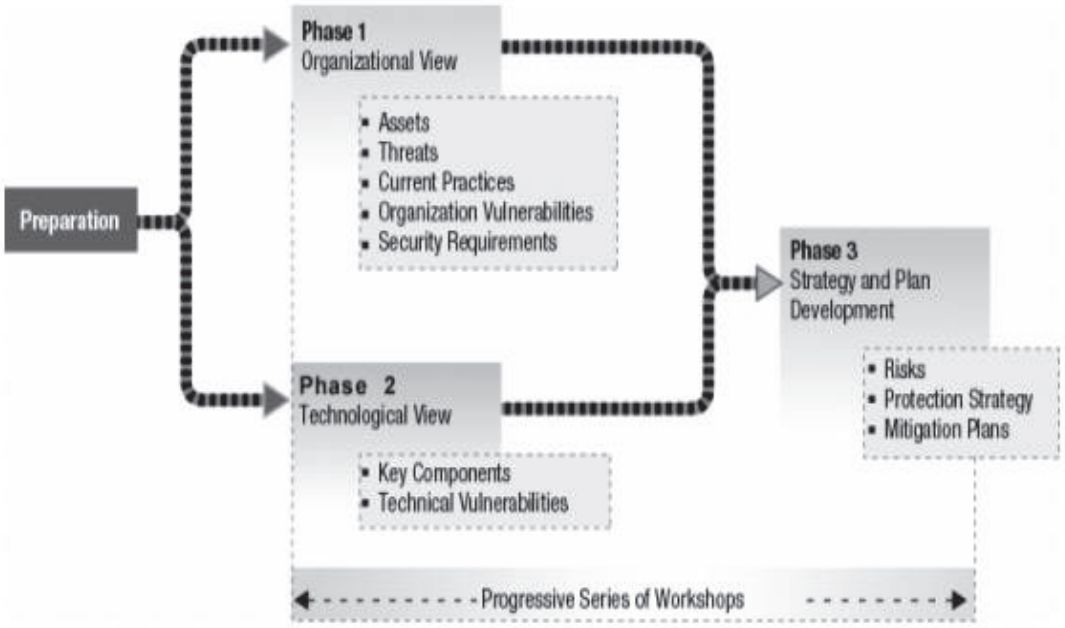

Figura 2.2.1. Fases del método Octave

Fuente: Richard Caralli, James Stevens, Lisa Young, William Wilson, Improving the Information Security risk Assessment Process Mayo 2007, pag,15.

Como se puede observar las fases involucra a la parte organizacional, tecnológica y de estrategia, en esencia hace uso de los conceptos revisados en la sección de definiciones fundamentales como activos, amenazas, riesgos, planes de mitigación, etc. Además el método Octave es un método cualitativo.

2.2.1.2. OCTAVE-S

Está enfocado está diseñado para pequeñas organizaciones alrededor de 100 o menos personas y consiste en tres similares fases del método anterior.

EL método no hace uso de talleres formales para la obtención de conocimiento ya que el equipo de trabajo (tres a cinco personas) tienen conocimiento de las necesidades de seguridad, otra característica del método es que esta mejor estructurado que el anterior. Por estar enfocado para organizaciones pequeñas, examinar la infraestructura de la información de la organización es menos extenso.

2.2.1.3. Octave-allegro

Diseñado para permitir una amplia evaluación de los riesgos operacionales de la organización sin tener una gran experiencia en el análisis de riesgo.

El enfoque de este método principalmente está centrado en los activos de información en el contexto de cómo son usados, donde son almacenados, transportados y procesados y como son expuestos a amenazas y vulnerabilidades.[33]

El método consta de 8 pasos o fases que se encuentran agrupadas en 4 grupos y que se describen más adelante.

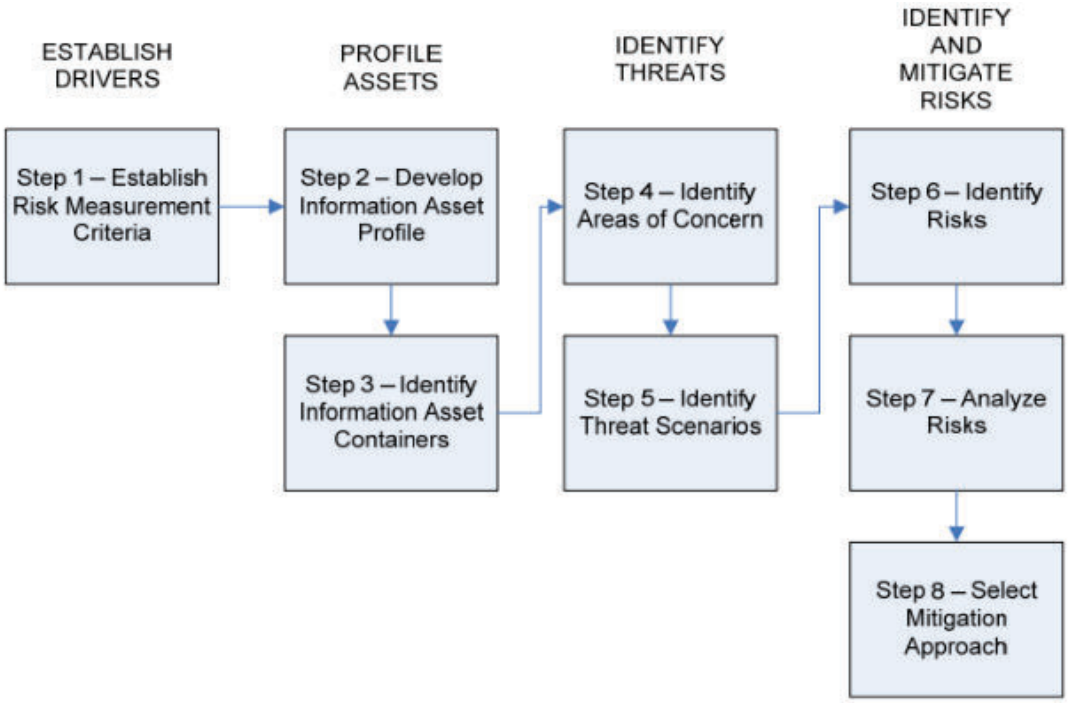

Figura 2.2.2. Fases del método Octave-Allegro

Fuente: Richard Caralli, James Stevens, Lisa Young, William Wilson, Improving the Information Security risk Assessment Process Mayo 2007

[33] Párrafo traducido textualmente de: Richard Caralli, James Stevens, lisa Young, William Wilson, Introducing OCTAVE Allegro, pág. 16.

2.2.1.3.1. Establecer los Controladores

Donde el criterio para el cálculo del riesgo debe estar consistente con los lineamientos de la Organización.

Paso 1:

Se determinara los controladores de la organización los cuales serán usados para la evaluación de los efectos del riesgo en la misión y visión de la organización (impacto). Los controladores son ubicados en un conjunto de criterios de medición del riesgo.

Los criterios de medición del riesgo son un conjunto de medidas cualitativas contra el cual los efectos de un riesgo realizado pueden ser medidos y formar base de la evaluación de riesgo de activos de información.[34]

Usando los correctos criterios se podrá determinar de una manera más correcta de como mitigar el riesgo.

2.2.1.3.2. Perfiles de los activos

Actividades donde se definen los activos de información, sus contenedores y perfiles en los cuales se aplicara el análisis de riesgo.

Paso 2:

En esta paso es donde se inicia el proceso de realizar los perfiles de los activos de información, hay que tomar en cuenta que el perfil describe las características únicas, cualidades y valor de un activo de información. Este proceso permite que el

[34] Párrafo traducido textualmente de: Richard Caralli, James Stevens, lisa Young, William Wilson, Introducing OCTAVE Allegro pág. 17.

activo sea descrito de manera más adecuada de acuerdo a los requerimientos de seguridad.

Paso 3:

Los contenedores describen los lugares donde los activos de información son almacenados, transportados y procesados. Estos contenedores no solo son internos y tampoco están bajo el control directo de la organización.

2.2.1.3.3. Identificar las amenazas

Actividades en las cuales se identifican las amenazas de los activos a través de un proceso estructurado, en el contexto de sus contenedores.

Paso 4:

Iniciar con una lluvia de ideas acerca de las posibles condiciones o situaciones que pueden amenazar al activo de información de la organización.[35]

Estos escenarios son conocidos como áreas de interés, las cuales representan amenazas y su impacto. El propósito del área de interés es reducir la lista de posibles amenazas que pueden afectar al activo de información.

Paso 5:

En este paso las áreas de interés se expanden a escenarios de amenaza, donde se detallan las propiedades de las mismas. Además se considera un rango más amplio de amenazas ya que las determinadas en las áreas de interés no proveen una robusta consideración de las amenazas de los activos de información, con el fin de examinar los escenarios de amenazas.

Para la facilitar la identificación de los escenarios de amenazas a través del árbol de amenazas el método OCTAVE-ALLEGRO contiene varios cuestionarios.

---

[35] Párrafo traducido textualmente de: Richard Caralli, James Stevens, lisa Young, William Wilson, Introducing OCTAVE Allegro pág. 18.

2.2.1.3.4. Identificar y mitigar los riesgos

Actividades donde los riesgos son identificados y analizados para poder determinar una estrategia de mitigación.

Paso 6:

En este paso se determina los posibles impactos causados por las amenazas identificadas, si estas se realizan.

Paso 7:

Se realiza un cálculo cualitativo en el grado en el cual la organización es impactada por una amenaza. Es decir identificar cuáles son los riegos que impactan realmente a la organización.

Paso 8:

Priorizar el riesgo identificado de tal manera que se puedan mitigar o desarrollar una estrategia para mitigarlos. Para el desarrollo de esta estrategia se debe considerar el valor de activo, sus requerimientos de seguridad, sus contenedores, y su único ambiente de operación.

2.2.2. MAGERIT (METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN)[36]

Desarrollado por el Consejo Superior de la Administración Electrónica (CSAE) con el fin de promover la confianza en los servicios de TI que la Administración Pública del gobierno Español brinda a la ciudadanía.

Dentro de Marco de la Gestión de Riesgo de la ISO 31000, MAGERIT define la implementación de la gestión de riesgos derivados del uso de las tecnologías de información.

[36] Libro 1, Magerit, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Ministerio de Hacienda y Administraciones Públicas, Gobierno de España.

Como se puede identificar el marco de gestión de riesgo del método de MAGERIT cumple un ciclo de vida, donde cada actividad o paso dependen del anterior para realizar dicha gestión. Siendo uno de esos pasos el análisis de riesgo del cual se realizara a continuación una breve revisión.

En el Fig.2.21, se puede observar el ciclo de vida de la gestión de la seguridad con sus fases.

Figura 2.2.3. Marco de gestión de riesgos

Fuente: Magerit Libro 1

2.2.2.1. Objetivos[37]

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y la necesidad de gestionarlos.

[37] Tomado de: Magerit V3 libro 1, pág. 7.

- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnológicas de la información y comunicación.
- Descubrir y planificar el tratamiento oportuno para mantener a los riesgos bajo control.
- Preparar a la organización para procesos de evaluación, auditoria, certificación o acreditación según el caso.

2.2.2.2. Actividades para la realización de Informes

- Modelo de valor
- Mapa de Riesgos
- Declaración de aplicabilidad
- Evaluación de Salvaguardas
- Estado de riesgo
- Informe de Insuficiencias
- Cumplimiento de normas
- Plan de seguridad

2.2.2.3. Estructura de la Metodología

Su estructura de 3 libros, libro I que define la metodología, libro II es un catálogo de amenazas y vulnerabilidades de los activos y guías técnicas.

2.2.2.3.1. Libro I

Consta de 8 capítulos, donde se detallan las actividades para la gestión de riesgos, se toma en cuenta que los primeros 2 capítulos son dedicados a conceptos y hacen un vistazo a las actividades a realizarse en la análisis de riesgos. En tanto que los últimos dos capítulos se enfocan las recomendaciones y conclusiones.

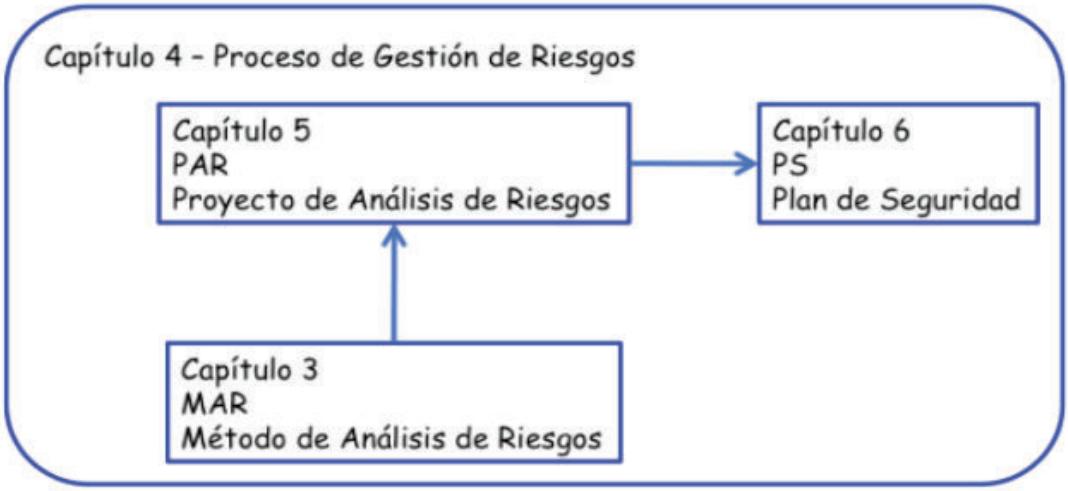

Figura 2.2.4. Proceso de la gestión de riesgos

Fuente: Magerit Libro 1

Las actividades del proceso de gestión de riesgo pueden ser complicadas cuando se trata de sistemas grandes o que involucran a varias partes, como por ejemplo grupos de trabajos con varias personas.

Principales elementos en el análisis de riesgo:

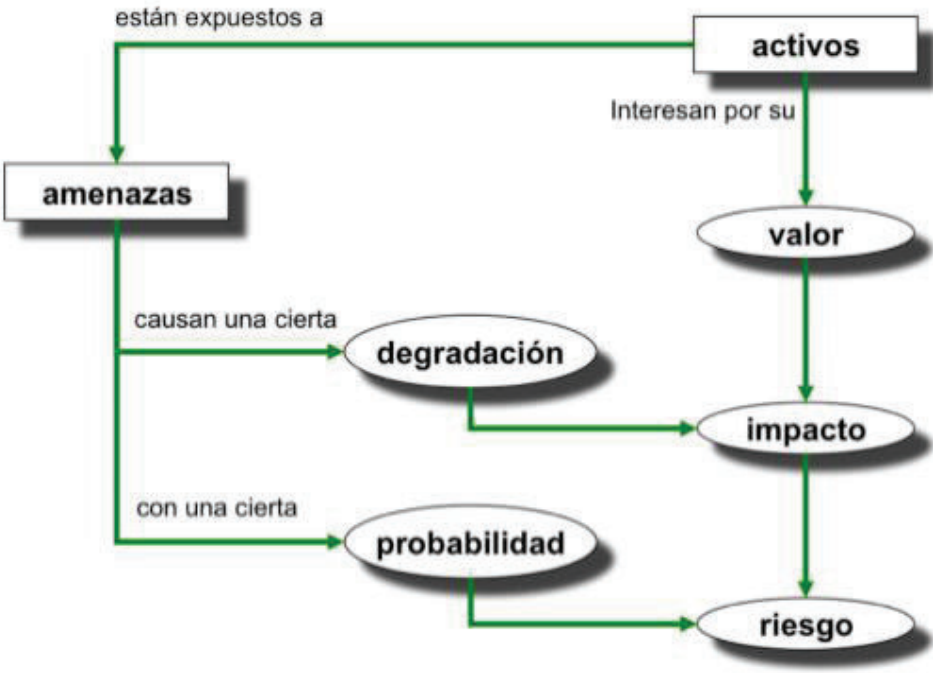

Figura 2.2.5. Actividades del proceso de gestión de riesgos

Fuente: artículo IT Risk Managemente, Suares-Mendez

2.2.2.3.2. Libro II

Libro que está enfocada en homogeneizar los resultados del análisis haciendo fácil para el personal encargado de dicho análisis.

Este libro es un catálogo de tipos de activos, dimensiones valoración de activos, criterios de valoración de activos, amenazas tipas sobre sistemas de información y salvaguardas.

2.2.2.3.3. Guía técnica

Libro en cual se encuentra información adicional de técnicas utilizadas para el análisis de riesgos como: análisis mediante tablas, análisis algorítmico, arboles de ataque, técnicas gráficas, sesiones de trabajo, valoración Delphi.

Para la acreditación y certificación de un sistema de gestión de seguridad lo que se requiere principalmente es el análisis de riesgo y los controles respectivos seleccionados.

2.2.3. FRAAP (FACILITATED RISK ANALYSIS AND ASSESSMENT PROCESS)[38]

Es un método de análisis de gestión de riesgo, el cual es un proceso disciplinado y eficiente, teniendo como objetivo asegurar los riesgos relacionados con la seguridad de la información de las operaciones del negocio estén considerados y documentados.

El proceso involucra la conformación de un equipo de trabajo formado por administradores de negocio, TI, el área de seguridad, etc., en cual se designará un coordinador para programar las tareas entre el equipo. Consta de tres fases:

[38] Thomas Peltier, Information security risk analysis.

2.2.3.1. Pre-FRAAP

Esta fase es donde se mantiene una reunión con las altas autoridades del negocio o algún representante de la misma con el fin de establecer el proyecto para la evaluación de riesgo, esta reunión no debe tomar más de una hora. En esta reunión se deberá establecer seis puntos claves.

2.2.3.1.1. Resultados preliminares

Cualquier resultado que podría alterar que la evaluación de riesgo se lleve a cabo.

2.2.3.1.2. Declaración sobre el alcance

La máxima autoridad o el representante de la misma definirá el alcance de la evaluación, este alcance debe ser realizado en palabras simples para poder ser revisado.

2.2.3.1.3. Diagrama visual

Es un diagrama con el proceso a ser revisado, este le sirve para familiarizar al equipo de donde empieza y termina el proceso.

2.2.3.1.4. Conformación del equipo

Se conforma entre 15 y 20 miembros de diferentes áreas del negocio.

2.2.3.1.5. Mecanismos de encuentros

Las sesiones será agendadas por una persona del área administrativa que no tenga nada que ver con el equipo de trabajo.

2.2.3.1.6. Acuerdo en definiciones

En esta reunión se acordara en las definiciones de las palabras relacionadas con la evaluación de riesgo y sobre los pilares de la seguridad de la información.

2.2.3.2. Sesión-FRAAP

Se divide en 2 etapas, la primera consiste en identificar las amenazas, establecer el nivel del riesgo, determinar los posibles controles. La sesión de esta etapa dura aproximadamente 4 horas pero dependiendo de la organización puede ser extendida, además el equipo de trabajo está formado por 15 y 25 miembros.

La segunda etapa se define los controles de la siguiente manera:

- Identificar los controles existentes.
- Seleccionar un control para las amenazas de alto nivel.
- Para cada control el equipo identificara el responsable para la implementación de ese control.

2.2.3.3. Post-FRAAP

En esta sesión, se genera reportes para determinar que se logró con la evaluación de riesgos, además se estable un plan de acción basado en la información obtenida en las sesiones anteriores.

Con la información de realizar un análisis de costos y la implementación de los controles. En esta sesión además se define 3 entrégales.

- Tiempos para la aplicación de controles.

- Resumen ejecutivo de la gestión.
- Una tabla cruzada de los controles aplicados.

2.2.4. ISO 27005 (INFORMATION TECHNOLOGY- SECURITY TECHNIQUES- INFORMATION SECURITYRISK MANAGEMENT)[39]

El estándar no provee una metodología específica de la gestión de riesgos de la información, todo depende de la organización, su foque, alcances, del sector.

El estándar provee directrices a las organizaciones que cuentan o quieren contar con un SGS. Además provee el proceso y actividades para la gestión de riesgos de información.

2.2.4.1. Estructura del estándar

En la Fig. 2.24 se describen las fases de la estructura del estándar ISO 2005.

El estándar está definido por 12 cláusulas, siendo las 6 primeras donde se define los alcances, definiciones, resumen de la norma.
Las actividades del proceso están definidas de la cláusula 7 a la12 y en las cuales se detalla el proceso de gestión de riesgo de la información. Además contiene anexos con información general de la evaluación de riesgos, amenazas y vulnerabilidades.

Cada clausula está definida por cuatro partes.[40]

2.2.4.1.1. Entrada

Identifica cualquier información necesaria para realizar la actividad.

[39] Norma ISO 27005, Information Security Risk Management.
[40] Definiciones tomadas de: Norma ISO 27005, Information Security Risk Management, pág.3.

2.2.4.1.2. Acción

Describe la actividad.

2.2.4.1.3. Guía de implementación

Proporciona guía para realizar la acción. Algunas de estas guías no pueden será adecuadas para todos los casos y en otros serían las adecuadas.

2.2.4.1.4. Salida

Identificar cualquier información después de la actividad realizada.

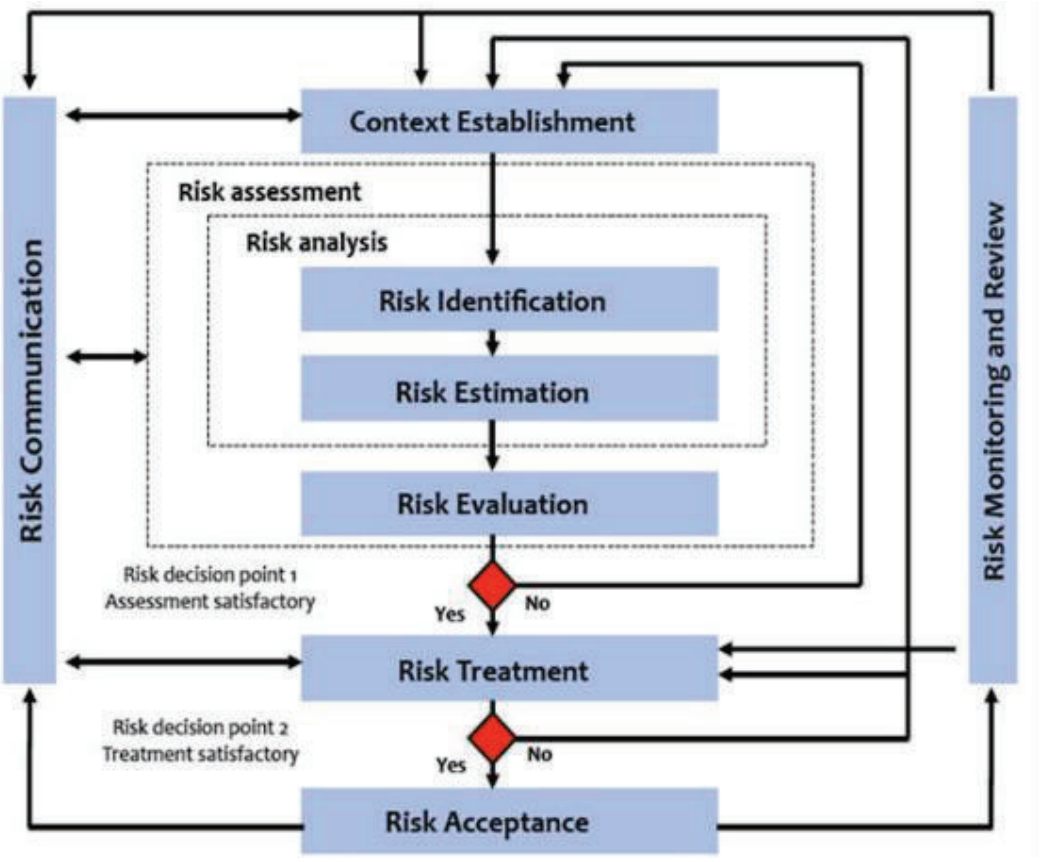

Figura 2.2.6. Proceso de gestión de riesgo ISO

Fuente: Norma ISO 27005

2.2.4.2. Establecimiento del contexto[41]

Información relevante acerca de la organización para el establecimiento del contexto.

2.2.4.2.1. Criterio básico

Para desarrollar un enfoque apropiado en la gestión de riesgos de debe contar con algunos criterios como el de evaluación de riesgos, impacto del riesgo, aceptación del riesgo.

Además hay que verificar que la organización cuente con los recursos necesarios para.

- Realizar un plan para la medición del riesgo y su tratamiento.
- Definir políticas y controles
- Monitoreo de controles
- Monitoreo el proceso de la gestión de riesgo de la seguridad de la información.

2.2.4.2.2. Criterio de evaluación de riesgo

Para la evaluación de riesgos se toma en cuenta:

- El valor estratégico del proceso de información del negocio.
- La criticidad de los activos de información involucrados.
- Regulaciones vigentes.
- Importancia de la disponibilidad, integridad y de la confidencialidad para el negocio.
- Expectativas y percepciones de las partes interesadas.

[41] Traducido textualmente de: Norma ISO 27005, Information Security Risk Management. Pág. 7,8.

2.2.4.2.3. Criterio de impacto de riesgo

Este criterio se desarrolla en términos de costos o daños que un evento puede causar a la organización, considerando los siguientes puntos.

- Nivel de clasificación del activo de información impactado.
- Brechas de seguridad de la información.
- Operaciones deficientes.
- Pérdida del valor de negocio y financiero.
- Interrupción de planes y plazos.
- Daño de la imagen de la organización.
- Brechas en las regulaciones vigentes.

2.2.4.2.4. Criterio de aceptación de riesgo

El criterio de la aceptación del riesgo depende de las políticas, objetivos, metas e intereses de las partes interesadas. La organización puede definir su nivel de aceptación del riesgo tomando en cuenta los siguientes puntos.

- Se debe incluir múltiples niveles de umbrales con un deseable nivel de riesgo, con la provisión de que los altos directivos acepten el riesgo por encima de estos umbrales en determinadas circunstancias.
- El criterio puede ser expresado como una relación del beneficio estimado con el riesgo estimado.
- Diferentes criterios de aceptación del riesgo se debe aplicar a diferentes clases de riesgos.
- El criterio debe incluir requerimientos para el tratamiento a futuro.

El criterio puede diferir de acuerdo al tiempo que el riesgo aceptado exista.

2.2.4.2.5. Límites y alcances

Se debe considerar la información más relevante de la organización para determinar el ámbito de dicha organización, para ello se considera los siguientes puntos.

- Misión y Visión de la organización.
- Proceso de negocio.
- Estructura Organizacional.
- Requerimientos legales o regulatorios vigentes.
- Política de seguridad de la información.
- Enfoque de la gestión de riesgos.
- Activos de información
- Características generales
- Restricción que afectan la organización.
- Expectativas de las partes de las interesadas.
- Medio ambiente socio-cultural.

2.2.4.2.6. Organización para la gestión de riesgo de la seguridad de la información

Para esta organización hay que tomar en cuenta los principales roles y responsabilidades los cuales deben ser aprobados por la alta gerencia.

- Desarrollar un proceso de gestión de riesgo de la seguridad de la información adecuado.
- Identificación de las partes interesadas.
- Definición de roles y responsabilidades de las partes internas y externas.
- Definición de la ruta para el escalamiento.

2.2.4.3. Evaluación de la gestión de riesgos

En la evaluación de riesgos determina el valor del activo de información, las amenazas y vulnerabilidades existentes o que podrían existir. La evaluación conlleva dos actividades.

2.2.4.3.1. Identificación de riesgo

El objetivo es identificar que podría la causar la perdida potencial de información, además tener una perspectiva de cómo, dónde y porque puede ocurrir dicha perdida.

Para la estimación del riesgo se realiza las siguientes actividades.

2.2.4.3.2. Identificación de Activos

Identificar los propietarios, lugares y funciones de los activos es primordial.

En primer lugar un activo es algo que tiene valor para la organización y además hay que tener presente que un activo no solo consiste en hardware y software.

El nivel de detalle con la que se realice la identificación del activo servirá de mucho para la evaluación de riesgo.

Cada activo debe tener un propietario quien sea responsable de él y que ayude en temas de auditoria del mismo. El propietario no siempre es alguien con derechos sobre el activo, sino alguien que sabe realmente su valor y que es responsable de su funcionalidad operacional y de seguridad.

2.2.4.3.3. Identificación de Amenazas

Las amenazas pueden hacer daño a los activos de información, procesos y sistemas, estos pueden ser de origen natural u origen humano, las amenazas de

origen humano pueden ser de tipo accidental o deliberado. Se debe tomar en cuenta que las amenazas podrían estar dentro de la organización.

Adicionalmente se puede hacer uso de catálogos de amenazas para la estimación y probabilidad de ocurrencia.

Una misma amenaza puede afectar a diferentes activos, por tal razón también puede tener diferente impacto en cada activo.

Se identifica la probabilidad de ocurrencia de la amenaza la cual se puede obtener del propietario del activo, usuarios, expertos de seguridad, etc.

2.2.4.3.4. Identificación de controles existentes

La identificación de los controles podría ser un trabajo innecesario y costoso, hay que asegurar que los controles estén trabajando correctamente ya que podrían ser causa de vulnerabilidades. Es importante realizar una lista de chequeo de los controles y del trabajo que deben cumplir y de ser es caso ser reemplazados por un nuevo control en un nuevo plan.

Los siguientes pasos ayudaran para la identificación de controles existentes.[42]

- Revisión de documentos que contengan información acerca de controles.
- Revisar con el oficial de seguridad de la información o alguien con los mismos roles y con los usuarios sobre los controles implementados.
- Realizar una revisión en sitio de los controles físicos y compararlos con los que podrían implementarse.
- Resultados de auditorías internas.

2.2.4.3.5. Identificación de vulnerabilidades

[42] Pasos traducidos textualmente de: Norma ISO 27005, Information Security Risk Management. Pág. 12.

Las vulnerabilidades pueden ser explotadas por las amenazas y causar daño a los activos.

Áreas donde se podría identificar vulnerabilidades.[43]

- Procesos y procedimientos.
- Rutinas de gestión.
- Personal.
- Ambiente físico.
- Configuración del sistema de información.
- Hardware, software o equipos de comunicación.
- Dependencia de terceros.

Una vulnerabilidad por sí sola no puede hacer daño se requiere de una amenaza para explotarla, para implementar controles una vulnerabilidad debe tener una correspondiente amenaza. Además una amenaza que no tiene su correspondiente vulnerabilidad no podría resultar en riesgo.

2.2.4.3.6. Identificación de consecuencias

En esta actividad se identifica los daños o consecuencias a la organización por la pérdida de confidencialidad, integridad y disponibilidad en los activos en un escenario de incidente, es la descripción de una amenaza explotando una o un conjunto de vulnerabilidades.

Las consecuencias pueden ser temporales o permanentes en el caso de destrucción de un activo, además se determinará las consecuencias de valor y de negocio.

Algunas consecuencias en escenarios de incidentes pueden ser, pérdida de tiempo de trabajo, costo financiero para la reparación del daño, reputación de la imagen, etc.

---

[43] Traducido textualmente de: Áreas donde identificar Vulnerabilidades, Norma ISO 27005, Information Security Risk Management. Pág. 7,8.

2.2.4.3.7. Metodologías de estimación

Dependiendo de las circunstancias se puede hacer uso de 2 metodologías de estimaciones, cuantitativa o cualitativa. Estas dos metodologías fueron estudiadas al inicio del capítulo.

La estimación cuantitativa hace uso de una escala la cual describe la magnitud de las consecuencias y de la probabilidad de que estas consecuencias ocurran.

La estimación cualitativa hace uso de una escala de valores los cuales dependen de datos históricos relacionados con incidentes en los sistemas de información.

2.2.4.3.8. Evaluación de consecuencias (impacto)

La evaluación de consecuencias inicia con la clasificación de los activos de acuerdo a su criticidad en los objetivos de la organización y se usa dos medidas.

- Costo de recuperar y reemplazar la información.
- Consecuencias de negocio por pérdida del activo.

Esta evaluación se puede obtener a partir de un BIA (análisis de impacto de negocio), además el criterio de impacto puede ser expresado en términos de económicos, técnicos o humanos.

2.2.4.3.9. Evaluación de la probabilidad de incidentes

La evaluación se lo realiza para cada escenario de incidencia haciendo uso de cualquier metodología de estimación, hay que tomar en cuenta con qué frecuencia las amenazas podrían ocurrir y podrían explotar las vulnerabilidades.

Para realizar un mejor evaluación se podría agrupar activos o separarlos en sus partes para relacionarlos con el escenario de incidencia.

2.2.4.3.10. Nivel de la estimación de riesgo

Es la combinación de la probabilidad de un escenario de incidencia y sus consecuencias.[44]

La evaluación de riesgos es tomar decisiones sobre acciones a definir que estén alineadas con los objetivos de la organización, estas decisiones son tomadas en base a un nivel aceptable de riesgo, además hay que tomar en cuenta las variables anteriormente definidas y regulaciones vigentes.

2.2.4.4. Tratamiento del riesgo de la seguridad de información

Se cuenta con cuatro opciones de tratamiento del riesgo.

2.2.4.4.1. Reducción del riesgo

La reducción del riesgo tiene que ver con la selección adecuada de controles los cuales deben proveer los siguientes tipos de protección: corregir, eliminar, prevenir, minimizar del impacto, disuasión, detección, recuperación, monitoreo y conocimiento.

Es importante tomar en cuenta durante la selección de los controles verificar que el costo de adquisición, implementación, operación, monitoreo y mantenimiento versus el costo del activo a proteger en términos de inversión, costo-beneficio.

2.2.4.4.2. Retención del riesgo

Si el nivel del riesgo es aceptable entonces no es necesario implementar controles para estos riesgos y se los retiene.

---

[44] Párrafo traducido textualmente de: Norma ISO27005 Information Security Risk Management.

2.2.4.4.3. Evadir del riesgo

Cuando el costo-beneficio de implementación de controles no es el adecuado es decir cuánto más costosa es la implementación que los beneficios.

Un ejemplo, tener un centro de datos en un lugar con alto riesgo naturales y tratar de establecer controles es más costoso que mover el centro de datos a otro sitio con menos riesgos.

2.2.4.4.4. Transferir los riesgos

El riesgo puede ser transferido a un tercero para su tratamiento paro se debe tomar en cuenta que esto crea nuevos riesgos que hay que evaluarlos. Se puede transferir la responsabilidad de la gestión del riesgo pero no la responsabilidad del impacto.

2.2.4.5. Aceptación del riesgo de la seguridad de la información

Un plan de tratamiento de riesgos debe ser presentado y aprobado, este plan será revisado de acuerdo al criterio de aceptación de riesgo el cual se basa en los lineamientos estratégicos de negocio u objetivos de la organización.

La organización definirá umbrales para los cuales se puede aceptar los riesgos, además se debe indicar por qué se aceptan.

2.2.4.6. Comunicación del riesgo de la seguridad de la información

Actividad donde se logra el un acuerdo sobre cómo manejar los riesgos, toda la información de las actividades que anteceden se debe presentar a las autoridades y a las partes interesadas.

En este documento se debe incluir las tanto las percepciones de riesgo como de beneficios que satisfagan a las autoridades y partes interesadas.

2.2.4.7. Revisión y monitoreo de los riesgos de la seguridad de la información

2.2.4.7.1. Monitoreo y revisión de los factores de riesgo

Ya que las amenazas y vulnerabilidades están en constante evolución llevar un monitoreo constante es primordial de tal manera que se pueda identificar cambios en cualquier activo que forme parte de la gestión o un nuevo que vaya a formar parte.

Los cambios afectaran a los niveles de probabilidad de ocurrencia y a las consecuencias (impacto) de la amenaza al explotar una vulnerabilidad.

Se debe preparar un plan de monitoreo constante con actividades de revisión.

2.2.4.7.2. Monitoreo, revisión y mejoramiento de la gestión de riesgos

El monitoreo y revisión del proceso de gestión de riesgos es importante para la mejora del mismo en cual debe ser notificado a las autoridades para su revisión y definir los cambios y acciones a tomar. El monitoreo y revisión se lo debe realizar sobre los parámetros estudiados en el proceso de la gestión de riesgo, como por ejemplo: valoración de activos, sobre los criterios de evaluación.

2.2.5. SELECCIÓN DEL MÉTODO DE ANÁLISIS DE RIESGO

Como antecedente, actualmente las instituciones gubernamentales deben implementar el Esquema Gubernamental de Seguridad de la Información que tiene

de carácter de prioritario, pero en sí, no es más que aplicar los controles de la norma ISO 27002 o NTE-INEN 27002 sin un previo análisis de riesgo, es decir que todas las instituciones tendrían las mismas amenazas con la misma probabilidad de ocurrencia. A pesar de esto, el EGSI determinó que controles eran prioritarios a cumplir, pero ciertas instituciones aun no cumplen con este objetivo. Una de la razones es que en las entidades públicas el personal cambia y hace difícil el implementar los controles y muchas veces con poca experiencia.

Las variables que se tomaron para definir el método de análisis de riesgo tienen que ver en algo con el antecedente planteado.

La variable costo (Tiempo de análisis y reuniones), aunque podrían ser altas no son relevantes ya que el proyecto está enfocado a un servicio que brinda el área TICs, estas reuniones se pueden llevar a cabo sin previa coordinación.

El equipo de trabajo era muy importante ya que se esperaba que se dé continuidad al análisis y no caer en el inconveniente de la implementación del EGSI. Aún más en una institución como la Presidencia donde el cambio de personal es a menudo. La experiencia de la persona que realice el análisis podría ser mínima.

Se busca un método que facilite el análisis por medio de plantillas, cabe indicar que esta variable está estrechamente relacionada con la variable anterior.

Las plantillas a más de ayudar a la persona que realice el análisis también tiene facilita la adquisición de información de los servicios identificados.

Método\ Variables	Costo(Tiempo análisis y reuniones)	Equipo de trabajo	Experiencia en análisis de riesgo	Uso de plantillas, guías, etc.
OCTAVE-ALLEGRO	Alto, en el tiempo de análisis.	Al menos 2 personas de TI.	No requerida	Si
MAGERIT	Alto, en el tiempo de análisis para conseguir los objetivos establecidos en la metodología.	De al menos 5 personas de las diferentes áreas de la institución.	No requerida	Sí, pero únicamente en partes específicas, por ejemplo árbol de amenazas.

FRAAP	Medio, en el tiempo de análisis.	De 10 a 15 personas de las diferentes áreas de la institución.	Requerida	No
ISO 27005	Alto, en el tiempo de análisis.	De al menos 1 persona de cada área involucrada.	Requerida	Algunas referencias de riesgos, y árboles de amenazas.

Tabla 2.27. Variables relevantes para las metodologías de análisis de riesgo

Del análisis de las variables anteriores de los métodos de gestión de riesgo se toma a Octave-Allegro para realizar el respectivo análisis del proceso del servicio de correo electrónico y el proceso del servicio de videoconferencia.

Como antecedente cabe mencionar que la Dirección de TICs provee de varios servicios a la Presidencia de la República tales como, servicio de correo electrónico, servicio de videoconferencia, servicio de telefonía ip, además de servicios web como agenda presidencial, decretos, acuerdos, etc.

A continuación se analizarán los servicios que son entregados por TICs.

El servicio de correo electrónico es, valga la redundancia, un servicio que es utilizado por alrededor de 500 usuarios diariamente durante la toda la jornada laboral, alrededor del 5% de estos usuarios lo utilizan casi 12 horas, como es el caso de Secretaría Jurídica, Agenda Presidencial, Despacho Presidencia y alrededor del 1% lo utiliza más de las 12 horas, en este porcentaje se encuentra el Señor Presidente y sus asesores.

En el caso de Agenda Presidencial el servicio de correo electrónico se torna crítico ya que es el medio por el cual se coordinan actividades del Señor Presidente como reuniones con ministros, sesiones, encuentros y varias actividades a nivel de despacho. Cabe indicar que el área de agenda consta de alrededor de 8 personas.

El servicio de videoconferencia provisto por el área de TICs tiene alcance nacional, es decir que puede ser utilizado por cualquier entidad de gobierno que se encuentre en dentro del anillo interministerial. El anillo interministerial es una red MPLS provista por CNT donde Ministerios, Secretarias y otras instituciones tienen acceso y además de proveen servicios a las organizaciones que la conforman.

El servicio de videoconferencia es utilizado diariamente por al menos 200 usuarios, el uso del servicio se lo realiza por medio de reservas de salas y disponibilidad de conexiones simultaneas. En ciertas ocasiones estas reuniones han servido para realizar COEs (Comités de Operaciones de Emergencia) que son dirigidas por la Secretaria de Riesgos, es decir el servicio se convierte en un medio para coordinar medidas contra desastres naturales.

El servicio de Videoconferencia se torna aún más crítico cuando se realizan gabinetes virtuales, en los cuales participan únicamente los Ministros de estado y el Señor Presidente ya que en estos se pueden estar tomando decisiones importantes para el país.

El servicio de telefonía ip es de carácter interno, lo usan de alrededor de 400 usuarios diariamente únicamente durante la jornada laboral. Este servicio no podría ser considerado crítico ya que los usuarios más críticos cuentan con planes de telefonía móvil celular.

En conclusión, de los servicios analizados, el servicio de correo electrónico y el servicio de videoconferencia son los que serán analizados. Cabe indicar que esta decisión se tomó en conjunto con el director del proyecto, apoyándonos a sus años de la experiencia en el área de TICs como administrador de la red de la Presidencia de la República y a los hechos diarios respecto a la evolución seguridad de la información durante los últimos años.

Se ha determinado los aspectos más relevantes por los cuales se seleccionaron los servicios antes mencionados.

- Por la relevancia de sus usuarios como el Señor Presidente, Asesores, Secretarios, Subsecretarios, Ministros, etc.

- Por la relevancia tecnológica, por ser un apoyo en la toma decisiones.
- Por su alcance, es decir que uno de ellos presta su servicio a varias entidades del gobierno central.

CAPÍTULO III

3.1. ANÁLISIS DE RIESGO DE LOS PRINCIPALES SERVICIOS DE PRESIDENCIA DE LA REPÚBLICA

Analizados los métodos de gestión de riesgo en el capítulo anterior, se ha defino realizar el análisis de riesgo en base el método OCTAVE-ALLEGRO, es un proceso que consta de 8 pasos o fases.

3.1.1. ESTABLECIMIENTO DEL CRITERIO DE MEDICIÓN DEL RIESGO

El criterio de medición de riesgo debe tomar en cuenta la misión de la institución y a sus objetivos estratégicos, ya que estos son lo que serían afectados si una amenaza llegara a materializarse.

En el capítulo 1 se menciona en estos objetivos y se realiza un análisis de cómo afectaría su confidencialidad, integridad y disponibilidad.

De acuerdo estatuto orgánico de la Presidencia establece la Misión de la Presidencia de la República, la cual establece:

“Somos la primera entidad de la Administración Pública Central, responsable de viabilizar el ejercicio de Gobierno y la Administración de la Presidencia de la República, a fin de coadyuvar para la consecución de los más altos intereses del Estado ecuatoriano.”[45]

3.1.1.1. Áreas de Impacto

[45] Estatuto Orgánico vigente de la Presidencia de la República del Ecuador, registro oficial N° 296, 24 Julio 2014.

Una vez definida la misión de la Institución se procederá a determinar las áreas de impacto, con las cuales servirán de base para la gestión de riesgo y más tarde para la definición de las políticas se seguridad de la información.

Las áreas de impacto de acuerdo a la metodología se deben considerar al menos las siguientes áreas: Reputación y Confianza, Financiera, Productividad, Seguridad y Salud, Multas o Sanciones Legales y áreas definidas por el usuario, en este caso se añadió el área de Regulaciones.

Los niveles definidos como baja, media y alta son propios del estándar. Los valores cualitativos de los niveles son con los que se podrá evaluar el efecto de un riesgo en la misión y objetivos estratégicos.

Para la reputación se tomaron los valores predefinidos en el método, como antecedente, la credibilidad que se basa en el cumplimiento de los objetivos definidos dentro de proyectos gubernamentales que deben permanecer lo más alto posible es decir cumplir la mayor parte de estos objetivos. Por lo tanto estos valores son tomados desde el menor porcentaje posible 10% y manteniendo la proporción de porcentaje.

En la Tabla 3.1 y 3.2 se muestra las áreas de impacto, reputación y confianza, y productividad respectivamente.

1	**REPUTACIÓN Y CONFIANZA**		
Área de impacto	**Baja**	**Media**	**Alta**
Reputación	Reputación tiene una afección mínima, la credibilidad no se ve afectada.	La reputación se daña, y se requiere poco esfuerzo para recuperarse.	La reputación es completamente afectada.
Credibilidad	Menos del 10% de reducción en la credibilidad.	Entre el 10% y 20% de reducción en la credibilidad.	Más del 20% de reducción en la credibilidad.
Social	NA	NA	NA
Político	NA	NA	NA

Tabla 3.11. Área de impacto, reputación y confianza

2	PRODUCTIVIDAD		
Área de impacto	**Baja**	**Media**	**Alta**
Horas de personal	Al menos 1 hora sin algún servicio.	De 1 a 2 horas sin algún servicio.	De 3 horas en adelante sin algún tipo de servicio.

Tabla 3.12. Área de impacto productividad

Esta área de impacto está enfocada principalmente a personal de áreas críticas como Despacho Presidencial y Secretaria Jurídica. De la experiencia, se ha tomado como unidad 1 hora para definir molestia y se ha incrementado de manera proporcional hasta llegar a la tercera hora. Cabe indicar que estos valores son relativos porque depende del tipo de personal.

3	CUMPLIMIENTO DE REGULACIONES		
Área de impacto	**Baja**	**Media**	**Alta**
Reglamentos			Cumplimiento del 100% acuerdo 166, EGSI.

Tabla 3.1.3. Área de impacto Regulaciones

Esta área de impacto está enfocada al cumplimiento obligatorio del Esquema gubernamental de Seguridad de la Información (EGSI).

A continuación se define la prioridad de las áreas de impacto antes definidas, esta prioridad en este análisis va desde 1 que es el más bajo hasta 3 que es el más alto.

Se ha tomado como prioridad más alta al área de impacto de reputación de confianza ya que es aquí donde se debe cumplir con la misión y objetivos estratégicos, es decir agilitar la gestión del Señor Presidente de la Republica.

Como se había revisado en capítulos anteriores TICs cumple un papel muy importante al ser un proceso adjetivo de apoyo para que la gestión se realice de manera normal.

Como se mencionó anteriormente la Productividad es algo muy importante a nivel del Despacho Presidencial y Secretaria Jurídica. A continuación se define la Tabla 3.4 en la cual se coloca la prioridad de las áreas de impacto definidas anteriormente.

4	PRIORIZACION DE LAS AREAS DE IMPACTO
PRIORIDAD	**ÁREAS DE IMPACTO**
3	Reputación y confianza
n/a	Financiero
2	Productividad
n/a	Seguridad y salud
n/a	Multas y penalizaciones legales
1	Cumplimiento de regulaciones

Tabla 3.14. Priorización de las áreas de impacto

3.1.2. DESARROLLO DE PERFILES DE ACTIVOS DE INFORMACIÓN

Este paso usa la plantilla 8 del método de Octave-Allegro que se encuentra en los anexos. En la plantilla se debe justificar la selección del activo de información, justificación que se realizó en el capítulo II.

En esta fase se determinan los activos de información más importantes para la organización.

- La información que genera el servicio de correo electrónico.
- La información que se genera con el uso del servicio de videoconferencia

También se define los propietarios del activo de información así como los requerimientos de seguridad de la información que no son más que los objetivos de la seguridad CID dando un ejemplo de cada uno de ser el caso y se selecciona cuál de ellos es el más importante para ese activo.

La Fig. 3.1 determina los pasos que se seguirán para obtener el análisis de riesgo de acuerdo al método Octave-Allegro.

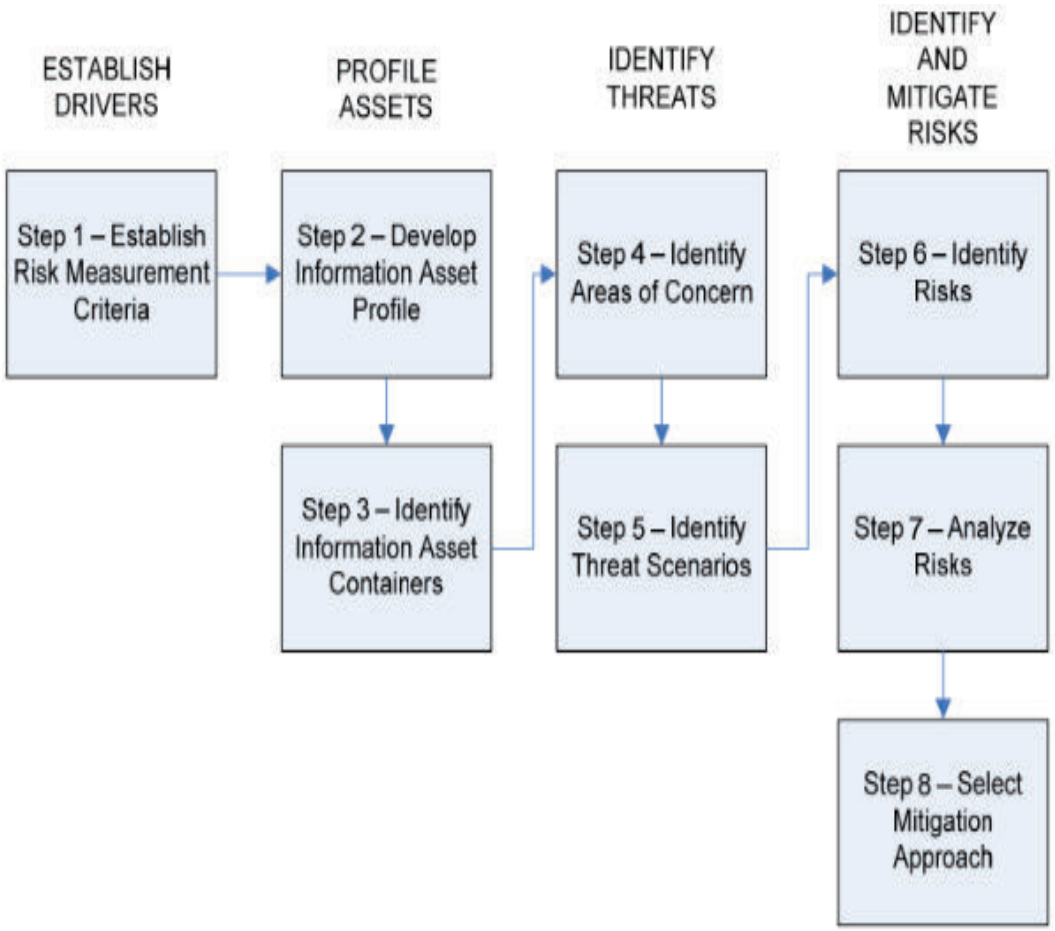

Figura 3.1.1. Proceso Octave-Allegro

Fuente: Richard Caralli, James Stevens, Lisa Young, William Wilson, Improving the Information Security risk Assessment Process Mayo 2007

El desarrollo de los perfiles de información consta de dos pasos:

- Desarrollo del perfil del activo de información.
- Determinar los contenedores del activo de información.

Los perfiles de activos de información que se obtendrán, serán el punto de partida para identificar los contenedores es decir, identificar donde el activo es procesado, transmitido y almacenado y poder identificar de esa manera las posibles amenazas.

A continuación se presenta los perfiles de activo de información crítico tanto para el servicio de correo electrónico como para el servicio de videoconferencia.

	PERFIL DE ACTIVO DE INFORMACIÓN CRÍTICO	
Activo Crítico	**Justificación de selección** (¿Por qué este activo de información es importante para la organización?)	**Descripción**
Información del servicio de correo electrónico.	Porque es el principal medio de comunicación de las diferentes áreas de la Presidencia, medio por el cual se coordinar actividades con las demás entidades públicas. Además del cumplimiento del acuerdo 166 de la SNAP.	Correo Electrónico
Propietarios		
Oficial de Seguridad. Área de redes y Comunicaciones.		
Requerimientos de seguridad		
CONFIDENCIALIDAD **X**	Solo personal autorizado puede ver o acceder este activo de información.	Solo usuarios de Presidencia que tienen un usuario y clave pueden tener acceso al activo de información para su uso.
INTEGRIDAD **X**	Solo personal autorizado puede modificar este activo de información.	El activo de información no debe ser alterado ni modificado incluso por personal de custodio de este activo bajo ningún motivo.
DISPONIBILIDAD **X**	Este activo de información debe estar disponible para los usuarios.	Solo los usuarios de Presidencia pueden hacer uso de este activo de información donde quiera y a cualquier hora, de tal manera que puedan realizar normalmente sus actividades
	Este activo de información debería estar disponible durante 24 horas, 7 días/semana, 365 días/año	
OTRO	N/A	N/A
El más importante requerimiento de seguridad		

Confidencialidad	x	Integridad	x	Disponibilidad	**X**	Otro	

Tabla 3.15. Perfil del Activo de información de servicio de correo electrónico

<table>
<tr><td></td><td colspan="4">PERFIL DE ACTIVO DE INFORMACIÓN CRÍTICO</td></tr>
<tr><td>Activo Crítico</td><td colspan="2">Justificación de selección

(¿Por qué este activo de información es importante para la organización?)</td><td colspan="2">Descripción</td></tr>
<tr><td>La información que se genera con el uso del servicio de videoconferencia</td><td colspan="2">Porque es el principal medio de comunicación cuando se realizan reuniones virtuales entre autoridades a nivel de gobierno o reuniones virtuales con autoridades de otros países. Además dar cumplimiento al acuerdo 166 de la SNAP.</td><td colspan="2">Videoconferencia</td></tr>
<tr><td colspan="5">Propietarios</td></tr>
<tr><td colspan="5">Oficial de Seguridad.

Área de redes y Comunicaciones.</td></tr>
<tr><td colspan="5">Requerimientos de seguridad</td></tr>
<tr><td>CONFIDENCIALIDAD</td><td>X</td><td colspan="2">Solo personal autorizado puede ver o acceder este activo de información.</td><td>Solo ciertos usuarios de los diferentes ministerios y Presidencia que tienen reserva de una sala virtual y tiene asignada una clave pueden tener acceso para hacer uso del activo de información.</td></tr>
<tr><td>INTEGRIDAD</td><td>X</td><td colspan="2">Solo personal autorizado puede modificar este activo de información.</td><td>El activo de información no debe ser alterado ni modificado incluso por personal de custodio de este activo bajo ningún motivo.</td></tr>
<tr><td rowspan="2">DISPONIBILIDAD</td><td rowspan="2">X</td><td colspan="2">Este activo de información debe estar disponible para los usuarios.</td><td>Solo ciertos usuarios de los diferentes ministerios y Presidencia pueden hacer uso de este activo de información donde quiera y a cualquier hora, de tal manera que puedan realizar su reunión virtual.</td></tr>
<tr><td colspan="2">Este activo de información debe estar disponible durante 24 horas, 7 días/semana, 365 días/año</td><td></td></tr>
<tr><td colspan="2">OTRO</td><td colspan="2">N/A</td><td>N/A</td></tr>
<tr><td colspan="5">El más importante requerimiento de seguridad</td></tr>
<tr><td colspan="5">Confidencialidad X | Integridad | Disponibilidad X | Otro</td></tr>
</table>

Tabla 3.16. Perfil del Activo de información de servicio de videoconferencia

3.1.3. IDENTIFICAR LOS CONTENEDORES DE LOS ACTIVOS DE INFORMACIÓN

Se debe mencionar que un contenedor es, donde un activo de información es almacenado, transportado, o procesado. Es el lugar donde el activo de información vive, en este caso puntual se evaluaran los activos tecnológicos, sitios físicos y las personas como contenedor de propiedad intelectual o conocimiento del servicio.

Se utilizan las plantillas Octave-Allegro 9a (activos tecnológicos), 9b (Lugares Físicos) y 9c (personas). Para cada servicio se identifica sus contenedores internos y externos de manera detallada.

3.1.3.1. Servicio de Correo Electrónico

	Contenedores Técnicos del activo de información
INTERNOS	
Descripción del contenedor	**Propietario**
1. La información es procesada por el servidor de MTA, el cual gestiona el envío y recepción de correos.	TI
2.- La información es almacena en el servidor de MAILBOX.	TI
3.- La información de la autenticación Es procesada por el servidor de LDAP el cual hace uso de las credenciales creadas en el servidor de Active Directory.	TI
4.- A nivel de red la información es procesada por los Switches de acceso/distribución/Core antes de llegar a su destino y al nivel de Core antes de ser procesada por los servidores.	TI
5.- Desde la PC/portátil la información es transportada por la LAN y WLAN hacia los servidores.	TI
6.- En la WLAN la información es procesada por la controladora antes de llegar a nivel de Core y posteriormente a los servidores.	TI
7.- A nivel de usuario final se requiere un navegador para procesar la información que se encuentra en el servidor del mailbox.	TI
8.- Dependiendo de la configuración del cliente de correo electrónico, la información puede estar almacenan en el disco local de PC/portátil.	TI
EXTERNOS	
Descripción del contenedor	**Propietario**
1. El Router de CNT procesa la información antes de enviarla a su WAN	CNT
2. La información es transportada a través de la WAN de CNT hacia la Internet	Desconocido

Tabla 3.17. Contenedores técnicos del servicio de correo electrónico

	Personas como contenedores del activo de información
INTERNOS	
Descripción del contenedor	**Propietario**
1. Administradores de redes e infraestructura responsables del servicio.	TI
2.- Personal de soporte técnico quienes ayudan al usuario final con la configuración de su cuenta de correo y respaldos.	TI
EXTERNOS	
Descripción del contenedor	**Propietario**
1. Personal de soporte del proveedor, en cual está destinado a resolución de problemas en los diferentes servidores donde se encuentra el activo de información.	SYNC

Tabla 3.18. Contenedores personas del servicio de correo electrónico

La Tabla 3.7 y 3.8 representan los contenedores tecnológicos y de persona del servicio de correo electrónico, de igual manera se realizara para el servicio de videoconferencia.

3.1.3.2. Videoconferencia

	Contenedores Técnicos del activo de información
INTERNOS	
Descripción del contenedor	**Propietario**
1. La información es procesada por el MCU para realizar la conexión y registro de los puntos finales al sistema de videoconferencia.	TI
2.- La información es procesada por el servidor de videoconferencia para la autentican respectiva y posterior ingreso a una sala virtual.	TI
3.- A nivel de red la información es procesada por los Switches de acceso/distribución antes de llegar a su destino y al nivel de Core antes de ser procesada por los servidores.	TI
4.- Desde la PC/portátil/equipo de videoconferencia la información es transportada por la LAN y WLAN, en la VLAN exclusiva para el sistema de videoconferencia, hacia los servidores.	TI
5.- En la WLAN la información es procesada por la controladora antes de llegar a nivel de Core y posteriormente al servidor.	TI
6.- La información de audio y video es procesada en los equipos de videoconferencia.	TI
7.- La información de audio y video es procesada por las PC/portátiles a través del acceso web al sistema de videoconferencia.	TI
EXTERNOS	
Descripción del contenedor	**Propietario**

1.- El Router de CNT procesa la información antes de enviarla a su WAN (Anillo Interministerial).	CNT
2.- La información es transportada a través del Anillo Interministerial provisto por CNT hacia las instituciones que hacen uso del sistema.	CNT
3.- La información de audio y video es procesada en los equipos de videoconferencia de las instituciones que pertenecen al Anillo Interministerial.	Ministerios, Secretarias y otras entidades del estado.
4.- La información de audio y video es procesada por las PC/portátiles a través del acceso web al sistema de videoconferencia.	Varios
5.- Como es servicio está publicado, la información es transportada a través de la Internet hacia sus usuarios en el mundo.	Desconocido

Tabla 3.19. Contenedores técnicos del servicio de videoconferencia

	Personas como contenedores del activo de información
INTERNOS	
Descripción del contenedor	**Propietario**
1. Administradores de redes e infraestructura responsables del servicio.	TI
2.- Personal de soporte técnico quienes ayudan a usuarios finales y en reuniones virtuales.	TI
EXTERNOS	
Descripción del contenedor	**Propietario**
1. Personal de soporte técnico quienes ayudan a usuarios finales y en reuniones virtuales.	Ministerios, Secretarias y otras entidades del estado.

Tabla 3.110. Contenedores personas del servicio de correo electrónico

3.1.4. IDENTIFICAR LOS ESCENARIOS DE AMENAZAS

Se hace uso de cuestionarios, anexo, para crear posibles escenarios que podrían afectar al activo de información en los diferentes contenedores anteriormente definidos. Se logra identificar, en el caso de que la respuesta sea afirmativa hay que pensar si este podría ocurrir de manera accidental o intencional.

En el escenario 3 se realizan preguntas enfocadas a indicar que tipo de impacto negativo tendría esa amenaza si se realizara.

Estas respuestas serán usadas como base en la identificación del riesgo.

3.1.4.1. Información del servicio correo electrónico

En las Tablas 3.11 a 3.14 se definen los posibles escenarios de amenazas para cada activo de información.

CUESTIONARIO 1	Contenedores Técnicos		
Escenario1: Pensar acerca de las personas que trabajan en la Institución. ¿Hay una situación en la que un empleado podría acceder a uno o más contenedores técnicos, accidentalmente o intencionalmente, causando que el activo de información sea:			
Expuesto a personas no autorizadas?	No	Si (Accidentalmente)	Si (Intencionalmente)
Modificado así que no sea utilizable para los fines previstos?.	No	Si (Accidentalmente)	Si (Intencionalmente)
Interrumpido así que no puede ser accedido para los fines previstos?.	No	Si (Accidentalmente)	Si (Intencionalmente)
Permanentemente destruido o temporalmente perdido así que no pueda ser usado para los fines previstos?.	No	Si (Accidentalmente)	Si (Intencionalmente)
Escenario2: Pensar en personas que son externas a la Institución. Podría incluir a personas que tienen relación de negocio con la Institución o no. ¿ Hay alguna situación en la cual un externo podría acceder a uno o más contenedores técnicos, accidental o intencionalmente, causando que el activo de información sea:			
Expuesto a personas no autorizadas?.	No	Si (Accidentalmente)	Si (Intencionalmente)
Modificado así que no sea utilizable para los fines previstos?.	No	Si (Accidentalmente)	Si (Intencionalmente)
Interrumpido así que no puede ser accedido para los fines previstos?.	No	Si (Accidentalmente)	Si (Intencionalmente)
Permanentemente destruido o temporalmente perdido así que no pueda ser usado para los fines previstos?.	No	Si (Accidentalmente)	Si (Intencionalmente)
Escenario3: Considerar situaciones que podrían afectar el activo de información en cualquier contenedor técnico identificado. Determinar si cualquiera de las siguientes situaciones podría ocurrir, y si es afirmativo, determinar si estas situaciones podrían causar uno o más de los siguientes resultados. • La divulgación no intencional del activo de información. • La modificación no intencional del activo de información. • La interrupción no intencional de la disponibilidad del activo de información. • La destrucción permanente o temporal no intencional del activo de información.			

Un defecto de software.	No	Si (Divulgación)	Si (Modificación)	Si (Interrupción)	Si (Perdida)

Un fallo del sistema de origen conocido o desconocido.	No	Si (Divulgación)	Si (Modificación)	Si (Interrupción)	Si (Perdida)
Un defecto de hardware.	No	Si (Divulgación)	Si (Modificación)	Si (Interrupción)	Si (Perdida)
Código malicioso (virus, gusanos, caballo de troya, o back door) es ejecutado.	No	Si (Divulgación)	Si (Modificación)	Si (Interrupción)	Si (Perdida)
Fuente de energía de los contenedores es interrumpida.	No	Si (Divulgación)	Si (Modificación)	Si (Interrupción)	Si (Perdida)
Problemas con las telecomunicaciones.	No	Si (Divulgación)	Si (Modificación)	Si (Interrupción)	Si (Perdida)
Otros problemas de terceros o sistemas.	No	Si (Divulgación)	Si (Modificación)	Si (Interrupción)	Si (Perdida)
Desastres naturales o causados por el hombre.	No	Si (Divulgación)	Si (Modificación)	Si (Interrupción)	Si (Perdida)

Tabla 3.111. Cuestionario 1 con posibles escenarios de amenazas.

CUESTIONARIO 2	**Contenedores del tipo persona**		
Escenario1: Pensar en las personas que trabajan en la Institución. ¿Hay una situación en la cual un empleado tiene conocimiento detallado de su activo de información y podría, accidental o intencionalmente, causar que el activo de información sea:			
Divulgado a personas no autorizadas?	No	Si (Accidentalmente)	Si (Intencionalmente)
Modificado, de tal manera que no sea utilizable para los fines previstos.	No	Si (Accidentalmente)	Si (Intencionalmente)
Interrumpido, así que no puede ser accedido para los fines previstos.	No	Si (Accidentalmente)	Si (Intencionalmente)
Permanentemente destruido o temporalmente perdido, así que no puede ser usado para los fines previstos.	No	Si (Accidentalmente)	Si (Intencionalmente)
Escenario2: Pensar en personas que son externas a la Institución. Esto podría personas quienes tienen una relación de negocio con al Institución o no. ¿Hay alguna situación en la cual un externo, accidental o intencionalmente, podría causar que el activo de información sea:			
Divulgado a personas no autorizadas?	No	Si (Accidentalmente)	Si (Intencionalmente)

Tabla 3.112. Cuestionario 2 con posibles escenarios de amenazas

3.1.4.2. Información del servicio de Videoconferencia

CUESTIONARIO 1	Contenedores Técnicos		
Escenario1: Pensar acerca de las personas que trabajan en la Institución. ¿Hay una situación en la que un empleado podría acceder a uno o más contenedores técnicos, accidentalmente o intencionalmente, causando que el activo de información sea:			
Expuesto a personas no autorizadas?.	No	Si (Accidentalmente)	Si (Intencionalmente)
Modificado así que no sea utilizable para los fines previstos?.	No	Si (Accidentalmente)	Si (Intencionalmente)
Interrumpido así que no puede ser accedido para los fines previstos?.	No	Si (Accidentalmente)	Si (Intencionalmente)
Permanentemente destruido o temporalmente perdido así que no pueda se usado para los fines previstos?.	No	Si (Accidentalmente)	Si (Intencionalmente)
Escenario2: Pensar en personas que son externas a la Institución. Podría incluir a personas que tienen relación de negocio con la Institución o no. ¿ Hay alguna situación en la cual un externo podría acceder a uno o más contenedores técnicos, accidental o intencionalmente, causando que el activo de información sea:			
Expuesto a personas no autorizadas?.	No	Si (Accidentalmente)	Si (Intencionalmente)
Modificado así que no sea utilizable para los fines previstos?.	No	Si (Accidentalmente)	Si (Intencionalmente)
Interrumpido así que no puede ser accedido para los fines previstos?.	No	Si (Accidentalmente)	Si (Intencionalmente)
Permanentemente destruido o temporalmente perdido así que no pueda ser usado para los fines previstos?	No	Si (Accidentalmente)	Si (Intencionalmente)
Escenario3: Considerar situaciones que podrían afectar el activo de información en cualquier contenedor técnico identificado. Determinar si cualquier de lo siguiente podría ocurrir, y si es afirmativo, determinar si etas situaciones podrían causar uno o más de los siguientes resultados. • La divulgación no intencional del activo de información. • La modificación no intencional del activo de información. • La interrupción no intencional de la disponibilidad del activo de información. • La destrucción permanente o temporal no intencional del activo de información.			
Un defecto de software.	No	Si (Divulgación)	Si (Modificación)	Si (Interrupción)	Si (Perdida)

Un fallo del sistema de origen conocido o desconocido.	No	Si (Divulgación)	Si (Modificación)	Si (Interrupción)	Si (Perdida)
Un defecto de hardware.	No	Si (Divulgación)	Si (Modificación)	Si (Interrupción)	Si (Perdida)
Código malicioso (virus, gusanos, caballo de troya, o back door) es ejecutado.	No	Si (Divulgación)	Si (Modificación)	Si (Interrupción)	Si (Perdida)
Fuente de energía de los contenedores es interrumpida.	No	Si (Divulgación)	Si (Modificación)	Si (Interrupción)	Si (Perdida)
Problemas con las telecomunicaciones.	No	Si (Divulgación)	Si (Modificación)	Si (Interrupción)	Si (Perdida)
Otros problemas de terceros o sistemas.	No	Si (Divulgación)	Si (Modificación)	Si (Interrupción)	Si (Perdida)
Desastres naturales o causados por el hombre	No	Si (Divulgación)	Si (Modificación)	Si (Interrupción)	Si (Perdida)

Tabla 3.113. Cuestionario 1 con posibles escenarios de amenazas

CUESTIONARIO 2	**Contenedores del tipo persona**		
Escenario1: Pensar en las personas que trabajan en la Institución. ¿Hay una situación en la cual un empleado tiene conocimiento detallado de su activo de información y podría, accidental o intencionalmente, causar que el activo de información sea:			
Divulgado a personas no autorizadas?	No	Si (Accidentalmente)	Si (Intencionalmente)
Modificado, de tal manera que no sea utilizable para los fines previstos.	No	Si (Accidentalmente)	Si (Intencionalmente)
Interrumpido, así que no puede ser accedido para los fines previstos.	No	Si (Accidentalmente)	Si (Intencionalmente)
Permanentemente destruido o temporalmente perdido, así que no puede ser usado para los fines previstos.	No	Si (Accidentalmente)	Si (Intencionalmente)

Escenario2: Pensar en personas que son externa a la Institución. Esto podría personas quienes tienen una relación de negocio con la Institución o no. ¿Hay alguna situación en la cual un externo, accidental o intencionalmente, causar que el activo de información sea:			
Divulgado a personas no autorizadas?	No	Si (Accidentalmente)	Si (Intencionalmente)

Tabla 3.114. Cuestionario 2 con posibles escenarios de amenazas

3.1.5. IDENTIFICAR ÁREAS DE INTERÉS Y RIESGOS DEL ACTIVO DE INFORMACIÓN

Para este paso se utiliza la plantilla 10 de Octave-Allegro que se encuentra en el anexo.

Un área de preocupación es una declaración descriptiva que detalla una condición o situación del mundo real que pueda afectar al activo de información. Cabe mencionar que para cada servicio se definieron alrededor de 25 áreas de preocupación.

De acuerdo al área de preocupación definida las consecuencias y la probabilidad de ocurrencia irán variando.

La sección de amenaza se compone algunas variables como, en si el activo de información, el área de preocupación, el actor (agente) es decir quien podría explotar el área de preocupación, el medio es como explotaría el área de preocupación, la motivación puede ser accidental o intencional, la consecuencia es lo que podría resultar de afectar al activo de información, los requerimientos de seguridad que podrían acortar la brecha y la probabilidad que este escenario de amenaza ocurra.

El campo severidad se conforma de las áreas de impacto seleccionadas en la sección 3.1, hay que tomar en cuenta que se usa el valor o escala de importancia de 1 a 3 siendo 1 el más bajo y 3 el más alto.

El campo valor se deriva de la escala seleccionada para cada área de impacto, la cual es alta, media y baja, para realizar el cálculo de la puntuación del riesgo estos niveles se traducen a números es decir alta=3, media=2, baja=1.

Al final se suma la columna de la puntuación para obtener el valor de riesgo en las áreas de interés con la amenaza analizada.

Las siguientes plantillas se han identificado son un número en la esquina superior derecha, ya que pertenecen a las plantillas definidas en el método para determinar las amenazas de un mismo activo de información.

3.1.5.1. Correo electrónico

1.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Correo Electrónico**			
		Áreas de preocupación	Que un empleado haga uso del equipo PC/portátil que no esté a su cargo y accidentalmente accede al buzón donde se encuentra el activo de información del usuario encargado de ese equipo.			
		Actor	Empleado			
		Medio	Acceso web en una PC/portátil			
		Motivo	Accidental			
		Consecuencias	**Divulgación**	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Tener un control de acceso a la red para que no se pueda faltar a la confidencialidad.			
		Probabilidad	Alta	**Media**	Baja	
	Consecuencias		**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
	Si este escenario ocurriera en el área de Talento Humano, se podría encontrar con posibles aspirantes a nuevos cargos y la información de remuneraciones.		Reputación.	Alto	9	
			Financiera.			
			Productividad.	Alto	6	
			Seguridad y salud.			
			Multas y sanciones legales.			
			Cumplimiento de regulaciones.	bajo	1	

2.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Correo Electrónico**			
		Áreas de preocupación	Un empleado intencionalmente haga uso del PC/portátil que no está a su cargo para obtener información.			
		Actor	Empleado			
		Medio	Acceso web en una PC/portátil			
		Motivo	Quiere obtener información y sacar provecho.			
		Consecuencias	**Divulgación**	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Mantener la confidencialidad a base de políticas que indiquen al usuario el uso de sus claves			
		Probabilidad	Alta	**Media**	Baja	
	Consecuencias		**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
	Conseguir la información tales de una cuenta de alguna autoridad y poder enviarle correos mal intencionado.		Reputación.	Medio	6	
			Financiera.			
			Productividad.	Bajo	4	
			Seguridad y salud.			
			Multas y sanciones legales.			
			Cumplimiento de regulaciones.	Bajo	2	

3.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Correo Electrónico**			
		Áreas de preocupación	El usuario dueño del activo de información realiza una mala configuración de respaldo de su buzón y su información se borra permanentemente.			
		Actor	Empleado			
		Medio	Acceso web en una PC/portátil o uso del cliente de escritorio.			
		Motivo	Accidental			
		Consecuencias	Divulgación	Modificación	**Destrucción**	Interrupción

DEL	A	**Requerimientos de seguridad**	Mejorar los procedimientos de manejo de respaldos de los usuarios.		
		Probabilidad	Alta	**Media**	Baja
	Consecuencias		**Severidad**		
			Área de impacto	**Valor**	**Puntuación**
ACTIVO	La pérdida definitiva de la información, ya que al momento de descargar los correo de manera local, se requiere un cliente de correo.		Reputación.	Bajo	3
			Financiera.		
DE			Productividad.	Alto	6
			Seguridad y salud.		
			Multas y sanciones legales.		
INFORMACIÓN			Cumplimiento de regulaciones.	Medio	2

4.			**RIESGO DEL ACTIVO DE INFORMACIÓN**			
	A	**Activo de Información**	**Correo Electrónico**			
	M	**Áreas de preocupación**	Un usuario busca la manera de obtener la clave de acceso a un buzón en particular para borrar un correo que no quiere que lea el remitente.			
	E	**Actor**	Empleado			
	N	**Medio**	Acceso web en una PC/portátil o uso del cliente de escritorio.			
	A	**Motivo**	Borrar información que pudiera comprometer al usuario en alguna situación.			
RIESGO	Z	**Consecuencias**	Divulgación	Modificación	**Destrucción**	Interrupción
	A	**Requerimientos de seguridad**	Almacenar los logs de cambios en un repositorio para una post auditoría.			
DEL		**Probabilidad**	Alta	**Media**	Baja	
	Consecuencias		**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
ACTIVO	Que el usuario obtenga la clave de esa persona y que lo difunda.		Reputación.	Alta	9	
			Financiera.			
DE			Productividad.	Alta	6	
			Seguridad y salud.			
			Multas y sanciones legales.			
INFORMACIÓN			Cumplimiento de regulaciones.	Alta	3	

5.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Correo Electrónico**			
		Áreas de preocupación	El robo del dispositivo donde se tiene configurado el buzón de correo, podría permitir el acceso al activo de información.			
		Actor	Ladrón			
		Medio	robo			
		Motivo	Accidental			
		Consecuencias	**Divulgación**	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Mantener la confidencialidad de la información por medio de un administrador de dispositivos móviles.			
		Probabilidad	Alta	Media	**Baja**	
		Consecuencias	**Área de impacto**	**Valor**	**Severidad** **Puntuación**	
		La información almacenada en el dispositivo móvil puede ser divulgada y/o vendida.	Reputación.	Alta	9	
			Financiera.			
			Productividad.	baja	2	
			Seguridad y salud.			
			Multas y sanciones legales.			
			Cumplimiento de regulaciones.	Media	2	

6.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO	AMENAZA	**Activo de Información**	**Correo Electrónico**			
		Áreas de preocupación	Hactivistas, haciendo uso métodos sofisticados de acceso, podrían acceder al servidor donde se encuentra la información.			
		Actor	Grupos de Hackers			
		Medio	Acceso vía web usando herramienta de hackeo.			
		Motivo	Supuesta lucha contra la libertad de expresión.			
		Consecuencias	**Divulgación**	Modificación	Destrucción	Interrupción

DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Requerimientos de seguridad**	Contar con equipos de seguridad perimetral y políticas fuertes de aseguramiento de claves.		
		Probabilidad	**Alta**	Media	Baja
		Consecuencias	**Severidad**		
			Área de impacto	**Valor**	**Puntuación**
		Robo de información confidencial, agenda, contactos, etc., de autoridades de la institución.	Reputación.	Alto	9
			Financiera.		
			Productividad.	Alto	6
			Seguridad y salud.		
			Multas y sanciones legales.		
			Cumplimiento de regulaciones.	Medio	3

7.			**RIESGO DEL ACTIVO DE INFORMACIÓN**			
RIESGO DEL ACTIVO DE	AMENAZA	**Activo de Información**	**Correo Electrónico**			
		Áreas de preocupación	Personal de la empresa proveedora que está encargada del soporte de la plataforma podría acceder de forma remota al activo para realizar cierta configuración y en el proceso baja un servicio de algún servidor de manera involuntaria.			
		Actor	SYNC			
		Medio	Acceso remoto usando algún tipo de agente			
		Motivo	Soporte remoto			
		Consecuencias	Divulgación	Modificación	Destrucción	**Interrupción**
		Requerimientos de seguridad	Mantener la el monitoreo de disponibilidad de los servidores.			
		Probabilidad	Alta	**Media**	Baja	
		Consecuencias	**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
		Que no se pueda despachar resúmenes informativos diarios a	Reputación.	Media	6	
			Financiera.			
			Productividad.	Alta	6	

INFORMACIÓN	las autoridades, incluso al Sr. Presidente.	Seguridad y salud.		
		Multas y sanciones legales.		
		Cumplimiento de regulaciones.	Baja	1

8.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	**AMENAZA**	**Activo de Información**	**Correo Electrónico**			
		Áreas de preocupación	Una persona externa haciendo uso de software malicioso puede realizar varias peticiones de conexión al MTA hasta que el servicio caiga.			
		Actor	Hacker			
		Medio	La Internet			
		Motivo	Diferencias en tendencias políticas.			
		Consecuencias	Divulgación	Modificación	Destrucción	**Interrupción**
		Requerimientos de seguridad	Mantener la el monitoreo de disponibilidad de los servidores.			
		Probabilidad	**Alta**	Media	Baja	
ACTIVO DE INFORMACIÓN	**Consecuencias**		**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
	Evitar que la información a cualquier evento que estaba planificada sea retrasada y genere retrasos a las personas que lo coordinan.		Reputación.	Alta	9	
			Financiera.			
			Productividad.	Alta	6	
			Seguridad y salud.			
			Multas y sanciones legales.			
			Cumplimiento de regulaciones.	Baja	1	

9.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Correo Electrónico**			
		Áreas de preocupación	Personal de la empresa proveedora que está encargada del soporte de la plataforma, en un mantenimiento podría borrar información del mailbox.			
		Actor	SYNC			
		Medio	Conexión remota			
		Motivo	Soporte y/o resolución de problemas			
		Consecuencias	Divulgación	Modificación	**Destrucción**	Interrupción
		Requerimientos de seguridad	Realizar respaldos periódicos en un servidor de respaldos.			
		Probabilidad	**Alta**	Media	Baja	

ACTIVO DE INFORMACIÓN	**Consecuencias**	**Severidad**		
		Área de impacto	**Valor**	**Puntuación**
	Perdida de información sensible para cada uno de los usuarios en cada ámbito de trabajo.	Reputación.	Alta	9
		Financiera.		
		Productividad.	Alta	6
		Seguridad y salud.		
		Multas y sanciones legales.		
		Cumplimiento de regulaciones.	Media	2

10.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO	AMENAZA	**Activo de Información**	**Correo Electrónico**			
		Áreas de preocupación	Una persona externa haciendo uso de un software malicioso de descubrimiento de claves para acceder al buzón de correo y borrar toda la información.			
		Actor	Hacker			
		Medio	La Internet			
		Motivo	Demostrar que se puede hacer a más de robar información.			
		Consecuencias	Divulgación	Modificación	**Destrucción**	Interrupción

DEL		**Requerimientos de seguridad**	Poder detectar a las intrusiones desde la Internet.		
		Probabilidad	**Alta**	Media	Baja
ACTIVO		**Consecuencias**	**Severidad**		
			Área de impacto	**Valor**	**Puntuación**
DE		Ataques dirigidos a las autoridades de la institución con el fin de obtener información en algunos casos sensible.	Reputación.	Alta	9
			Financiera.		
			Productividad.	Media	4
			Seguridad y salud.		
INFORMACIÓN			Multas y sanciones legales.		
			Cumplimiento de regulaciones.	Media	2

11.		**RIESGO DEL ACTIVO DE INFORMACIÓN**				
RIESGO	AMENAZA	**Activo de Información**	**Correo Electrónico**			
		Áreas de preocupación	Después de realizar una actualización de versión, los servicios no se ejecuten de manera adecuada.			
		Actor	TI, SYNC			
		Medio	Acceso remoto			
DEL		**Motivo**	Actualización de la versión de la plataforma.			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
ACTIVO		**Requerimientos de seguridad**	Generar un manual de procedimiento para las actualizaciones de la plataforma.			
		Probabilidad	Alta	**Media**	Baja	
DE		**Consecuencias**	**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
INFORMACIÓN		Malestar y retraso en la coordinación para ciertos eventos presidenciales. Además de malestar en los usuarios al no poder realizar su trabajo de manera ágil.	Reputación.	Baja	3	
			Financiera.			
			Productividad.	Alta	6	
			Seguridad y salud.			
			Multas y sanciones legales.			

		Cumplimiento de regulaciones.	Baja	1

12.		RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Correo Electrónico**		
		Áreas de preocupación	Al momento de usar un software de escritorio para realizar el archivado de correos antiguos este no realice el respaldo de manera adecuada y se pierda la información.		
		Actor	Usuario final		
		Medio	PC/portátil acceso vía cliente o web.		
		Motivo	Respaldo de la información.		
		Consecuencias	Divulgación	Modificación	Destrucción / Interrupción
		Requerimientos de seguridad	Generar un manual de procedimiento de configuración de respaldos para usuarios finales.		
		Probabilidad	**Alta**	Media	Baja
	Consecuencias		**Severidad**		
			Área de impacto	**Valor**	**Puntuación**
	No poder utilizar alguna información anterior para algún tipo de informe o investigación.		Reputación.	Baja	3
			Financiera.		
			Productividad.	Alta	6
			Seguridad y salud.		
			Multas y sanciones legales.		
			Cumplimiento de regulaciones.	baja	1

13.		RIESGO DEL ACTIVO DE INFORMACIÓN	
	AMENAZA	**Activo de Información**	**Correo Electrónico**
		Áreas de preocupación	Fallo del sistema base en los servidores donde se encuentra la plataforma de correo.
		Actor	TI
		Medio	Servidor

RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Motivo**	Configuración errónea del sistema base.			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Guía de configuración específica.			
		Probabilidad	Alta	**Media**	Baja	
		Consecuencias	**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
		Podría causar la pérdida total de la información y afectar la disponibilidad.	Reputación.	Baja	3	
			Financiera.			
			Productividad.	Alta	6	
			Seguridad y salud.			
			Multas y sanciones legales.			
			Cumplimiento de regulaciones.	baja	1	

14.			**RIESGO DEL ACTIVO DE INFORMACIÓN**			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Correo Electrónico**			
		Áreas de preocupación	Insuficientes recursos de memoria y/o CPU en la plataforma de virtualización y por tal razón los servidores no procesarían el activo de información de manera adecuada.			
		Actor	TI			
		Medio	Virtualización			
		Motivo	Falta de recursos			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Plan de contingencia.			
		Probabilidad	Alta	**Media**	Baja	
		Consecuencias	**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	

INFORMACIÓN	Indisponibilidad de la plataforma, no procesamiento de ciertos correos y hasta pérdida de los mismos.	Reputación.	Alta	9
		Financiera.		
		Productividad.	Alta	6
		Seguridad y salud.		
		Multas y sanciones legales.		
		Cumplimiento de regulaciones.	Media	3

15.			**RIESGO DEL ACTIVO DE INFORMACIÓN**			
RIESGO DEL ACTIVO DE INFORMACIÓN	**AMENAZA**	**Activo de Información**	**Correo Electrónico**			
		Áreas de preocupación	Abrir de correos de remitentes desconocidos que contienen adjuntos, que al momento de dar clic se ejecuta un backdoor que podrían realizar un reenvió de los correo a sitios externos.			
		Actor	Usuario			
		Medio	PC/portátil del usuario			
		Motivo	Abrir correos maliciosos por curiosidad			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Educar al usuario final			
		Probabilidad	**Alta**	Media	Baja	
	Consecuencias		**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
	Divulgación de información en algunos casos sensible y en otra información de eventos presidenciales.		Reputación.	Alta	9
			Financiera.			
			Productividad.	Baja	3	
			Seguridad y salud.			
			Multas y sanciones legales.			
			Cumplimiento de regulaciones.	Baja	1	

16.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Correo Electrónico**			
		Áreas de preocupación	Ingreso de un gusano/troyano a través de la Internet, el cual por medio de la red llegue al servidor de MTA y/o Mailbox y que contenga en su código una instrucción de apagado de los servidores.			
		Actor	Usuario			
		Medio	PC/portátil del usuario			
		Motivo	Abrir correos maliciosos por curiosidad			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Educar al usuario final sobre los sitios maliciosos que podrían visitar.			
		Probabilidad	**Alta**	Media	Baja	
		Consecuencias	**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
		Perdida de información en procesamiento, malestar en los cerca de 600 usuarios, y que no llegue información importante desde otras entidades públicas.	Reputación.	Alta	9	
			Financiera.			
			Productividad.	Alta	6	
			Seguridad y salud.			
			Multas y sanciones legales.			
			Cumplimiento de regulaciones.	Media	2	

17.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO	AMENAZA	**Activo de Información**	**Correo Electrónico**			
		Áreas de preocupación	Ingreso de un virus a través de la Internet a la PC del usuario, que contenga en su código una instrucción de borrado de la PC, en el supuesto de tener mis correos de almacenados de manera local.			
		Actor	Usuario			
		Medio	PC/portátil del usuario y la Internet			
		Motivo				
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Educar al usuario final			

DEL		**Probabilidad**	Alta	**Media**	Baja
		Consecuencias	**Severidad**		
			Área de impacto	**Valor**	**Puntuación**
ACTIVO	Dañar la PC, y por ende dañar la información de los correos si se la configuración de él se encuentran en carpetas locales.		Reputación.	baja	3
			Financiera.		
DE			Productividad.	Alta	6
			Seguridad y salud.		
			Multas y sanciones legales.		
INFORMACIÓN			Cumplimiento de regulaciones.	Baja	2

18.			**RIESGO DEL ACTIVO DE INFORMACIÓN**			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Correo Electrónico**			
		Áreas de preocupación	Configuración de rutas en el Switch de Core podrían impedir que el activo de información sea procesado de manera adecuada.			
		Actor	TI			
		Medio	Acceso remoto			
		Motivo	Configuración de rutas			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Manuales de procedimiento por parte de TI			
		Probabilidad	Alta	Media	**Baja**	
		Consecuencias	**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
	No se envíen los correos y se queden encolados en el MTA, por lo tanto no se coordina de mejor manera algún tipo de evento presidencial.		Reputación.	Media	6	
			Financiera.			
			Productividad.	Alta	6	
			Seguridad y salud.			
			Multas y sanciones legales.			
			Cumplimiento de regulaciones.	Baja	1	

19.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Correo Electrónico**			
		Áreas de preocupación	Que los enlaces provistos por el ISP dejen de prestar su servicio de un momento a otro.			
		Actor	CNT			
		Medio	Acceso remoto al router			
		Motivo	Configuración del equipo de borde			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Monitoreo de los enlaces con			
		Probabilidad	Alta	Media	**Baja**	
ACTIVO DE INFORMACIÓN	**Consecuencias**		**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
	No envío de correos en algunos casos urgentes a varios ministerios por parte de autoridades de la Presidencia.		Reputación.	Alto	9	
			Financiera.			
			Productividad.	Alto	6	
			Seguridad y salud.			
			Multas y sanciones legales.			
			Cumplimiento de regulaciones.	bajo	1	

20.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Correo Electrónico**			
		Áreas de preocupación	Un incendio en el Centro de Datos.			
		Actor	NA			
		Medio	Acceso físico			
		Motivo	NA			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Monitoreo de los enlaces con			
		Probabilidad	Alta	Media	**Baja**	
ACTIVO DE INFORMACIÓN	**Consecuencias**		**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	

DE INFORMACIÓN	Despido de personal de TI y pérdida definitiva de la información.	Reputación.	Baja	3
		Financiera.		
		Productividad.	Alta	6
		Seguridad y salud.		
		Multas y sanciones legales.		
		Cumplimiento de regulaciones.	Baja	1

21.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Correo Electrónico**			
		Áreas de preocupación	El o los administradores del servicio, al momento de realizar un seguimiento y monitoreo de los correos se verifica el origen, destino y cuerpo del mensaje.			
		Actor	Administrador			
		Medio	Consola de administración			
		Motivo	Hacer seguimiento			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Acuerdo de confidencialidad para los Administradores.			
		Probabilidad	Alta	**Media**	Baja	
	Consecuencias		**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
	Divulgación de información en algunos casos sensible.		Reputación.	Alta	9	
			Financiera.			
			Productividad.	Media	4	
			Seguridad y salud.			
			Multas y sanciones legales.			
			Cumplimiento de regulaciones.	Media	2	

22.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Correo Electrónico**			
		Áreas de preocupación	Un ex administrador del servicio que podría buscar lucrar con la información que maneja.			
		Actor	Administrador enojado que salió.			
		Medio	Vía Internet			
		Motivo	Hacer seguimiento			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Acuerdo de confidencialidad para los Administradores.			
		Probabilidad	Alta	Media	**Baja**	
	Consecuencias		**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
	Pérdida de confianza en el área de TI.		Reputación.	Alta	9	
			Financiera.			
			Productividad.	Media	4	
			Seguridad y salud.			
			Multas y sanciones legales.			
			Cumplimiento de regulaciones.	Media	2	

23.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Correo Electrónico**			
		Áreas de preocupación	Personal de TI en un mantenimiento no planificado.			
		Actor	Administrador de TI			
		Medio	Vía remota			
		Motivo	Mantenimiento			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Planificar los mantenimientos.			
		Probabilidad	Alta	**Media**	Baja	
			Severidad			
			Área de impacto	**Valor**	**Puntuación**	

	Consecuencias			
DE	Perdida de disponibilidad del servicio por varias horas y despidos en el área de TI.	Reputación.	Alta	9
		Financiera.		
		Productividad.	Alta	6
INFORMACIÓN		Seguridad y salud.		
		Multas y sanciones legales.		
		Cumplimiento de regulaciones.	Media	2

24.			**RIESGO DEL ACTIVO DE INFORMACIÓN**			
	A	**Activo de Información**	**Correo Electrónico**			
	M	**Áreas de preocupación**	Alguna persona del personal de TI que quiera causar daño a la institución.			
	E	**Actor**	Un administrador de TI			
	N	**Medio**	Vía remota, web, etc.			
RIESGO	**A**	**Motivo**	Robar información sensible.			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
DEL	**Z**	**Requerimientos de seguridad**	Control de acceso para mantener la confidencialidad de la información.			
	A	**Probabilidad**	**Alta**	Media	Baja	
			Severidad			
ACTIVO	**Consecuencias**		**Área de impacto**	**Valor**	**Puntuación**	
	Pérdida de confianza en el uso del servicio por parte de los usuarios.		Reputación.	Baja	3	
DE			Financiera.			
			Productividad.	Alta	6	
			Seguridad y salud.			
INFORMACIÓN			Multas y sanciones legales.			
			Cumplimiento de regulaciones.	Media	2	

25.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Correo Electrónico**			
		Áreas de preocupación	Personal de TI al momento de realizar el backup de la información del usuario final en carpetas locales no realiza el procedimiento correcto.			
		Actor	Persona de TI			
		Medio	PC/portátil acceso web o por cliente de escritorio			
		Motivo	respaldos			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Tener un sitio de respaldos par que el respaldo se quede almacenada.			
		Probabilidad	**Alta**	Media	Baja	
	Consecuencias		**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
	No poder entregar informes haciendo uso de información anterior como antecedente.		Reputación.	Baja	3	
			Financiera.			
			Productividad.	Alta	6	
			Seguridad y salud.			
			Multas y sanciones legales.			
			Cumplimiento de regulaciones.	Baja	1	

26.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Correo Electrónico**			
		Áreas de preocupación	Personal de la empresa proveedora, en una revisión preventiva autorizada al mailbox podría encontrarse con información sensible.			
		Actor	SYNC			
		Medio	Acceso remoto			
		Motivo	Revisión de servidores			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Gestión de cambios			
		Probabilidad	Alta	**Media**	Baja	

		Severidad		
	Consecuencias	**Área de impacto**	**Valor**	**Puntuación**
DEL	Conocer de primera mano y con anterioridad la ubicación de los eventos del Sr. Presidente.	Reputación.	Alta	9
		Financiera.		
ACTIVO		Productividad.	Baja	2
		Seguridad y salud.		
		Multas y sanciones legales.		
DE		Cumplimiento de regulaciones.	Baja	1
INFORMACIÓN				

27.		**RIESGO DEL ACTIVO DE INFORMACIÓN**			
	AMENAZA	**Activo de Información**	**Correo Electrónico**		
		Áreas de preocupación	Personal de la empresa proveedora que tiene autorización para el acceso remoto puede extraer información.		
		Actor	SYNC		
		Medio	Acceso remoto		
RIESGO		**Motivo**	Revisión de servidores o mantenimiento		
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
DEL		**Requerimientos de seguridad**	Control de acceso para usuarios remotos		
		Probabilidad	Alta	Media	Baja

		Severidad		
	Consecuencias	**Área de impacto**	**Valor**	**Puntuación**
ACTIVO	Conocer de primera mano y con anterioridad la ubicación de los eventos del Sr. Presidente y además conocer el trabajo de los usuarios.	Reputación.	Alta	9
		Financiera.		
DE		Productividad.	Baja	2
		Seguridad y salud.		
		Multas y sanciones legales.		
INFORMACIÓN		Cumplimiento de regulaciones.	Baja	1

3.1.5.2. Videoconferencia

1.						
		RIESGO DEL ACTIVO DE INFORMACIÓN				
RIESGO DEL ACTIVO DE INFORMACIÓN	**AMENAZA**	**Activo de Información**	**Videoconferencia**			
		Áreas de preocupación	Una persona que conozca las credenciales de la sala virtual donde se llevará a cabo la reunión y accede vía web a dicha sala.			
		Actor	Empleado			
		Medio	A través de la red o la Internet			
		Motivo	Venta de información			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Crear métodos de autenticación para que la confidencialidad no sea vulnerada.			
		Probabilidad	**Alta**	Media	Baja	
		Consecuencias	**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
		Divulgar información tratada en la reunión entre el Sr. Presidente y Ministros.	Reputación.	Alta	9	
			Financiera.			
			Productividad.	Baja	2	
			Seguridad y salud.			
			Multas y sanciones legales.			
			Cumplimiento de regulaciones.	Media	3	

2.						
		RIESGO DEL ACTIVO DE INFORMACIÓN				
	AMENAZA	**Activo de Información**	**Videoconferencia**			
		Áreas de preocupación	Un empleado curioso quiere de ingresar vía web al sistema de videoconferencia, de tal manera que busca una herramienta generadora de claves de acceso, esto podría ocasionar demasiadas peticiones de conexión que el servicio podría caerse.			
		Actor	Empleado			
		Medio	A través de la red o la Internet			
		Motivo	Curiosidad			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción

RIESGO	A	**Requerimientos de seguridad**	Crear un política de numero de intentos de login		
		Probabilidad	Alta	**Media**	Baja
DEL		**Consecuencias**	**Severidad**		
			Área de impacto	**Valor**	**Puntuación**
ACTIVO		Causar retraso en caso una reunión entre autoridades del país.	Reputación.	Baja	3
			Financiera.		
			Productividad.	Alta	6
DE			Seguridad y salud.		
			Multas y sanciones legales.		
INFORMACIÓN			Cumplimiento de regulaciones.	Media	2

3.			RIESGO DEL ACTIVO DE INFORMACIÓN			
	A	**Activo de Información**	**Videoconferencia**			
	M	**Áreas de preocupación**	Personal de otros ministerios que requieren hacer pruebas las hace sin previa coordinación, podría ingresar a una sala que no sea de pruebas y se esté llevando a cabo una reunión.			
	E	**Actor**	Empleado de al Ministerio			
	N	**Medio**	A través del anillo Interministerial o la Internet			
RIESGO	A	**Motivo**	Pruebas			
	Z	**Consecuencias**	Divulgación	Modificación	Destrucción	Interrupción
DEL	A	**Requerimientos de seguridad**	Informa a los usuarios sobre el procedimiento para pruebas.			
		Probabilidad	**Alta**	Media	Baja	
ACTIVO		**Consecuencias**	**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
DE		Conocer información tratada en la reunión entre el Sr. Presidente y Ministros o entre Ministros.	Reputación.	Alta	9	
			Financiera.			
			Productividad.	Baja	2	
INFORMACIÓN			Seguridad y salud.			
			Multas y sanciones legales.			
			Cumplimiento de regulaciones.	Alta	3	

4.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Videoconferencia**			
		Áreas de preocupación	Personas externas que quieren ingresar a la sala virtual vía web, podrían hacer uso de herramientas sofisticada de generación de claves, de tal manera que encuentren una para el acceso a una sala.			
		Actor	Hacker			
		Medio	A través del anillo Interministerial o la Internet			
		Motivo	Conocer información confidencial			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Informa a los usuarios sobre el procedimiento para pruebas.			
		Probabilidad	**Alta**	Media	Baja	
		Consecuencias	**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
		Conocer información tratada en la reunión entre el Sr. Presidente y Ministros o entre Ministros.	Reputación.	Alta	9	
			Financiera.			
			Productividad.	Baja	2	
			Seguridad y salud.			
			Multas y sanciones legales.			
			Cumplimiento de regulaciones.	Media	3	

5.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Videoconferencia**			
		Áreas de preocupación	Generar alto tráfico de entrada hasta que el Router del ISP deje de funcionar.			
		Actor	Hacker			
		Medio	A través del anillo Interministerial o la Internet			
		Motivo	Ego o iniciación en el camino de un atacante.			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Informa a los usuarios sobre el procedimiento para pruebas.			
		Probabilidad	Alta	**Media**	Baja	

ACTIVO DE INFORMACIÓN	**Consecuencias**	**Severidad**		
		Área de impacto	**Valor**	**Puntuación**
	Causar retraso en caso una reunión entre autoridades del país.	Reputación.	Baja	3
		Financiera.		
		Productividad.	Alta	6
		Seguridad y salud.		
		Multas y sanciones legales.	Baja	1
		Cumplimiento de regulaciones.		

6.			**RIESGO DEL ACTIVO DE INFORMACIÓN**			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Videoconferencia**			
		Áreas de preocupación	El acceso vía web solo requiere un pin de 4 dígitos numéricos, por esta razón es más probable que se descubre un pin de acceso.			
		Actor	Cualquiera			
		Medio	A través del anillo Interministerial o la Internet vía web			
		Motivo	Accidental			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Encontrar algún método que proteja el acceso via web.			
		Probabilidad	**Alta**	Media	Baja	
ACTIVO DE INFORMACIÓN	**Consecuencias**	**Severidad**				
		Área de impacto	**Valor**	**Puntuación**		
	Acceso a una sala determinada y obtener información confidencial.	Reputación.	Alta	9		
		Financiera.				
		Productividad.	Baja	2		
		Seguridad y salud.				
		Multas y sanciones legales.				
		Cumplimiento de regulaciones.	Media	2		

7.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Videoconferencia**			
		Áreas de preocupación	Por ser software antiguo podrida causar que los servicios dejen de funcionar.			
		Actor	Servidor			
		Medio	Servidor			
		Motivo	Software antiguo			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	De ser posible actualizar el software a una versión más actual.			
		Probabilidad	**Alta**	Media	Baja	
	Consecuencias		**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
	Retraso en alguna tipo de reunión entre el Sr. Presidente y Ministros.		Reputación.	Baja	3	
			Financiera.			
			Productividad.	Alta	6	
			Seguridad y salud.			
			Multas y sanciones legales.			
			Cumplimiento de regulaciones.	Media	2	

8.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Videoconferencia**			
		Áreas de preocupación	En algunas ocasiones los servicio de videoconferencia y acceso vía web se deshabilitan sin ninguna razón.			
		Actor	Servidor			
		Medio	Servidor			
		Motivo	Software antiguo			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	De ser posible actualizar el software a una versión más actual.			
		Probabilidad	Alta	**Media**	Baja	
	Consecuencias		**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	

DE INFORMACIÓN	Retrasaría el inicio de un gabinete virtual.	Reputación.	Baja	3
		Financiera.		
		Productividad.	Alta	6
		Seguridad y salud.		
		Multas y sanciones legales.		
		Cumplimiento de regulaciones.	Baja	1

9.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Videoconferencia**			
		Áreas de preocupación	Los discos de servidor pueden dañarse y por ser un servidor descontinuado, es casi imposible obtener discos de nuevos para su reemplazo.			
		Actor	Servidor			
		Medio	Servidor			
		Motivo	Servidor antiguo			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	De ser posible actualizar el hardware para evitar la indisponibilidad			
		Probabilidad	Alta	Media	**Baja**	
	Consecuencias		**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
	Retrasaría el inicio de un gabinete virtual.		Reputación.	Baja	3	
			Financiera.			
			Productividad.	Alta	6	
			Seguridad y salud.			
			Multas y sanciones legales.			
			Cumplimiento de regulaciones.	Baja	1	

10.			RIESGO DEL ACTIVO DE INFORMACIÓN
	AM	**Activo de Información**	**Videoconferencia**
		Áreas de preocupación	Algún tipo de backdoor en el servidor o PC/portátil, el cual este redirigiendo la información de las sesiones de las salas virtuales.

RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Actor**	Software malicioso en el servidor, PC/portátil			
		Medio	Red			
		Motivo	Enviar información a destinos no autorizados			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Proteger la confidencialidad del activo con la instalación de algún tipo de antivirus tanto en la PC como a nivel de servidor.			
		Probabilidad	Alta	**Media**	Baja	
ACTIVO DE INFORMACIÓN	**Consecuencias**		**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
	Divulgación de la reunión mantenida entre Sr. Presidente y ministros.		Reputación.	Alta	9	
			Financiera.			
			Productividad.	Baja	2	
			Seguridad y salud.			
			Multas y sanciones legales.			
			Cumplimiento de regulaciones.	Media	2	

11.			**RIESGO DEL ACTIVO DE INFORMACIÓN**			
RIESGO DEL ACTIVO DE	AMENAZA	**Activo de Información**	**Videoconferencia**			
		Áreas de preocupación	Un gusano o troyano que llegue al servidor y desactive los servicios.			
		Actor	Software malicioso en el servidor, PC/portátil			
		Medio	Red			
		Motivo	Enviar información a destinos no autorizados			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Proteger la confidencialidad evitando el ingreso de este tipo de malware a la red.			
		Probabilidad	**Alta**	Media	Baja	
	Consecuencias		**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
	Retraso en alguna tipo de reunión entre el Sr.		Reputación.	Baja	3	
			Financiera.			

INFORMACIÓN	Presidente y Ministros. Incluso un gabinete virtual.	Productividad.	Alta	6
		Seguridad y salud.		
		Multas y sanciones legales.		
		Cumplimiento de regulaciones.	Baja	1

12.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	**AMENAZA**	**Activo de Información**	**Videoconferencia**			
		Áreas de preocupación	Falla de la fuente eléctrica del servidor por falta de manteamiento.			
		Actor	TI			
		Medio	Centro de datos			
		Motivo	No mantenimiento			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Realizar un cronograma de los mantenimientos preventivos de los servidores.			
		Probabilidad	Alta	**Media**	Baja	
	Consecuencias		**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
	Retraso en alguna tipo de reunión entre el Sr. Presidente y Ministros. Incluso un gabinete virtual.		Reputación.	Baja	3	
			Financiera.			
			Productividad.	Alta	6	
			Seguridad y salud.			
			Multas y sanciones legales.			
			Cumplimiento de regulaciones.	Baja	1	

13.			RIESGO DEL ACTIVO DE INFORMACIÓN
	AMEN	**Activo de Información**	**Videoconferencia**
		Áreas de preocupación	Falla del Router del proveedor por donde sale al videoconferencia.
		Actor	ISP –CNT
		Medio	Router

RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Motivo**	Falla			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Realizar el monitoreo de los equipos de frontera incluyendo los del ISP.			
		Probabilidad	**Alta**	Media	Baja	
		Consecuencias	**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
		Retraso en alguna tipo de reunión entre el Sr. Presidente y Ministros. Incluso un gabinete virtual.	Reputación.	Baja	3	
			Financiera.			
			Productividad.	Alta	6	
			Seguridad y salud.			
			Multas y sanciones legales.			
			Cumplimiento de regulaciones.	Media	2	

14.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Videoconferencia**			
		Áreas de preocupación	Un Router en mal funcionamiento en la MPLS del proveedor.			
		Actor	ISP –CNT			
		Medio	WAN			
		Motivo	Falla de Router			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Redundancia a nivel caminos en la WAN para mantener la disponibilidad del servicio.			
		Probabilidad	Alta	**Media**	Baja	
		Consecuencias	**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
		Retraso en alguna tipo de reunión entre el Sr. Presidente y Ministros. Incluso un gabinete virtual o itinerante.	Reputación.	Baja	3	
			Financiera.			
			Productividad.	Alta	6	
			Seguridad y salud.			
			Multas y sanciones legales.			

		Cumplimiento de regulaciones.	Media	2

15.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Videoconferencia**			
		Áreas de preocupación	Apagado del sistema de aire acondicionado del centro del datos.			
		Actor	TI			
		Medio	Centro de Datos			
		Motivo	Falla de aire acondicionado			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Planificar el mantenimiento preventivo del aire acondicionado.			
		Probabilidad	Alta	**Media**	Baja	
		Consecuencias	**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
		Retraso en alguna tipo de reunión entre el Sr. Presidente y Ministros. Incluso un gabinete virtual o itinerante.	Reputación.	Baja	3	
			Financiera.			
			Productividad.	Alta	6	
			Seguridad y salud.			
			Multas y sanciones legales.			
			Cumplimiento de regulaciones.	Media	2	

16.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Videoconferencia**			
		Áreas de preocupación	Personal de TI y AT que esta como apoyo a momento de realizar la videoconferencia puede escuchar la reunión.			
		Actor	Equipo de TI o AT			
		Medio	Sala de virtual			
		Motivo	Soporte			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Control de acceso a la sala virtual.			

DEL	A	**Probabilidad**	**Alta**	Media	Baja
		Consecuencias	**Severidad**		
			Área de impacto	**Valor**	**Puntuación**
ACTIVO		Divulgación de alguna reunión entre el Sr. Presidente y otras autoridades.	Reputación.	Alta	9
			Financiera.		
DE			Productividad.	Baja	2
			Seguridad y salud.		
			Multas y sanciones legales.		
INFORMACIÓN			Cumplimiento de regulaciones.	Alta	3

17.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO	AMENAZA	**Activo de Información**	**Videoconferencia**			
		Áreas de preocupación	Personal de TI que conoce las claves y las usa para ingresar a una sala virtual cuando se esté llevando a cabo una reunión.			
		Actor	Personal de TI con otros intereses			
		Medio	Sala de virtual			
		Motivo	Captura de información confidencial			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Control de acceso a la sala virtual.			
		Probabilidad	**Alta**	Media	Baja	
		Consecuencias	**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
DEL		Divulgar información de un gabinete virtual en el cual se vaya a dar alguna disposición.	Reputación.	Alta	9	
ACTIVO			Financiera.			
			Productividad.	Baja	2	
DE			Seguridad y salud.			
			Multas y sanciones legales.			
INFORMACIÓN			Cumplimiento de regulaciones.	Alta	3	

18.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Videoconferencia**			
		Áreas de preocupación	Personal de TI al momento de realizar alguna configuración en el servidor de sala virtual baje los servicios.			
		Actor	Personal de TI			
		Medio	Red			
		Motivo	Configuración de sala virtuales			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Monitoreo de la sala virtuales y sus servicios,			
		Probabilidad	**Alta**	Media	Baja	
	Consecuencias		**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
	Retraso de las sesiones virtuales que tienen agendado los ministerios.		Reputación.	Alta	9	
			Financiera.			
			Productividad.	Alta	6	
			Seguridad y salud.			
			Multas y sanciones legales.			
			Cumplimiento de regulaciones.	Baja	1	

19.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Videoconferencia**			
		Áreas de preocupación	Personal TI al momento de cambiar algún disco y de reiniciar el servidor los servicios no suban.			
		Actor	Personal de TI			
		Medio	Centro de Datos			
		Motivo	Mantenimiento			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Generar un manual de procedimiento para el cambio de hardware en servidores antiguos.			
		Probabilidad	**Alta**	Media	Baja	
	Consecuencias		**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	

DE INFORMACIÓN	Retraso de las sesiones virtuales que tienen agendado los ministerios	Reputación.	Alta	9
		Financiera.		
		Productividad.	Alta	6
		Seguridad y salud.		
		Multas y sanciones legales.		
		Cumplimiento de regulaciones.	Baja	1

20.			RIESGO DEL ACTIVO DE INFORMACIÓN			
RIESGO DEL ACTIVO DE INFORMACIÓN	AMENAZA	**Activo de Información**	**Videoconferencia**			
		Áreas de preocupación	Personal técnico de las instituciones que hacen uso del servicio, y que presten la ayuda en reunión virtual.			
		Actor	Apoyo técnico en los Ministerios			
		Medio	Acceso a un equipo de video o vía web (anillo Interministerial o red Lan).			
		Motivo	Soporte videoconferencia			
		Consecuencias	Divulgación	Modificación	Destrucción	Interrupción
		Requerimientos de seguridad	Mantener control en el acceso de las salas virtuales.			
		Probabilidad	Alta	**Media**	Baja	
	Consecuencias		**Severidad**			
			Área de impacto	**Valor**	**Puntuación**	
	Divulgación de alguna reunión entre el Sr. Presidente y otras autoridades donde se de alguna disposición.		Reputación.	Alta	9	
			Financiera.			
			Productividad.	Baja	2	
			Seguridad y salud.			
			Multas y sanciones legales.			
			Cumplimiento de regulaciones.	Baja	1	

<table>
<tr><td colspan="3">21.</td><td colspan="5">RIESGO DEL ACTIVO DE INFORMACIÓN</td></tr>
<tr><td rowspan="10">RIESGO DEL ACTIVO DE INFORMACIÓN</td><td rowspan="7">AMENAZA</td><td>Activo de Información</td><td colspan="5">Videoconferencia</td></tr>
<tr><td>Áreas de preocupación</td><td colspan="5">Personal de ISP pueden estar capturando tráfico en alguno dispositivo de la WAN.</td></tr>
<tr><td>Actor</td><td colspan="5">Personal de ISP</td></tr>
<tr><td>Medio</td><td colspan="5">Anillo Interministerial</td></tr>
<tr><td>Motivo</td><td colspan="5">Captura de trafico</td></tr>
<tr><td>Consecuencias</td><td>Divulgación</td><td>Modificación</td><td>Destrucción</td><td colspan="2">Interrupción</td></tr>
<tr><td>Requerimientos de seguridad</td><td colspan="5">Mantener la confidencialidad a través de la encripción de la información.</td></tr>
<tr><td colspan="2">Probabilidad</td><td>Alta</td><td colspan="2">Media</td><td>Baja</td></tr>
<tr><td colspan="2" rowspan="2">Consecuencias</td><td colspan="5">Severidad</td></tr>
<tr><td>Área de impacto</td><td colspan="2">Valor</td><td>Puntuación</td></tr>
<tr><td colspan="2" rowspan="6">Divulgación de alguna reunión entre el Sr. Presidente y otras autoridades donde sé de alguna disposición, incluso de gabinetes virtuales.</td><td>Reputación.</td><td colspan="2">Alta</td><td>9</td></tr>
<tr><td>Financiera.</td><td colspan="2"></td><td></td></tr>
<tr><td>Productividad.</td><td colspan="2">Baja</td><td>2</td></tr>
<tr><td>Seguridad y salud.</td><td colspan="2"></td><td></td></tr>
<tr><td>Multas y sanciones legales.</td><td colspan="2"></td><td></td></tr>
<tr><td>Cumplimiento de regulaciones.</td><td colspan="2">Alta</td><td>3</td></tr>
</table>

3.1.6. IDENTIFICACIÓN DE LOS RIESGOS

Se tabula las repuestas afirmativas de cada cuestionario y se realiza una referencia cruzada con cada escenario de posibles amenazas descritas en la sección anterior con sus respectivas consecuencias. Además se agrega el valor de la suma de la columna puntuación de cada posible amenaza.

Además se incorpora las la columna de prioridad de mitigación por área de impacto el cual se basa en la Tabla 3.4.

CORREO ELECTRÓNICO			
ESCEARIO DE MENAZA	CONSECUENCIA	POSICIÓN DE RIESGO	PRIORIDAD DE MITIGACIÓN POR AREA DE IMPACTO
CUESTIONARIO 1			
Escenario 1			
Que un empleado haga uso del equipo PC/portátil que no esté a su cargo y accidentalmente accede al buzón donde se encuentra el activo de información del usuario encargado de ese equipo.	Si este escenario ocurriera en el área de Talento Humano, se podría encontrar con posibles aspirantes a nuevos cargos y la información de remuneraciones.	16	1
Un empleado intencionalmente haga uso del PC/portátil que no está a su cargo para obtener información.	Conseguir la información tales de una cuenta de alguna autoridad y poder enviarle correos males intencionados.	12	2
El usuario dueño del activo de información realiza un mala configuración de respaldo de sus buzón y su información se borra permanentemente	La pérdida definitiva de la información, ya que al momento de descargar los correo de manera local, se requiere un cliente de correo.	11	2
Un usuario busca la manera de obtener la clave de acceso a un buzón en particular para borrar un correo que no quiere que lea el remitente	Que el usuario obtenga la clave de esa persona y que lo difunda.	18	1
Escenario 2			
El robo del dispositivo donde se tiene configurado el buzón de correo, podría permitir el acceso al activo de información.	La información almacenada en el dispositivo móvil puede ser divulgada y/o vendida.	13	2
Hacktivistas, haciendo uso métodos sofisticados de acceso, podrían acceder al servidor donde se encuentra la información.	Robar información confidencial, agenda, contactos, etc., de autoridades de la institución.	18	1
Personal de la empresa proveedora que está encargada del soporte de la plataforma podría acceder de forma remota al activo para realizar cierta configuración y en el proceso baja un servicio de algún servidor de manera involuntaria.	Que no se pueda despachar resúmenes informativos diarios a las autoridades, incluso al Sr. Presidente.	13	2
Una persona externa haciendo uso de software malicioso puede realizar varias peticiones de conexión al MTA hasta que se venga abajo el servicio.	Evitar que la información a cualquier evento que estaba planificada sea retrasada y genere retrasos a las personas que lo coordinan.	16	1

Personal de la empresa proveedora que está encargada del soporte de la plataforma, en un mantenimiento podría borrar información del mailbox.	Perdida de información sensible para cada uno de los usuarios en cada ámbito de trabajo.	17	1
Una persona externa haciendo uso de un software malicioso de descubrimiento de claves para acceder al buzón de correo y borrar toda la información.	Ataques dirigidos a las autoridades de la institución con el fin de obtener información en algunos casos sensible.	15	1
Escenario 3			
Después de realizar una actualización de versión los servicios no se ejecuten de manera adecuada.	Malestar y retraso en la coordinación para ciertos eventos presidenciales. Además de malestar en los usuarios al no poder realizar su trabajo de manera ágil.	10	3
Al momento de usar un software de escritorio para realizar el archivado de correos antiguos este no realice el respaldo de manera adecuada y se pierda la información.	No poder utilizar alguna información anterior para algún tipo de informe o investigación.	10	3
Fallo del sistema base en los servidores donde se encuentra la plataforma de correo.	Podría causar la pérdida total de la información y afectar la disponibilidad.	10	3
Insuficientes recursos de memoria y/o CPU en la plataforma de virtualización y por tal razón los servidores no procesarían el activo de información de manera adecuada.	Indisponibilidad de la plataforma, no procesamiento de ciertos correos y hasta pérdida de los mismos.	18	1
Abrir correos de remitentes desconocidos con adjuntos, que al momento de dar clic se ejecuta un backdoor que podrían realizar un reenvió de los correo a sitios externos.	Divulgación de información en algunos casos sensible y en otra información de eventos presidenciales.	13	2
Ingreso de un gusano/troyano a través de la Internet, el cual por medio de la red llegue al servidor de MTA y/o Mailbox y que en su código contenga una instrucción de apagado de los servidores.	Perdida de información en procesamiento, malestar en los cerca de 600 usuarios, y que no llegue información importante desde otras entidades públicas.	17	1
Ingreso de un virus a través de la Internet a la PC del usuario, que contenga en su código una instrucción de borrado de la PC, en el supuesto de tener mis correos almacenados de manera local.	Dañar la PC, y por ende dañar la información de los correos si se la configuración de el se encuentran en carpetas locales.	11	3
Fallo en el sistema de respaldo de energía eléctrica en una situación	Malestar por no poder realizar la gestión o coordinación de todas		

de corte de energía por la parte de la empresa proveedora de electricidad.	las oficinas que componen la presidencia.		
Configuración de rutas en el Switch de Core podrían impedir que el activo de información sea procesado de manera adecuada.	No se envíen los correos y se queden encolados en el MTA, por lo tanto no se coordina de mejor manera algún tipo de evento presidencia.	13	2
Que los enlaces provistos por el ISP dejen de prestar sus servicios de un momento a otro.	No envío de correos en algunos casos urgentes a varios ministerios por parte de autoridades de la Presidencia.	16	1
Terremoto	Podría causar pérdida total de la información.		
Un incendio en el Centro de Datos	Despido de personal de TI y pérdida definitiva de la información.	10	3
CUESTIONARIO 2			
Escenario 1			
El o los administradores del servicio, al momento de realizar un seguimiento y monitoreo de los correos se verifica el origen, destino y cuerpo del mensaje.	Divulgación de información en algunos casos sensible.	15	1
Un ex administrador del servicio que podría buscar lucrar con la información que maneja.	Pérdida de confianza en el área de TI.	15	1
Personal de TI en un mantenimiento no planificado.	Perdida de disponibilidad del servicio por varias horas y despidos en el área de TI.	17	1
Alguna persona de TI que quiera causar daño a la institución.	Pérdida de confianza en el uso del servicio por parte de los usuarios.	11	2
Personal de TI al momento de realizar el backup de la información del usuario final en carpetas locales no realiza el procedimiento correcto.	No poder entregar informes haciendo uso de información anterior como antecedente.	10	3
Personas de TI que tengan acceso y tengan el conocimiento para entrar al servidor mailbox para realizar un borrado de algún tipo de información.	Pérdida total de la información incluyendo al buzón del Sr. Presidente		
Escenario 2			
Personal de la empresa proveedora, en una revisión preventiva autorizada al mailbox podría encontrarse con información sensible.	Conocer de primera mano y con anterioridad la ubicación de los eventos del Sr. Presidente.	12	2

Personal de la empresa proveedora que tiene autorización para el acceso remoto puede extraer información.	Conocer de primera mano y con anterioridad la ubicación de los eventos del Sr. Presidente y además conocer el trabajo de los usuarios.	12	2

Tabla 3.115. Identificación escenarios de amenazas con riesgo alto

VIDEOCONFERENCIA			
ESCEARIO DE MENAZA	CONSECUENCIA	POSICIÓN DEL RIESGO	PRIORIDAD DE MITIGACIÓN POR AREA DE IMPACTO
CUESTIONARIO 1			
Escenario 1			
Una persona que conozca las credenciales de la sala virtual donde se llevará a cabo la reunión y accede vía web a dicha sala.	Divulgar información tratada en la reunión entre el Sr. Presidente y Ministros.	14	1
Un empleado quiere de ingresar vía web al sistema de videoconferencia, de tal manera que busca una herramienta generadora de claves de acceso, esto podría ocasionar demasiadas peticiones de conexión que el servicio podría caerse.	Divulgar información tratada en la reunión entre el Sr. Presidente y Ministros.	11	2
Escenario 2			
Personal de otros ministerios que requiere hacer pruebas las hace sin previa coordinación, podría ingresar a una sala que no sea de pruebas y se esté llevando a cabo una reunión.	Conocer información tratada en la reunión entre el Sr. Presidente y Ministros o entre Ministros.	14	1
Personas externas que quieren ingresar a la sala virtual vía web, podrían hacer uso de herramientas sofisticada de generación de claves, de tal manera que encuentren una para el acceso a una sala.	Conocer información tratada en la reunión entre el Sr. Presidente y Ministros o entre Ministros.	14	1
Generar alto tráfico de entrada hasta que el Router del ISP deje de funcionar.	Causar retraso en caso una reunión entre autoridades del país.	10	3
Escenario 3			
El acceso vía web solo requiere un pin de 4 dígitos numéricos, por esta razón es más probable que se descubre un pin de acceso.	Acceso a una sala determinada y obtener información confidencial.	13	2

Por ser software antiguo podrida causar que los servicios dejen de funcionar.	Retraso en alguna tipo de reunión entre el Sr. Presidente y Ministros.	11	2
En algunas ocasiones los servicio de videoconferencia y acceso vía web se deshabilitan sin ninguna razón.	Retrasaría el inicio de un gabinete virtual.	10	3
Los discos de servidor pueden dañarse y por ser un servidor descontinuado, es casi imposible obtener discos de nuevos para su reemplazo.	Retrasaría el inicio de un gabinete virtual.	10	3
Algún tipo de backdoor en el servidor, el cual este redirigiendo la información de las sesiones de las salas virtuales.	Divulgación de la reunión mantenida entre Sr. Presidente y ministros.	13	2
Un gusano o troyano que llegue al servidor y desactive los servicios.	Retraso en alguna tipo de reunión entre el Sr. Presidente y Ministros. Incluso un gabinete virtual.	10	3
Falla de la fuente eléctrica del servidor por falta de manteamiento.	Retraso en alguna tipo de reunión entre el Sr. Presidente y Ministros. Incluso un gabinete virtual.	10	3
Falla del router del proveedor por donde sale la videoconferencia.	Retraso en alguna tipo de reunión entre el Sr. Presidente y Ministros. Incluso un gabinete virtual.	11	2
Un Router en mal funcionamiento en la MPLS del proveedor.	Retraso en alguna tipo de reunión entre el Sr. Presidente y Ministros. Incluso un gabinete virtual o itinerante.	11	2
Apagado del sistema de aire acondicionado del centro del datos.	Retraso en alguna tipo de reunión entre el Sr. Presidente y Ministros. Incluso un gabinete virtual o itinerante.	11	2
CUESTIONARIO 2			
Escenario 1			
Personal de TI y AT que esta como apoyo a momento de realizar la videoconferencia.	Divulgación de alguna reunión entre el Sr. Presidente y otras autoridades.	14	1
Personal de TI que conoce las claves y las usa para ingresar a una sala virtual cuando se esté llevando a cabo una reunión.	Divulgar información de un gabinete virtual en el cual se vaya a dar alguna disposición.	14	1
Personal de TI al momento de realizar alguna configuración en el servidor de sala virtual baje los servicios.	Retraso de las sesiones virtuales que tienen agendado los ministerios.	16	1
Personal de TI en un mantenimiento del servidor al momento de terminar no sube los servicios.	Retraso de las sesiones virtuales que tienen agendado los ministerios. Incluso retraso en gabinetes virtuales	16	1

Personal TI al momento de cambiar algún disco y de reiniciar el servidor los servicios no suban.	Retraso de las sesiones virtuales que tienen agendado los ministerios.	16	1
Escenario 2			
Personal técnico de las instituciones que hacen uso del servicio, y que presten la ayuda en reunión virtual.	Divulgación de alguna reunión entre el Sr. Presidente y otras autoridades donde se de alguna disposición.	12	2
Personal de ISP pueden estar capturando tráfico en alguno dispositivo de la WAN.	Divulgación de alguna reunión entre el Sr. Presidente y otras autoridades donde se de alguna disposición, incluso de gabinetes virtuales.	14	1

Tabla 3.116. Identificación escenarios de amenazas con riesgo alto

3.1.7. ANÁLISIS DE RIESGOS Y SELECCIÓN DE MITIGACIÓN

Como se definió en el capítulo II hay 3 maneras de tratar el riesgo aceptarlo, mitigarlo o aplazarlo.

Se utilizara el método de categorización realizado en Octave-Allegro que indica que hay que clasificar los riesgos de mayor a menor y agruparlos en rangos de riesgos.

3.1.7.1. Método de asignación de mitigación de riesgo

Rango	Tipo de mitigación
Rango 1	Mitigarlo
Rango 2	Mitigarlo o Aplazarlo
Rango 3	Aplazarlo o aceptarlo
Rango 4	Aceptarlo

Tabla 3.117. Rangos para selección de mitigación

3.1.7.2. Matriz de riesgo

Una vez definido los rangos se procede a tabularlos en la matriz de riesgo y poder identificar la probabilidad de riesgo alta y media.

MATRIZ DE RIESGO			
Probabilidad	Posición del Riesgo		
	14-18	11-13	6-10
Alta	Rango 1	Rango 2	Rango 3
Media	Rango 2	Rango 3	Rango 4
Baja	Rango 3	Rango 4	Rango 4

Tabla 3.118. Matriz de riesgo y rango de mitigación

Como se muestra, solo los de la posición 1, 2 con prioridad alta y media serán usados para seleccionar los controles.

3.1.7.3. Selección de controles

CONTROLES ISO 27002 USADOS
10.4 Protección contra código malicioso y móvil(descargable)
10.4.1 Protección contra código malicioso
10.4.2 Protección contra código móvil
10.6 Gestión de las seguridades de la redes
10.6.1 Controles de red
10.6.2 Seguridad de los servicios de red
10.8 Intercambio de información
10.8.4 Mensajería electrónica
11.1 Control de acceso
11.1.1 Política de control de acceso
11.2 Gestión de acceso del usuario
11.2.2 Gestión de Privilegios
11.3 Responsabilidad del usuario
11.3.1 Uso de contraseñas
11.3.2 Equipo de usuario desatendido
11.3.3 Política de puesto de trabajo despejado y pantalla limpia
11.4 Control de acceso a la red

11.4.1 Política del uso de los servicios de red
11.4.2 Autenticación del usuario para conexiones externas
11.4.3 Identificación de los equipos en la red
11.4.4 Protección del acceso remoto
11.4.5 Segregación de redes
11.4.6 Control de conexión a la red
11.4.7 Control de ruteo
11.5 Control de acceso al sistema operativo
11.5.1 Procedimiento seguros de inicio de sesión

Tabla 3.119. Dominios y Controles para la mitigación de riesgos y creación de políticas

Para que la selección de controles se haga de una manera práctica se realiza una tabla en la cual se coloca los escenarios de amenaza con su respectiva consecuencia, la posición de riesgo en este caso únicamente los que se definió en el paso anterior es decir lo del rango que se mitigaran. Además se ha colocado la posición de mitigación que no es más que la prioridad de los riesgos a mitigar y al final los controles que se seleccionaran, estos controles como se definió en el alcance del proyecto únicamente son los que red y usuario final.

Inicialmente se define la tabla cruzada para el servicio de correo electrónico y luego para el servicio de videoconferencia.

Cabe mencionar que únicamente se definió los numerales que hacen referencia a los controles 27002 definidos en el alcance de este proyecto.

CORREO ELECTRÓNICO				
ESCEARIO DE AMENAZA	CONSECUENCIA	POSICIÓN DE RIESGO	POSICION DE MITIGACIÓN	CONTROL ISO 27002
CUESTIONARIO 1				
Escenario 1				
Que un empleado haga uso del equipo PC/portátil que no esté a su cargo y accidentalmente accede al buzón donde se encuentra el activo de información del usuario encargado de ese equipo.	Si este escenario ocurriera en el área de Talento Humano, se podría encontrar con información enviada desde el MRL de posibles aspirantes a nuevos cargos y la información de remuneraciones.	16	1	11.3.3 11.1.1
Un empleado intencionalmente haga uso del PC/portátil que no está a su cargo para obtener información.	Conseguir la información tales de una cuenta de alguna autoridad y poder enviarle correos mal intencionado.	12	2	11.2.2 11.4.6 11.1.1 11.3.2
Un usuario busca la manera de obtener la clave de acceso a un buzón en particular para borrar un correo que no quiere que lea el remitente	Que el usuario obtenga la clave de esa persona y que lo difunda.	18	1	11.2.2 11.3.1
Escenario 2				
El robo del dispositivo donde se tiene configurado el buzón de correo, podría permitir el acceso al activo de información.	La información almacenada en el dispositivo móvil puede ser divulgada y/o vendida.	13	2	11.4.3 11.4.4
Hacktivistas, haciendo uso métodos sofisticados de acceso, podrían acceder al servidor donde se encuentra la información.	Robar información confidencial, agenda, contactos, etc de autoridades de la institución.	18	1	10.6.1 10.6.2 11.4.4
Personal de la empresa proveedora que está encargada del soporte de la plataforma podría acceder de forma remota al activo para realizar cierta configuración y en el proceso baja un servicio de algún servidor de manera involuntaria.	Que no se pueda despachar resúmenes informativos diarios a las autoridades, incluso al Sr. Presidente.	13	2	11.4.4 11.2.2 11.4.4
Una persona externa haciendo uso de software malicioso puede realizar varias peticiones de conexión al MTA hasta que se venga abajo el servicio.	Evitar que la información a cualquier evento que estaba planificada sea retrasada y genere retrasos a las personas que lo coordinan.	16	1	10.4.1 11.4.4 10.4.6

Personal de la empresa proveedora que está encargada del soporte de la plataforma, en un mantenimiento podría borrar información del mailbox.	Perdida de información sensible para cada uno de los usuarios en cada ámbito de trabajo.	17	1	10.4.1 11.4.4 10.4.6
Una persona externa haciendo uso de un software malicioso de descubrimiento de claves para acceder al buzón de correo y borrar toda la información.	Ataques dirigidos a las autoridades de la institución con el fin de obtener información, en algunos casos, sensible.	15	1	11.1.1 11.4.4
Escenario 3				
Abrir correos de remitentes desconocidos con adjuntos, que al momento de dar clic se ejecuta un backdoor que podrían realizar un reenvió de los correo a sitios externos.	Divulgación de información, en algunos casos, sensible y en otros, información de eventos presidenciales.	13	2	10.4.1 10.4.2
Ingreso de un gusano/troyano a través de la Internet, el cual por medio de la red llegue al servidor de MTA y/o Mailbox y que en su código contenga una instrucción de apagado de los servidores.	Perdida de información en procesamiento, malestar en los cerca de 600 usuarios, y que no llegue información importante desde otras entidades públicas.	17	1	10.4.1
Ingreso de un virus a través de la Internet a la PC del usuario, que contenga en su código una instrucción de borrado de la PC, en el supuesto de tener mis correos almacenados de manera local.	Dañar la PC, y por ende dañar la información de los correos si se la configuración de el se encuentran en carpetas locales.	11	3	10.4.1
Configuración de rutas/reglas inapropiadas en el Switch/dispositivo de frontera podrían impedir que el activo de información sea procesado de manera adecuada.	No se envíen los correos y se queden encolados en el MTA/ANTISPAM, por lo tanto no se coordina de mejor manera algún tipo de evento presidencia.	13	2	11.4.7
CUESTIONARIO 2				
Escenario 1				
Él o los administradores del servicio, al momento de realizar un seguimiento y monitoreo de los correos se verifica el origen, destino y cuerpo del mensaje.	Divulgación de información, en algunos casos, sensible.	15	1	11.4.4 11.4.6
Un ex administrador del servicio que podría buscar lucrar con la información que maneja.	Pérdida de confianza en el área de TI.	15	1	10.6.1 11.3.1
Personal de TI en un mantenimiento no planificado.	Perdida de disponibilidad del servicio por varias horas y despidos en el área de TI.	17	1	11.4.6 11.4.3

Alguna persona de TI que quiera causar daño a la institución.	Pérdida de confianza en el uso del servicio por parte de los usuarios.	11	2	10.6.1 10.4.1
Personas de TI que tengan acceso y tengan el conocimiento para entrar al servidor mailbox para realizar un borrado de algún tipo de información.	Pérdida total de la información incluyendo al buzón del Sr. Presidente			11.3.1 11.2.2 11.4.7
Escenario 2				
Personal de la empresa proveedora, en una revisión preventiva autorizada al mailbox podría encontrarse con información sensible.	Conocer de primera mano y con anterioridad la ubicación de los eventos del Sr. Presidente.	12	2	11.4.4 11.4.7 11.3.1
Personal de la empresa proveedora que tiene autorización para el acceso remoto puede extraer información.	Conocer de primera mano y con anterioridad la ubicación de los eventos del Sr. Presidente y además conocer el trabajo de los usuarios.	12	2	11.4.4 11.4.7 11.3.1

Tabla 3.120. Selección de controles para mitigar los riesgos del Servicio de Correo

VIDEOCONFERENCIA				
ESCEARIO DE MENAZA	CONSECUENCIA	POSICIÓN DEL RIESGO	TIPO DE MITIGACIÓN	CONTROL ISO 27002
CUESTIONARIO 1				
Escenario 1				
Una persona que conozca las credenciales de la sala virtual donde se llevará a cabo la reunión y accede vía web a dicha sala.	Divulgar información confidencial tratada en la reunión entre el Sr. Presidente y Ministros o reuniones virtuales entre instituciones de gobierno.	14	1	11.2.2 11.3.1
Un empleado quiere de ingresar vía web al sistema de videoconferencia, de tal manera que busca una herramienta generadora de claves de acceso, esto podría ocasionar demasiadas peticiones de conexión que el servicio podría verse afectado.	Divulgar información confidencial tratada en alguna reunión entre el Sr. Presidente y Ministros o reuniones virtuales entre instituciones de gobierno.	11	2	11.4.6 10.4.1
Escenario 2				
Personal de otros ministerios que requieren realizar pruebas, las hace sin previa coordinación, podría ingresar a una sala que no sea la de	Conocer información tratada en la reunión entre el Sr. Presidente y Ministros o entre Ministros o reuniones	14	1	11.4.4 11.3.1

pruebas donde sé este llevando a cabo una reunión.	virtuales entre instituciones de gobierno.			11.4.2
Personas externas que quieren ingresar a la sala virtual vía web, podrían hacer uso de herramientas sofisticada de generación de claves, de tal manera que encuentren una para el acceso a una sala.	Conocer información tratada en la reunión entre el Sr. Presidente y Ministros o entre Ministros o reuniones virtuales entre instituciones de gobierno.	14	1	11.4.2 10.4.1
Escenario 3				
El acceso vía web solo requiere un pin de X dígitos numéricos, por esta razón es más probable que se descubre un pin de acceso.	Acceso a una sala determinada y obtener información confidencial.	13	2	11.3.1 11.4.2
Algún tipo de backdoor en el servidor, el cual este redirigiendo la información de las sesiones de las salas virtuales.	Divulgación de la reunión mantenida entre Sr. Presidente y ministros.	13	2	10.4.1
Falla del Router del proveedor por donde sale la videoconferencia.	Retraso en algún tipo de reunión entre el Sr. Presidente y Ministros. Incluso un gabinete virtual.	11	2	11.4.7
Un Router en mal funcionamiento en la MPLS del proveedor.	Retraso en algún tipo de reunión entre el Sr. Presidente y Ministros. Incluso un gabinete virtual o itinerante.	11	2	11.4.7
CUESTIONARIO 2				
Escenario 1				
Personal de TI y AT que esta como apoyo a momento de realizar la videoconferencia.	Divulgación de alguna reunión entre el Sr. Presidente y otras autoridades.	14	1	11.2.2
Personal de TI que conoce las claves y las usa para ingresar a una sala virtual cuando sé este llevando a cabo una reunión.	Divulgar información de un gabinete virtual en el cual se vaya a dar alguna disposición.	14	1	11.2.2 11.3.1 11.4.6
Personal de TI al momento de realizar alguna configuración en el servidor de sala virtual baje los servicios.	Retraso de las sesiones virtuales que tienen agendado los ministerios.	16	1	11.3.1 11.4.3
Escenario 2				
Personal técnico de las instituciones que hacen uso del servicio, y que presten la ayuda en reunión virtual.	Divulgación de alguna reunión entre el Sr. Presidente y otras autoridades donde sé de alguna disposición.	12	2	11.3.1 11.4.2

Personal de ISP pueden estar capturando tráfico en alguno dispositivo de la WAN.	Divulgación de alguna reunión entre el Sr. Presidente y otras autoridades donde sé de alguna disposición, incluso de gabinetes virtuales.	14	1	11.4.1

Tabla 3.121. Selección de controles para mitigar los riesgos del Servicio de Videoconferencia.

3.1.8. POLÍTICAS DE SERGURIDAD DE LA INFORMACIÓN

Conociendo que la información es el activo más valioso que una organización posee y además que la continuidad de la organización depende de su protección, es decir que se debe garantizar la confidencialidad, integridad y disponibilidad de con el fin de que objetivos de la organización se cumplan. Siendo los objetivos estratégicos lo siguientes.

- Proporcionar productos y servicios de carácter jurídico para asesoramiento y patrocinio jurídico del Presidente/a de la República, de las máximas autoridades de la Presidencia de la República y la institución.

- Diseñar e implementar un modelo de gestión para el levantamiento de escenarios que permitan emitir un adecuado y oportuno asesoramiento para la toma de decisiones.

- Alcanzar y mantener un alto nivel de gestión operativa financiera, para apoyar eficiente y eficazmente las actividades y proyectos de la Presidencia de la República.

3.1.8.1. Política de seguridad de la información

Objetivos

- Asegurar los activos de información, servicios, procesos más importantes para el cumplimiento de la misión de la Presidencia de la Republica. Los procesos relevantes son los Adjetivos, Sustantivos y Gobernantes que se definen en el estatuto de la Presidencia de la República.

- Evitar que los activos de información de la Presidencia de la Republica pierdan su confidencialidad, integrada y disponibilidad.
- Asegurar que la información sea almacenada, procesada y transmitida adecuadamente.

Alcance

Se definirá políticas haciendo uso de normas tanto locales e internacionales, y en base a estas se realizaran procedimientos a nivel de res y de usuario final.

La política se extenderá a todo los usuarios que hagan uso del servicio de correo electrónico y el servicio de videoconferencia. En el caso del servicio de correo electrónico el alcance seria local es decir únicamente a usuarios de Presidencia que cuentan con este servicio.

Para el caso del servicio de videoconferencia únicamente se extenderá a los niveles jerárquicos de Presidencia y de las instituciones de Gobierno.

Roles y responsabilidades

Debe existir la coordinación de todas las partes involucradas para que la política se pueda implementar y sea sustentable en el tiempo.

- **Responsable de Seguridad (CIO)**, sus responsabilidades entre las más importantes deben ser, gestión de las políticas de seguridad de la información, revisión de las políticas, gestión de riesgos.

- **Empleados,** responsables de cumplimiento de las políticas y de reportar problemas en la gestión de la seguridad de la información.

- **Dirección de tecnología (TI),** responsable del día a día de la administración de las políticas.

- **SSI (Subsecretaria de Seguridad de la Información),** revisión de la gestión de riesgos y de políticas.

Cumplimiento

Para poder cumplir las políticas se debe definir un rol que supervise es decir que monitoree y un rol de auditor que se encargaría de las revisiones formales de las mismas, estos dos roles no deben pertenecer al área de TI.

3.1.8.2. Política se seguridad para el servicio de Correo electrónico

La Presidencia a través del servicio de correo electrónico provee, a todo el personal de las distintas áreas, una herramienta que facilita la comunicación entre servidores públicos tanto en la misma institución como entre instituciones del sector.

El uso de correo institucional debe ser estrictamente para uso oficial, es decir que la comunicación y transferencia de información interna y con los demás ministerios se lo debe realizar únicamente por este medio. El uso de correo público puede ser usado siempre y cuando se tomen las precauciones que se indican más adelante.

La responsabilidad de buen uso del servicio que provee la Presidencia debe estar a cargo de cada una de las personas que tienen cuenta del servicio.

3.1.8.2.1. Política de control de acceso

Todos los usuarios que pertenezcan formalmente a la Presidencia de la República deben estar registrados en una base de datos como por ejemplo un LDAP para que

puedan hacer uso de la red y de los diferentes servicios que proporciona la Dirección de Tecnología de la Presidencia como es el caso del correo electrónico.

La política debe ser aplicada a todos los funcionarios que hacen uso del servicio provisto por la Dirección de Tecnología de la Presidencia. El control de acceso estará basado en un modelo de AAA.

Procedimientos

- El acceso a la red, servicios y/o sistemas se lo debe realizar por medio de usuario y clave, las credenciales serán proporcionados por la Dirección de Tecnología una vez que la autorización de creación de usuario haya llegado a la misma.

- El control de acceso de red, servicio y/o sistemas debe ser validado a través de Directorio Activo. De esta manera se podrá identificar quien, como y donde hubo un acceso autorizado o no autorizado. Esto plica tanto a nivel de usuario final como de usuario administrador.

- Usuarios que accedan a la red, servicios y/o sistemas con credenciales que no le pertenecen será considerada como una falta grave, y podría tomarse sanciones de ley una vez comprobada dicha falta.

En la Fig. 3.2 se muestra el procedimiento para el acceso a la red tanto cableada como inalámbrica.

3.1.1.1.1. Gestión de privilegios

La responsabilidad del servicio de correo electrónico es de la Dirección de Tecnología área de Redes y comunicaciones, Subsecretaria de Seguridad de la información y el proveedor encargado del soporte proactivo y reactivo de la solución.

Procedimiento

- El acceso como súper usuario a los distintos contenedores que componen la solución de correo electrónico se lo debe realizar a través del método de llave pública y privada, entre las máquinas de los administradores y los contenedores.
- La asignación de privilegios para la subsecretaria de Seguridad de la información únicamente serán para auditoria.
- Los privilegios del proveedor deben ser explícitos en el Término de Referencia (TDR).
- Los privilegios más bajos serán para los usuarios del servicio.

3.1.1.1.2. Uso de contraseñas

Estos controles tienen alcance para cualquier sistema o aplicaciones que se implementen en la Presidencia de la Republica y para usuarios que hicieran uso de esos sistemas o aplicaciones.

- Los usuarios al momento de elegir una clave deben considerar:
    - Elegir una frase o palabra con un mínimo de o caracteres fácil de recordar y que no involucre información personal.
    - La clave de contener al menos un símbolo especial y un número.

- Para los servicios que son web en especial el correo electrónico y videoconferencia se debe evitar dar clic en recordar contraseña en los exploradores web usados.
- Se debe realizar el cambio de claves al menos una vez cada 60 días.
- Las claves de los usuarios administradores deben ser cambiados al menos 1 vez cada 30 días.

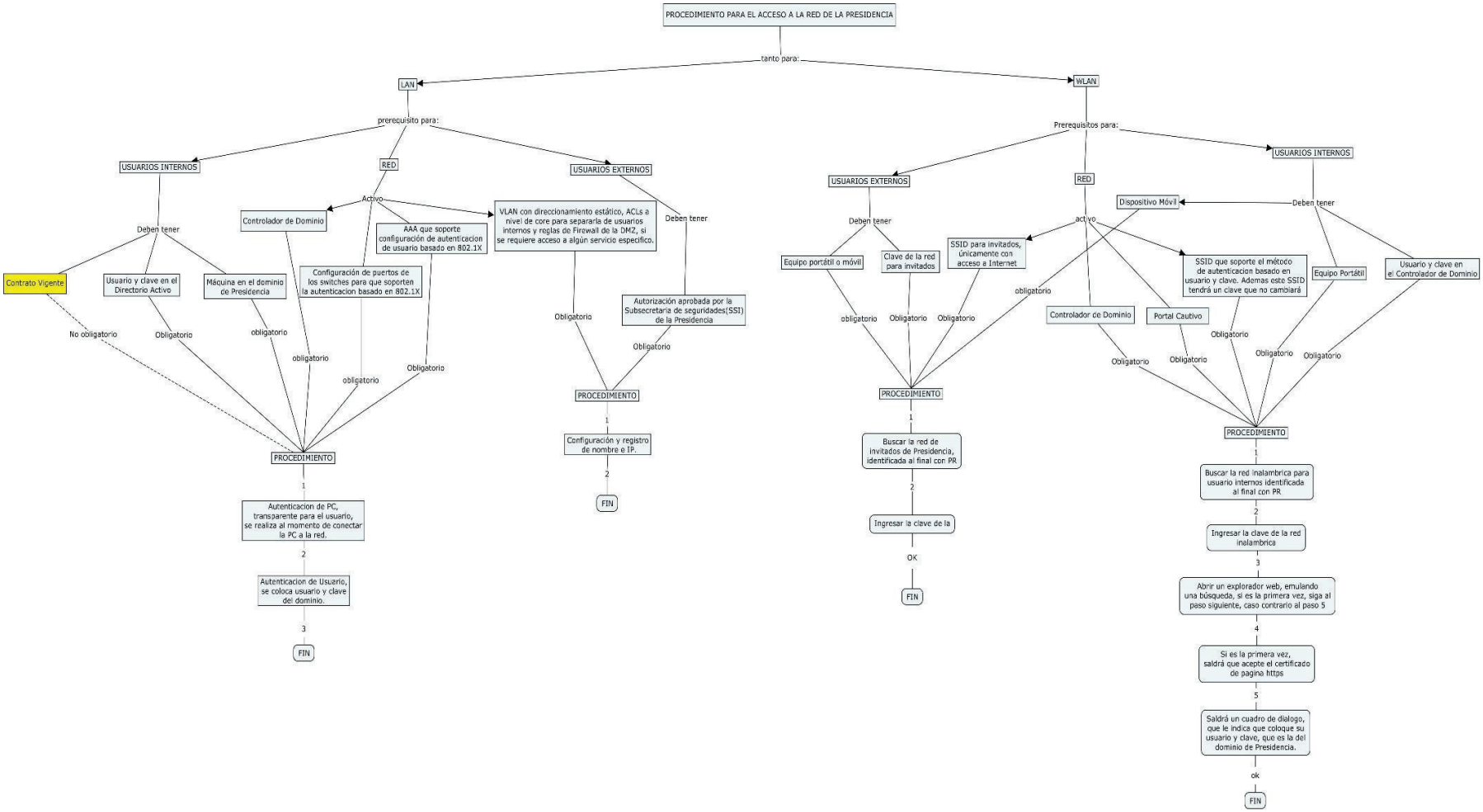

Figura 3.2. Diagrama de flujo de procedimiento de control de acceso correo

- Las claves de los usuarios administradores deben tener el siguiente formato
    - Pertenencia + Servicio(Sistema/aplicación) donde:
        - Pertenencia es el acrónimo del área responsable del servicio
        - Servicio debe contener al menos 5 caracteres y debe contener símbolos y números.

3.1.1.1.3. Equipo de usuario desatendido

- Cuando no se haga uso del cliente web, siempre cerrar sesión, se complementa con la política anterior.
- Cuando se haga uso del cualquier cliente de correo de escritorio, se deberá configurar el cierre automático del mismo al no ser utilizado.
- El cierre de sesión debe ser aplicado cuando no se esté utilizando la PC/portátil.
- Configuración de GPO política de grupo para el cierre de sesión automático al cabo de 2 minutos de inactividad.

3.1.1.1.4. Identificación de los equipos en la redes

Estos controles tienen un alcance a nivel de usuario y sistema. Además estos controles complementan la auditoria de eventos en los contenedores del servicio de correo electrónico.

- El identificador de equipo para las autoridades que utilizan la red inalámbrica será la dirección MAC de su equipo, la cual será reservada en el servidor de DHCP el cual permitirá una conexión satisfactoria.
- Un identificador único de equipo debe ser aplicado a los equipos de presidencia antes o durante el ingreso del equipo al dominio.
- La identificación en la red cableada se la debe realizar a través de 802.1x y autenticación de usuario del dominio y equipo de dominio.

3.1.1.1.5. Protección de los puertos de diagnóstico y configuración remota

- El único método de acceso remoto a los contenedores que conforman el servicio de correo electrónico debe ser a través de SSH.
- A nivel de perímetro únicamente los puertos para el uso de correo deben estar permitidos el acceso.
- Debe complementarse con los controles de gestión de privilegios.

3.1.1.1.6. Control de enrutamiento en la red

- Configurar reglas para permitir adjuntos en el envío y recepción de correos electrónicos.
- Identificar IP de origen que se encuentren en listas negras para evitar recibir correo no deseado.
- Bloquear remitentes que intenten realizar algún tipo de Phishing.

3.1.1.1.7. Controles para código malicioso

- Contar un antivirus a nivel de usuario para poder realizar un monitoreo y escaneo de las distintas amenazas de correo electrónico.
- Identificar los equipos que poseen clientes de correo electrónico y poder realizar el escaneo de carpetas con las que trabaja.
- Concienciar a los usuarios sobre la existencia de los diferentes tipos de ataques a través de correo electrónico como:

    - Spam
    - Distribution de Malware (virus, gusanos, rootkits, trayanos, keyloggers, spyware, adware, etc.)
    - Phishing

- Contar con los últimos parches o raleases en los contenedores del servicio de correo electrónico.

- Implementar IPS para detección de posibles ataques no solo a nivel de correo electrónico.

3.1.1.1.8. Controles de red

Estos controles son complementarios a los anteriores y que de alguna u otra manera uno depende del otro. Adicionalmente son controles de propósito general es decir no aplican exclusivamente al servicio de correo electrónico.

- El acceso de usuarios a la red inalámbrica debe realizarse haciendo uso de usuario y contraseña de domino.
- El acceso a la red inalámbrica de las autoridades se la hará a través del identificador único en base a una reserva de dirección MAC.
- El acceso para la administración de dispositivos activos de red se lo realizará a través de una VLAN de administración.
- El acceso al segmento de red donde se encuentran los contenedores del servicio de correo electrónico se lo debe realizar a través de listas de acceso y de ser el caso reglas en el firewall basadas en directorio Activo.
- Crear VLAN privadas para el acceso de las autoridades que usan de la red cableada.
- El control de acceso debe ser centralizado a través de algún sistema de AAA.
- Se complementa los controles de identificación de quipos en la red.
- Los dispositivos que no sean un bien de Presidencia, deberán hacer uso de la red para invitados.
- La red de invitados debe estar aislada de todas las redes internas de Presidencia, salvo algún caso especial y aprobado por la SSI.

3.1.1.1.9. Seguridad de los servicios de red

- Definir un contrato con el ISP los niveles de servicio que al menos cubran el 99.6% de disponibilidad en cada uno de los servicios de la WAN.

- Se debe incluir un monitoreo proactivo de cada uno de los servicios por parte del ISP.
- Para enlaces críticos se debe considerar redundancia de proveedores para cumplir con la alta disponibilidad.
- Los proveedores deberán trabajar con un protocolo de balanceo de carga como es el GLBP.

3.1.1.2. Política de seguridad para el servicio de Videoconferencia

3.1.1.2.1. Controles para código malicioso

Estos controles son aplicables a nivel general y complementar los anteriormente definidos.

- TI a través de soporte técnico es el único para poder realizar instalación de software o programas en las PC/portátiles de presidencia.
- Definir reglas de filtrado URL y aplicaciones con definiendo niveles de riego alto para evitar la descarga de cualquier tipo de malware que afecte a la máquina del usuario.
- El usuario detecta algún tipo de incidente deberá comunicarse a la mesa de servicio indicando el incidente y esta dirigirá el incidente al área correspondiente.
- El área de soporte definirá el procedimiento para la instalación de software en los equipos de los usuarios finales.

3.1.1.2.2. Gestión de privilegios y uso de claves secretas

- La administración de los contenedores del sistema de videoconferencia es del área de Redes y Comunicaciones y será responsable de la asignación de clave o pin de sala y de moderador.

- Los pin de salas virtuales y moderador serán entregadas únicamente o funcionarios o área de presidencia o alguna institución que se encuentre autorizada por la Dirección de Tecnología.
- El manejo de los pin de sala y moderador será responsabilidad de la institución quien solicita la reunión virtual.
- El pin de la sala deber ser cambiado cada 30 días en el caso de las instituciones gubernamentales y 15 días en el caso de las salas virtuales usadas para reuniones presidenciales oficiales.
- El pin de moderador será únicamente utilizada por la persona designa por la Dirección de Tecnología para ser el moderador de la reunión en Gabinete Virtual.
- Únicamente usuarios citados a la reunión virtual tendrán acceso al pin de sala.

3.1.1.2.3. Política sobre el uso de los servicios de la red

- Únicamente podrán hacer uso del sistema de videoconferencia instituciones quienes hayan solicitado formalmente la asignación de una sala virtual con sus pin.
- El uso del servicio de videoconferencia será de uso exclusivo de Presidencia en sesiones de Gabinete Virtual o algún tipo de reunión oficial presidencial.
- El uso es exclusivo para autoridades de las distintas instituciones que cumplan con el primer punto.
- Reuniones virtuales del tipo; video llamada y videoconferencia que se llevan a cabo las instituciones y eventos presidenciales, se las debe realizar haciendo uso del servicio gubernamental.
- El uso del servicio con el fin de probar la comunicación de los equipos de videoconferencia deberá ser coordinado con la Dirección de tecnología de la Presidencia.
- En Presidencia únicamente sesiones virtuales autorizadas podrán tener acceso al servicio así como a la red donde se encuentra el servicio.

- El acceso al servicio para las distintas instituciones deberán pertenecer al anillo interministerial o únicamente una conexión de internet.

3.1.1.2.4. Autenticación de los usuarios para las conexiones remotas

- La método de conexión remota a los contenedores de videoconferencia debe ser realizada a través de RDP y autenticación de usuario de dominio.
- La consola de administración debe usar una variación del puerto 443 para asegurar la comunicación entre los contenedores y los administradores.

3.1.1.2.5. Identificación de los equipos en las redes y control de conexión a la red

Algunos de estos controles se pueden aplicar de manera general a la red de Presidencia y como complemento de los controles de acceso a la red.

- El identificador de equipos de videoconferencia debe ser unas direcciones H.323.
- Definir reglas en el firewall de perímetro basado en direcciones IP de las instituciones quienes hacen uso del sistema de videoconferencia.
- El registro del identificador lo realizara el gatekeeper.
- El acceso al servicio de videoconferencia de lo debe realizar a través del anillo interministerial o a través de la web

3.1.1.2.6. Control de routing de la red

- Definir a nivel de ISP las rutas más eficientes para alcanzar el servicio de videoconferencia.
- Creación de reglas en el firewall de perímetro para permitir el paso de los protocolos necesarios en la comunicación de la videoconferencia.

CAPITULO IV

4.1. CONCLUSIONES Y RECOMENDACIONES

4.1.1. CONCLUSIONES

- A pesar que este trabajo analizó los riesgos a nivel de usuario final para y de la red para poder mitigarlos, la brecha de la seguridad de la información en la Presidencia aun es grande ya que no solo se trata de tecnología, sino más bien de procedimientos y procesos claros al usar la información generada en cualquier formato, sea este digital o escrito.

- La Presidencia de la Republica a pesar de que está trabajando en la aplicación del EGSI, aún no ha podido resolver el inconveniente de identificar los riesgos de la seguridad de la información. El presente trabajo servirá de guía para que se pueda iniciar con la identificación de los riesgos.

- En el presente análisis se identificó niveles de riesgo altos a nivel de usuario final, esto se debe primeramente a la falta o escaza información que se tenía de lo que es la seguridad de la información, así también a que no existían procedimientos tecnológicos que el usuario debía seguir.

- A pesar de que los niveles de riesgo de acceso a la red en algunos casos también fueron altos, los controles a aplicar son mínimos ya que el área de Redes y Conectividad ha trabajado, aunque sin un análisis de riesgo previo, en cerrar las brechas de seguridad basadas en las necesidades de los usuarios a la información.

- Algo muy interesante que se encontró con este trabajo es la confusión que existe, incluso de algunas las personas de TI, al pensar que únicamente con

el uso de métodos de encripción o cifrado está cubierta la brecha de la seguridad de la información. Tal vez no sea en la única institución que ocurra esto.

- Presidencia como institución podría implementar cualquier método de análisis de riesgo, el único requisito es el compromiso que las máximas autoridades deben tener al momento de aplicar las políticas y no solo dejarlas en letra muerta.

- El método Octave-Allegro desde mi punto de vista es el más practico al momento de realizar el análisis de riesgo, ya que provee plantillas, en las cuales se pueden aumentar algún tipo de parámetro requerido y se enfoca principalmente en encontrar los escenarios de amenazas más reales para la organización.

- Algo muy interesante del método Octave-Allegro es que no se requirió un análisis de vulnerabilidades, ya que el análisis se basa en escenarios de posibles amenazas.

- Crear una política de seguridad de la información no es solo realizar el análisis correspondiente de los activos de información críticos, sino es de trasmitir conciencia de seguridad a toda la organización.

- La política de seguridad de información debe ser los más clara posible y en lenguaje no técnico, ya que esta será comunicada a personas que tienen el conocimiento del tema.

4.1.2. RECOMENDACIONES

- Cuando se inicia con la gestión de riesgos de la seguridad de la información de debe iniciar únicamente tomando en cuenta las tres variables principales confidencialidad, integridad, disponibilidad. Ya que se requiere un poco más de experiencia para poder involucrar otras variables.

- Cuando en la organización existen varios actores que participan en la protección de la información, se debe definir los roles y responsabilidades de dichos actores y su alcance. Esto podrá optimizar el tiempo de implementación de cualquier tipo de política.

- Se recomienda que cualquier metodología que se vaya aplicar para la gestión de riesgos se la debe alinear con los objetivos estratégicos de la organización, así evitar que la selección de controles no sea la adecuada.

- Es recomendable para organizaciones que no poseen un historial de incidentes de seguridad de la información durante algunos años atrás realizar un análisis de riesgo cualitativo.

- Como la gestión de riesgo es un proceso constante y de igual manera las amenazas cada vez son sofisticadas, el área de seguridad de la información o los responsables de la misma deberían esta suscritos a sitios informativos donde se publiquen nueva amenazas, vulnerabilidad y ataques, y así poder mantener bajo niveles de riesgos.

REFERENCIAS BIBLIOGRÁFICAS

Libros

- Stallings Wiliam, “Network Security Essentials,” 4ta edición, Prentice Hall 2011.
- Peltier Tomas, “Information Security Policies, Procedures and Standars,” Auerbach 2002.
- Andress Jason, “the Basics of Information Security, Singress,” Elsevier 2011.
- Stuart Jacob, “Engeneering Information Security,” Willey 2011.
- Kurosse-Ross,” Computer Networking, sexta edición. Pearson 2013.
- TanenBaum-Wetherall,” Computer Networks,” quinta edición.
- Evan Wheeler, Security risk Management, Elsevier 2011.
- Josseph Migga Kizza, “Computer Network Security,” Springer 2005
- Eric Conrad, Seth Misenar, Joshua Feldman, “Official CISSP Study Guide,” cuarta edición, Elsevier 2012
- Krausz Michel, “Management Information Security Breaches,” IT Governance Publishing 2010.

Sitios web

- http://www.etuttor.com/index.php/component/k2/item/284-not1
- http://www.unl.edu.ar/emprendedores/?p=4776
- http://www.elergonomista.com/relacioneslaborales/rl83.html
- http://es.scribd.com/doc/39430270/codigo-movil
- https://sites.google.com/site/ticsing9estadistica/tics-en-las-empresa
- http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1

Normas

- ISO 27002, Code of practice for information security management
- ISO 27005, Information Security risk Management.
- ISO 27033, Security techniques-Network security.
- Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process
- MAGERIT v3.0, Metodología de Análisis y Gestión de Riesgos de los sistemas de información, Libro I,II,III

ANEXOS