UNA PERSPECTIVA GLOBAL PARA LA APLICACIÓN DE LA SEGURIDAD INFORMÁTICA, EN LAS ENTIDADES PÚBLICAS DEL ESTADO COLOMBIANO

Mosquera Tribales Darío Osvaldo
dario.osvaldo.mosquera@gmail.com
Universidad Piloto de Colombia

***Resumen*—** El documento presenta un esquema que permite a los funcionarios públicos identificar las actividades que deberían planear para la aplicación de la seguridad informática de forma integral dentro de cada entidad, presentando las generalidades a tener en cuenta.

Abstract— The document presents a scheme that allows public officials to identify the activities they should plan for the application of computer security in an integral way within each entity, presenting the generalities to be taken into account.

***Índice de Términos*—** Riesgo informático, entidades públicas, estado colombiano, Conpes 3701, Conpes 3854, gestión del riesgo, seguridad informática, SGSI, criptografía.

I. INTRODUCCIÓN.

Las entidades del estado Colombiano, se encuentran en un proceso de apropiación y aplicación de las diferentes metodologías y técnicas existentes que permitan encarar los riesgos y amenazas a las que se exponen estas organizaciones, y así evitar graves afectaciones como las que vivió el Estado de Estonia en el año 2007, en donde a través de la utilización de diferentes tipos de botnets instalados en host a través del todo el mundo, dirigieron un ataque de denegación del servicio a diferentes router y servidores de este país.

El Estado Colombiano, a través del Ministerio de Tecnologías de la Información y las Comunicaciones, ha iniciado en la estrategia de gobierno en línea, la aplicación de estándares de seguridad que proporcionan una base para la minimización del impacto de los riesgos asociados a la infraestructura informática.

El trabajo del Estado Colombiano que busca minimizar los riesgos en la entidades públicas, no solo se queda con lo definido en la estrategia de gobierno en línea, pues la definición de documentos técnicos denominados Conpes, han definido actividades que permitió la asignación de recursos económicos para la conformación de dependencias dentro de algunos ministerios o unidades administrativas, la promoción de las capacitaciones dirigidas para los funcionarios publicas que contaran con el perfil y la iniciativa de desarrollar programas académicos orientados a la seguridad informática, la capacitación especializada con organizaciones internaciones para los grupos de defensa nacional, entre otras.

Este documento presenta las etapas que podría implementar una entidad del Estado Colombiano, para gestionar y minimizar el riesgo en sus activos de información.

II. AMENAZAS Y VULNERABILIDAD INFORMÁTICAS.

Durante lo corrido del año 2016, en américa latina, al igual que el resto del mundo, el sector público se ha convertido en un objetivo importante para los criminales informáticos, en donde aprovechan las vulnerabilidades que se encuentran presentes en los sistemas operativos.

En Colombia, muchas de las entidades gubernamentales utilizan sistemas operativos con más de 5 años de haber sido lanzados al mercado los cuales poseen vulnerabilidades conocidas solucionadas hace más de 3 años y que a pesar de esto, aún siguen sin ser aplicadas las medidas de seguridad que mitigarían estas vulnerabilidades.

Dada la anterior situación, los administradores de infraestructuras tecnológicas reconocen que las principales amenazas de seguridad están representadas principalmente en vulnerabilidades de los sistemas operativos y/o del software, malware, acceso no autorizado a sistemas informáticos, fraude informático, ataques de denegación de servicio, phishing, ataques de ingeniería social, entre otros [1], todas estas penalizadas por la Ley 1273 de 2009.

Como ejemplo reciente de vulnerabilidad de los sistemas operativos y/o del software se encuentra el ataque denominado FREAK Attack (CVE-2015-0204), de alto impacto, el cual fue dado a conocer al público el 27 de marzo de 2015, donde se evidencio una vulnerabilidad en el protocolo criptográfico SSL/TLS el cual es utilizado en el protocolo HTTPS. Otro ejemplo para el caso de malware, que se presentó durante el mes de octubre de 2016 en Colombia, es el denominado RDN/Downloader.a!qk por McAfee, Trojan.Win32.Badur.hryp por Kaspersky, Troj/Agent-AGXX por Sophos y Win32/TrojanDownloader.Wauchos por ESET, donde una vez instalado en el PC Windows, descarga e instala software sin la autorización del usuario, para lo cual, previamente desactiva la funcionalidad del principio de mínimo privilegio (Least user access) denominado en el sistema operativo Windows 10 como control de cuentas de usuario, modificando el registro.

Dentro del software malicioso, existen dos familias de amenazas denominadas ransomware y botnets las cuales cuentan con especial presencia en américa latina.

El malware de la familia botnets, busca principalmente utilizar los recursos de procesamiento y/o almacenamiento del host huésped en el envío de spam, la propagación de malware,

minería de bitcoins, el robo de la información almacenada del host huésped y/o para el direccionamiento de solicitudes a servidores que permitan consumir los recursos de trasmisión y/o procesamiento de datos (DDoS).

Ransomware, se presenta con tres variantes. La primera es el cifrado de los archivos de usuarios, la segunda, el cifrado de los archivos de los usuarios y del sistema provocando la inutilización del sistema operativo, y la última, el cifrado de los archivos de los usuarios, del sistema y bloqueo total del sistema operativo. Es actualmente, el malware que mayor daño ha generado y el que mayor beneficio económico ha otorgado a los ciberdelincuentes, dado que utilizan como vectores de propagación el correo electrónico, publicidad malintencionada alojada en páginas web, vulnerabilidades de red y de los servidores.

Ransomware ha sido fortalecido mediante el desarrollo de nuevas estrategias de propagación, haciendo que este malware emerja como una industria criminal global, mediante ejecutables que se auto propagan, utilizando las técnicas de los gusanos. Los ejecutables se apoyan en las siguientes debilidades y/o vectores [2]:

(i) Uso de una vulnerabilidad de un producto ampliamente usado.
(ii) Replicación en todas las unidades disponibles.
(iii) Infecciones de archivos.
(iv) Actividad de fuerza bruta limitada.
(v) Comando y control resistentes.
(vi) Uso de otras puertas traseras.

El anterior panorama, es apenas una muy breve descripción de la realidad que están afrontando las diferentes organizaciones (pequeña, mediana o grande) en sus infraestructuras tecnológicas, teniendo en cuenta que ahora los ciberdelincuentes dirigen su mayor esfuerzo a los ataques hacia servidores convirtiéndose estos en persistentes.

III. ESTRATEGIAS EN CIBERSEGURIDAD ADOPTADAS EN COLOMBIA.

El 23 de noviembre de 2001, los estados miembros del Consejo de Europa firmaron el convenio No 185 sobre la ciberdelincuencia. “La convención” es el primer tratado internacional sobre los crímenes cometidos a través de Internet y otras redes informáticas, que trata sobre todo con las infracciones de los derechos de autor, el fraude informático, la pornografía infantil y violaciones de seguridad de la red. También contiene una serie de competencias y procedimientos tales como la búsqueda de las redes informáticas y la interceptación.

Su objetivo principal, que figura en el preámbulo, es llevar a cabo una política penal común encaminada a la protección de la sociedad contra el delito cibernético, especialmente mediante la adopción de una legislación apropiada y el fomento de la cooperación internacional [3]”.

El convenio entró en vigor a partir del 1 de julio de 2004 y desde entonces 30 estados lo han firmado, ratificado y adherido, mientras que otros 16 solo lo han firmado.

Colombia, en el año 2012 solicitó al Consejo de Europa una invitación para hacer parte de la Convención de Budapest, y esta invitación fue generada en el año 2013, para lo cual el Estado Colombiano tiene 5 años para cumplir con los lineamientos del Convenio y adherirse a este.

A. Conpes 3701.

Para el año 2011, Colombia no poseía un lineamiento rector a nivel nacional que impulsara la seguridad cibernética en el territorio, para lo cual identificaron 3 ejes problemáticos que fueron definidos de la siguiente forma [4]:

(i) Falta de coordinación en la iniciativas y operaciones de ciberseguridad y ciberdefensa.
(ii) Falta de capacitación especializada en ciberseguridad y ciberdefensa.
(iii) Debilidad en la regulación y legislación en la protección de los datos.

Como resultado del anterior análisis, el Estado Colombiano expidió el documento Conpes (Consejo Nacional de Política Económica y Social) 3701 el cual definió los lineamientos de política para ciberseguridad y ciberdefensa y buscó fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético, creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio [4] .

B. Conpes 3854.

Esta estrategia adoptada el 11 de abril de 2016 se enfocada en la gestión del riesgo informático, y acoge la recomendación de OCDE, el cual definió 4 principios fundamentales y cinco dimensiones estratégicas, siendo estas las siguientes:

Principios fundamentales:

(i) Salvaguardar los derechos humanos y los valores fundamentales.
(ii) Adoptar un enfoque incluyente y colaborativo.
(iii) Asegurar una responsabilidad compartida.
(iv) Adoptar un enfoque basado en la gestión de riesgos.

Dimensiones estratégicas:

(i) Gobernanza de la seguridad digital.
(ii) Marco legal y regulatorio de la seguridad digital.
(iii) Gestión sistemática y cíclica del riesgo de seguridad digital.
(iv) Cultura ciudadana para la seguridad digital.
(v) Capacidades para la gestión del riesgo de seguridad digital.

C. Marcos jurídicos de seguridad cibernética en Colombia.

Ley 1273 de 2009, tipifica como delitos informáticos una serie de conductas que generan daño civil a los ciudadanos colombianos.

Ley 906 de 2004, reconoce los tratados internacionales con Interpol y Europol.

Ley 1581 de 2012, protección de datos, divulgación y denuncia de las violaciones de seguridad.

Decreto 1377 de 2013, reglamenta la Ley 1581 de 2012.

Ley 527 de 1999, define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación

D. Capacidad de seguridad cibernética en Colombia [5].

El Estado Colombiano ha participado activamente en el programa de seguridad cibernética del Comité interamericano contra el terrorismo de la OEA, programa creado en el año 2014, mediante la autorización de los estados miembros de la

OEA. Bajo el desarrollo de las actividades del programa, se encuentra el observatorio de la ciberseguridad en América Latina y el Caribe, el cual aplico en los estados miembros una encuesta del nivel de aplicación del modelo de madurez de capacidad de seguridad cibernética desarrollado el Centro de la capacidad mundial de seguridad cibernética (Global Cyber Security Capacity Centre (GCSCC)) de la Universidad de Oxford, el cual evalúa cinco dimensiones, siendo estas las siguientes:

(i) Políticas y estrategia nacional de seguridad cibernética.
(ii) Cultura cibernética y sociedad.
(iii) Educación, formación y competencias en seguridad cibernética.
(iv) Marco jurídico y reglamentario.
(v) Normas, organizaciones y tecnologías.

La aplicación de los 49 tópicos de las anteriores dimensiones contribuye a que los estados posean mejores niveles de seguridad frente a las amenazas actuales.

El nivel de madurez posee cinco niveles de calificación, siendo estos los siguientes:

(i) Inicial.
(ii) Formativo.
(iii) Establecido.
(iv) Estratégico.
(v) Dinámico.

Para el caso de Colombia, los resultados fueron los siguientes:

TABLA I.
Nivel de madures CMM [5]

DIMENSIONES	NIVEL CMM
POLÍTICA Y ESTRATEGIA	
Estrategia nacional de seguridad cibernética oficial o documentada	
Desarrollo de la estrategia	ESTABLECIDO
Organización	FORMATIVO
Contenido	ESTABLECIDO
Defensa cibernética	
Estrategia	FORMATIVO
Organización	ESTABLECIDO
Coordinación	FORMATIVO
CULTURA Y SOCIEDAD	
Mentalidad de seguridad cibernética	
En el gobierno	FORMATIVO
En el sector privado	FORMATIVO
En la sociedad	ESTABLECIDO
Conciencia de seguridad cibernética	
Sensibilización	ESTABLECIDO
Confianza en el uso de Internet	
En los servicios en línea	ESTABLECIDO
En el gobierno electrónico	ESTABLECIDO
En el comercio electrónico	FORMATIVO
Privacidad en línea	
Normas de privacidad	ESTABLECIDO
Privacidad del empleado	ESTABLECIDO
EDUCACIÓN	
Disponibilidad nacional de la educación y formación cibernéticas	
Educación	ESTABLECIDO
Formación	FORMATIVO
Desarrollo nacional de la educación de seguridad cibernética	
Desarrollo nacional de la educación de seguridad cibernética	FORMATIVO
Formación e iniciativas educativas públicas y privadas	
Capacitación de empleados en seguridad cibernética	ESTABLECIDO
Gobernanza corporativa, conocimiento y normas	
Comprensión de la seguridad cibernética por parte de empresas privadas y estatales	FORMATIVO
MARCOS LEGALES	
Marcos jurídicos de seguridad cibernética	
Para la seguridad de las TIC	FORMATIVO
Privacidad, protección de datos y otros derechos humanos	ESTABLECIDO
Derecho sustantivo de delincuencia cibernética	ESTABLECIDO
Derecho procesal de delincuencia cibernética	ESTABLECIDO
Investigación jurídica	
Cumplimiento de la ley	ESTABLECIDO
La fiscalía	FORMATIVO
Tribunales	FORMATIVO
Divulgación responsable de la información	
Divulgación responsable de la información	INICIAL
TECNOLOGÍAS	
Adhesión a las normas	
Aplicación de las normas y prácticas mínimas aceptables	FORMATIVO
Adquisiciones	FORMATIVO
Desarrollo de software	FORMATIVO
Organizaciones de coordinación de seguridad cibernética	
Centro de mando y control	ESTABLECIDO
Capacidad de respuesta a incidentes	FORMATIVO
Respuesta a incidentes	
Identificación y designación	FORMATIVO
Organización	FORMATIVO
Coordinación	FORMATIVO
Resiliencia de la infraestructura nacional	
Infraestructura tecnológica	ESTABLECIDO
Resiliencia nacional	FORMATIVO
Protección de la Infraestructura Crítica Nacional (ICN)	
Identificación	FORMATIVO
Organización	FORMATIVO
Planeación de respuesta	INICIAL
Coordinación	FORMATIVO
Gestión de riesgos	FORMATIVO
Gestión de crisis	
Planeación	FORMATIVO
Evaluación	FORMATIVO
Redundancia digital	
Planeación	FORMATIVO
Organización	FORMATIVO
Mercado de la ciberseguridad	
Tecnologías de seguridad cibernética	FORMATIVO
Seguros de delincuencia cibernética	FORMATIVO

Este resultado demuestra la imperiosa necesidad de mejora continua que requiere Colombia en cuanto a seguridad de la información.

IV. ESTRATEGIA DE GOBIERNO EN LÍNEA.

Esta estrategia definida en el Decreto 1078 de 2015, está diseñada para el desarrollo de cuatro componentes, siendo estos los siguientes:

(i) TIC para servicios.
(ii) TIC para gobierno abierto.
(iii) TIC para gestión.
(iv) Seguridad y privacidad de la información.

El componente de seguridad y privacidad de la información está orientado al desarrollo y/o implementación de la NTC-ISO/IEC 27001:2013 bajo ciclo PHVA.

La estrategia para este componente propone el desarrollo de las siguientes actividades:

(i) Diagnóstico de seguridad y privacidad.
(ii) Plan de seguridad y privacidad de la información.

(iii) Gestión de riesgos de seguridad y privacidad de la información.
(iv) Evaluación del desempeño.

V. ETAPAS PARA LA APLICACIÓN DE LA SEGURIDAD INFORMÁTICA.

A. Implementación del Sistema de gestión de seguridad de la información [6].

1) Fase de diagnóstico.

a) Diagnóstico del estado actual de la entidad.

Determinar el estado actual de la gestión de seguridad de la información dentro de la entidad, teniendo como fundamento el cumplimiento de los requerimientos de la norma y los controles de la NTC-ISO/IEC 27001:2013.

b) Identificar el nivel de madurez de seguridad de la información.

Utilizando el modelo de integración de la capacidad y madurez (CMMI) versión 1.3, determinar el nivel de cumplimiento frente a la norma NTC-ISO/IEC 27001:2013, teniendo como base la siguiente figura:

TABLA II.
Comparación de los niveles de capacidad y madurez [7]

NIVEL	Representación continua Niveles de capacidad	Representación continua Niveles de madurez
Nivel 0	Incompleto	
Nivel 1	Realizado	Inicial
Nivel 2	Gestionado	Gestionado
Nivel 3	Definido	Definido
Nivel 4		Gestionado cuantitativamente
Nivel 5		En optimización

c) Identificar vulnerabilidades técnicas y administrativas.

Aplicar herramientas que permitan identificar todas las vulnerabilidades que posean los activos de información de la entidad, describiendo los hallazgos identificados.

2) Fase de planeación.

a) Definición de las políticas de seguridad y privacidad de la información.

Generar un documento aprobado por la alta gerencia de la entidad, donde se especifique los objetivos, alcance y nivel de cumplimiento de las políticas del SGSI. La política deberá darse a conocer al interior de la entidad.

b) Manual de políticas de seguridad y privacidad de la información.

Documento en el cual serán explicadas las políticas, los principios de seguridad y la normatividad vigente aplicable.

c) Definición, identificación y/o actualización de los procedimientos de seguridad de la información.

Las entidades publicas, según sea el caso, deberá poseer de una serie de procedimientos formalizados que permitirán gestionar la seguridad de la información en cada uno de los procesos que la entidad desarrolla (apoyo, misionales, estratégicos, etc.).

d) Definición de roles, responsabilidades y gobierno de la seguridad y privacidad de la información.

La entidad debe definir claramente, teniendo como base el organigrama institucional, la estructura del gobierno de la seguridad de la información, al cual le serán asignados roles y responsabilidades para la correcta implementación y continuidad del programa de SGSI. Estos roles permitirán identificar como se asignan las responsabilidades y a su vez, como cada quien responde a su obligaciones.

e) Definición del inventario de activos de la información de la entidad.

Cada entidad posee información y/o datos que son vitales para el cumplimiento de sus funciones, los cuales pueden estar almacenados en medios físicos (papel) o digitales (servidores, dispositivos de almacenamiento externo), los cuales deberán ser identificados, descritos y clasificados, para luego asignarles un valor de importancia dentro de la organización.

f) Integrar el SGSI con el sistema de gestión documental.

La gestión documental en las entidades públicas se encuentra orientada por el Archivo General de la Nación, el cual, a través de una serie de normas establecen como se debe aplicar la gestión documental. Por tal motivo, el SGSI debe estar armonizado con estas normas.

g) Identificación, valoración y tratamiento de riesgos.

Una vez identificados los activos de información de cada uno de los procesos de la entidad, se debe establecer una metodología para identificar, evaluar, tratar y dar seguimiento a los riesgos de estos activos. Es importante apropiar una metodología para el tratamiento de los riesgos, y se recomienda el uso de NTC/ISO 31000-2011. Como complemento a esta etapa, debe armonizase esta actividad con la Guía para la administración del riesgo diseñada por el Departamento Administrativo de la Función Pública.

3) Fase de implementación.

a) Planificación y control de la implementación.

La entidad debe planear, implementar y controlar las actividades necesarias para cumplir con la política, objetivos, alcance planteado y el nivel de cumplimiento definido del SGSI para lo cual, debe aplicarse la metodología de la guía PMBOK.

b) Implementación del plan de tratamiento del riesgo.

Se inicia la aplicación del plan de tratamientos del riesgo, con el objeto de minimizar el impacto negativo de los riesgos identificados. El control sobre los riesgos identificados deberá estar aprobados por el dueño del proceso.

c) Medición de la gestión.

La entidad deberá medir y definir indicadores que permitan medir la efectividad, eficiencia y eficacia en la puesta en marcha del SGSI.

Los indicadores medirán los siguientes lineamientos:
(i) Efectividad de los controles.
(ii) Eficiencia del SGSI al interior de la entidad.
(iii) Identificar el nivel de seguridad dentro de la entidad.

4) Seguimiento y monitoreo.

a) Revisión y seguimiento a la implementación.

Esta actividad requiere el diseño de un plan que permita desarrollar las siguientes actividades:

(i) Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.
(ii) Revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de controles y medidas administrativas.
(iii) Seguimiento a la programación y ejecución de las actividades de autorías internas y externas del SGSI.
(iv) Seguimiento al alcance y a la implementación del SGSI.
(v) Seguimiento a los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o desempeño de la seguridad de la información al interior de la entidad.
(vi) Medición de los indicadores de gestión del SGSI.
(vii) Revisiones de acciones o planes de mejora (solo aplica en la segunda revisión del SGSI).

b) Programa de auditorías.

El sistema de gestión en cumplimiento del numeral 9.2 de la NTC/ISO 27001:2013, indica la necesidad de aplicar auditorías internas a intervalos planificados, para lo cual se debe aplicar la NTC/ISO 19011:2012, la cual indica la metologia para la aplicación de las auditorias de los sitemas de calidad.

5) Fase de mejora continua.

Los resultados de las auditorias, siempre desencadenan necesidades de mejora y/o optimización de algún control que define la norma, por lo cual, se debe establecer un plan de mejoramiento que busque alcanzar un alto nivel de capacidad y madurez en la aplicación de la NTC/ISO 27001:2013.

B. Uso de la criptografía para el aseguramiento de la información.

La criptografía es una técnica que se encuentra intrínseca dentro del aseguramiento de la información, y permite disminuir la exposición a los riesgos.

Una entidad pública, debe implementar los siguientes controles criptográficos:

1) Firma digital.

Este método criptográfico, aporta la identificación de un individuo a un mensaje o documento y a su vez la integridad de los datos firmados. Es un elemento indispensable y debe utilizarse en los siguientes casos:

a) Firma digital en correos electrónicos.

La mensajería a través de las aplicaciones de correo electrónico debe de asegurarse con el objeto de garantizar confidencialidad e integridad. Para este fin es indispensable la configuración del servicio OpenPGP con el protocolo RFC 6637 (Elliptic Curve Cryptography (ECC) in OpenPGP).

b) Firma digital en documentos electrónicos.

Los documentos digitales generados en paquetes de ofimática y/o lectores digitales tales como pdf o ePub, requieren garantizar su autenticidad e integridad y las firmas digitales son un medio que permiten introducirle estas características. Estas firmas se disponen a través del servicio OpenPGP con el protocolo RFC 6637 (Elliptic Curve Cryptography (ECC) in OpenPGP).

2) Certificados electrónicos en servidores.

Spoofing es un ataque muy utilizado por los ciberdelicuentes y una estrategia para evitar esta modalidad es la utilización de certificados de autenticidad.

Los servidores que se encuentran expuestos a la web y los certificados electrónicos deben ser adquiridos ante una entidad certificadora que cuente con la infraestructura de clave pública la cual, debe ser consultada por todos los usuarios web.

Para los servidores que se encuentran en la red interna de la entidad, es necesario la configuración del servicio OpenLDAP, el cual está conformado por los siguientes componentes:

(i) Autoridad de certificación (CA)
(ii) Autoridad de registro (RA)
(iii) Servidor de certificados
(iv) Repositorio de certificados
(v) Autoridad de sellado de tiempo

3) Comunicaciones seguras.

Cuando no se aplican los protocolos criptográficos, las comunicaciones a través de la web, se realizan mediante texto plano permitiendo a cualquier interesado que tenga la capacidad de interceptar el canal, capturar las cargas útiles de las tramas de los paquetes de datos. Las comunicaciones, según sea el tipo de implementación, requieren la aplicación de un protocolo criptográfico y/o una técnica de comunicación. A continuación, se presentan las siguientes opciones:

a) Red privada virtual.

Esta técnica de comunicación implementa entre dos o más nodos, la confiabilidad e integridad de los datos transportados. Para este caso, debe utilizarse el protocolo criptográfico IPSec, el servicio OpenVPN y configurando las siguientes variaciones de VPN:

(i) VPN de acceso remoto: esta opción permite a varios usuarios dispersados geográficamente conectarse al servidor VPN mediante la utilización de usuario y contraseña.
(ii) VPN punto a punto: esta opción permite la conexión de dos sitios remotos a través de la configuración de un túnel de comunicación mediante el uso de protocolos criptograficos, configurado a través de software o Gateway. Esta opción ofrece características de confidencialidad.
(iii) VPN tunneling: consiste en encapsular un protocolo de red dentro de otro, creando un túnel digital dentro de la red mediante el uso de protocolos criptográficos. Esta configuración gestada a través de gateway define el recorrido de los datos a través de los diferentes saltos entre router, sin permitir que la información se visible.

b) Cifrado web.

Para esta opción de protección criptográfica, se debe configurar la versión segura del protocolo HTTP dentro del servicio que provee la aplicación APACHE del contenedor y/o servidor de aplicaciones web. El protocolo criptográfico a ser utilizado será TLS 1.2.

c) Mensajería instantánea.

Dentro de las entidades, la mensajería instantánea es una opción de optimización del trabajo de los usuarios, razón por la cual es de interés configurar opciones criptográficas que minimicen la interceptación de los paquetes.

Existen dos métodos criptográficos que son de mayor uso, el primero XMPP, utilizado por WhatsApp, google talk, entre otros, y el segundo, el aportado por Skype, que utiliza el protocolo P2P, el cual incorpora algoritmos de cifrado AES-256, RSA-2048.

El software de mensajería instantánea posee sus propias técnicas de cifrado y no requiere de la configuración de servicios dentro de la entidad.

d) Cifrado de disco duro.

Esta técnica permite cifrar total o parcialmente el disco duro de un equipo de cómputo o los discos duros de un arreglo de discos para el almacenamiento masivo de información.

La configuración de cifrado total del disco, cifra la totalidad de los sectores del disco, requiriendo una clave para dar inicio a la carga del sistema operativo.

Otra opción, es el arranque transparente mediante el uso de TPM, tecnología que se encuentra incorporada en la board.

Como recomendación gratuita para la aplicación del cifrado, está disponible GNUPGP.

C. Aseguramiento de las aplicaciones en las entidades públicas.

Este aspecto es el de menor importancia en las entidades públicas colombianas, dada la falta de perfiles de desarrolladores que incorporen en el código fuente, buenas prácticas de desarrollo seguro, la falta de configuración de firewall de aplicaciones.

1) Buenas prácticas de seguridad para el desarrollo de software.

Actualmente en los ciclos de vida de desarrollo de software, se encuentran con amplia aceptación buenas prácticas tales como OWASP e ISO/IEC 27034:2011, pero para el caso en particular, es recomendado el uso de OWASP, el cual, para la fase de SDLC, propone las siguientes fases:

(i) OWASP [8]: es un proyecto abierto que busca minimizar las causas que generan software inseguro durante la etapa de desarrollo. Define 5 fases a tener en cuenta durante la construcción del software. Estas fases y sus respectivas actividades son las siguientes:

a. Antes de iniciar el desarrollo: definir un ciclo de vida de desarrollo de software que incluya la seguridad como un componente transversal; revisar políticas y estándar; definir métricas, criterios de medición y asegurar la trazabilidad del desarrollo.
b. Durante el análisis y diseño: revisión de los requerimientos de seguridad; revisar diseño y arquitectura; crear y revisar los modelos UML; crear y revisar los modelos de amenazas.
c. Durante el desarrollo: análisis del código; revisión del código.
d. Durante la implementación: aplicación de pruebas de penetración; pruebas de gestión de la configuración.
e. Mantenimiento y operación: revisar la gestión de la operación del aplicativo e infraestructura; realizar revisiones periódicas de la integridad del aplicativo; probar niveles de seguridad después de cambios.

2) Firewall de aplicaciones.

Los firewall de aplicaciones son un software que a través de un conjunto de reglas filtran y analizan el tráfico que fluye entre la aplicación web y el servidor, con el objeto de prevenir ataques que se incorporan en los paquetes HTTP y/o TCP/IP.

Existen 3 tipos de firewall de aplicaciones: modo puente transparente, proxy inverso, modo embebido en el servidor e incrustado en código fuente [9].

(i) El modo puente transparente utiliza un equipo que interconecta 2 segmentos de red, permitiendo la protección de varios servidores de aplicaciones web.
(ii) El modo proxy inverso, realiza la conexión de 2 o más segmentos de red, contando un IP propia, analiza las peticiones HTTP y responde a las peticiones web que realizan los usuarios.
(iii) Modo embebido en el servidor: es un software que se configura dentro del servidor que expone el servicio de la página web.
(iv) Modo incrustado en el código fuente: a través de librerías propias del código de programación en el cual fue desarrollado la aplicación web, se incorpora la defensa a nivel de código.

D. Defensa perimetral en seguridad informática.

La seguridad perimetral exige una gran inversión económica dentro de la infraestructura de red de una entidad pública, pero estos aportan en la minimización del acceso de intrusos que buscan la explotación de las vulnerabilidades que puedan tener los activos de información. Una red corporativa, que posea varias VPN debido a la existencia de sedes en distintos lugares geográficos, requiere la implementación de las siguientes configuraciones o elementos de hardware:

1) Segmentación de red – VLAN.

Esta configuración funciona a través del protocolo Ethernet 802.1Q, el cual da los parámetros para configurar varias VLAN dentro de un mismo switch. La configuración de VLAN, crea varios segmentos de red lógicos, que aíslan los segmentos, evitando que cualquier tipo de usuario pueda trasladarse entre los segmentos. Esta configuración, en caso de acceso no autorizado a los equipos de red del segmento, demora el

compromiso de la red corporativa, permitiendo aislar los segmentos vulnerados.

2) Switch.

La entidad requiere la utilización de switch gestionables, tanto perimetrales como de prestaciones medias o altas, según los requerimientos de configuración de la red. Estos switch permiten la gestión y correcta configuración de los diferentes segmentos de red, incluyendo características de seguridad lógica o física.

3) Router OSPF (Open Shortest Path First/Abrir la ruta corta primero).

Estos router hacen uso del algoritmo Dijkstra que calculan la ruta idónea entre dos router. Estos equipos, según la ubicación que posean dentro de la red, reciben la siguiente clasificación:

(i) Router interno.
(ii) Router de respaldo.
(iii) Router de área perimetral (ABR).
(iv) Router limítrofe del sistema autónomo (ASBR).

Estos elementos de red, permiten una alta configuración y gestión de las capas TCP y control de la dirección IP, lo cual es redundante en el control de las tramas trasmitidas, tanto del interior hacia el exterior y viceversa.

4) Servidor proxy.

Estos servidores se utilizan buscando seguridad mediante el control de acceso, registro del tráfico, balanceo de carga, almacenamiento en cache de los datos de navegación con el objeto de reducir el consumo de ancho de banda, el filtrado de tramas, ocultamiento de direcciones IP privadas. La configuración de un servidor proxy con las características puntuales de las necesidades requeridas, crea una capa de seguridad extra dentro de la infraestructura de la entidad.

5) Firewall.

Estos elementos de hardware de amplio uso se presentan con los siguientes tipos:

a) Filtrado estático de paquetes.

Este tipo de cortafuegos realiza filtrado en las direcciones IP de origen o destino, números de puertos de origen o destino, y el tipo de tráfico o protocolo utilizado. Este tipo de filtrado presenta debilidades y no es recomendado su uso.

b) Filtrado dinámico de paquetes.

Este tipo de filtrado además de realizar filtrado estático, verifica el estado de la conexión y forma de establecimiento. Este tipo de cortafuegos se recomiendo su uso, en combinación de cortafuegos de aplicaciones.

c) Filtrado a nivel de aplicación.

Estos cortafuegos, además de comprobar los paquetes, tienen poseen propiedades de inspección y control de aplicaciones e inspección profunda de paquetes, lo que permite analizar los protocolos en la capa de aplicación y el contenido de los paquetes. Este tipo de cortafuegos es muy recomendado para la protección de servidores que sean identificados y valorados con alto nivel de criticidad e importancia.

6) Sistemas para la detección y prevención de intrusiones.

Son aplicaciones de software que monitorean redes o sistemas informáticos en busca de actividad maliciosa o violaciones de políticas de seguridad. Si es detectado algún evento clasificado con algún nivel de riesgo, este software, en tiempo real bloquea la conexión y/o aísla el elemento que genera el riesgo. Estos sistemas son configurados en combinación con sistemas (SIEM) que ayudan en la administración de los eventos y gestión de las amenazas de la seguridad de la información.

Los IDPS poseen características para el análisis y detección de eventos, que deben ser evaluadas según las necesidades de la entidad, pero deben tenerse en cuenta alguna de las siguientes especificaciones generales que se presentan a continuación:

a) Tipo de IDPS.

Existen cuatro tipos: a) IDPS que analiza la red LAN o MAN; b) IDPS que analiza las redes inalámbricas; c) IDPS que analiza el comportamiento de la red; d) IDPS que analiza los ejecutables del host.

b) Método de detección.

Existen tres modelos implementados en los IDPS que son utilizados para la detección de los eventos: a) Basado en firmas; b) Basado en anomalías (heurística); c) Basado en políticas; d) Basado en políticas; d) Basado en protocolos.

7) Honeypot – HoneyNet.

En informática, es un elemento de hardware o software que busca atraer la atención de los atacantes, buscando detectar, desviar o bloquear la actividad peligrosa dirigida a la infraestructura informática de la entidad.

Al igual que muchos elementos de seguridad informática, estos tarros de miel o señuelos se encuentran clasificados según el uso o servicios que este presten. Estas clasificaciones son:

a) Según el uso dado.

Estos usos pueden ser:

(i) Honeypost en producción: estos son los configurados por organizaciones con elementos de hardware real y puesto en producción con el resto de elementos de la red, y buscan detectar con anticipación cualquier tipo de ataque.
(ii) Honeypost de investigación: estas suelen ser maquinas simuladas, que buscan generar estadísticas de explotación, detectar patrones de ataque o detectar nuevo tipo de malware. Este tipo de elemento no es recomendado para la infraestructura de una entidad pública convencional, dado que requiere de personal especializado que gestione y analice los datos capturados.

Un honeypot de producción, puede a su vez estar configurado con alguno de los siguientes tipos:

(i) Honeypot puro: son los utilizados en sistemas que están en producción y se monitorea constantemente el equipo. Se recomienda para las entidades públicas.

(ii) Honeypot de alta interacción: son equipos virtualizados que poseen gran cantidad de servicios expuestos, buscando aumentar el tiempo de identificación de activos, por parte de un intruso.

(iii) Honeypot de baja interacción: estos se diferencian de los anteriores, es en la cantidad de servicios y/o máquinas virtuales dispuesta para esta tarea.

8) Pasarella antivirus y anti spam.

Estas configuraciones permiten la integración y administración de los servicios de detección de malware dentro de los host y servidores de la organización. Estas son herramientas utilizadas por un gran número de organizaciones y el no uso, aumentaría el nivel de riesgo.

VI. RECOMENDACIONES.

La aplicación de la seguridad informática en las entidades públicas del Estado Colombiano requiere gran habilidad gerencial para lograr que la alta dirección apoye efectivamente el proceso, dado que la gerencia de las entidades enfocan sus esfuerzos y presupuesto en actividades que produzcan réditos políticos y de opinión pública positiva.

Para que la aplicación de una metodología de seguridad de frutos, deberá compartir los beneficios de la metodología dentro del grupo de funcionarios de planta que apoyan las actividades de subdirectores o su equivalente, en cada una de las dependencias, los cuales, una vez integrados al proceso servirán de ayuda para el posicionamiento dentro de los directivos. Esta actividad requiere gran habilidad, pues identificar a estos funcionarios dentro de las entidades requiere de tiempo y del apoyo de personas que conozcan el talento humano.

VII. REFERENCIAS

[1] ESET, «Eset Security Report Latinoamérica 2016,» Buenos Aires, 2016.

[2] Cisco Systems, Inc., «Informe semestral de ciberseguridad 2106 de Cisco,» San Jose California, 2016.

[3] Council of Europe, «Oficina de tratados del Consejo de Europa,» 2016. [En línea]. Available: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. [Último acceso: 30 10 2016].

[4] Consejo Nacional de Política Económica y Social, «CONPES 3701,» Bogotá, 2011.

[5] OBSERVATORIO DE LA CIBERSEGURIDAD EN AMÉRICA LATINA Y EL CARIBE, «Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Informe Ciberseguridad 2016,» ORGANIZACION DE LOS ESTADOS AMERICANOS, 2016.

[6] Ministerio de Tecnologías de la Información y las Comunicaciones, «Modelo de Seguridad y Privacidad de la Información,» Ministerio de Tecnologías de la Información y las Comunicaciones, Bogota, 2016.

[7] Carnegie Mellon University, «CMMI para Desarrollo, Versión 1.3,» Editorial Universitaria Ramón Areces, 2010.

[8] OWASP, «Testing guide 4.0 release,» 2016.

[9] D. O. Ramírez López y S. S. Diaz Mendez, «REVISTA .SEGURIDAD, DEFENSA DIGITAL,» Universidad Nacional Autónoma de México, 02 05 2013. [En línea]. Available: http://revista.seguridad.unam.mx/numero-17/firewall-de-aplicaci%C3%B3n-web-parte-ii. [Último acceso: 07 11 2016].

VII. TABLAS