Universidad Cenfotec

Maestría en Ciberseguridad

Documento Final Proyecto de Investigación Aplicada II

Diseño de una estrategia para la implementación de un programa de Seguridad Informática en Ministerio de Seguridad Pública

Barquero Mena Oscar Andrés

Setiembre 2017

Tabla de contenido

Índice de Figuras

1. Introducción

1.1 Antecedentes

El Ministerio de Seguridad Pública, desde el 4 de febrero del 2000, cuenta con un Reglamento de Normas y Políticas de Informática definido por el Presidente de la República mediante decreto ejecutivo 28921, cuyo propósito es garantizar la eficiencia y la buena administración de los equipos de cómputo.

Para esto se define una estructura organizativa y división departamental de la siguiente manera:

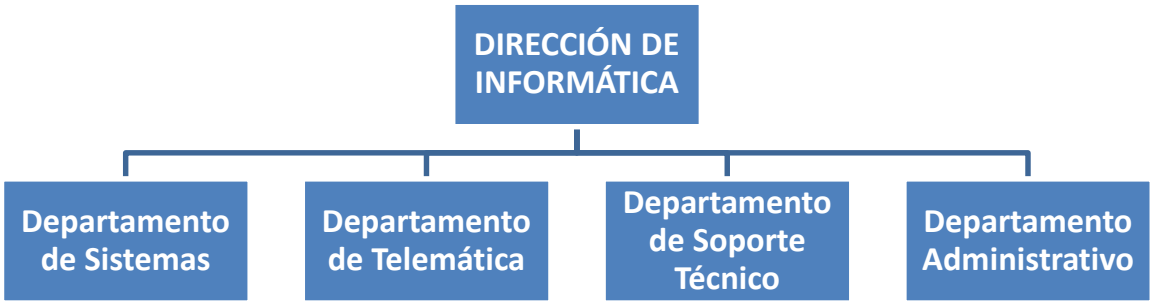

Figura 1. Estructura actual de la Dirección de Informática
Fuente: Dirección de Tecnologías de la Información del MSP

El caso en estudio se realiza propiamente sobre la Dirección de Informática del Ministerio de Seguridad Pública, el cual es responsable de los siguientes apartados:

a) Del buen funcionamiento de la red de información computarizada del Ministerio.
b) De la instalación de los diferentes equipos que conforman el sistema, tanto lo correspondiente a la fuente de energía como el software que necesitan para la operación en conjunto.
c) Fijar las políticas de trasiego de información.
d) Realizar gestiones con otras instituciones para compartir recursos.
e) Fijar los estándares de protocolos de comunicación.
f) Establecer y mantener la conexión con Internet.

1.2 Justificación

En esta sección se presenta el valor e impacto que tendrá este trabajo para mejorar el proceso en la gestión de Seguridad en las Tecnologías de la Información en el Ministerio de Seguridad Pública (MSP[1]). A lo largo de los años se ha logrado entender que muchas de las tareas diarias que se realizan tanto de manera personal como laboral conllevan la utilización de un dispositivo tecnológico, sin embargo, el solo utilizarlo puede generar riesgos de una u otra manera, por lo tanto, este proyecto pretende desarrollar una estrategia organizacional que pueda lograr, a nivel de Ciberseguridad, un apoyo al recurso humano actual que gestiona la plataforma tecnológica del Ministerio de Seguridad Pública.

1.3 Planteamiento del problema

En la actualidad, el Ministerio se encuentra en un momento decisivo respecto al uso de la tecnología para extender y fortalecer la red institucional. El modo en que se producen las interacciones gubernamentales en el ámbito policial cambia en forma continua para estar al día con la evolución de la tecnología respecto al gobierno digital.

En la etapa de su desarrollo tecnológico como institución, la confidencialidad, integridad y disponibilidad de los datos tiene un papel importante, esto por cuanto se brindan servicios

[1] MSP siglas de Ministerio de Seguridad Pública

diseñados específicamente para la gestión policial, lo cual implica un Ministerio con información crítica y sensible para el Gobierno de Costa Rica.

La mayoría de servicios que se han desarrollado brindan, a través de la red, facilidad y rapidez en la ejecución de tareas, por lo que se han implementado plataformas robustas y redes interconectadas, para satisfacer la gran cantidad de datos que demandan las Delegaciones Policiales y que tienen que ser protegidos.

Internet ha dado un giro importante a través de los años y ha pasado a ser una red de comunicación educativa a una red mundial conectada, donde los dispositivos que manipulan los seres humanos se encuentran conectados a ella, provocando la creación de estrategias a nivel nacional, la definición de nuevos roles y funciones, los cuales deben ser desarrollados tanto a nivel gubernamental como a nivel privado, el desarrollo debe ser paralelo a nivel académico y las escuelas, colegios y universidades tienen una gran responsabilidad, la creación de programas de Seguridad, crear mecanismos que permitan al ciudadano tener un apoyo directo de conocimiento para la toma de decisiones y recibir apoyo del Gobierno creando centros de atención al ciudadano tales como el CSIRT[2],

[2] CSIRT por sus siglas en inglés Computer Security Incident Response corresponde a un grupo de profesionales que dan respuesta a incidentes de seguridad dentro de una organización.

centros de investigación, estudiar la realidad nacional para identificar la cultura del país a nivel de CiberSeguridad y darle un mayor conocimiento a la población.

Hoy los cyber ataques liberan una variedad de herramientas y suites sofisticadas para el acceso de los datos en Internet, por esto, es de suma importancia desarrollar mecanismos de defensa proactiva que involucren una gestión enfocada a la ciberseguridad de manera dinámica.

Mientras tanto, el objeto de esta investigación hace énfasis en implementar un modelo que permita contribuir con la actualización del riesgo institucional a través de la recopilación de datos que brinden información para proponer una postura de seguridad deseable, es un hecho que debemos combatir los defectos de seguridad inherentes en la arquitectura de red actual.

1.4 Alcances

A raíz de esta investigación se realiza un análisis detallado para la implementación del modelo de seguridad en la plataforma tecnológica del Ministerio de Seguridad Pública. A lo largo de este estudio se realizan comprobaciones para asegurar que la implementación se está realizando adecuadamente. Entre los alcances se tienen:

1. Descripción detallada del estado de seguridad actual, a través de cuestionarios específicos que brinden la información requerida. Estos cuestionarios se realizan a los líderes en gestión actual de la plataforma tecnológica del MSP.
2. Se utilizan marcos de referencia como ISO 27001, COBIT 5 para Riesgos, NIST, SANS.org, etc.
3. Se presenta un proceso para implementar políticas y controles basados en análisis de riesgos asociados a la gestión de Seguridad actual.
4. Se presenta un modelo para la gestión del riesgo a nivel de CiberSeguridad.
5. Propuesta del programa de seguridad justificado para el Ministerio de Seguridad Pública.

1.5 Limitaciones

1. La disposición de recurso humano capacitado para el desarrollo del programa de Ciberseguridad.
2. La capacitación y conocimiento de personal actual en temas de Ciberseguridad.
3. Recursos presupuestales a nivel Gubernamental para adquisición de plataformas específicas de Seguridad.
4. Políticas de Seguridad Implementadas.
5. Procesos de Seguridad documentados.

6. Lineamientos de Seguridad implementados
7. Plataformas de Seguridad obsoletas.
8. Metodologías de Ciberseguridad sin aplicar.

1.6 Objetivos

1.6.1 Objetivo General

Desarrollar un diseño para la implementación de un programa de Seguridad en la plataforma tecnológica del Ministerio de Seguridad Pública.

1.6.2 Objetivos Específicos

- Identificar la postura de seguridad tecnológica actual del Ministerio de Seguridad Pública.
- Reconocer los Riesgos asociados al conjunto de plataformas que componen la red actual y de los servicios críticos que se brindan en el Ministerio.
- Analizar las plataformas de seguridad y la cobertura sobre datos críticos o sensibles del Ministerio.

- Analizar las posibles mejoras para brindar un informe detallado con los cambios requeridos para el desarrollo de un modelo de Ciberseguridad.
- Brindar un modelo de Ciberseguridad como postura para su implementación a mediano plazo o largo plazo.
- Recomendar posibles perfiles de Recurso Humano para desarrollar el programa.

2. Estado de la Cuestión

El proceso utilizado para desarrollar el estado de la cuestión se basa principalmente en los procedimientos propuestos por Barbara Kitchenham para elaborar revisiones sistemáticas, en su publicación "Procedures for Performing Systematic Reviews." Ella menciona que una evaluación sistemática es un medio por el cual "se evalúan e interpretan todas las investigaciones disponibles sobre un tema, pregunta o fenómeno de interés." (Kitchenham, 2004, p. 7). De esta forma se llega a tener un mejor entendimiento acerca de la información actual sobre un tema y a la misma vez, se pueden llegar a identificar áreas que no se han desarrollado aún, como, por ejemplo, la gestión de la Ciberseguridad en instituciones del Gobierno de Costa Rica.

2.1 Planeamiento

En la actualidad, el diseño de una arquitectura de seguridad en cualquier organización conlleva insumos de conocimiento dinámico y gran labor para lograr identificar y clasificar los activos críticos, si se habla de riesgos de seguridad en activos que gestionan la información, es sin duda un reto poder iniciar con un proceso de documentación que permita desarrollar con claridad una visión para poder administrar el riesgo a nivel de seguridad digital.

La pregunta es, ¿sobre quién recae la responsabilidad para desarrollar un programa de seguridad para proteger los activos digitales de la institución? A lo largo de esta cátedra se ha tratado de entender el perfil que podría encajar en esta gestión, sin embargo, cuanto más se profundizase considera que se debería empezar por reconocer conceptos básicos. Según (ISACA)Ciberseguridad reúne términos como Seguridad de Computadoras, Seguridad de Red, y Seguridad de la Información, entre otros, por tanto se puede decir que Ciberseguridad es un término utilizado para describir la protección de los activos digitales de la información en determinada organización, de una manera dinámica.

Para poder desarrollar e implementar el diseño de una estrategia para un programa de Seguridad Informática es necesario realizar un análisis de lecturas, normas, estándares y *White papers* relacionados con el tema.

2.2 Protocolo de Revisión

Se llevan a cabo los procesos de recopilación de información

2.2.1 Preguntas de Investigación

Por medio de la investigación a través de cuestionarios realizados se busca la información atinente al desarrollo de esta propuesta, considerando las siguientes 5 aristas:

- **Información de los Sistemas**

¿Cuál es la distribución de sistemas operativos en la institución?

¿Existe un software Antivirus para servidores?

¿Existe la integración de auditorías de seguridad con alguna plataforma SIEM[3]?

- **Control de accesos**

¿Existe una solución para la gestión de identidades?

¿Está deshabilitado y/o restringido el acceso para utilizar usuarios locales de administrador por defecto?

¿Se realizan controles periódicos para garantizar que el acceso de usuarios coincide con sus responsabilidades?

- **Información de la Seguridad de la Red**

¿Existen muros de fuego en la institución, tiene conocimientos si son NGFW[4]?

¿Disponen de un Sistema de Detección de Intrusiones? (IDS[5])

[3] Security Information Security Management- Centraliza el almacenamiento y la interpretación de registros y permite un análisis casi en tiempo real para tomar medidas de seguridad defensivas más rápidamente.

[4] Next Generation Firewall por sus siglas en inglés es sistema de seguridad para redes dentro de un dispositivo de Hardware basado en software que es capaz de detectar y prevenir ataques sofisticados.

¿Existen controles para asegurar el acceso a la red? (NAC[6])

- **Análisis de Amenazas**

¿Existe alguna solución para el análisis del tráfico web?

¿Se realiza inspección y validación de tráfico SSL?

¿Hay alguna solución para la protección ante Amenazas Persistentes Avanzadas?

- **Información de Servicios**

¿Qué servicios se publican en Internet?

¿Se cuenta con alguna solución contra las debilidades y vulnerabilidades de las aplicaciones web? (WAF)[7] (Ej. CSS[8], SQL INJ[9]).

[5] Intrusion Detection System por sus siglas en inglés es un sensor virtual, ya sea por software o hardware que permite la detección de accesos no autorizados en un computador o una red.

[6] Network Access Control por sus siglas en inglés, es una plataforma que se utiliza para reforzar y asegurar la red a nivel políticas sobre usuarios, dispositivos, aplicaciones, etc.

[7] Web Application Firewall por sus siglas en inglés se trata de un firewall específico para proteger aplicaciones WEB

¿Qué tipo de autenticación se utiliza en los servicios web?

2.2.2 Criterios de Inclusión

- Identificar por medio de cuestionarios específicos la situación actual y la madurez en el campo de Ciberseguridad en el Ministerio de Seguridad Pública.
- Comparar contra estándares el nivel de riesgo asociado con nuevas tendencias de ataques cibernéticos que pueden vulnerar las plataformas que actualmente protegen la plataforma tecnológica.
- Analizar las plataformas de seguridad actual y presentar propuestas de cambio,
- Entre las posibles ventajas de la implementación del diseño de seguridad se encuentran las nuevas tendencias de protección, marcos de referencias tropicalizados al Ministerio mediante fusión de normativas, marcos de trabajo, estándares de última generación.

[8] Cross Site Scripting por sus siglas en inglés es un ataque dirigido a páginas web que muestran información de manera dinámica el contenido de los usuarios y no se toman controles de seguridad para verificar y codificar la información ingresada por ellos.

[9] SQL (motor de base de datos) Injection por sus siglas en inglés, se trata de un ataque con un método para infiltración de código malicioso sobre la base de datos aprovechando brechas vulnerabilidades de seguridad.

- Entre las posibles desventajas de la implementación del modelo se pueden encontrar la falta de recursos presupuestarios, falta de recurso profesional y especializado en ciberseguridad.

2.2.3 Criterios de Exclusión

Lecturas que contienen las siguientes características fueron excluidas de los resultados de la búsqueda. Esto se debe a que son fuentes no confiables que pueden ocasionar confusión a la hora de analizar datos de la investigación.

2.3 Revisión

2.3.1 Fuentes buscadas

Las fuentes se detallan en el Anexo 1.

2.3.2 Estudios seleccionados

El proceso de investigación involucra procesos de identificación que presenten temas de interés y los cuales puedan ser utilizados para la preparación de este trabajo, a continuación, las lecturas primarias para el desarrollo del estado de la cuestión

Documentos Primarios

Título: ISO 27001 2005

Autor: Organización Internacional para la Estandarización e IEC (la Comisión Electrotécnica Internacional).

Tipo: Norma

Descripción: Proporciona un modelo a establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información.

Título: Transforming Cybersecurity - NEXUS

Autor: ISACA.org

Tipo: Libro

Descripción: Aplica COBIT 5 orientado a la Ciberseguridad, habilita un marco de gobierno para riesgos y administración sobre organizaciones. Provee una guía detallada de conceptos y pasos en la transformación de la Ciberseguridad.

Título: Framework for Improving Critical Infraestructure CyberSecurity

Autor: National Institute of Standars and Technology.

Tipo: WhitePaper

Descripción: Muestra procesos detallados para la implementación de un marco de trabajo enfocado a la seguridad, describe postura de CiberSeguridad actual, brinda una guía de cómo identificar y priorizar activos, plataformas y tecnologías críticas de una organización.

Título: B.A.S.E - A Security Assessment Methology

Autor: Gregory Brauton

Tipo:WhitePaper

Descripción: Propone elementos para la implementación de un estándar de líneas base organizacional, basado en Baseline, Audit and Assess, Secure, Evaluate and Educate, es un desarrollo para una metodología de evaluación de seguridad continua.

Título: Cobit 5 Procesos Habilitadores

Autor: ISACA

Tipo: Libro

Descripción: Define cómo implementar un proceso de Seguridad Informática basado en entrega, servicio y soporte

Título: Security and Privacy Controls for Federal Information Systems and Organizations

Autor: National Institute of Standars and Technology

Tipo: WhitePaper

Descripción: Define controles de Seguridad que deben ser implementados en una organización.

2.3.3 Documentación de Resultado

Un proceso de madurez para la integración de todas las plataformas y documentación de Seguridad conlleva a la disposición de recursos tanto tecnológicos como humanos, los avances en la tecnología para mantener información y comunicaciones crean un reto a nivel laboral que motivan un crecimiento masivo en el trasiego de información, por lo que genera un riesgo de seguridad sino se llevan a cabo procesos documentados que permitan un control y cumplimiento para proteger los activos digitales, el proceso de evolución une términos a nivel de Seguridad, tales como *Computer Security*, *Network Security*, *CyberSecurity*, etc

Según (ISACA).en *CyberSecurity fundamentals*, los términos anteriores describen con facilidad la protección de activos de la información, salvaguardando que la información de determinada organización es *per se* una prioridad mantenerla segura, disponible y privada.

Basado en lo anterior, se deben tener claros los tres componentes que rodean el objetivo de la seguridad de la información, son conceptos que deben ser prioritarios y tienen que ser los pilares para que cualquier profesional especializado domine antes de comenzar con el desarrollo de un plan, diseño o programa exclusivo de Ciberseguridad.

Resaltando que este proyecto tiene como prioridad mantener la información segura, privada y disponible, la triada de la Ciberseguridad es la siguiente:

Figura 2. Triada de la Seguridad
Fuente: Elaboración propia basada en las observaciones de la investigación.

Estos componentes pueden ser catalogados como críticos cuando se gestiona Seguridad,

Confidencialidad hace mención a la protección de accesos no autorizados, mientras que la

Integridad hace mención a la protección de modificaciones no autorizadas y la

Disponibilidad hace mención a la protección contra interrupciones durante un acceso.

Confidencialidad, Integridad y Disponibilidad Modelo e Impacto Relacional		
Requerimiento	**Impacto y Consecuencias Potenciales**	**Métodos de Control**
Confidencialidad: Protección de la información contra divulgación no autorizada.	La pérdida de Confidencialidad puede tener las siguientes repercusiones: • Divulgación de información privada. • Perdida de confidencia pública • Perdida de ventaja competitiva • Acciones legales contra la organización • Interferencias con seguridad nacional.	La Confidencialidad puede ser preservada usando los siguientes métodos de control: • Control de acceso • Permisos sobre archivos • Encripción
Integridad Exactitud e integridad de la información de acuerdo con los valores y expectativas organizacionales	La pérdida de integridad puede tener las siguientes repercusiones: • Fraude • Inexactitud • Decisiones Erróneas	La Integridad puede ser preservada usando los siguientes métodos de control: • Control de acceso • Logging • Firma digital • Hashes • Encripción
Disponibilidad Capacidad de tener acceso a la información y otros recursos de información a través de procesos de la organización	La pérdida de integridad puede tener las siguientes repercusiones: • Pérdida de operaciones efectivas y funcionales • Perdida de tiempos de producción • Interferencia con los objetivos de negocio	La Disponibilidad puede ser preservada usando los siguientes métodos de control: • Redundancia • Respaldos • Controles de acceso

Figura 3. ISACA, CRISC Review Manual, USA, 2014
Fuente: Adaptado de CyberSecurity –Fundamentals ISACA

Durante este proceso se debe involucrar una variedad de métodos para diseñar de manera específica una arquitectura de seguridad. Estos métodos que se ampliarán definen un ambiente de seguridad estándar.

COMPONENTE	MÉTODOS DE SEGURIDAD
PERSONAS	• Limitaciones físicas de acceso al hardware y documentación. • A través de procesos de identificación y autenticación. • Asegúrese de que el colaborador es quien dice ser a través del uso de dispositivos, tales como tarjetas de identificación, contraseñas, huellas dactilares, etc. • Capacitaciones sobre la importancia de la seguridad y cómo proteger los activos de la organización. • Establecer políticas de seguridad y procedimientos.
APLICACIONES	• Autenticación de usuarios cuando utilizan determinada aplicación. • Monitoreo • Autenticación tipo Single Sign-on (Un método para firmar una sola vez para diferentes aplicaciones web)
RED	• Configuración acertada de firewalls. • Autenticación. • Monitoreo. • Segmentación de redes. • Conectividad por VPN desde redes externas. • Diagramas de red.

SISTEMAS OPERATIVOS	• Autenticación. • Detección de intrusos (HIDS). • Políticas de contraseñas. • Cuentas de usuarios.
ADMINISTRACIÓN DE BASES DE ARCHIVOS	• Autenticación. • Auditorías habilitadas. • Recursos de DB limitadas. • Políticas de contraseñas.
ARCHIVOS	• Permisos sobre carpetas. • Monitoreo de accesos.
DATA	• Validación de datos. • Restricciones. • Encripción de datos. • Acceso a los datos.

Figura4. Métodos de Seguridad utilizados para proteger un ambiente de datos
Fuente: Adaptado de Database Security and Auditing, Hassan A. Afyouni, 2006

Dado lo anterior, para poder implementar esta estrategia se debe tener un entendimiento completo de las plataformas, tecnologías y los sistemas de información que el Ministerio hasta el día de hoy ha logrado implementar. Este Plan de Investigación busca un diseño robusto para crear una arquitectura de Seguridad para cualquier proyecto de Tecnologías de la Información.

Existen enfoques para la gestión de la seguridad que podrían calar en esta investigación.

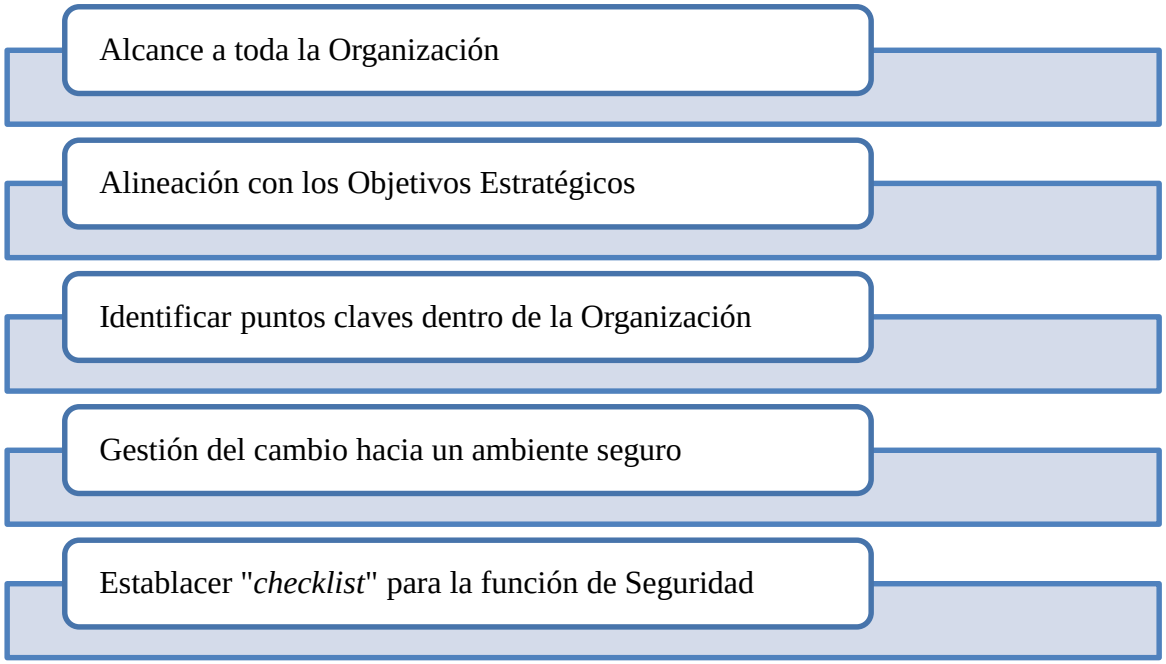

Figura5. Enfoques para la gestión de la seguridad
Fuente: Elaboración propia basada en las observaciones de la investigación

Uno de los conceptos más interesantes que también se toma en cuenta para este plan de estudio recae sobre el **ciclo de Deming** el cual mejora los procesos y se convierte en un imperativo importante para la supervivencia de las organizaciones entornos competitivos y cambios constantes que se vuelven cada vez más frecuentes.

El ciclo PDCA (o ciclo de Deming) es una de las sistemáticas más utilizadas para implantar un sistema de mejora continua cuyo objetivo principal es la autoevaluación, destacando los

puntos fuertes que hay que tratar de mantener y las áreas de mejora en las que se deberá actuar.

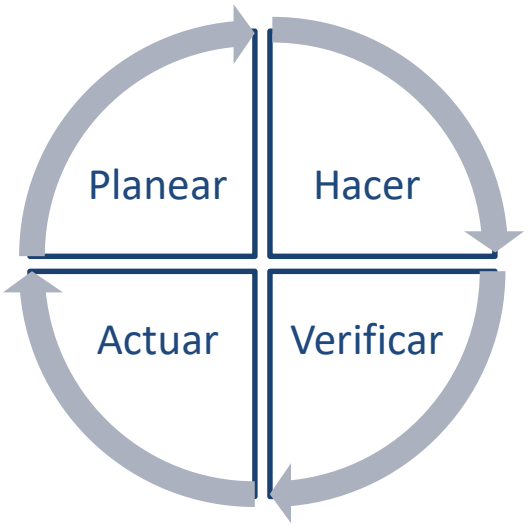

Figura 6. Ciclo de Deming
Fuente: Elaboración propia basada en las observaciones de la investigación

Según la *National Institute of standars and technology* (NIST) para proteger los activos digitales de determinada organización se deben aplicar metodologías que conlleven a las siguientes actividades:

Figura 7. Metodología para un marco de seguridad según NIST
Fuente: Adaptado de Framework Infraestructure CyberSecurity, National Institute of Standard and Technology, 2014

3. Marco Teórico

El Marco Teórico es una recopilación sistemática de la información pública relacionada con el tema que ocupa a esta investigación. En la actualidad, la humanidad está sometida a una avalancha de información en cuanto a ciberseguridad respecta.

El diseño de una estructura de seguridad es un trabajo de ingeniería complejo, que consta de varias etapas interdependientes. En particular, no se puede aislar el problema de diseñar la red física y su topología, del problema de distribuir servicios de red y analizar el tráfico potencial de los diferentes componentes orientados a la seguridad.

Según (Rolf M. von Roessing, 2014) una arquitectura de seguridad provee soporte fundamental para cualquier actividad y administración de Ciberseguridad, los gestores de seguridad deben incluir cualquier especificación y requerimiento necesario para defender contra ataques y brechas de seguridad.

Es importante destacar que formular una arquitectura específica para cierta plataforma tecnológica debe llevar consigo un estudio integral de todos los componentes dentro de la plataforma, así como diseñar políticas y lineamientos que permitan tener mapeados los procesos de Seguridad, según (CyberSecurity Fundamentals, pág. 8) la estructura y gobierno de cada organización es diferente y varía dependiendo el tipo de organización y cada una debe tener su propia misión (razón de ser), tamaño, industria, cultura y

regulaciones legales. Es decir, toda organización tiene la responsabilidad y obligación de proteger los activos y sus operaciones.

Este documento busca diseñar una arquitectura de Seguridad a través de un estudio de la situación actual y como poder obtener una postura de Seguridad deseable.

3.2 Inicios de CiberSeguridad

La CiberSeguridad empieza a aparecer en los años 80´s cuando se realizaron pruebas para replicar y propagar código, construyendo el primer virus en una computadora, seguidamente los códigos empezaron a mutar y nacieron otras variantes de virus conocidos como *wormns* gusanos, *troyans horses* o caballos de troya, *root kits*, y muchos más, consecuente a la ola de virus en aquel momento, nacen soluciones administrables para detectar y proteger contra virus, estas plataformas se conocen como antivirus y su principal objetivo era eliminar infecciones por vulnerabilidades y amenazas conocidas, sin embargo, aunado a lo anterior, nace el término "inocencia informática "que aparte del desarrollo de *malware*[10]existía un número limitado de intentos criminales y otros objetivos, de ahí nace el término "Hacking" el cual es un concepto que combina habilidades orientadas a esa

[10] Malware por sus siglas en inglés Se trata de un software diseñado y que tiene como objetivo infiltrarse en un sistema operativo o una red con el fin de realizar daños específicos.

actividad de una manera diferente para buscar la forma de vulnerar cada vez más los sistemas de protección.

Ya para inicios del año 2000 aparece una nueva forma de aumentar la economía, nace *e-commerce* evoluciona rápidamente, sin embargo, para ese momento las encuestas y reportes mencionan que existe una limitada atención en la inversión a la seguridad, esto obedece al bajo presupuesto otorgado durante años a bajos niveles para el desarrollo de seguridad de la información, por lo tanto, este período fue denominado los años de "complacencia" dado el numeroso incremento del riesgo a través de nuevas amenazas y vulnerabilidades hacia las plataformas. El incremento en popularidad de banca electrónica activa una gran cantidad de ataques a entidades financieras que han provocado pérdidas significativas a lo largo de los años.

Del año 2005 al 2010 la seguridad de la información incrementa a nivel de concienciación y gastos, ahora los ataques forman parte de crimen organizado, esta época es llamada "computer crime" "cybercrimen" en este contexto el gasto en presupuesto en infraestructura de TI conlleva a una de las industrias de mayor atención de alta gerencia.

A partir del año 2010, el número de amenazas, así como los escenarios de riesgo ha crecido exponencialmente, la ciberseguridad ha evolucionado a nuevos campos de interés, obteniendo atención de los Gobiernos directamente por lo que se deben de crear mecanismos de defensa, y en otros casos tanto en ofensa como en defensa por tema de

ciberguerra o *cyberwar*.Para el día de hoy la Ciberseguridad ya es parte de los proyectos necesarios de un país, para poder cumplir como desarrollo de la sociedad.

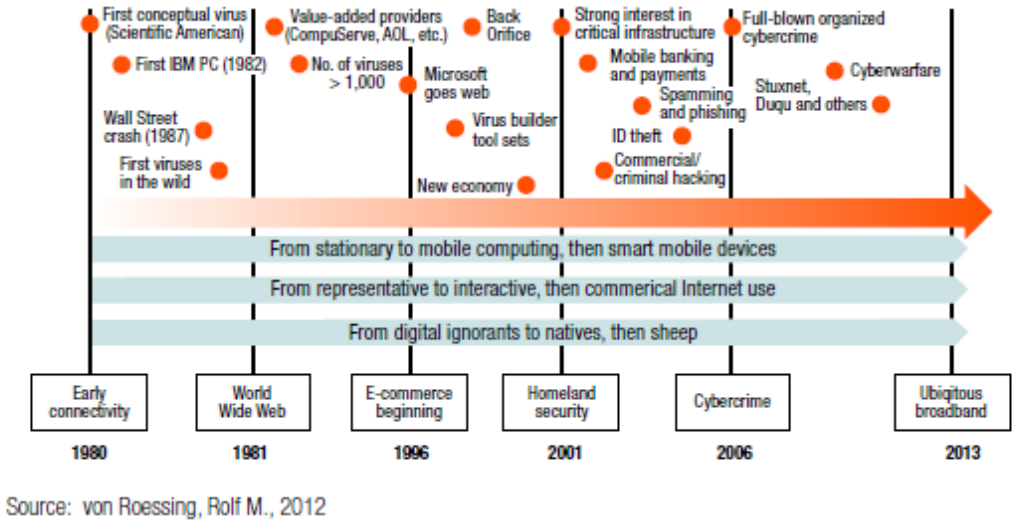

Figura 8. Línea de Tiempo de la CiberSeguridad
Fuente: Adaptado de Transforming CyberSecurity, ISACA.org, von Roessing, Rolf M., 2012

3.3. Visión General de la Gestión del Programa de Seguridad de la Información (CISM[11])

Un programa de seguridad de la información comprende todas las actividades y recursos que proporcionan colectivamente servicios de seguridad de la información a una organización.

Las actividades primarias de los programas suponen el diseño, desarrollo e integración de los controles en toda empresa relacionados con la seguridad de la información, así como la administración continua y la gestión de estos controles.

Según (ISACA-CISM, 2015) existen tres elementos esenciales para asegurar el éxito del diseño, implementación y gestión continua del programa:

1. Un programa debe ser la ejecución de una estrategia de seguridad de la información bien desarrollada y estrechamente alineada a los objetivos organizacionales a respaldar.
2. El programa debe ser bien diseñado con la cooperación y el respaldo de la gerencia y de las partes interesadas.

[11] Certified Information Security Manager por sus siglas en inglés se trata de una certificación emitida por ISACA para profesionales que deseen especializarse en Seguridad Informática y su gestión dentro de una organización.

3. Se deben de desarrollar métricas eficaces para las fases de implementación y diseño del programa, así como para las fases subsiguientes continuas de la gestión del programa de seguridad con el fin de proporcionar la retroalimentación necesaria para guiar la ejecución del programa hacia el logro de resultados definidos.

De acuerdo con la mayoría de los marcos tradicionales para la seguridad de la información, el desarrollo de un programa de seguridad de la información comienza con la valoración de riesgos y conduce a la definición de una estrategia para gestionar los riesgos.

La realidad es que muchas organizaciones aún no están listas para hacer frente a los costos y los esfuerzos que se requieren para implementar el gobierno de la seguridad de la información.

En estos casos, se puede lograr, mediante la utilización de un marco de referencia estándar tal como COBIT o ISO /IEC27001, en conjunto con una escala del modelo de madurez de capacidad (CMM) (*Capability –Maturity Model*), establecer el enfoque que permitirá determinar qué proceso seguir para la implementación de un programa y definir objetivos específicos mediante la estrategia para alcanzarlos.

3.4 Importancia del programa de Seguridad de la Información

ISACA indica que lograr los niveles adecuados de seguridad de la información a un costo razonable requiere una buena planificación, una estrategia efectiva y administración capaz. La gestión de un programa de seguridad de la información es un requerimiento constante que sirve para proteger los activos de información, cumplir con las obligaciones regulatorias y minimizar posibles exposiciones legales y de responsabilidad civil. Si se diseña, implementa y gestiona adecuadamente, proporciona un soporte crucial a muchas áreas de negocio que simplemente no serían factibles si no se cuenta con dicha gestión.

Un programa de seguridad bien ejecutado ayudará a diseñar, implementar, gestionar y monitorear de forma efectiva los programas de seguridad que conviertan la estrategia en realidad. También aumenta la probabilidad de integrar adecuadamente los esfuerzos, lo que disminuye el costo de mantenimiento y administración y proporciona un nivel de seguridad uniforme en toda la empresa.

Cabe aclarar que un programa de seguridad requiere de mucha planificación, así como conocimientos especializados y recursos. Una planificación eficaz puede beneficiarse en gran medida del desarrollo de una arquitectura de seguridad empresarial a los niveles conceptual, lógico, funcional y físico.

3.5Resultados de la Gestión de un Programa de Seguridad de la Información

Por otra parte, ISACA establece que un programa eficaz de gestión de seguridad de la información debe alcanzar los objetivos que se hayan definido en la estrategia de seguridad. Tal como sucede con otras actividades de gestión las metas deben definirse en términos específicos, objetivos, y cuantificables. Así deben establecer métricas apropiadas para determinar si las metas se han alcanzado y, en caso contrario, cuanto faltó para alcanzarlas y cómo se podría mejorar el desempeño.

Ya sea que se haya implementado o no el gobierno formal de la seguridad de la información, los seis resultados que se presentan a continuación deben considerarse los objetivos de un programa eficaz de la seguridad de la información:

- Alineación Estratégica
- Gestión de Riesgos
- Entrega de Valor
- Gestión de Recursos
- Medición del desempeño
- Integración del proceso de aseguramiento

El desarrollo de una estrategia y la definición de los atributos del programa de seguridad de la información son ante todo ejercicios conceptuales y lógicos. Para desarrollar el programa es necesario transformar los conceptos y las relaciones lógicas en tecnologías y procesos. Desde el punto de vista de la arquitectura, para llevar a cabo dicha información se deben de desarrollar los componentes tanto físicos como funcionales y operativos que sean necesarios para alcanzar los objetivos que se hayan definido.

Alineación estratégica

Continuando con ISACA, para que la seguridad de la información sea efectiva de manera continua con los objetivos de la misión o del negocio es preciso establecer una interacción frecuente con los altos jerarcas o bien los dueños de negocio y entender sus planes y objetivos. Esto a menudo depende de recopilar las contribuciones de las principales unidades operativas y generar consenso entre ellas dentro de la organización. Este consenso incluye temas tales como la comprensión de:

- Riesgos de información de la organización.
- Selección de estándares y objetivos de control apropiados.

- Delegar a un acuerdo respecto del riesgo aceptable y la tolerancia al riesgo.
- Definiciones de limitaciones financieras, operacionales y de otra índole.

Ello se puede lograr a través de un comité directivo de seguridad, si los altos jerarcas o sus delegados sin miembros y participantes activos de dicho comité.

Gestión de Riesgos

ISACA indica que el análisis de riesgo debe basarse en los requerimientos de negocio y en comprensión de los procesos, cultura y la tecnología de la organización. Una gestión efectiva del riesgo supone una comprensión total por parte del gerente seguridad de las amenazas que enfrenta la organización, sus vulnerabilidades, su perfil de riesgos y el nivel de riesgo que la gerencia determina que es aceptable.

El impacto potencial de las amenazas que se pueden materializar debe evaluarse y utilizarse para establecer prioridades sobre el tratamiento. Los riesgos deben gestionarse para llevarlos a un nivel que considere aceptable para la organización. Sin embargo, el panorama de riesgo siempre está cambiando e inevitablemente surgirán otros nuevos durante el desarrollo y la administración del programa.

Es importante que se mantenga un proceso continuo de gestión de riesgos durante el desarrollo, la implementación y la evolución del programa.

Entrega de Valor

ISACA menciona que la entrega de valor como objetivo requiere que la seguridad de la información entregue el nivel requerido de seguridad de manera eficaz y coherente.

Las inversiones que se hagan en materia de seguridad deben de gestionar para optimizar el apoyo a los objetivos de negocio y entregar valor claro a la organización. El Gerente de Seguridad de la Información debe concentrar esfuerzos en logar la creación de un conjunto estándar de prácticas de seguridad aunados al riesgo.

Una entrega de valor requiere que se institucionalicen las soluciones de seguridad como prácticas normales y esperadas basadas en estándares. Las soluciones deben tratar los temas lógicos, técnicos, operativos y físicos de forma exhaustiva con base en un entendimiento de los procesos operativos integrales de la organización.

Gestión de Recursos

Continuando con ISACA, menciona que se utilizarán diversos recursos para desarrollar y gestionar un programa de seguridad. Estos recursos incluyen personas, tecnología y procesos. El Gerente de seguridad de la información debe esforzarse por aplicar los recursos humanos, financieros, técnicos y de conocimientos con eficacia y efectividad.

Los recursos humanos se utilizan eficientemente al asegurar que se dispone de destrezas y conocimientos adecuados, una gestión apropiada y un seguimiento del desempeño. Los procesos y prácticas de seguridad deben de estar documentados y ser congruentes con los estándares y políticas. La planificación de proyectos, la selección de tecnología y la adquisición o desarrollo de habilidades incidirán significativamente en la efectividad de la gestión de recursos.

Se deben de desarrollar arquitecturas de seguridad para definir y utilizar las infraestructuras que permitan alcanzar los objetivos de seguridad de manera eficiente.

Medición del desempeño

Por tanto, ISACA establece que, si se ha desarrollado una estrategia de seguridad de la información, debería haberse identificado un conjunto de requerimientos importantes de monitoreo y métricas. Es probable que durante la evolución y la gestión de un programa de seguridad se vuelvan evidentes oportunidades adicionales para desarrollar métricas o puntos de monitoreo útil.

El desarrollo e implementación del programa de seguridad requerirá por sí mismo, de medios para medir el progreso y monitorear las actividades. Un programa eficaz de seguridad de la información resulta en procesos diseñados para alcanzar los objetivos de

gobierno, así como también en elementos mensurables que demuestran si los objetivos han sido cumplidos. Los procesos de seguridad deberían ser diseñados con puntos de control medibles que permitan a los auditores independientes certificar que el programa está en marcha y es eficazmente gestionado.

Integración del proceso de aseguramiento

Por otro lado, ISACA indica que es importante que el Gerente de seguridad de la información sea consciente y entienda todas las funciones de aseguramiento organizacional porque invariablemente son importantes para la seguridad de la información. El gerente de seguridad de la información debe establecer relaciones formales con otros proveedores de aseguramiento y esforzarse para integrar esas actividades de seguridad de la información. En una organización típica esto puede incluir seguridad física, gestión de riesgos, oficinas para asuntos de privacidad, aseguramiento de la calidad (quality assurance), auditoría, gestión de cambios, seguros, recursos humanos, continuidad de negocio, recuperación en caso de desastre, etc.

3.6Recursos Tecnológicos

Según ISACA, en su manual para la certificación de seguridad, en la mayoría de casos, un programa de seguridad de la información incorporará diversas tecnologías además de los procesos, políticas y personas. El Gerente de seguridad de la información tienen que estar calificado para tomar decisiones con respecto a la tecnología, incluyendo la viabilidad y la aplicabilidad de las soluciones que se encuentran disponibles en términos de metas y los objetivos del programa. Así mismo, es importante conocer cuando determinada tecnología se adapta al marco básico de prevención, detección, contención, reacción y recuperación, así como ayudará a implementar los elementos estratégicos.

A continuación, se muestra un ejemplo de las tecnologías directamente relacionadas con seguridad de la información con las que el gerente de seguridad de la información debe estar familiarizado:

- Cortafuegos(firewall)
- Sistema Antivirus
- Métodos de respaldos y archivado tales como los arreglos redundantes de disco a bajo costo (RAID)
- Atribuciones de seguridad inherentes en los dispositivos de conexión de redes (routers, switches)

- Sistemas de detección de intrusos (IDS) basados en host (HIDS) y basados en Network (NIDS).
- Sistemas de prevención de intrusos (IPS) basados en host (HIPS) y basados en Network (NIPS).
- Técnicas criptográficas (eje. Infraestructura de llave pública, estándares de Encripción de datos).
- Firmas digitales
- Tarjetas inteligentes
- Métodos de autenticación y autorización (contraseñas de un solo uso) one time passwords, desafío respuesta, certificados de PKI autenticación multifactorial, biometría).
- Metodologías de seguridad de redes inalámbricas
- Metodologías de seguridad de aplicaciones
- Plataformas móviles
- Metodologías de acceso remoto (VPN)
- Técnicas de seguridad web
- Herramienta de recolección, análisis y correlación de registros (logs), Gestión de eventos a través de plataforma SIEM
- Escaneo de vulnerabilidades con herramientas para pruebas de penetración.

- Metodologías de prevención de fuga de datos (seguridad de los medios extraíbles, filtrado de contenidos, DLP etc)
- Controle de integridad de datos, por ejemplo, respaldos, estado instantáneo de datos, replicación de datos, RAID, replicación en tiempo real a través de una SAN, etc.
- Sistema de gestión de identidad y acceso.

Aun cuando muchas de estas tecnologías están relacionadas específicamente con la seguridad y la mayoría funcionan como controles, el gerente de seguridad de la información debe de reconocer que casi todas las tecnologías que se utilicen tendrán implicaciones de seguridad.

Además de las tecnologías que están relacionadas con la seguridad, el gerente de seguridad debe estar familiarizado con los aspectos más generales de la tecnología de la información incluyendo, pero sin limitarse por ello:

- Redes de Área local (LAN)
- Redes de Área amplia (WAN)
- Redes de área de almacenamiento (SAN)
- Protocolos de Internet y de red (TCP/IP, UDP, etc.)
- Sistemas operativos
- Conceptos y protocolos de redes y de enrutamiento

- Bases de datos
- Servidores
- Arquitecturas empresariales (servidores de clientes en dos y tres capas, mensajería)
- Virtualización
- Computación en la nube (Cloud Computing)
- Tecnologías y arquitecturas relacionadas con la web
- Traiga su propio dispositivo (BYOD)

El centro de conocimiento en el sitio web de ISACA (www.isaca.org) contiene un almacén de información con búsquedas completas en forma de libros blancos (*White papers*), artículos de revistas y otras publicaciones que abordan muchas tecnologías, tendencias y conceptos importantes para los administradores de seguridad de la información.

3.7Alcance y estatutos del Gobierno de la Seguridad de la Información

ISACA en su manual menciona que cuando se requiere formar un departamento de Seguridad de la Información existen un gran número de consideraciones para tomar en cuenta, es importante determinar el alcance, las responsabilidades y los estatutos del departamento. No es común que estos elementos estén claramente definidos y documentados, excepto por las responsabilidades técnicas generales para elementos como cortafuegos (firewalls), IDS's, detección de virus, etc, los cuales se encuentran generalmente documentados. Si no se cuenta con responsabilidades definidas no será fácil

determinar lo que se debe gestionar o que también está alcanzando los objetivos en el área de seguridad.

Se recomienda que aquellos gerentes de seguridad de la información que se enfrenten a una nueva situación inviertan tiempo y esfuerzo considerable para obtener la comprensión de aquellos a quienes les reportan en lo que respecta a expectativas, responsabilidades, alcance, autoridad, presupuestos, requerimientos de reportes, etc. Será de gran utilidad documentar de forma específica dichos elementos y obtener el acuerdo de los altos Jerarcas.

En términos de línea de mando, es fundamental conocer la estructura organizacional y en donde se ubica el área de seguridad dentro de dicha estructura. En muchas situaciones, el gerente debe ser consciente de que habrá conflictos estructurales inherentes y deberá darles la debida consideración. También resulta prudente discutir cualquier posible conflicto de intereses con la dirección y entender cómo se gestionará. El departamento de seguridad de la información actúa en gran medida, como un área regulatoria interna, y su capacidad para funcionar con eficacia imposibilita la presentación de información a aquellos que se supone que debe regular. Aun cuando podría haber excepciones, en general es cierto que los gerentes de seguridad de la información quienes reportan a un área tecnológica o a otros gerentes operativos están limitados en su capacidad para proporcionar una seguridad eficaz de la información de toda la organización.

3.8ISO 27000

ISO/IEC 27000 es un conjunto de estándares desarrollados, o en fase de desarrollo, por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) que proporcionan un marco de seguridad de la información utilizable para cualquier tipo de organización, pública o privada, grande o pequeña.

3.9Origen de ISO 27000

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution, la organización británica equivalente a AENOR en España) es responsable de la publicación de importantes estándares tales como:

1979 Publicación BS 5750 –ahora ISO 9001

1992 Publicación BS 7750 – ahora ISO 14000

1996 Publicación BS 8800 – ahora OHSAS 18001

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de la información.

La primera parte de la norma (BS-7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. En la segunda parte (BS 7799-2), publicado por

primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información (SGSI), sin cambios sustanciales, como ISO 17790 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistema de gestión.

En 2005 con más de 1700 empresas certificadas en BS7799-2, este esquema se publica en ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO 17799. Esta última norma se renombra como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido, así como el año de publicación formal para su revisión.

Figura 9. Historia ISO 27001
Fuente: www.iso27000.es

En Marzo 2006, posteriormente a la publicación de la ISO27001:2005, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información

3.10 Enfoque del proceso – ISO 27001

Según ISO2700 este estándar Internacional promueve la adopción de un enfoque del proceso a establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI de una organización.

La aplicación de un sistema de procesos dentro de una organización, junto con la identificación y las interacciones de estos procesos y su gestión, puede considerarse un enfoque del proceso.

Un enfoque del proceso para la gestión de la seguridad de la información presentado en este estándar internacional fomenta que sus usuarios enfaticen la importancia de:

a) Entender los requerimientos de seguridad de la información de una organización y la necesidad establecer una política y objetivos para la seguridad de la información;
b) Implementar y operar controles para manejar los riesgos de la seguridad de la información;
c) Monitorear y revisar el desempeño y la efectividad del SGSI; y
d) Mejoramiento continuo con base en la medición del objetivo.

Este estándar Internacional adopta el modelo del proceso Planear-Hacer-Chequear-Actuar (PDCA), el cual se puede aplicar a todos los procesos SGSI. La figura 8 muestra como un SGSI toma como insumo los requerimientos y expectativas de la seguridad de la información de las partes interesadas y a través de acciones y procesos necesarios produce resultados de seguridad de la información que satisfacen aquellos requerimientos y expectativas.

La adopción de un modelo PDCA proporciona principios en aquellos lineamientos que gobiernan la evaluación del riesgo, diseño e implementación de seguridad, gestión y re-evaluación de la seguridad.

Ejemplo 1

Un requerimiento podría ser que las violaciones de seguridad de la información no causen daño financiero a la organización y/o causen vergüenza a la organización.

Ejemplo 2

Una expectativa podría ser que si ocurre un incidente serio tal vez el pirateo del web site eBusiness de una organización-debería contarse con las personas con capacidad suficiente y los procedimientos apropiados para minimizar el impacto.

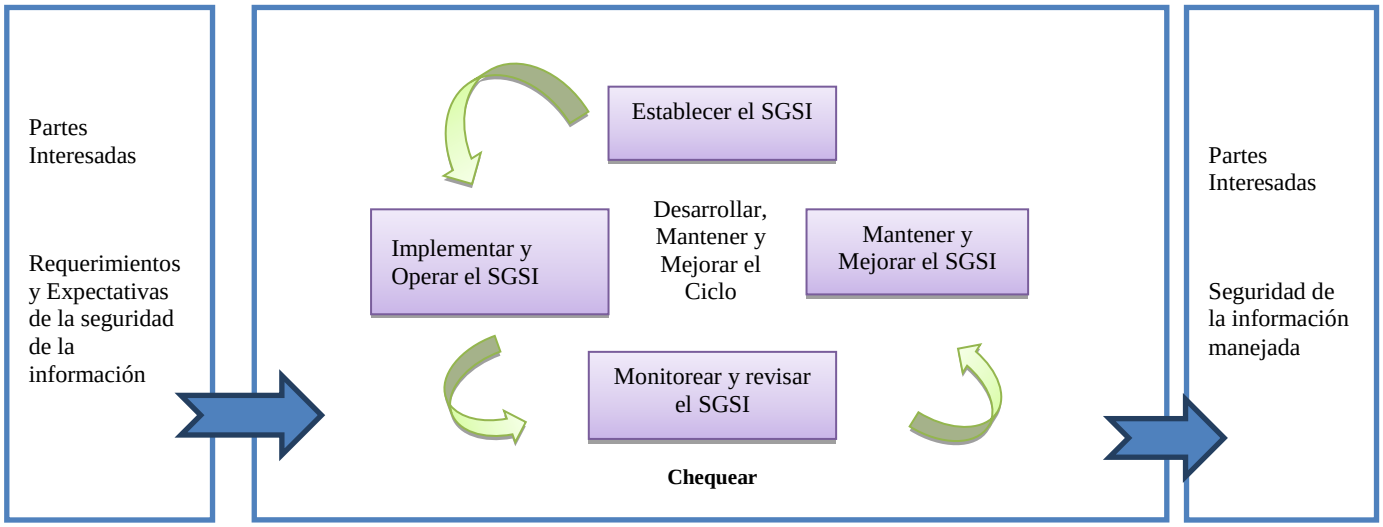

Figura 10. Modelo PDCA aplicado a los procesos SGSI
Fuente: Elaboración propia basada en las observaciones de la investigación

Planear (establecer el SGSI)	Establecer políticas, objetivos, procesos y procedimientos del SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la Organización.
Hacer (implementar el SGSI)	Implementar y operar la política, controles, procesos y procedimientos del SGSI
Chequear (monitorear y revisar el SGSI)	Evaluar donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas del SGSI y reportar los resultados a la gerencia para su revisión.
Actuar (mantener y mejorar el SGSI)	Tomar decisiones correctivas y preventivas, basadas en resultados de la auditoría interna de SGSI, y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI

Figura11. Cuadro Resumen Proceso de Gestión de la Seguridad de la Información ISO 27001
Fuente: Elaboración propia basada en las observaciones de la investigación

3.11 Establecer y manejar el SGSI

3.11.1 Establecer el SGSI

Según ISO 27001 para lograr involucrar y establecer un Sistema de Gestión de Seguridad se debe hacer lo siguiente:

a) Definir el alcance y los límites del SGSI en términos de las características del negocio, la organización, su ubicación, activos e incluyendo los detalles de y la justificación de cualquier exclusión del alcance.

b) Definir una política SGSI en términos de las características del negocio, la organización, su ubicación, activos y tecnología que:

    1) Incluya un marco referencial para establecer sus objetivos y establezca un sentido de dirección general y principios para la acción con relación a la seguridad de la información.
    2) Tome en cuenta los requerimientos comerciales y legales o reguladores y las obligaciones de seguridad contractual.
    3) Este alineada con el contexto de la gestión del riesgo estratégico de la organización en cual se dará el establecimiento y mantenimiento del SGSI.
    4) Establezca un criterio con que se evaluará el riesgo.
    5) Haya sido aprobada por la alta Gerencia.

c) Definir el enfoque de evaluación del riesgo de la organización

    1) Identificar una metodología de cálculo del riesgo para el SGSI y los requerimientos identificados de seguridad, legales y reguladores de la información.

2) Desarrollar criterios para aceptar los riesgos e identificar los niveles de riesgo aceptables.

Existen diferentes metodologías para el cálculo del riesgo. Los ejemplos de la metodología del cálculo del riesgo se discuten en la ISO/IEC TR 13335-3, Tecnología de la información – Lineamiento para la gestión de la Seguridad de TI – Técnicas para la gestión de la seguridad TI

d) Identificar los riesgos

1) Identificar los activos dentro del alcance del SGSI y los propietarios de estos activos.
2) Identificar las amenazas de estos activos.
3) Identificar las vulnerabilidades que podrían ser explotadas por las amenazas.
4) Identificar los impactos que pueden tener las pérdidas de confidencialidad, integridad y disponibilidad de los activos.

e) Analizar y Evaluar el Riesgo

1) Calcular el impacto sobre la organización que podría resultar una falla en la seguridad, tomando en cuenta las consecuencias de una

pérdida de confidencialidad, integridad o disponibilidad de los activos.

2) Calcular la probabilidad realista de que ocurra dicha falla a la luz de las amenazas y vulnerabilidades prevalecientes, y los impactos asociados con estos activos y los controles implementados actualmente.
3) Calcular los niveles de riesgo.
4) Determinar si el riesgo es aceptable o requiere un tratamiento utilizando el criterio de la aceptación del riesgo establecido.

f) Identificar y evaluar las opciones para el tratamiento de riesgos

    1) Aplicar los controles apropiados;
    2) Aceptar los riesgos consciente y objetivamente, siempre que satisfagan claramente las políticas y el criterio de la aceptación del riesgo de la organización;
    3) Evitar los riesgos y
    4) Transferir los riesgos comerciales asociados a otras entidades; por ejemplo: aseguradores, proveedores, etc.

g) Seleccionar objetivos de control y controles para el tratamiento de los riesgos

Se deben de seleccionar e implementar los objetivos de control y controles para cumplir con los requerimientos identificados por el proceso de tasación del riesgo y tratamiento del riesgo.

h) Obtener la aprobación de la gerencia para los riesgos residuales propuestos.

i) Obtener la autorización de la gerencia para implementar y operar el SGSI

j) Proponer un enunciado de Aplicabilidad

Se debe de preparar un enunciado de Aplicabilidad que incluya lo siguiente:

1) Los objetivos de control y los controles seleccionados y las razones para su selección.
2) Los objetivos de control y controles implementados actualmente y
3) La exclusión de cualquier objetivo de control y su justificación.

3.11.2 Implementar y operar un SGSI

Para implementar y dar gestión al modelo propuesto por la ISO 27001, la organización debe hacer lo siguiente:

a) Formular un plan de tratamiento de riesgo que identifique la acción gerencial apropiada, los recursos, las responsabilidades y prioridades para manejar los riesgos de la seguridad de la información.

b) Implementar un plan de tratamiento de riesgo para poder lograr los objetivos de control identificados, los cuales incluyen tener en consideración el financiamiento y asignación de roles y responsabilidades.

c) Implementar los controles seleccionados en 3.11.1 para satisfacer los objetivos de control.

d) Definir cómo medir la efectividad de los controles o grupos de controles seleccionados y especificar como se van a utilizar estas mediciones para evaluar la efectividad el control para producir resultados comparables y reproducibles

e) Implementar los programas de capacitación y conocimiento.

f) Manejar las operaciones del SGSI.

g) Manejar recursos para el SGSI,

h) Implementar los procedimientos y otros controles capaces de permitir pronta detección y respuesta a incidentes de seguridad

3.11.3 Monitorear y revisar el SGSI

El monitoreo es importante dentro de esta propuesta, por lo tanto, la organización debe de mantener en constante monitoreo el modelo, esto con el fin de mantenerlo actualizado, en este caso debe hacer lo siguiente:

a) Ejecutar procedimientos de monitoreo y revisión, además de otros controles para:

    1) Detectar los errores en los resultados de procesamiento;

2) Identificar los incidentes y violaciones de seguridad fallidos y exitosos;
3) Permitir a la gerencia determinar si las actividades de seguridad delegadas a las personas o implementadas mediante la tecnología de información se están realizando como se esperaba;
4) Ayudar a detectar los eventos de seguridad, evitando así los incidentes de seguridad mediante el uso de indicadores y
5) Determinar si son efectivas las acciones tomadas para resolver una violación de seguridad.

b) Realizar revisiones regulares de la efectividad del SGSI (incluyendo satisfacer la política y los objetivos de seguridad del SGSI, y revisar los controles de seguridad) tomando en cuenta los resultados de auditorías de seguridad, incidentes, mediciones de seguridad, sugerencias y retroalimentación de todas las partes interesadas.
c) Medir la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad.
d) Revisar las evaluaciones del riesgo intervalos planeados y revisar el nivel de riesgo residual y riesgo aceptable identificado, tomando en cuenta los cambios en:
    1) La organización;
    2) Tecnología;
    3) Objetivos y procesos de negocio;

4) Amenazas identificadas
5) Efectividad de los controles identificados
6) Eventos externos, como cambios en el ambiente legal o regulatorio, cambios en obligaciones contractuales y cambios en el clima social

e) Realizar auditorías al SGSI internas a intervalos planeados

Nota: Las auditorías internas, algunas veces llamadas auditorías de primera persona, son realizadas por, o en representación de, la organización misma para propósitos internos.

f) Realizar una revisión general del SGSI sobre una base regular para asegurar que el alcance permanezca adecuado y se identifiquen las mejoras del proceso SGSI

g) Actualizar los planes de seguridad para tomar en cuenta los descubrimientos de las actividades de monitoreo y revisión.

h) Registrar las acciones y eventos que podrían tener impacto sobre la efectividad o desempeño del SGSI.

3.11.4 Mantener y mejorar el SGSI

Al tratarse de un proyecto sumamente dinámico donde prácticamente todas las tecnologías de las plataformas se ven beneficiadas con el modelo, la organización debe realizar regularmente revisiones, con el fin de mejorar y mantenerse acorde a las nuevas tendencias, parte de las opciones para este punto son los siguientes:

a) Implementar las mejoras identificadas en el SGSI

b) Tomar acciones correctivas y preventivas apropiadas en concordancia con acciones correctivas y acciones preventivas.

   Aplicar las lecciones aprendidas de las experiencias de seguridad de otras organizaciones y aquellas de la organización misma.

c) Comunicar los resultados y acciones a todas las partes interesadas con un nivel de detalle apropiado de acuerdo a las circunstancias y, cuando sea relevante, acordar como proceder.

d) Asegurar que las mejoras logren sus objetivos señalados.

3.12 COBIT 5

Es un marco referencial publicado por ISACA (Information System Audit and Control Association) que se centra en la gestión de TI Corporativa. Es diferente porque refleja el rol central que tiene la tecnología de la información en las organizaciones modernas. Como sucede en otros marcos referenciales, también se basa en el concepto de riesgos y mantener dentro de un nivel aceptable los riesgos relacionados con TI; talvez su mejor característica es que proporciona una relación directa entre los objetivos estratégicos de una empresa y el uso de TI.

3.12.1 Beneficios de COBIT

El marco referencial de COBIT ayuda a las organizaciones de cualquier tamaño a:

- Mejorar y mantener información de alta calidad para apoyar las decisiones empresariales.
- Utilizarlo eficazmente para alcanzar los objetivos empresariales.
- Utilizar la tecnología para promover la excelencia operacional.
- Garantizar que el riesgo de TI se gestione eficazmente.
- Asegurar que las organizaciones se den cuenta del valor de sus inversiones en TI.
- Cumplir con las leyes, reglamentos y acuerdos contractuales.

3.12.2 Estructura de COBIT

Según ISACA, COBIT 5 proporciona cinco principios de alto nivel que son esenciales para la gestión y gobernanza eficaces de la TI empresarial:

Principio 1: Satisfacer las necesidades de las partes interesadas.

Principio 2: Cobertura de la organización de extremo a extremo.

Principio 3: Aplicación de un marco único integrado.

Principio 4: Habilitación de un enfoque holístico.

Principio 5: Separar la gobernanza de la gestión.

Indica ISACA que estos cinco principios permiten a una organización construir un marco de trabajo holístico para la gobernanza y gestión de TI que se basa en siete facilitadores, los cuales son:

- Personas, políticas y marcos
- Procesos
- Estructuras Organizacionales
- Cultura, Ética y Comportamiento
- Información
- Servicios, Infraestructura y Aplicaciones
- Personas, Habilidades y Competencias

Para el caso que compete a esta investigación, el contenido detallado y relacionado con el proceso que se requiere implementar hace referencia al siguiente Dominio:

Entrega, Servicio y Soporte (DSS), específicamente en su proceso 05 Gestionar servicios de Seguridad.

3.12.3 Contenidos de la Guía de Referencia de Procesos COBIT 5

Según Cobit 5 en este proceso, se intenta realizar una gestión holística sobre la protección de la información institucional, sin embargo, para el estudio en cuestión se han seleccionado ciertos puntos a los cuales vamos hacer referencia. Ver proceso en ANEXO 2.

1.12.4 Matriz RACI DSS05

ISACA indica en esta matriz que establece la asignación sugerida del nivel de responsabilidad para prácticas del proceso a diferentes roles y estructuras. Los roles de la empresa listados están más sombreados que los roles de TI. Los distintos niveles de implicados son:

- **R (esponsable)**--¿Quién está haciendo la tarea? Hace referencia a los roles que se encargan de la actividad principal para completar la actividad y producir la salida esperada.
- **A (responsable de que se haga) [del inglés, accountable]** –¿Quién rinde cuentas sobre el éxito de la tarea? Asigna la responsabilidad de la consecución de la tarea (donde termina la responsabilidad). Tenga en cuenta que el rol mencionado es el nivel más bajo apropiado para rendir cuentas, hay presupuesto, más altos niveles de

rendición de cuentas también. Para activar la potenciación de la empresa, la responsabilidad de rendir cuentas se descompone con la mayor granularidad posible. La rendición de cuentas no indica que el rol no tenga actividades operativas; es probable que el rol se involucre en la tarea. Como principio, la rendición de cuentas no puede ser compartida.

- **C(onsultado)**--¿Quién proporciona entradas? Estos roles que proporcionan entradas son clave. Tenga en cuenta que corresponde a los roles de responsable y de rendir cuentas obtener información de otras unidades o, también de interesados externos. En cualquier caso, las entradas de estos roles enumerados deben de ser consideradas y, si se requiere, tomar medidas necesarias para que se escalen, incluyendo la información del propietario del proceso y/o del comité de Dirección.
- **I(nformado)** ¿Quién recibe la información? Estos roles que son informados de los logros y/o entregables de las tareas. Por supuesto, el rol del 'responsable de hacer' deber recibir siempre información apropiada para supervisar la tarea, al igual que los roles de responsables del área de interés.

Matriz RACI DSS05																										
Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
DSS05.01 Proteger contra software malicioso (*malware*).						R	I				C	A			R	C	C	C	I	R	R		I	R		
DSS05.02 Gestionar la seguridad de la red y las conexiones.						I					C	A				C	C	C	I	R	R		I	R		
DSS05.03 Gestionar la seguridad de los puestos de usuario final.						I					C	A				C	C	C	I	R	R		I	R		
DSS05.04 Gestionar la identidad del usuario y el acceso lógico.						R					C	A			I	C	C	C	I	C	R		I	R		C
DSS05.05 Gestionar el acceso físico a los activos de TI.						I					C	A				C	C	C	I	C	R		I	R	I	
DSS05.06 Gestionar documentos sensibles y dispositivos de salida.											I					C	C	A			R					
DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.				I		C					I	A				C	C	C	I	C	R		I	R	I	I

Figura 12. ***Matriz RACI DSS05***
Fuente: Cobit 5, Procesos Catalizadores, 2012

1.12.5 Prácticas y Actividades del proceso DSS05

1.12.5.1 Proteger contra software malicioso (Malware)

Implementar y mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus). Las prácticas de gestión se pueden observar en el Anexo 3.

1.12.5.2 Gestionar la seguridad de la red y las comunicaciones

Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión. Éstas prácticas de gestión se incluyen en el Anexo 4.

3.12.5.3 Gestionar la seguridad de los puestos de usuario final

Asegurar que los puestos de usuario final (es decir, portátil, equipo desktop, servidor y otros dispositivos y software móviles y de red). Ver prácticas de gestión en Anexo 5.

3.12.5.4 Gestionar la identidad del usuario y acceso lógico

Asegurar que todos los usuarios tengan derechos de acceso a la información de acuerdo con los requerimientos de negocio y coordinar con las unidades de negocio que gestionan sus propios derechos de acceso con los procesos de negocio. Ver prácticas de gestión en Anexo 6.

3.12.5.5 Gestionar el acceso físico a los activos de TI

Definir e implementar procedimientos para conceder, limitar y revocar acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. Ver prácticas de gestión en Anexo 7.

3.12.5.6 Gestionar documentos sensibles y dispositivos de salida

Establecer salvaguardas físicas apropiadas, prácticas de contabilidad y gestión del inventario para activos de TI sensibles. Ver prácticas de gestión en Anexo 8.

3.12.5.7 Supervisar la infraestructura para detectar eventos relacionados con la seguridad

Se puede lograr cumplir con este enunciado usando herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados. Ver prácticas de gestión en Anexo 9.

3.13 NIST (CS-IC)

Este marco contiene un conjunto de directrices sobre ciberseguridad para ayudar a proteger infraestructuras críticas, y está basado en la gestión de riesgos para la ciberseguridad, este marco de trabajo se compone de tres partes: ***el núcleo del marco de trabajo***, presenta estándares de la industria, directrices y prácticas, ***niveles de aplicación del marco de trabajo***, que proporciona un contexto de como una organización entiende y gestiona el riesgo de la ciberseguridad, ***perfil de marco de trabajo***, representa resultados de las necesidades del negocio que se han seleccionado en las categorías y subcategorías del marco de trabajo. A continuación se extrae la información más importante de la publicación Framework for Improving Critical Infrastructure Cybersecurity (NIST.GOV, 2014).

3.13.1 Introducción al Marco referencial

El Marco se basa en una variedad de normas, directrices y prácticas existentes para permitir que los proveedores de infraestructura crítica logren resiliencia. Al confiar en los estándares, directrices y prácticas globales desarrollados, administrados y actualizados por la industria, las herramientas y métodos disponibles para lograr los resultados del Marco se escalarán a través del exterior, reconocerán el carácter global de los riesgos de seguridad cibernética y evolucionarán con los avances tecnológicos y los requisitos de negocio.

El uso de estándares existentes y emergentes permite economías de escala e impulsa el desarrollo de productos, servicios y prácticas eficaces que satisfacen las necesidades

identificadas del mercado. La competencia en el mercado también promueve una difusión más rápida de estas tecnologías y prácticas y la realización de muchos beneficios por parte de las partes interesadas en estos sectores. Basándose en esas normas, directrices y prácticas, el Marco proporciona una taxonomía y un mecanismo común para que las organizaciones:

1) Describan su postura actual en materia de seguridad cibernética;

2) Describir su estado objetivo para la ciberseguridad;

3) Identificar y priorizar las oportunidades de mejora en el contexto de un proceso continuo y repetible;

4) Evaluar el progreso hacia el estado objetivo;

5) Comunicarse entre las partes interesadas internas y externas sobre el riesgo de ciberseguridad.

El Marco complementa y no reemplaza el proceso de gestión de riesgos de una organización y el programa de ciberseguridad. La organización puede utilizar sus procesos actuales y aprovechar el Marco para identificar oportunidades para fortalecer y comunicar su gestión del riesgo de seguridad cibernética al tiempo que se alinea con las prácticas de la industria. Alternativamente, una organización sin un programa de ciberseguridad existente puede utilizar el Marco como una referencia para establecer uno. Así como el Marco no es

específico de la industria, la taxonomía común de normas, directrices y prácticas que proporciona también no es específica de cada país. Las organizaciones fuera de los Estados Unidos también pueden utilizar el Marco para fortalecer sus propios esfuerzos de ciberseguridad y el Marco puede contribuir a desarrollar un lenguaje común para la cooperación internacional en ciberseguridad de infraestructura crítica.

3.13.2 Visión General del Marco

Para (NIST.GOV, 2014)El Marco es un enfoque basado en el riesgo para su gestión en la seguridad cibernética, y se compone de tres partes: el núcleo del marco, los niveles de implementación del marco y los perfiles del marco. Cada componente del Marco refuerza la conexión entre los impulsores del negocio y las actividades de seguridad cibernética. Estos componentes se explican a continuación:

El ***Framework Core*** es un conjunto de actividades de seguridad cibernética, que brinda resultados deseados y referencias aplicables que son comunes en infraestructuras críticas. El Núcleo presenta los estándares, directrices y prácticas de la industria de una manera que permite la comunicación de las actividades de seguridad cibernética y los resultados en toda la organización desde el nivel ejecutivo hasta el nivel de implementación / operaciones.

El Framework Core consta de cinco funciones simultáneas y continuas: **Identificar, Proteger, Detectar, Responder y Recuperar**. Cuando se consideran conjuntamente, estas

Funciones proporcionan una visión estratégica de alto nivel del ciclo de vida de la gestión de riesgos de ciberseguridad de una organización.

Seguidamente, identifica las categorías y sub-categorías clave subyacentes para cada función y las compara con el ejemplo Referencias informativas, como normas, directrices y prácticas existentes para cada sub-categoría

Los niveles de implementación del marco ("Tiers") proporcionan contexto sobre cómo una organización ve el riesgo de la seguridad cibernética y los procesos implementados para manejar ese riesgo. Las escalas describen el grado en que las prácticas de gestión del riesgo de ciberseguridad de una organización exhiben las características definidas en el Marco (por ejemplo, riesgo y amenaza conscientes, repetibles y adaptables). Los *Tiers* caracterizan las prácticas de una organización en un rango, desde *Partial (Tier 1)* hasta *Adaptive (Tier 4)*. Estos niveles reflejan una progresión desde respuestas informales y reactivas a enfoques que son ágiles y están informados sobre el riesgo. Durante el proceso de selección de *Tier*, una organización debe considerar sus actuales prácticas de gestión de riesgos, entorno de amenazas, requisitos legales y regulatorios, objetivos de negocio / misión y restricciones de organización.

Según (NIST.GOV, 2014)**Un Perfil de Marco ("Framework Profile")** representa los resultados basados en las necesidades empresariales que una organización ha seleccionado de las Categorías de Marco y Sub-categorías. El Perfil puede caracterizarse como la

alineación de estándares, directrices y prácticas con el Framework Core en un escenario de implementación particular. Los perfiles pueden usarse para identificar oportunidades para mejorar la postura de la seguridad cibernética comparando un perfil "actual" (el estado "tal cual") con un perfil "objetivo" (el estado "ser"). Para desarrollar un Perfil, una organización puede revisar todas las Categorías y Sub-categorías y, sobre la base de los impulsores del negocio y una evaluación de riesgos, determine cuáles son los más importantes; Pueden agregar categorías y subcategorías según sea necesario para abordar los riesgos de la organización. El perfil actual puede utilizarse para apoyar la priorización y la medición del progreso hacia el perfil objetivo, a la vez que toma en cuenta otras necesidades empresariales, incluyendo la rentabilidad y la innovación. Los perfiles se pueden utilizar para realizar autoevaluaciones y comunicarse dentro de una organización o entre organizaciones.

3.13.3 Conceptos básicos del Marco (Framework)

El Marco proporciona un lenguaje común para comprender, gestionar y expresar el riesgo de ciberseguridad tanto interna como externamente. Se puede utilizar para ayudar a identificar y priorizar acciones para reducir el riesgo de ciberseguridad y es una herramienta para alinear los enfoques de políticas, negocios y tecnológicos para manejar ese riesgo. Puede utilizarse para gestionar el riesgo de ciberseguridad en organizaciones enteras o puede centrarse en la prestación de servicios críticos dentro de una organización.

Diferentes tipos de entidades - incluyendo las estructuras de coordinación de un departamento en específico, asociaciones y organizaciones - pueden utilizar el Marco para diferentes propósitos, incluyendo la creación de perfiles comunes.

3.13.3.1 Núcleo del marco de trabajo (Framework Core)

El núcleo del marco de trabajo proporciona un conjunto de actividades para lograr resultados específicos de seguridad cibernética y hace referencia a ejemplos de orientación para lograr esos resultados. El núcleo no es una lista de comprobación de acciones a realizar. Presenta los resultados clave de ciberseguridad identificados por la industria como útiles para el manejo del riesgo de ciberseguridad. El núcleo comprende cuatro elementos: Funciones, categorías, sub-categorías y referencias informativas.

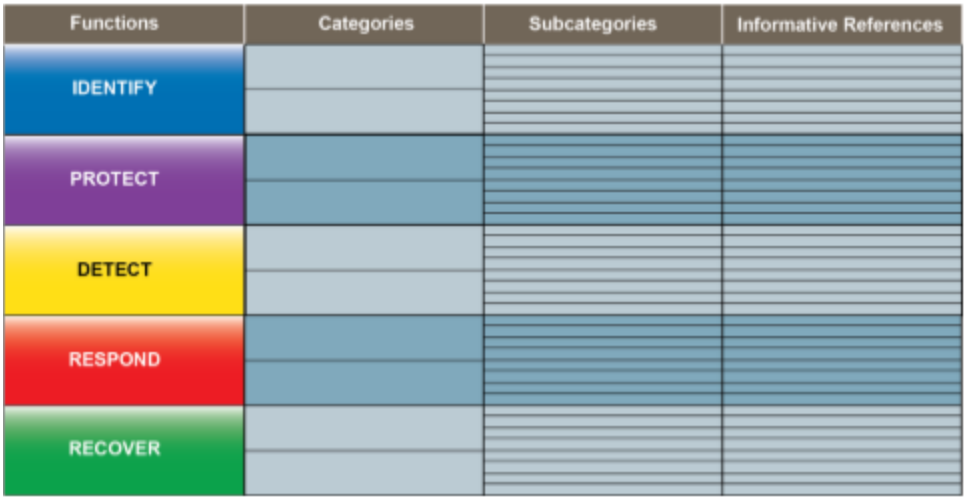

Figura 13. Framework Core Estructura

Fuente: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Según (NIST.GOV, 2014)los elementos básicos del marco de trabajo trabajan juntos de la siguiente manera:

Las funciones organizan las actividades básicas de ciberseguridad en su nivel más alto. Estas funciones son **Identificar, Proteger, Detectar, Responder y Recupera**r. Ayudan a una organización a expresar su gestión del riesgo de seguridad cibernética organizando información, permitiendo decisiones de gestión de riesgos, abordando amenazas y mejorando aprendiendo de actividades anteriores. Las Funciones también se alinean con las metodologías existentes para la gestión de incidentes y ayudan a mostrar el impacto de las inversiones en ciberseguridad. Por ejemplo, las inversiones en planificación y ejercicios apoyan acciones de respuesta y recuperación oportunas, lo que reduce el impacto en la prestación de servicios.

Las categorías son las subdivisiones de una función en grupos de resultados de seguridad cibernética estrechamente vinculados a las necesidades programáticas y a las actividades particulares. Ejemplos de categorías incluyen "Gestión de activos", "Control de acceso" y "Procesos de detección".

Las referencias informativas son secciones específicas de normas, directrices y prácticas comunes entre sectores de infraestructura crítica que ilustran un método para lograr los

resultados asociados con cada sub-categoría. Las Referencias Informativas presentadas en el Marco Núcleo son ilustrativas y no exhaustivas. Se basan en la orientación intersectorial que se menciona con más frecuencia durante el proceso de desarrollo del Marco.

A continuación, se definen las cinco funciones básicas del marco. Estas Funciones no tienen la intención de formar una ruta en serie, o conducir a un estado final deseado estático. Por el contrario, las Funciones se pueden realizar simultánea y continuamente para formar una cultura operativa que se ocupe del riesgo dinámico de seguridad cibernética

1) **Identificar -** Desarrollar la comprensión organizacional para gestionar el riesgo de seguridad cibernética a los sistemas, activos, datos y capacidades. Las actividades de la Función de Identificación son fundamentales para el uso efectivo del Marco. Entender el contexto empresarial, los recursos que soportan funciones críticas y los riesgos relacionados con la seguridad cibernética, permite a una organización centrarse y priorizar sus esfuerzos, de acuerdo con su estrategia de gestión de riesgos y sus necesidades empresariales. Ejemplos de categorías de resultados dentro de esta Función incluyen: Gestión de Activos; Ambiente de negocios; Gobierno; Evaluación de riesgos; Y Estrategia de Gestión de Riesgos.
2) **Proteger** - Desarrollar e implementar las salvaguardias apropiadas para asegurar la provisión de servicios de infraestructura crítica. La función de protección es compatible con la capacidad de limitar o contener el impacto de un posible evento

de ciberseguridad. Ejemplos de categorías de resultados dentro de esta función incluyen: Control de acceso; Concienciación y Capacitación; Seguridad de datos; Procesos y procedimientos de protección de la información; Mantenimiento; Y Tecnología de Protección.

3) **Detectar** - Desarrollar e implementar las actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad. La función de detección permite el descubrimiento oportuno de eventos de ciberseguridad. Ejemplos de categorías de resultados dentro de esta Función incluyen: Anomalías y Eventos; Vigilancia continua de la seguridad; Y procesos de detección.
4) **Responder** - Desarrollar e implementar las actividades apropiadas para tomar medidas con respecto a un evento de ciberseguridad detectado. La Función de Respuesta apoya la capacidad de contener el impacto de un posible evento de ciberseguridad. Ejemplos de categorías de resultados dentro de esta Función incluyen: Planificación de Respuesta; Comunicaciones; Análisis; Mitigación; Y Mejoras.
5) **Recuperar** - Desarrollar e implementar las actividades apropiadas para mantener los planes de resiliencia y restaurar las capacidades o servicios que se vieron afectados debido a un evento de ciberseguridad. La Función Recuperar soporta la recuperación oportuna a las operaciones normales para reducir el impacto de un

evento de ciberseguridad. Ejemplos de categorías de resultados dentro de esta función incluyen: Planificación de la recuperación; Mejoras; y Comunicaciones.

3.13.3.2 Niveles de Aplicación del marco de Trabajo (Tiers)

Los niveles de aplicación del marco ("Tiers") proporcionan contexto sobre cómo una organización ve el riesgo de seguridad cibernética y los procesos implementados para manejar ese riesgo. Los niveles varían de parcial (Tier1) a nivel adaptativo (Tier4) y describen un grado cada vez mayor de rigor y sofisticación en las prácticas de gestión del riesgo cibernético y la medida en que la gestión del riesgo cibernético se basa en las necesidades empresariales y se integran prácticas de maneo del riesgo global de una organización.

Las consideraciones sobre la gestión de riesgos incluyen muchos aspectos de la seguridad cibernética, incluyendo el grado en el que las consideraciones de privacidad y libertades civiles se integran en la gestión de riesgos de ciberseguridad de la organización y las posibles respuestas de riesgo.

El proceso de selección de Tier considera las prácticas actuales de gestión de riesgos de una organización, el entorno de las amenazas, los requisitos legales y reglamentarios, los objetivos de la empresa / misión y las limitaciones de la organización. Las organizaciones deben determinar el Nivel deseado, asegurarse de que el nivel seleccionado cumpla con los

objetivos de la organización, sea factible de implementar y reduzca el riesgo de seguridad cibernética a activos y recursos críticos a niveles aceptables para la organización.

Si bien se anima a las organizaciones identificadas como Nivel 1 (Parcial) a considerar la posibilidad de avanzar hacia el Nivel 2 o superior, los niveles no representan los niveles de madurez. Se fomenta la progresión a niveles superiores cuando tal cambio reducirá el riesgo de ciberseguridad y será rentable. La implementación exitosa del Marco se basa en el logro de los resultados descritos en el Perfil de Objetivos de la organización y no en la determinación de Nivel.

Según (NIST.GOV, 2014)los siguientes niveles son fundamentales para el desarrollo del proceso:

Nivel 1: Parcial

•***Proceso de Gestión de Riesgos*** - No se formalizan las prácticas organizativas de gestión de riesgo de ciberseguridad y se gestiona el riesgo de manera ad hoc y a veces reactiva. La priorización de las actividades de seguridad cibernética puede no estar directamente relacionada con los objetivos de riesgo de la organización, el entorno de la amenaza o los requisitos de la empresa / misión.

•***Programa de Gestión Integrada de Riesgos*** - Se conoce poco el riesgo de seguridad cibernética a nivel organizativo y no se ha establecido un enfoque de toda la organización

para gestionar el riesgo de ciberseguridad. La organización implementa la gestión del riesgo de la seguridad cibernética de manera irregular, caso por caso debido a la diversidad de experiencia o información obtenida de fuentes externas. Es posible que la organización no tenga procesos que permitan compartir la información de seguridad cibernética dentro de la organización.

•***Participación Externa*** - Una organización puede no tener los procesos establecidos para participar en la coordinación o colaboración con otras entidades.

Nivel 2:

Riesgo Informado

•***Proceso de Gestión de Riesgos*** - Las prácticas de gestión de riesgos son aprobadas por la administración, pero pueden no establecerse como políticas de toda la organización. La priorización de las actividades de seguridad cibernética está directamente relacionada con los objetivos de riesgo de la organización, el entorno de la amenaza o los requisitos de la empresa / misión.

•**Programa de Gestión Integrada de Riesgos** - Se conoce el riesgo de seguridad cibernética a nivel organizativo, pero no se ha establecido un enfoque a nivel de toda la organización para gestionar el riesgo de ciberseguridad. Se definen y aplican procesos y procedimientos basados en la información y el manejo de riesgos, y el personal cuenta con

los recursos adecuados para desempeñar sus funciones de ciberseguridad. La información sobre ciberseguridad se comparte en la organización de manera informal.

•**Participación Externa** - La organización conoce su papel en el ecosistema más grande, pero no ha formalizado sus capacidades para interactuar y compartir información externamente.

Nivel 3:

Repetible

•***Proceso de Gestión de Riesgos*** - Las prácticas de gestión de riesgos de la organización son formalmente aprobadas y expresadas como políticas. Las prácticas organizativas de seguridad cibernética se actualizan periódicamente basándose en la aplicación de los procesos de gestión de riesgos a los cambios en los requisitos de las empresas / misiones y en un panorama cambiante de la amenaza y la tecnología.

•***Programa de Gestión Integrada de Riesgos*** - Existe un enfoque de toda la organización para gestionar el riesgo de ciberseguridad. Las políticas, procesos y procedimientos informados por el riesgo se definen, implementan según lo previsto y se revisan. Existen métodos consistentes para responder eficazmente a los cambios en el riesgo. El personal posee los conocimientos y habilidades para desempeñar sus funciones y responsabilidades.

•***Participación Externa*** **-** La organización entiende sus dependencias y socios y recibe información de estos socios que permite la colaboración y las decisiones de gestión basadas en el riesgo dentro de la organización en respuesta a eventos.

Nivel 4:

Adaptable

•***Proceso de Gestión de Riesgos*** - La organización adapta sus prácticas de ciberseguridad basadas en las lecciones aprendidas y los indicadores predictivos derivados de las actividades de seguridad cibernética, anteriores, y actuales. A través de un proceso de mejora continua que incorpora tecnologías y prácticas avanzadas de ciberseguridad, la organización se adapta activamente a un panorama cambiante de ciberseguridad y responde a amenazas evolutivas y sofisticadas de manera oportuna.

•**Programa de Gestión Integrada de Riesgos** - Existe un enfoque a nivel de toda la organización para gestionar el riesgo de ciberseguridad que utiliza políticas, procesos y procedimientos informados por el riesgo para abordar eventos potenciales de ciberseguridad. La gestión del riesgo cibernético es parte de la cultura organizacional y evoluciona a partir de una toma de conciencia de las actividades anteriores, la información compartida por otras fuentes y la conciencia continua de las actividades en sus sistemas y redes.

•***Participación externa***: la organización gestiona el riesgo y comparte activamente la información con los socios para garantizar que se distribuye y consume información precisa y actual para mejorar la seguridad cibernética antes de que se produzca un evento de ciberseguridad.

3.13.3.3 Perfil del Marco de Trabajo (Framework Profile)

El Perfil de Marco de Trabajo ("Profile") es la alineación de las Funciones, Categorías y Sub-categorías con los requisitos de negocio, la tolerancia al riesgo y los recursos de la organización. Un perfil permite a las organizaciones establecer una hoja de ruta para reducir el riesgo de ciberseguridad que está bien alineado con los objetivos organizacionales y departamentales, considera los requisitos legales / normativos y las mejores prácticas de la industria y refleja las prioridades de gestión de riesgos.

Dada la complejidad de muchas organizaciones, pueden optar por tener múltiples perfiles, alinearse con componentes particulares y reconocer sus necesidades individuales. Los perfiles del marco pueden usarse para describir el estado actual o el estado objetivo deseado de las actividades específicas de seguridad cibernética. El perfil actual indica los resultados de seguridad cibernética que se están alcanzando actualmente. El perfil objetivo indica los resultados necesarios para alcanzar los objetivos de gestión del riesgo de seguridad cibernética deseados. Los perfiles apoyan los requerimientos de negocios / misión y ayudan en la comunicación de riesgos dentro y entre organizaciones. Este documento marco no

prescribe modelos de perfil, lo que permite flexibilidad en la implementación. La comparación de perfiles (por ejemplo, el perfil actual y el perfil objetivo) puede revelar las lagunas que deben abordarse para cumplir con los objetivos de gestión del riesgo de seguridad cibernética. Un plan de acción para abordar estas lagunas puede contribuir a la hoja de ruta descrita anteriormente. La priorización de la mitigación de la brecha se basa en las necesidades empresariales de la organización y en los procesos de gestión de riesgos. Este enfoque basado en el riesgo permite a una organización medir las estimaciones de recursos (por ejemplo, la dotación de personal, la financiación) para alcanzar las metas de seguridad cibernética de una manera rentable y priorizada.

3.13.4 ¿Cómo utilizar el marco de trabajo?

Para desarrollar un marco de trabajo la (NIST.GOV, 2014) indica que una organización puede utilizar el Marco como una parte clave de su proceso sistemático para **identificar, evaluar y gestionar el riesgo de ciberseguridad**. El Marco no está diseñado para reemplazar los procesos existentes; Una organización puede utilizar su proceso actual y superponerlo en el Marco para determinar lagunas en su actual enfoque de riesgo de ciberseguridad y desarrollar una hoja de ruta para la mejora. Utilizando el Marco como una herramienta de gestión del riesgo de seguridad cibernética, una organización puede determinar las actividades que son más importantes para la prestación de servicios críticos

y priorizar los gastos para maximizar el impacto de la inversión. El Marco está diseñado para complementar las operaciones comerciales y de ciberseguridad existentes.

Puede servir de base para un nuevo programa de ciberseguridad o un mecanismo para mejorar un programa existente. El Marco proporciona un medio de expresar los requisitos de seguridad cibernética a los socios comerciales y los clientes y puede ayudar a identificar brechas en las prácticas de seguridad cibernética de una organización. También proporciona un conjunto general de consideraciones y procesos para considerar las implicaciones de privacidad y libertades civiles en el contexto de un programa de ciberseguridad.

3.13.5 Establecer o mejorar un Programa de CiberSeguridad

(NIST.GOV, 2014) Indica que los siguientes pasos ilustran cómo una organización podría utilizar el Marco para crear un nuevo programa de seguridad cibernética o mejorar un programa existente. Estas medidas deben repetirse según sea necesario para mejorar continuamente la seguridad cibernética.

Paso 1: Priorizar y Alcance. La organización identifica sus objetivos de negocio / misión y prioridades organizacionales de alto nivel. Con esta información, la organización toma decisiones estratégicas con respecto a implementaciones de seguridad cibernética y determina el alcance de los sistemas y activos que soportan la línea o proceso de negocio seleccionado. El Marco puede adaptarse para apoyar las diferentes líneas de negocio o

procesos dentro de una organización, que pueden tener diferentes necesidades de y la tolerancia de riesgo asociada.

Paso 2: Enfoque. Una vez que se ha determinado el alcance del programa de ciberseguridad para la línea o proceso de negocio, la organización identifica los sistemas y activos relacionados, los requisitos reglamentarios y el enfoque de riesgo general. A continuación, la organización identifica amenazas y vulnerabilidades de dichos sistemas y activos.

Paso 3: Crear un perfil actual. La organización desarrolla un perfil actual indicando cuáles son los resultados de categoría y sub-categoría del marco básico que se están alcanzando actualmente.

Paso 4: Realizar una evaluación de riesgos. Esta evaluación podría guiarse por el proceso general de gestión de riesgos de la organización o por actividades anteriores de evaluación de riesgos. La organización analiza el entorno operacional con el fin de discernir la probabilidad de un evento de ciberseguridad y el impacto que el evento podría tener en la organización. Es importante que las organizaciones busquen incorporar los riesgos emergentes y los datos de amenazas y vulnerabilidades para facilitar una sólida comprensión de la probabilidad y el impacto de los eventos de ciberseguridad.

Paso 5: Crear un perfil de destino. La organización crea un perfil objetivo que se centra en la evaluación de las categorías y sub-categorías del marco que describen los resultados

deseados de seguridad cibernética de la organización. Las organizaciones también pueden desarrollar sus propias categorías y subcategorías adicionales para tener en cuenta los riesgos organizativos únicos. La organización también puede considerar influencias y requerimientos de actores externos como entidades del sector, clientes y socios comerciales al crear un perfil objetivo.

Paso 6: Determinar, analizar y priorizar las brechas (gaps). La organización compara el perfil actual y el perfil objetivo para determinar las brechas. A continuación, crea un plan de acción priorizado para abordar las brechas que se basan en los impulsores de la misión, un análisis de costo / beneficio y la comprensión del riesgo para lograr los resultados en el perfil objetivo. A continuación, la organización determina los recursos necesarios para abordar las brechas. El uso de Perfiles de esta manera permite a la organización tomar decisiones informadas sobre las actividades de seguridad cibernética, apoya la gestión de riesgos y permite a la organización realizar mejoras rentables y específicas.

Paso 7: Implementar el Plan de Acción. La organización determina qué acciones tomar en relación con las lagunas, si las hay, identificadas en el paso anterior. Luego, monitorea sus prácticas actuales de seguridad cibernética contra el Perfil de Objetivo. Para más orientación, el Marco identifica ejemplos de referencias informativas sobre las categorías y subcategorías, pero las organizaciones deben determinar qué normas, directrices y prácticas, incluidas las que son sectoriales, funcionan mejor para sus necesidades.

Una organización puede repetir los pasos necesarios para evaluar y mejorar continuamente su ciberseguridad. Por ejemplo, las organizaciones pueden encontrar que la repetición más frecuente del Mejora la calidad de las evaluaciones de riesgos. Además, las organizaciones pueden monitorear el progreso a través de actualizaciones iterativas al perfil actual, comparando posteriormente el perfil actual con el perfil objetivo. Las organizaciones también pueden utilizar este proceso para alinear su programa de ciberseguridad con el nivel de implementación del marco deseado.

3.13.6 Comunicación de los requisitos de seguridad cibernética con las partes interesadas

El Marco proporciona un lenguaje común para comunicar los requisitos entre las partes interesadas interdependientes responsables de la prestación de servicios esenciales de infraestructura crítica. Algunos ejemplos incluyen:

- Una organización puede utilizar un perfil objetivo para expresar los requisitos de gestión de riesgos de seguridad cibernética a un proveedor de servicios externo (por ejemplo, un proveedor de la nube al que exporta datos).

- Una organización puede expresar su estado de seguridad cibernética a través de un perfil actual para informar los resultados o comparar con los requisitos de adquisición.

• Un propietario / operador de infraestructura crítico, después de haber identificado a un socio externo de quien depende la infraestructura, puede usar un perfil objetivo para transmitir las categorías y sub-categorías requeridas.

• Un sector de infraestructura crítico puede establecer un Perfil de Objetivo que pueda ser utilizado entre sus constituyentes como perfil de línea de base inicial para construir sus Perfiles de destino adaptados.

1.13 B.A.S.E Metodología de Evaluación de Seguridad

Es una metodología expuesta por (Braunton, 2005) en el sitio de SANS.org el cual desarrolla un proceso de evaluación constante de seguridad y detalla herramientas que pueden ser utilizadas para esta gestión.

Como ya se ha dicho anteriormente, Internet depende de las redes colectivas e individuales de hogares, pequeñas oficinas y empresas. Fáciles de adquirir y desplegar, estas redes están aumentando en complejidad y conectividad dentro y fuera de sus límites lógicos.

La huella típica de los servicios prestados o utilizados en estas proliferantes redes incluye

- Compartición de archivos e impresoras
- Sistemas operativos en red

- Correo electrónico
- Mensajería instantánea
- Procesamiento de documentos
- Servicios de copia de seguridad básicos
- Protección contra virus
- Servicios de Internet en funcionamiento
- Puntos de acceso inalámbricos

Para ello se requiere conocimiento mínimo y experiencia para desplegar una red completamente funcional con servicios de acceso a Internet, impresión, correo electrónico, ftp, web, inalámbrico y firewall.

3.13.1 Definición de B.A.S.E

Lo que se necesita es una estrategia básica basada en los fundamentos de los conceptos de aseguramiento de la información, pero se presta a la utilización en un estilo *ad-hoc* directamente adaptado para asegurar una red básica. Para cumplir con este requisito, este documento propone un protocolo de evaluación llamado BASE que significa Baseline, Audit and Assess, Secure, and Evaluate and Educate por (Braunton, 2005).

Baseline. El paso más importante es la línea base o Baseline. Esto quiere decir que debemos basar el entorno en términos de patrones de acceso, rendimiento, configuraciones

de hardware, servicios, aplicaciones instaladas, aplicaciones y comportamientos humanos, etc. Es difícil, pero no imposible, detectar y aislar anomalías, cambios en un sistema o red si no se conoce y documenta el comportamiento operativo diario normal.

En este paso, la línea de base como medición para detectar la intrusión no es el único patrón. La línea base proporciona patrones e información sobre las necesidades operacionales y de mantenimiento del sistema. Y un estado final crítico para este paso es la documentación. La documentación de la información de línea de base recogida resulta esencial para la solución de problemas y sirve como base valiosa para establecer un camino de recuperación de desastres que es un precursor esencial para asegurar la disponibilidad del sistema.

Auditoría y Evaluación. Utilizando tanto tareas manuales como herramientas automatizadas, planifique y ejecute auditorías del entorno operativo contra la línea de base previamente establecida y contra las prácticas de seguridad de la información en evolución. La tarea complementaria de este paso consiste en evaluar los resultados de la auditoría tanto en términos de configuración técnica como de necesidades empresariales. Técnicamente, la evaluación revela qué medidas adicionales de endurecimiento se requieren, pero no deben implementarse con la exclusión de la funcionalidad requerida del sistema. Cuando la seguridad invade la necesidad funcional del negocio, debe realizarse un análisis de riesgo. Usando el análisis de riesgo, se hace una determinación para aplicar seguridad adicional en

el riesgo de pérdida de funcionalidad o productividad o ingresos. O, en su lugar, aceptar el riesgo de operaciones continuadas en un estado vulnerable. Independientemente de si se invoca o no el análisis de riesgos, el estado final de este paso es una explicación de las potenciales vulnerabilidades identificadas y la decisión que se solucionará en el siguiente paso.

Asegurar. La evaluación se alimenta directamente en este paso.

Aquí, el plan de remediación se ejecuta para remediar aquellas áreas previamente evaluadas como una posible área de vulnerabilidad. Esto incluye cambios técnicos en el entorno, así como políticas o procedimientos que rigen el uso y la gestión de los recursos de TI.

Evaluar y Educar. Evaluar los resultados de la "seguridad" que se ejecutó.

Principalmente, para asegurar que las necesidades funcionales del negocio no fueron afectadas negativamente por los ajustes erróneos o demasiado restrictivos, sino también como un seguimiento para determinar si las configuraciones / cambios hechos realmente remediaron la amenaza evaluada. Cuando el aumento de la seguridad afecta a los requisitos funcionales del negocio, la aceptación del riesgo debe ser evaluada y una decisión ponderada, justificada y documentada en favor de la seguridad con el riesgo de pérdida o reducción de la funcionalidad o en favor de la funcionalidad ante el riesgo de pérdida de

seguridad. Además, para evitar la duplicación de esfuerzos, adaptar e integrar las configuraciones resultantes donde sea posible como un estándar recomendado en entornos similares en la organización. Con éxito o sin éxito, capturar las lecciones aprendidas para servir como una herramienta para educar más, según sea apropiado, técnico, administrativo y personal de usuario. El elemento educativo es esencial ya que continuará aumentando la conciencia y la competencia en muchos niveles, elevando así permanentemente el nivel de seguridad colectiva de la organización.

1.14 Red de Datos y Aspectos Técnicos

Una red se puede definir como un grupo de objetos conectados entre sí por algún tipo de medio y que comparten cierta información entre sí. En el ámbito de la informática una red es un conjunto de dispositivos (a menudo denominados nodos), conectados por enlaces de un medio físico. Un nodo puede ser una computadora, una impresora o cualquier otro dispositivo capaz de enviar y recibir datos generados por otros nodos en la red (Forouzan, 2007).

Una red trabaja con ciertos conjuntos de reglas llamados **protocolos de red**. Un protocolo de red es una descripción formal de un conjunto de reglas y convenciones que gobiernan el modo en que se comunican los dispositivos de una red. Los protocolos controlan todos los

aspectos de la comunicación de datos, determinan como se construye la red física, la conexión de las computadoras, como se formatean los datos para la trasmisión y el envío de los datos.

Todas estas reglas son creadas y mantenidas por diferentes organizaciones internacionales como son:

IEEE, la ANSI, la TIA, la EIA y la ITU (Cisco Systems Inc., 2004).

1.14.1 Tipos de Redes

Las redes de datos o informáticas pueden clasificarse de distintas formas ya sea por su uso, su dimensión o tamaño y estructura física. La infraestructura de una red puede variar en gran medida en términos de tamaño del área cubierta, la cantidad de usuarios conectados y la cantidad de servicios disponibles, en el Ministerio de Seguridad se cuenta con 6 Módulos principales y los cuales se encuentras separados por Vlan's, cada módulo cuenta con su respectivo direccionamiento, podemos decir que se trata de una red bastante grande, ya que aunado a lo anterior también existe una gran red VPN por la cual se interconectan de manera lógica todas las Delegaciones Policiales del País y otras unidades para el trasiego de información.

La clasificación que más se maneja es de acuerdo a su tamaño, es decir, el territorio

geográfico que puede cubrir. En este caso se consideran tres tipos principales de redes LAN, MAN y WAN. Actualmente existen autores que aún conservan esta clasificación como Xavier Hesselbach Serra y Jordi Altés Bosch, Behrouz A. Forouzan, Andrew S. Tanenbaum y la propia Cisco Systems Inc. Sin embargo, hay autores como W. Stalling quien solo maneja los términos de LAN y WAN en su libro "Comunicación y redes de computadores." (Stalling, 2003) La categoría de redes MAN actualmente ya no es muy considerada para la clasificación de las redes por área geográfica cubierta, haciendo la distinción sólo entre redes LAN y WAN ya que básicamente estas abarcan las características de una MAN. Por tales razones en este trabajo sólo se manejará estos dos tipos y agregamos la red VPN.

1.14.2 LAN

Una LAN se considera generalmente como una red individual que cubre una única área geográfica y proporciona servicios y aplicaciones a personas dentro de una estructura organizacional común, como una empresa o un campus. Por lo general está administrada por una organización única. Todos los dispositivos tales como las estaciones de trabajo, computadoras personales, impresoras, teléfonos, en las oficinas normalmente están conectadas a una LAN y se conocen comúnmente como nodos con los que un usuario es capaz de compartir información y recursos, tanto físicos como lógicos. (Tanenbaum, 2003).

1.14.3 WAN

Una red WAN es una red que abarca una gran extensión geográfica, que podría llegar de un continente a otro. Esta WAN está constituida principalmente por redes de área local que están distribuidas en distintas ubicaciones geográficas. Los enlaces atraviesan áreas públicas locales, nacionales o internacionales, usando en general como medio de transporte la red pública telefónica. Por lo general, las WAN son construidas para organizaciones individuales que alquilan las conexiones a través de una red de TSPs. (Stalling, 2000)

1.14.4Virtual Private Network

Según Microsoft Technet en su *whitepaperVirtual Private Networking: An Overview, Set 04 2001 u*na red privada virtual (VPN) es la extensión de una red privada que abarca enlaces a través de redes públicas o compartidas como Internet. Una VPN le permite enviar datos entre dos equipos a través de una red compartida o pública de una manera que emula las propiedades de un enlace privado punto a punto. El acto de configurar y crear una red privada virtual se conoce como redes privadas virtuales, en este caso los administradores de red del Ministerio de Seguridad Pública han logrado trabajar muy bien esta extensión, ampliando grandes servicios tales como telefonía IP, aplicaciones web, administración de objetos en la red tales como carpetas compartidas, y todo esto requiere de involucrar procesos de seguridad que permitan la protección continua de las diferentes tecnologías.

Para emular un enlace punto a punto, los datos se encapsulan o se envuelven con un encabezado que proporciona información de enrutamiento que le permite recorrer la red interna de transporte compartido o público para alcanzar su punto final. Para emular un enlace privado, los datos que se envían se cifran para garantizar la confidencialidad. Los paquetes que son interceptados en la red pública o compartida son indescifrables sin las claves de cifrado. La parte de la conexión en la que se encapsulan los datos privados se conoce como túnel. La parte de la conexión en la que se cifran los datos privados se conoce como conexión de red privada virtual (VPN).

1.15 Protocolo

Un **protocolo** es un método estándar que permite la comunicación entre procesos (que potencialmente se ejecutan en diferentes equipos), es decir, es un conjunto de reglas y procedimientos que deben respetarse para el envío y la recepción de datos a través de una red.

Existen diversos protocolos de acuerdo a cómo se espera que sea la comunicación. Algunos protocolos, por ejemplo, se especializarán en el intercambio de archivos (FTP); otros pueden utilizarse simplemente para administrar el estado de la transmisión y los errores (como es el caso de ICMP), etc.

En Internet, los protocolos utilizados pertenecen a una sucesión de protocolos o a un conjunto de protocolos relacionados entre sí. Este conjunto de protocolos se denomina

TCP/IP. .

Entre otros, contiene los siguientes protocolos:

- HTTP, FTP, ARP, ICMP, IP, TCP, UDP, SMTP, Telnet, NNTP

En este punto es importante mencionar que los protocolos fueron creados para establecer un lenguaje común de comunicación entre los diferentes servicios, fueron pensado para este origen, sin embargo, nunca se pensó en seguridad, los módulos de seguridad llegan ya cuando existen plataformas interconectadas y realizando diferentes labores y las cuales se pueden ver comprometidas si no integramos opciones de protección y por tanto el módulo de seguridad a cada protocolo, por ejemplo: https aplica su módulo de seguridad en el protocolo https, ftp aplica su módulo de seguridad en el protocolo sftp, etc.

3.15.1 Protocolo orientado a conexión y protocolo no orientado a conexión

Generalmente, los protocolos se clasifican en dos categorías según el nivel de control de datos requerido:

3.15.2 Protocolos orientados a conexión

Estos protocolos controlan la transmisión de datos **durante** una comunicación establecida entre dos máquinas. En tal esquema, el equipo receptor envía acuses de recepción durante

la comunicación, por lo cual el equipo remitente es responsable de la validez de los datos que está enviando. Los datos se envían entonces como flujo de datos.

3.15.3 Protocolo UDP

UDP es un protocolo no orientado a conexión ya que no envía alguna confirmación al emisor de que los paquetes que haya enviado se recibieron con éxito. Es definido en el RFC 768. Es considerado como un sistema de entrega "de mejor esfuerzo" por lo que no tiene que hacer ninguna confirmación de la llegada de los paquetes. La idea consiste en que no se garantiza que los paquetes lleguen pero que existen grandes probabilidades de que esto suceda. La retransmisión de confirmaciones es una operación que se considera un retraso o reducir la velocidad en la entrega de los datos. (IETF, 1980)

Un ejemplo de una aplicación que utiliza UDP es la radio por Internet. Si parte del mensaje se pierde durante su transmisión, no se vuelve a retransmitir. Sin embargo, con TCP los paquetes serían reenviados nuevamente lo que produciría una pausa notoria en la transmisión a la hora de reenviar los paquetes.

3.15.4 Protocolos no orientados a conexión

Este es un método de comunicación en el cual el equipo remitente envía datos sin avisarle al equipo receptor, y éste recibe los datos sin enviar una notificación de recepción al remitente. Los datos se envían entonces como bloques (datagramas). UDP es un protocolo no orientado a conexión.

3.15.5 Protocolo TCP

De acuerdo al RFC 793 el protocolo TCP está pensado para ser utilizado como un protocolo "host a host" muy fiable entre miembros de redes de comunicación de computadoras por intercambio de paquetes y en un sistema interconectado de tales redes. (IETF, 1981, *Trasmision Control Protocol*).

El propósito principal de TCP consiste en proporcionar un servicio de conexión o circuito lógico fiable y seguro entre pares de procesos. Su funcionamiento consiste en dividir los mensajes en partes pequeñas conocidas como segmentos, estos son enumerados en secuencia y pasan al proceso IP para armarse en paquetes. Se realiza un seguimiento del número que se enviaron a un host específico desde una aplicación específica. De esta forma, el emisor debe recibir una confirmación del receptor que el paquete ha llegado, si no la recibe, el emisor envía nuevamente el paquete o la parte del paquete que no haya llegado hasta que la reciba. Así, en el host receptor TCP se encarga de rearmar los segmentos del mensaje y de pasarlos a la aplicación. (Tanenbaum, 2003)

FTP y HTTP son ejemplos de aplicaciones que utilizan TCP para garantizar la entrega de datos. Por esta razón este protocolo es conocido también como orientado a conexión ya que tiene la capacidad de confirmar al emisor la llegada de los paquetes de datos.

3.15.6 Protocolo e implementación

Un protocolo define únicamente cómo deben comunicar los equipos, es decir, el formato y la secuencia de datos que van a intercambiar. Por el contrario, un protocolo no define cómo se programa el software para que sea compatible con el protocolo. Esto se denomina **implementación** o la conversión de un protocolo a un lenguaje de programación.

Las especificaciones de los protocolos nunca son exhaustivas. Asimismo, es común que las implementaciones estén sujetas a una determinada interpretación de las especificaciones, lo cual genera especificidades de ciertas implementaciones o, aún peor, incompatibilidad o fallas de seguridad.

3.15.7 Protocolo IP

De acuerdo al RFC 791, el protocolo de Internet está diseñado para su uso en sistemas interconectados de redes de comunicación de computadoras por intercambio de paquetes. A un sistema de este tipo se le conoce como catenet. El IP proporciona los medios necesarios para la transmisión de bloques de datos llamados datagramas desde el origen al destino, que

son hosts identificados por direcciones de longitud fija. Este protocolo también se encarga, si es necesario, de la fragmentación y el re ensamblaje de grandes datagramas para su transmisión a través de redes de trama pequeña (IETF, 1981, *Internet Protocol*).

IP utiliza el datagrama como la unidad de información intercambiada, que contiene un encabezado y un área de datos. No especifica el contenido del área de datos, ésta será utilizada arbitrariamente por el protocolo de transporte encargado de la transmisión de los datos. No existen mecanismos para aumentar la fiabilidad de datos entre los extremos, control de flujo, secuenciamiento u otros servicios que se encuentran normalmente en otros protocolos "host a host". IP puede aprovecharse de los servicios de sus redes de soporte para proporcionar varios tipos y calidades de servicio. (Tanenbaum, 2003)

Para que una computadora dentro de una red se pueda comunicar con otra, debe haber un esquema de direccionamiento, utilizado para identificar a cada host con que se requiere establece una comunicación, a esto se le llama direccionamiento lógico. Actualmente, se utiliza el concepto dirección IP para denominar una dirección lógica a nivel de red del conjunto de protocolos TCP/IP. Existen dos tipos principales de direccionamiento, IPv4 en IPv6.

3.15.10 Protocolos Seguros

Un **protocolo de seguridad** (también llamado **protocolo criptográfico** o **protocolo de cifrado**) es un protocolo abstracto o concreto que realiza funciones relacionadas con la seguridad, aplicando métodos criptográficos.

Un protocolo describe la forma en que un algoritmo debe usarse. Un protocolo lo suficientemente detallado incluye detalles acerca de las estructuras de datos y representaciones, punto en el cual puede usarse para implementar versiones interoperables múltiples de un programa.

3.15.11 Secure Sockets Layers (SSL)

*SSL (**Secure Socket Layers**)* es un proceso que administra la seguridad de las transacciones que se realizan a través de Internet. El estándar SSL fue desarrollado por *Netscape*, junto con *Mastercard*, *Bank of America*, *MCI* y *Silicon Graphics*. Se basa en un proceso de cifrado de clave pública que garantiza la seguridad de los datos que se envían a través de Internet. Su principio consiste en el establecimiento de un canal de comunicación seguro (cifrado) entre dos equipos (el cliente y el servidor) después de una fase de autenticación.

El sistema SSL es independiente del protocolo utilizado; esto significa que puede asegurar transacciones realizadas en la Web a través del protocolo HTTP y también conexiones a través de los protocolos FTP, POP e IMAP. SSL actúa como una capa adicional que

permite garantizar la seguridad de los datos y que se ubica entre la capa de la aplicación y la capa de transporte (por ejemplo, el protocolo TCP).

De esta forma, SSL es transparente para el usuario (es decir, el usuario puede no conocer que está usando SSL). Por ejemplo, un usuario que utiliza un navegador de Internet para conectarse a una página Web de comercio electrónico protegido por SSL enviará datos cifrados sin tener que realizar ninguna operación especial.

Actualmente, casi todos los navegadores soportan el protocolo SSL. Por ejemplo, *google chrome* muestra un candado de color verde cerrado para indicar la conexión a un sitio Web con seguridad SSL y un candado abierto en el caso opuesto, en tanto que *Microsoft Internet Explorer* muestra un candado sólo si establece una conexión con un sitio Web SSL.

Figura 14. Ejemplo del protocolo SSL en navegador google chrome
Fuente: Elaboración propia basada en las observaciones de la investigación

Figura 15. Ejemplo del protocolo SSL en navegador IE 10
Fuente: Elaboración propia basada en las observaciones de la investigación

Un servidor de Web seguro tiene una dirección URL que empieza con *https://*, en el que la "s" obviamente significa *secured*, seguro.

A mediados de 2001, la patente SSL, que hasta ese momento había pertenecido a Netscape, fue adquirida por *IETF* (*Internet Engineering Task Force*) y adoptó el nombre de **TLS** (*Transport Layer Security*).

SSL 2.0

La seguridad de las transacciones a través de SSL 2.0 se basa en el intercambio de claves entre un cliente y un servidor. Una transacción segura SSL se realiza de acuerdo al siguiente modelo:

- Primero, el cliente se conecta al servidor comercial protegido por SSL y pide la autenticación. El cliente también envía la lista de los criptosistemas que soporta, clasificada en orden descendente por la longitud de la clave.

- El servidor que recibe la solicitud envía un certificado al cliente que contiene la clave pública del servidor firmado por una entidad de certificación (CA), y también el nombre del criptosistemas que está más alto en la lista de compatibilidades (la longitud de la clave de cifrado - 40 o 128 bits - será la del criptosistemas compartido que tiene el tamaño de clave de mayor longitud).
- SSL 2.0 está desactivado por defecto, a partir de: Internet Explorer 7, Mozilla Firefox 2, Opera 9.5 y Safari. Después de que se envía un "ClientHello" TLS, si Mozilla Firefox comprueba que el servidor no puede completar el handshake, intentará volver a caer a la utilización de SSL 3.0 con un SSL 3.0 "ClientHello" en formato SSL 2.0 para maximizar la probabilidad de éxito del handshake con los servidores más antiguos. Permitir SSL 2.0 (y sistemas de cifradas débiles de 40 y 56 bits), ha sido completamente eliminado de Opera desde la versión 10

SSL 3.0

SSL 3.0 mejoró SSL 2.0 mediante la adición de cifrado SHA-1 y soporte para autenticación de certificados.

Desde el punto de vista de seguridad, SSL 3.0 debería considerarse menos deseable que TLS 1.0. Las suites de cifrado de SSL 3.0 tienen un proceso de derivación de claves débiles, la mitad de la llave maestra que se establece es totalmente dependiente de la función hash MD5, que no es resistente a los choques y, por lo tanto, no es considerado

seguro. Bajo TLS 1.0, la llave maestra que se establece depende tanto MD5 y SHA-1 por lo que su proceso de derivación no está actualmente considerado débil. Es por esta razón que las implementaciones SSL 3.0 no pueden ser validados bajo FIPS 140-2.

Hay algunos ataques contra la implementación en lugar del propio protocolo: En las implementaciones anteriores, algunas entidades emisoras no establecieron explícitamente basicConstraintsCA=False para los *nodos hoja*. Como resultado, estos *nodos hoja* podían firmar certificados piratas. Además, algunos programas de (incluyendo IE6 y Konqueror) no comprobó este campo para nada. Esto puede ser explotado en ataques man-in-the-middle a todas las conexiones posibles SSL. Algunas implementaciones (incluyendo versiones anteriores de la API de cifrado de Microsoft, Network Security Services y GnuTLS) dejan de leer los caracteres que siguen al carácter nulo en el campo del nombre del certificado, lo que puede ser explotado para engañar al cliente en la lectura del certificado como si fuera originado en el sitio auténtico. (Por ejemplo, PayPal.com\0.badguy.com sería confundido como proveniente del sitio PayPal.com en lugar de badguy.com). Los navegadores implementaron mecanismos de degradación del protocolo a una versión anterior en SSL/TLS por razones de compatibilidad. La protección ofrecida por los protocolos SSL/TLS contra un downgrade a una versión anterior de un ataque man-in-the-middle activo puede ser inutilizados por tales mecanismos.

3.15.12 IPsec

IPsec (abreviatura de Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

Los protocolos de IPsec actúan en la capa de red, la capa 3 del modelo OSI. Otros protocolos de seguridad para Internet de uso extendido, como SSL, TLS y SSH operan de la capa de transporte (capas OSI 4 a 7) hacia arriba. Esto hace que IPsec sea más flexible, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP y UDP, los protocolos de capa de transporte más usados. IPsec tiene una ventaja sobre SSL y otros métodos que operan en capas superiores. Para que una aplicación pueda usar IPsec no hay que hacer ningún cambio, mientras que, para usar SSL y otros protocolos de niveles superiores, las aplicaciones tienen que modificar su código.

IPsec está implementado por un conjunto de protocolos criptográficos para (1) asegurar el flujo de paquetes, (2) garantizar la autenticación mutua y (3) establecer parámetros criptográficos.

La arquitectura de seguridad IP utiliza el concepto de asociación de seguridad (SA) como base para construir funciones de seguridad en IP. Una asociación de seguridad es simplemente el paquete de algoritmos y parámetros (tales como las claves) que se está

usando para cifrar y autenticar un flujo particular en una dirección. Por lo tanto, en el tráfico normal bidireccional, los flujos son asegurados por un par de asociaciones de seguridad. La decisión final de los algoritmos de cifrado y autenticación (de una lista definida) le corresponde al administrador de IPsec.

Para decidir qué protección se va a proporcionar a un paquete saliente, IPsec utiliza el índice de parámetro de seguridad (SPI), un índice a la base de datos de asociaciones de seguridad (SADB), junto con la dirección de destino de la cabecera del paquete, que juntos identifican de forma única una asociación de seguridad para dicho paquete. Para un paquete entrante se realiza un procedimiento similar; en este caso IPsec coge las claves de verificación y descifrado de la base de datos de asociaciones de seguridad.

En el caso de multicast, se proporciona una asociación de seguridad al grupo, y se duplica para todos los receptores autorizados del grupo. Puede haber más de una asociación de seguridad para un grupo, utilizando diferentes SPIs, y por ello permitiendo múltiples niveles y conjuntos de seguridad dentro de un grupo. De hecho, cada remitente puede tener múltiples asociaciones de seguridad, permitiendo autenticación, ya que un receptor sólo puede saber que alguien que conoce las claves ha enviado los datos. Hay que observar que el estándar pertinente no describe cómo se elige y duplica la asociación a través del grupo; se asume que un interesado responsable habrá hecho la elección.

3.15.12.1 Modos de funcionamiento

Modo Transporte

En modo transporte, sólo la carga útil (los datos que se transfieren) del paquete IP es cifrada y/o autenticada. El enrutamiento permanece intacto, ya que no se modifica ni se cifra la cabecera IP; sin embargo, cuando se utiliza la cabecera de autenticación (AH), las direcciones IP no pueden ser traducidas, ya que eso invalidaría el hash. Las capas de transporte y aplicación están siempre aseguradas por un hash, de forma que no pueden ser modificadas de ninguna manera (por ejemplo, traduciendo los números de puerto TCP y UDP). El modo transporte se utiliza para comunicaciones ordenador a ordenador.

Una forma de encapsular mensajes IPsec para atravesar NAT ha sido definidapor RFCs que describen el mecanismo de NAT-T

El propósito de este modo es establecer una comunicación segura punto a punto, entre dos hosts y sobre un canal inseguro. Este ejemplo ilustra esto:

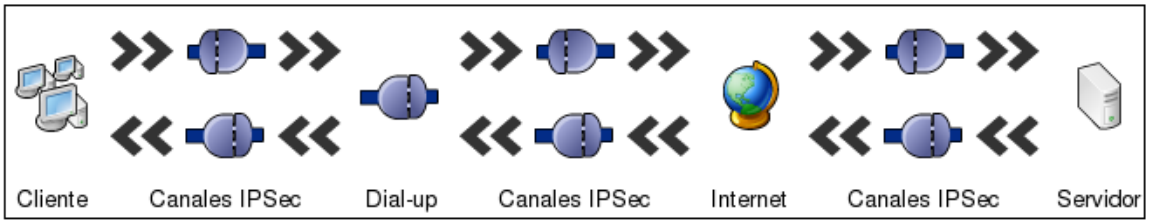

Figura 16. Encapsulamiento de los paquetes por medio de IPsec (modo transporte)
Fuente: Elaboración propia basada en las observaciones de investigación

Modo túnel

En el modo túnel, todo el paquete IP (datos más cabeceros del mensaje) es cifrado y/o autenticado. Debe ser entonces encapsulado en un nuevo paquete IP para que funcione el enrutamiento. El modo túnel se utiliza para comunicaciones red a red (túneles seguros entre routers, p.e. para VPNs) o comunicaciones ordenador a red u ordenador a ordenador sobre Internet. El propósito de este modo es establecer una comunicación segura entre dos redes remotas sobre un canal inseguro. Este ejemplo ilustra esto:

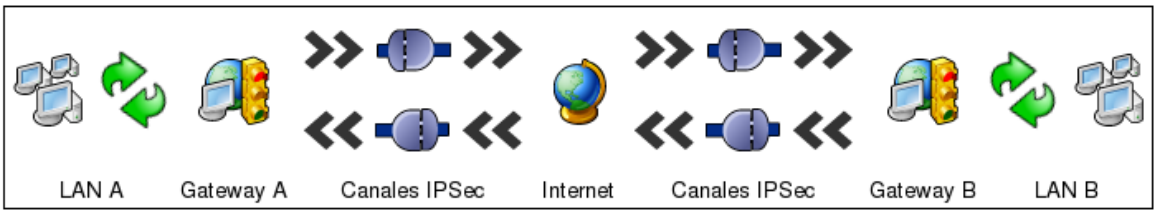

Figura 17. Encapsulamiento de los datos por medio de IPSec (Modo Túnel o VPN))
Fuente: Elaboración propia basada en las observaciones de investigación

3.17 Criptografía

3.17.1 ¿Para qué sirve la criptografía?

Para (LUCENA LÓPEZ, 1999) los seres humanos siempre han sentido la necesidad de ocultar información, mucho antes de que existieran los primeros equipos informáticos y calculadores.

Desde su creación, Internet ha evolucionado hasta convertirse en una herramienta esencial de la comunicación. Sin embargo, esta comunicación implica un número creciente de problemas estratégicos relacionados con las actividades de las empresas en la Web. Las transacciones que se realizan a través de la red pueden ser interceptadas y, sobre todo, porque actualmente, resulta difícil establecer una legislación sobre Internet. La seguridad de esta información debe garantizarse: éste es el papel de la criptografía.

3.17.2 ¿Qué es la criptografía?

La palabra criptografía es un término genérico que describe todas las técnicas que permiten cifrar mensajes o hacerlos ininteligibles sin recurrir a una acción específica. El verbo asociado es cifrar.

La criptografía se basa en la aritmética: En el caso de un texto, consiste en transformar las letras que conforman el mensaje en una serie de números (en forma de bits ya que los equipos informáticos usan el sistema binario) y luego realizar cálculos con estos números para:

- modificarlos y hacerlos incomprensibles. El resultado de esta modificación (el mensaje cifrado) se llama texto cifrado, en contraste con el mensaje inicial, llamado texto simple.
- asegurarse de que el receptor pueda descifrarlos.

El hecho de codificar un mensaje para que sea secreto se llama cifrado. El método inverso, que consiste en recuperar el mensaje original, se llama descifrado.

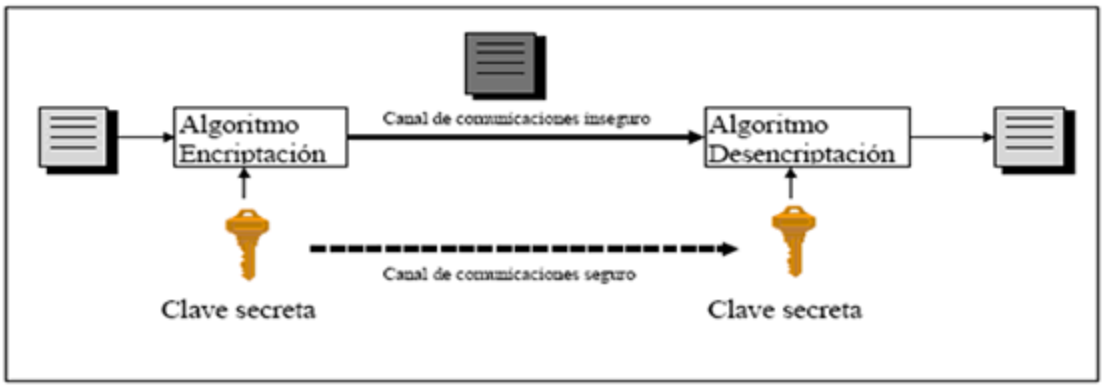

Figura 18. Ejemplo de Criptografía
Fuente: seguridadsegura.tumblr.com

Según (LUCENA LÓPEZ, 1999)El cifrado normalmente se realiza mediante una *clave de cifrado* y el descifrado requiere una *clave de descifrado*. Las claves generalmente se dividen en dos tipos:

- *Las claves simétricas*: son las claves que se usan tanto para el cifrado como para el descifrado. En este caso hablamos de cifrado simétrico o cifrado con clave secreta.
- *Las claves asimétricas*: son las claves que se usan en el caso del cifrado asimétrico (también llamado *cifrado con clave pública*). En este caso, se usa una clave para el cifrado y otra para el descifrado.

En inglés, el término *decryption* (descifrado) también se refiere al acto de intentar *descifrar en forma ilegítima* el mensaje (ya conozca o no el *atacante* la clave de descifrado).

Cuando el atacante no conoce la clave de descifrado, hablamos de **criptoanálisis** o **criptoanálisis** (también se usa el término *decodificación*).

La **cristología** es la ciencia que estudia los aspectos científicos de estas técnicas, es decir, combina la criptografía y el criptoanálisis.

3.17.3 Funciones de la Criptografía

(LUCENA LÓPEZ, 1999) Menciona que la criptografía se usa tradicionalmente para ocultar mensajes de ciertos usuarios. En la actualidad, esta función es incluso más útil ya que las comunicaciones de Internet circulan por infraestructuras cuya fiabilidad y confidencialidad no pueden garantizarse. La criptografía se usa no sólo para proteger la confidencialidad de los datos, sino también para garantizar su integridad y autenticidad.

3.17.4 Criptoanálisis

Extraído de (LUCENA LÓPEZ, 1999) indica que el **criptoanálisis** consiste en la reconstrucción de un mensaje cifrado en texto simple utilizando métodos matemáticos. Por lo tanto, todos los criptosistemas deben ser resistentes a los métodos de criptoanálisis. Cuando un método de cripto-análisis permite descifrar un mensaje cifrado mediante el uso de un cripto-sistemas, decimos que el algoritmo de cifrado ha sido decodificado.

Generalmente, se distinguen cuatro métodos de criptoanálisis:

- Un **ataque de sólo texto cifrado** consiste en encontrar la clave de descifrado utilizando uno o más textos cifrados;
- Un **ataque de texto simple conocido** consiste en encontrar la clave de descifrado utilizando uno o más textos cifrados conociendo el texto correspondiente;
- Un **ataque de texto simple elegido** consiste en encontrar la clave de descifrado utilizando uno o más textos cifrados. El atacante tiene la opción de generarlos a partir de textos simples;
- Un **ataque de texto cifrado elegido** consiste en encontrar la clave de descifrado utilizando uno o más textos cifrados. El atacante tiene la opción de generarlos a partir de los textos simples.

3.17.5 Cifrado por sustitución

El cifrado de sustitución consiste en reemplazar una o más entidades (generalmente letras) de un mensaje por una o más entidades diferentes.

Existen varios tipos de criptosistemas de sustitución:

- La **sustitución monoalfabética** consiste en reemplazar cada una de las letras del mensaje por otra letra del alfabeto.
- La **sustitución polialfabética** consiste en utilizar una serie de cifrados monoalfabéticos que son re-utilizados periódicamente.
- La **sustitución homófona** hace posible que cada una de las letras del mensaje del texto plano se corresponda con un posible grupo de caracteres distintos.
- La **sustitución poligráfica** consiste en reemplazar un grupo de caracteres en un mensaje por otro grupo de caracteres.

3.17.6 Cifrado por transposición

El método de cifrado por transposición consiste en reordenar datos para cifrarlos a fin de hacerlos ininteligibles. Esto puede significar, por ejemplo, reordenar los datos geométricamente para hacerlos visualmente inutilizables.

La técnica asiria

La técnica de cifrada asiria es, probablemente, la principal prueba de que los métodos de cifrado se utilizaron en Grecia ya en el año 600 AC para encubrir mensajes escritos en tiras de papiro.

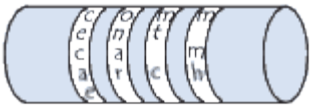

Figura 19. Ejemplo de la técnica Asiria
Fuente: http://es.ccm.net/contents/142-cifrado-de-transposicion

La técnica consiste en:

- enrollar una tira de papiro alrededor de un cilindro llamado **scytale**,
- escribir el texto a lo largo en la tira enrollada (el mensaje del ejemplo mostrado arriba es "comment ça marche").

Cuando se desenrolla el mensaje, ya no tiene significado ("cecaeonar mt c m mh"). Para descifrar el mensaje, el destinatario simplemente necesita tener un cilindro del mismo diámetro. En realidad, un descifrador de códigos (¡había descifradores de códigos en esa época!) puede descifrar el mensaje probando cilindros con una serie de diámetros diferentes; esto significa que el método puede romperse estadísticamente (los caracteres sólo tienen que tomarse uno a uno, separados por una determinada distancia).

3.17.7 Cifrado Simétrico

El cifrado simétrico (también conocido como *cifrado de clave privada* o *cifrado de clave secreta*) consiste en utilizar la misma clave para el cifrado y el descifrado.

Figura 20.Cifrado con clave simétrica
Fuente: http://www.cert.fnmt.es/curso-de-criptografia/criptografia-de-clave-simetrica

El cifrado consiste en aplicar una operación (un algoritmo) a los datos que se desea cifrar utilizando la clave privada para hacerlos ininteligibles. El algoritmo más simple (como un OR exclusivo) puede lograr que un sistema prácticamente a prueba de falsificaciones (asumiendo que la seguridad absoluta no existe).

Sin embargo, en la década de 1940, *Claude Shannon* demostró que, para tener una seguridad completa, los sistemas de clave privada debían usar claves que tengan, como mínimo, la misma longitud del mensaje cifrado. Además, el cifrado simétrico requiere que se utilice un canal seguro para intercambiar la clave y esto disminuye en gran medida la utilidad de este tipo de sistema de cifrado.

La mayor desventaja de un criptosistemas de clave secreta está relacionada con el intercambio de las claves. El cifrado simétrico se basa en el intercambio de un secreto (las claves). Surge, entonces, el problema de la distribución de las claves:

Así, un usuario que desea comunicarse con varias personas y garantizar al mismo tiempo niveles separados de confidencialidad debe utilizar el mismo número de claves privadas que de personas. Para un grupo de una cantidad *N* de personas que utilizan un criptosistemas de clave secreta, es necesario distribuir una cantidad de claves equivalente a *N* (N-1) / 2*.

En la década de 1920, Gilbert Vernam y Joseph Mauborgne desarrollaron el método *One-Time Pad* (también conocido como "One-Time Password", abreviado *OTP*), basado en una clave privada generada de forma aleatoria que se usa sólo una vez y después se destruye. En el mismo período, el Kremlin y la Casa Blanca se comunicaban a través del famoso **teléfono rojo**, un teléfono que cifraba las llamadas mediante una clave privada que utilizaba el método *one-time pad*. La clave privada se intercambiaba a través de valija diplomática (que cumplía el papel de canal seguro).

3.17.8 Cifrado Asimétrico

El principio del **cifrado asimétrico** (también conocido como **cifrado con clave pública**) apareció en 1976, con la publicación de un trabajo sobre criptografía por *Whitfield Diffie* y *Martin Hellman*.

En un criptosistemas asimétrico (o *criptosistemas de clave pública*), las claves se dan en pares:

- Una clave pública para el cifrado;
- Una clave secreta para el descifrado.

En un sistema de cifrado con clave pública, los usuarios eligen una clave aleatoria que sólo ellos conocen (ésta es la *clave privada*). A partir de esta clave, automáticamente se deduce

un algoritmo (la clave pública). Los usuarios intercambian esta clave pública mediante un canal no seguro.

Cuando un usuario desea enviar un mensaje a otro usuario, sólo debe cifrar el mensaje que desea enviar utilizando la clave pública del receptor (que puede encontrar, por ejemplo, en un servidor de claves como un directorio LDAP). El receptor podrá descifrar el mensaje con su clave privada (que sólo él conoce).

Figura 21. Cifrado Asimétrico
Fuente: http://www.cert.fnmt.es/curso-de-criptografia/criptografia-de-clave-asimetrica

Este sistema se basa en una función que es fácil de calcular en una dirección (llamada *función trapdoor de único sentido*) y que, matemáticamente, resulta muy difícil de invertir sin la clave privada (llamada *trapdoor*).

Para ilustrarlo con un ejemplo, sería como si un usuario creara de forma aleatoria una pequeña llave metálica (la clave privada) y luego produjera una gran cantidad de candados (claves públicas) que guarda en un casillero al que puede acceder cualquiera (el casillero sería el canal no seguro). Para enviarle un documento, cada usuario puede usar un candado (abierto), cerrar con este candado una carpeta que contiene el documento y enviar la carpeta al dueño de la clave pública (el dueño del candado). Sólo el dueño podrá abrir la carpeta con su clave privada.

Ventajas y Desventajas

El problema de la comunicación de la clave de descifrado ya no existe, ya que las claves públicas se pueden enviar libremente. Por lo tanto, el cifrado con clave pública permite a las personas intercambiar mensajes de cifrado sin tener que compartir un secreto.

Por otro lado, el problema consiste en asegurarse de que la clave pública que se obtiene pertenece realmente a la persona a la que desea enviar la información cifrada.

3.17 9 Firmas Electrónicas

(es.ccm.net, s.f.) El paradigma de **firmas electrónicas** (también llamadas *firmas digitales*) es un proceso que hace posible garantizar la autenticidad del remitente (función de *autenticación*) y verificar la integridad del mensaje recibido.

Las firmas electrónicas también poseen una función de reconocimiento de autoría, es decir, hacen posible garantizar que el remitente ha enviado verdaderamente el mensaje (en otras palabras, se aseguran de que el remitente no pueda negar el envío del mensaje).

3.17.10 Que es una función HASH

Como afirma (es.ccm.net, s.f.) una **función hash** es una función que hace posible obtener un hash (también llamado *resumen de mensaje*) de un texto, es decir, obtener una serie corta de caracteres que representan el texto al cual se le aplica esta función hash. La función hash debe ser tal que asocie únicamente un hash con un texto plano (esto significa que la mínima modificación del documento causará una modificación en el hash). Además, debe ser una función unidireccional, para que el mensaje original no pueda ser recuperado a partir del hash. Si existiera una forma de encontrar el texto plano desde el hash, se diría que la función hash presenta una "trapdoor".

Figura 22. Ejemplo de la función Hash
Fuente: http://armandotorreslanuza.blogspot.com/2015/02/como-funciona-el-certificado-digital.html

Tal y como lo menciona (ccm.net, 2017), puede decirse que la función hash representa la *huella digital* de un documento.

Continuando con la extracción de información de (ccm.net, 2017) , los algoritmos hash más utilizados son:

MD5 (*MD* que significa *Message Digest; en castellano, Resumen de mensaje*).

Desarrollado por Rivest en 1991, el MD5 crea, a partir de un texto cuyo tamaño es elegido al azar, una huella digital de 128 bits procesándola en bloques de 512 bits. Es común observar documentos descargados de Internet que vienen acompañados por archivos MD5: este es el hash del documento que hace posible verificar su integridad.

SHA (*Secure Hash Algorithm; en castellano, Algoritmo Hash Seguro*) crea una huella digital que tiene 160 bits de longitud.

SHA-1 es una versión mejorada de SHA que data de 1994. Produce una huella digital de 160 bits a partir de un mensaje que tiene una longitud máxima de 2^{64} bits y los procesa en bloques de 512 bits.

Al enviar un mensaje junto con su hash, es posible garantizar la integridad de dicho mensaje, es decir, el destinatario puede estar seguro de que el mensaje no ha sido alterado (intencionalmente o por casualidad) durante la comunicación.

Cuando un destinatario recibe un mensaje simplemente debe calcular el hash del mensaje recibido y compararlo con el hash que acompaña el documento. Si se falsificara el mensaje (o el hash) durante la comunicación, las dos huellas digitales no coincidirían.

3.17.11 Sellado de datos

(es.ccm.net, s.f.) Menciona que al utilizar una función hash se puede verificar que la huella digital corresponde al mensaje recibido, pero nada puede probar que el mensaje haya sido enviado por la persona que afirma ser el remitente.

Para garantizar la autenticidad del mensaje, el remitente simplemente debe cifrar (generalmente decimos *firmar*) el hash utilizando su clave privada (el *hash firmado* se denomina **sello**) y enviar el sello al destinatario.

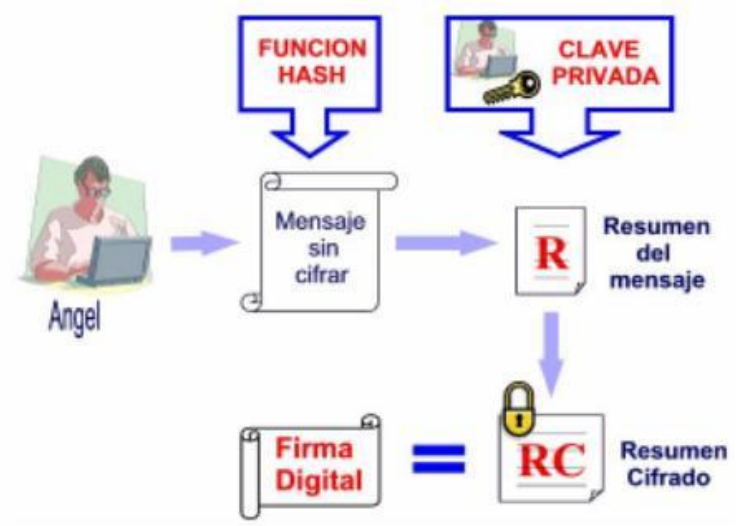

Figura 23. Ejemplo del sellado de datos en la función Hash
Fuente: http://firmaelectronica.gob.es/Home/Ciudadanos/Certificados-Electronicos.html#certificado_electronico

Al recibir el mensaje, el destinatario deberá descifrar el sello con la clave pública del remitente, luego deberá comparar el hash obtenido con la función hash del hash recibido como adjunto. Esta función de creación de sellos se llama *sellado.*

3.18 Certificados

(es.ccm.net, s.f.) Los algoritmos de cifrado asimétrico se basan en el hecho de compartir una clave pública entre varios usuarios. En general, esta clave se comparte mediante un directorio electrónico (normalmente en formato LDAP) o una página Web.

Sin embargo, este modo de compartir presenta un inconveniente importante: **nada garantiza que la clave pertenezca al usuario con el que está asociada**. Un hacker puede corromper la clave pública que aparece en el directorio remplazándola con su propia clave pública. Por consiguiente, el hacker podrá descifrar todos los mensajes que se cifraron con la clave que aparece en el directorio.

Un certificado permite asociar una clave pública con una entidad (una persona, un equipo, etc.) para garantizar su validez. El certificado es como la tarjeta de identificación de la clave, emitida por una entidad llamada *Entidad de certificación* (que frecuentemente se abrevia **CA**, por sus siglas en inglés).

La entidad de certificación es responsable de emitir los certificados, de asignarles una fecha de validez (similar a la fecha de vencimiento de los alimentos) y de revocarlos antes de esta fecha en caso de que la clave (o su dueño) estén en una situación de riesgo.

3.18.1 Estructura de los certificados

Según (es.ccm.net, s.f.) Los certificados son pequeños archivos divididos en dos partes:

- La parte que contiene la información.
- La parte que contiene la firma de la entidad de certificación.

La estructura de los certificados está estandarizada por la norma **X.509** (más precisamente, X.509v3) de la UIT, que define la información que contiene el certificado:

- La versión de X.509 a la que corresponde el certificado;
- El número de serie del certificado;
- El algoritmo de cifrado utilizado para firmar el certificado;
- El nombre (DN, siglas en inglés de *Nombre distinguido*) de la entidad de certificación que lo emite;
- La fecha en que entra en vigencia el certificado;
- La fecha en que finaliza el período de validez del certificado;
- El objeto de utilización de la clave pública;
- La clave pública del dueño del certificado;
- La firma del emisor del certificado (*huella digital*).

La entidad de certificación firma toda esta información (información + clave pública del solicitante) y esto implica que una función hash crea una huella digital de esta información y luego este hash se cifra con la clave privada de la entidad de certificación. La clave pública se distribuye antes de tiempo para permitir a los usuarios verificar la firma de la *entidad de certificación* con su clave pública.

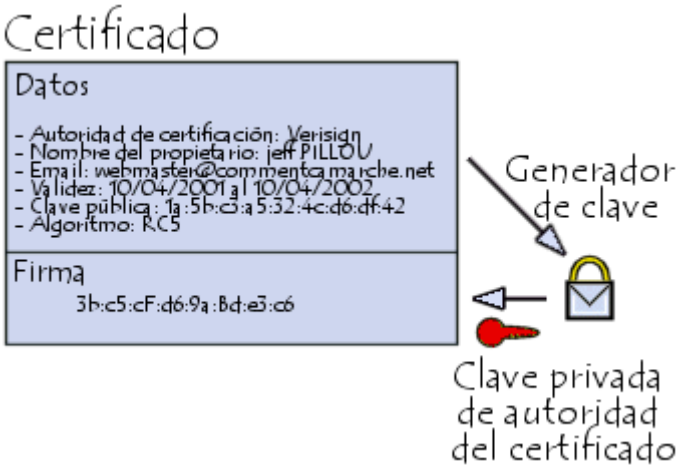

Figura 24. Estructura de un certificado digital
Fuente: http://es.ccm.net/contents/124-certificados

Cuando un usuario desea comunicarse con otra persona, sólo debe obtener el certificado del receptor. Este certificado contiene el nombre y la clave pública del receptor, y está firmado por la entidad de certificación. De esta forma, es posible verificar la validez del mensaje aplicando, primero, la función hash a la información contenida en el certificado y, segundo, descifrando la firma de la entidad de certificación con la clave pública y comparando los dos resultados.

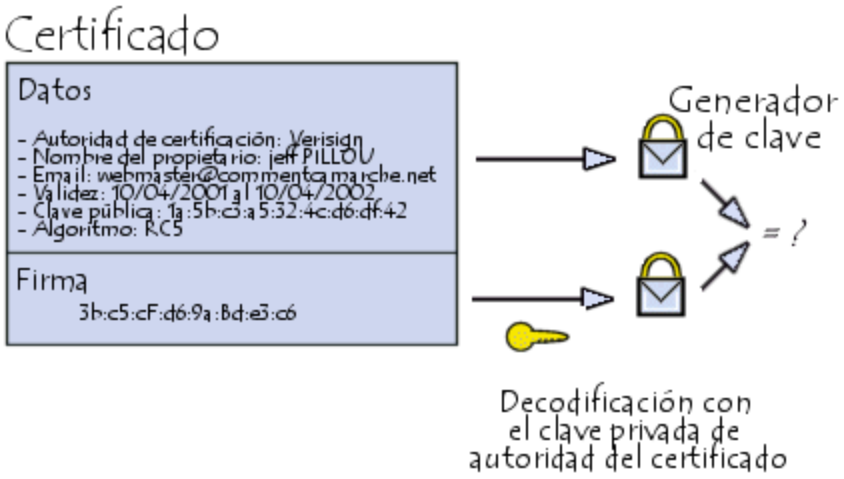

Figura 25. Decodificación de un certificado digital
Fuente: http://es.ccm.net/contents/124-certificados

3.18.2 Firmas del certificado

Como afirma (ccm.net, 2017) Existen varios tipos de certificados en función del nivel de sus firmas:

- **Los certificados firmados localmente** son certificados de uso interno. Al estar firmados por un servidor local, este tipo de certificados permiten garantizar los

intercambios confidenciales dentro de una organización, por ejemplo, en una Intranet. Los certificados firmados localmente se pueden usar para autentificar usuarios.

- **Los certificados firmados por una entidad de certificación** son necesarios cuando se deben garantizar los intercambios seguros con usuarios anónimos, por ejemplo, en el caso de una página Web segura al que pueda acceder el público general. La certificación de un tercero garantiza al usuario que el certificado pertenece efectivamente a la organización a la que dice pertenecer.

3.18.3 Tipos de uso

Los certificados se utilizan principalmente en tres tipos de contextos:

- **Los certificados de cliente** se almacenan en la estación de trabajo del usuario o se integran en un contenedor como una tarjeta inteligente, y permiten identificar a un usuario y asociarlo con ciertos privilegios. En la mayoría de los casos, se transmiten al servidor cuando se establece una conexión y el servidor asigna privilegios en función de la acreditación del usuario. Son verdaderas tarjetas de identificación digitales que usan un par de claves asimétricas con una longitud de 512 a 1024 bits.

- **Los certificados de servidor** se instalan en un servidor Web y permiten conectar un servicio con el dueño del servicio. En el caso de página Web, permiten garantizar que la dirección URL de la página Web y especialmente su dominio pertenece realmente a tal o cual compañía. También permiten proteger las transacciones con usuarios gracias al protocolo SSL.
- **Los certificados VPN** (Red privada virtual) se instalan en un equipo de red y permiten cifrar flujos de comunicación de extremo a extremo entre dos puntos (por ejemplo, dos ubicaciones de una compañía). En este tipo de escenario, los usuarios tienen un certificado cliente, los servidores aplican un certificado de servidor y el equipo de comunicación usa un certificado especial (generalmente un certificado IPsec).

3.19 Firewall (Cortafuergos)

Cada computadora que se conecta a internet (y, básicamente, a cualquier red de computadoras) puede ser víctima del ataque de un hacker. La metodología que generalmente usan los hackers consiste en analizar la red (mediante el envío aleatorio de paquetes de datos) en busca de una computadora conectada. Una vez que encuentra dicha computadora, el hacker busca un punto débil en el sistema de seguridad para explotarlo y tener acceso a los datos de la máquina.

Por muchas razones, esta amenaza es aún mayor cuando la máquina está permanente conectada a Internet:

- Es probable que la máquina elegida esté conectada pero no controlada.
- Generalmente, la máquina conectada que se elige posee un ancho de banda más elevado.
- La máquina elegida no cambia las direcciones IP o lo hace muy ocasionalmente.

Por lo tanto, es necesario que tanto las redes de las compañías como los usuarios de Internet con conexiones por Fibra Óptica, enlaces de cobre simétricos, cable o ADSL se protejan contra intrusiones en la red instalando un dispositivo de protección.

Según (es.ccm.net, s.f.) Un **firewall** es un sistema que protege a una computadora o a una red de computadoras contra intrusiones provenientes de redes de terceros (generalmente desde Internet). Un sistema de firewall filtra paquetes de datos que se intercambian a través de Internet. Por lo tanto, se trata de un conjunto de filtros que comprende al menos las siguientes interfaces de red:

- una interfaz para la red protegida (red interna).
- una interfaz para la red externa.

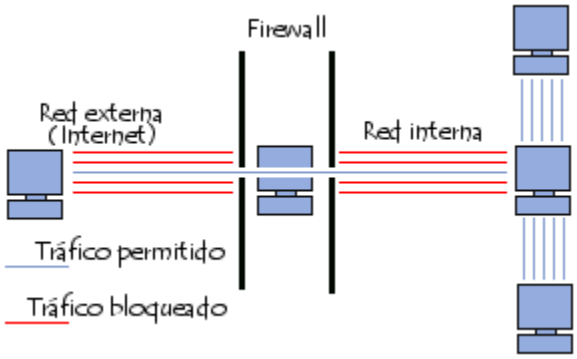

Figura 26. Ejemplo de un Firewall
Fuente: http://es.ccm.net/contents/590-firewall

El sistema firewall es un sistema de software, comúnmente embebido un hardware de red dedicado, que actúa como intermediario entre la red local (computadora local) y una o más redes externas. Un sistema de firewall puede instalarse en servidores que utilicen cualquier sistema siempre y cuando:

- La máquina tenga capacidad suficiente como para procesar el tráfico
- El sistema sea seguro
- No se ejecute ningún otro servicio más que el servicio de filtrado de paquetes en el servidor

Como funciona un firewall

Un sistema firewall contiene un conjunto de reglas predeterminadas que le permiten al sistema:

- Autorizar la conexión (*permitir*)
- Bloquear la conexión (*denegar*)
- Rechazar el pedido de conexión sin informar al que lo envió (*negar*)

Todas estas reglas implementan un método de filtrado que depende de la **política de seguridad** adoptada por la organización. Las políticas de seguridad se dividen generalmente en dos tipos que permiten:

- la autorización de sólo aquellas comunicaciones que se autorizaron explícitamente: "Todo lo que no se ha autorizado explícitamente está prohibido"
- el rechazo de intercambios que fueron prohibidos explícitamente

El primer método es sin duda el más seguro. Sin embargo, impone una definición precisa y restrictiva de las necesidades de comunicación.

Filtrado de paquetes

(es.ccm.net, s.f.) Un sistema de firewall opera según el principio del filtrado simple de paquetes, o *filtrado de paquetes stateless*. Analiza el encabezado de cada paquete de datos (*datagrama*) que se ha intercambiado entre un ordenador de red interna y un ordenador externo.

Así, los paquetes de datos que se han intercambiado entre un ordenador con red externa y uno con red interna pasan por el firewall y contienen los siguientes encabezados, los cuales son analizados sistemáticamente por el firewall:

- La dirección IP del ordenador que envía los paquetes
- La dirección IP del ordenador que recibe los paquetes
- El tipo de paquete (TCP, UDP, etc.)
- El número de puerto (recordatorio: un puerto es un número asociado a un servicio o a una aplicación de red).

Las direcciones IP que los paquetes contienen permiten identificar el ordenador que envía los paquetes y el ordenador de destino, mientras que el tipo de paquete y el número de puerto indican el tipo de servicio que se utiliza.

Regla	Acción	IP fuente	IP destino	Protocolo	Puerto fuente	Puerto destino
1	Aceptar	192.168.10.20	194.154.192.3	tcp	cualquiera	25
2	Aceptar	cualquiera	192.168.10.3	tcp	cualquiera	80
3	Aceptar	192.168.10.0/24	cualquiera	tcp	cualquiera	80
4	Negar	cualquiera	cualquiera	cualquiera	cualquiera	cualquiera

Figura27. Ejemplo de reglas de Firewall
Fuente: http://es.ccm.net/contents/590-firewall

Los puertos reconocidos (cuyos números van del 0 al 1023) están asociados con servicios ordinarios (por ejemplo, los puertos 25 y 110 están asociados con el correo electrónico y el puerto 80 con la Web o procesos de sistema) por otro lado existen los puertos registrados (cuyos números van del 1024 al 49151) y por último los puertos dinámicos y/o privados (cuyos números van del 49152 al 65535). La mayoría de los dispositivos de firewall se configuran al menos para filtrar comunicaciones de acuerdo con el puerto que se usa. Normalmente, se recomienda bloquear todos los puertos que no son fundamentales (según la política de seguridad vigente).

Por ejemplo, el puerto 23 a menudo se bloquea en forma predeterminada mediante dispositivos de firewall, ya que corresponde al protocolo TELNET, el cual permite a una

persona emular el acceso terminal a una máquina remota para ejecutar comandos a distancia. Los datos que se intercambian a través de TELNET no están codificados. Esto significa que es probable que un hacker observe la actividad de la red y robe cualquier contraseña que no esté codificada. Generalmente, los administradores prefieren el protocolo SSH, el cual tiene la reputación de ser seguro y brinda las mismas funciones que TELNET.

Limitaciones del firewall

Por supuesto que los sistemas firewall no brindan seguridad absoluta; todo lo contrario. Los firewalls sólo ofrecen protección en tanto todas las comunicaciones salientes pasen sistemáticamente a través de éstos y estén configuradas correctamente. Los accesos a la red externa que sortean el firewall también son puntos débiles en la seguridad. Claramente, éste es el caso de las conexiones que se realizan desde la red interna mediante cualquier enlace (Fibra Óptica, Simétrico, ADSL, etc.) de conexión que evite el firewall.

Asimismo, la adición de medios externos de almacenamiento a los ordenadores de sobremesa o portátiles de red interna puede dañar enormemente la política de seguridad general.

Para garantizar un nivel máximo de protección, debe ejecutarse un firewall en la computadora y su registro de actividad debe controlarse para poder detectar intentos de intrusión o anomalías. Además, se recomienda controlar la seguridad (por ejemplo,

inscribiéndose para recibir alertas de seguridad de CERT) a fin de modificar los parámetros del dispositivo de firewall en función de las alertas publicadas.

La instalación de un firewall debe llevarse a cabo de la mano de una política de seguridad real.

3.20 DMZ (Zona desmilitarizada)

Continuando con términos referentes a la investigación, me pareció importante analizar y agregar el término DMZ, el cual consiste en la segmentación de una red de producción hacia servicios que se brindan en Internet, por lo tanto, es importante tomarla en cuenta porque esta zona conlleva a muchos controles optimizados para que la plataforma trabaje adecuadamente en un ambiente de seguridad.

Concepto de Aislamiento

Según (es.ccm.net, s.f.) Los sistemas *Firewall* permiten definir las reglas de acceso entre dos redes. Sin embargo, en la práctica, las compañías cuentan generalmente con varias sub-redes con diferentes políticas de seguridad. Por esta razón, es necesario configurar arquitecturas de firewall que aíslen las diferentes redes de una compañía. Esto se denomina "**aislamiento de la red.**"

3.20.1 Arquitectura DMZ

Respecto a la arquitectura, depende mucho del desarrollo inicial y los servicios que se brindaban, se entiende que las tecnologías se han venido desarrollando de una manera inesperada, es por esto que cuando hay que realizar cambios pensados en seguridad se corrigen muchas ineficiencias y conllevan a trabajos más controlados, (ccm.net, 2017) menciona que algunas máquinas de la red interna deben ser accesibles desde una red externa (servidores web, servidores de correo electrónico, servidores FTP), a veces es necesario crear una nueva interfaz hacia una red separada a la que se pueda acceder tanto desde la red interna como por vía externa sin correr el riesgo de comprometer la seguridad de la compañía. El término "**zona desmilitarizada**" o **DMZ** hace referencia a esta zona aislada que posee aplicaciones disponibles para el público. La DMZ actúa como una "zona de búfer" entre la red que necesita protección y la red hostil.

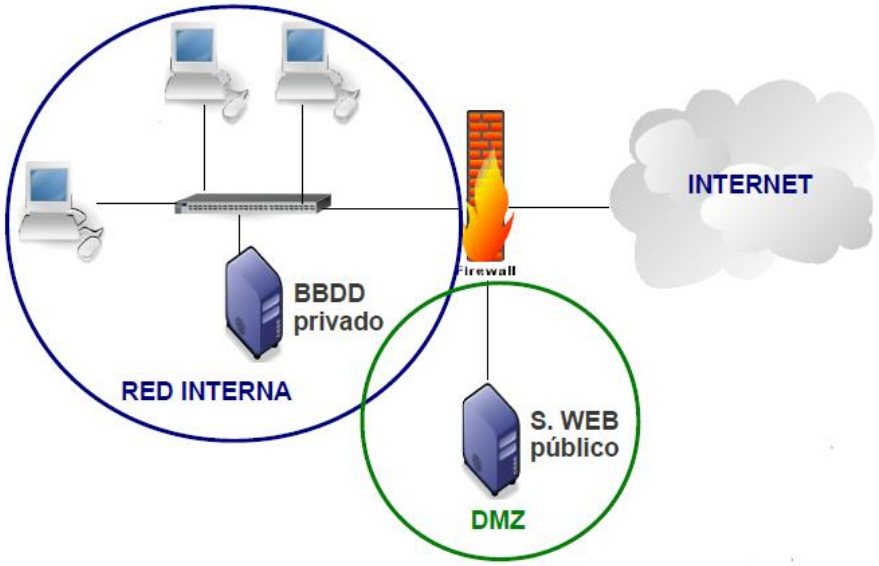

Figura 28. Estructura DMZ
Fuente: Elaboración propia basada en las observaciones de la investigación

Continuando con los términos, (es.ccm.net, s.f.) Afirma que los servidores en la DMZ se denominan "**anfitriones bastión**" ya que actúan como un puesto de avanzada en la red de la compañía.

Por lo general, la política de seguridad para la DMZ es la siguiente:

- El tráfico de la red externa a la DMZ está **autorizado**
- El tráfico de la red externa a la red interna está **prohibido**
- El tráfico de la red interna a la DMZ está **autorizado**
- El tráfico de la red interna a la red externa está **autorizado**

- El tráfico de la DMZ a la red interna está **prohibido**
- El tráfico de la DMZ a la red externa está **denegado**

De esta manera, la DMZ posee un nivel de seguridad intermedio, el cual no es lo suficientemente alto para almacenar datos imprescindibles de la compañía.

Debe observarse que es posible instalar las DMZ en forma interna para aislar la red interna con niveles de protección variados y así evitar intrusiones internas.

4. Marco Metodológico

4.1Tipo de Investigación

Esta investigación es de alcance descriptivo ya que comprende la descripción, registro, análisis e interpretación de la naturaleza actual, y la composición o procesos de los fenómenos. El enfoque se hace sobre conclusiones dominantes o sobre como una persona, grupo se conduce o funciona en el presente. (Hernández, Fernandez, & Baptista, 2010).

La investigación descriptiva trabaja sobre realidades de hechos, y su característica fundamental es la de presentarnos una interpretación correcta. Básicamente, se dirigen a la descripción de fenómenos sociales o educativos, en una circunstancia temporal y especial determinada. Los diferentes niveles de investigación difieren en el tipo de pregunta que pueden formular. Las interrogaciones están guiadas por esquemas descriptivos y taxonomías; sus preguntas se enfocan hacia las variables de los sujetos o de la situación.

En este estudio se selecciona una serie de cuestiones y se mide cada una de ellas independientemente, para así describir lo que se investiga. Los estudios descriptivos miden de forma más independiente los conceptos o variables a los que se refieren, es decir, miden con la mayor precisión posible.

4.2 Enfoque

En el caso específico de esta investigación, se utilizó la forma descriptiva, ya que se busca especificar las propiedades importantes que puede dar una nueva estrategia de Seguridad en la plataforma tecnológica del Ministerio de Seguridad.

Con un diseño transaccional descriptivo, el cual tiene como características propias basarse en hechos, describir de forma sistemática y precisa una situación o área de interés. Aportando por último el reporte de lo que brindan estos datos, ya sea de manera escrita como gráfica.

Este trabajo de investigación se sitúa en este tipo de investigación por diferentes razones, algunas de ellas son:

- Se recolectarán datos sobre operación y gestión de la Seguridad en la plataforma tecnológica del Ministerio de Seguridad.
- Se desarrolla el diseño de una estrategia para la implementación de un programa de Seguridad Informática basado en estándares que brindan información técnica y requisitos de cómo establecer, implantar un diseño de Seguridad tales como: ISO 27001, NIST Serie 800, Cobit 5, SANS.org etc.

Cabe señalar que las variables y conceptos a utilizar, se manejan en forma independiente, permitiendo una medición con la mayor precisión posible.

4.3 Ubicación

El proyecto está enfocado, de manera primordial, hacia la implementación en la plataforma tecnológica del Ministerio de Seguridad.

4.4 Medios e Instrumentos

Toda medición o instrumento de recolección de los datos debe reunir dos requisitos esenciales, confiabilidad y validez.

La confiabilidad de un instrumento de medición se refiere al grado en que su aplicación repetida al mismo sujeto u objeto produce iguales resultados.

Para determinar la magnitud del impacto se realizó un análisis detallado del estado actual de la Postura de Seguridad, en lo que respecta al desarrollo de la estrategia en la plataforma tecnológica del Ministerio de Seguridad, además se incluyeron cada uno de los factores u elementos vinculados a éste. Para ello se realizaron los siguientes procedimientos de recolección de datos:

- **Observación**: por medio de la observación, se pueden identificar características importantes en el campo estudiado. Es esencial documentar debidamente todos los hallazgos para que puedan ser utilizados en la fase de análisis.
- **Entrevistas**: por medio de esta técnica se solicita información relacionada con la Postura de Seguridad, así como el conocimiento y madurez actual. Adicionalmente, se hacen preguntas que ayuden a identificar los requerimientos del proyecto.
- **Grupos de Enfoque**: a través de esta técnica el investigador trata de comprender e interpretar el ambiente en el que se desarrolla la investigación por medio de los participantes. En este caso, específicamente sobre gestores de Seguridad en la plataforma tecnológica.
- **Revisión de Documentación Histórica**: la Institución contiene documentación de procesos y configuraciones, que son revisados con el fin de extraer la información relevante a la investigación.

4.5 Población

Durante la investigación, se estuvo en contacto con las personas que pueden proveer información de importancia relacionada con el tema.

- Directora de Tecnologías de Información.
- Administradores de Red
- Administradores de Seguridad

4.6 Tipo de Población utilizada

Para el presente estudio, se tomaron dos variedades de poblaciones; en este caso se refiere como poblaciones a las plataformas detectadas y las cuales tienen la función de gestión de Seguridad en la plataforma tecnológica del MSP.

La investigación posee una población infinita, ya que la implementación del programa no tiene un tiempo establecido o limitado y de la cual se obtiene la información para estimar lo pertinente a los objetivos de la misma, en donde la característica principal es que es una implementación importante y heterogénea.

4.7 Muestra

Cuando la población es muy grande (véase como políticas, procesos y controles establecidos que regulan las plataformas), es obvio que la observación de todos los elementos se dificulte en cuanto al trabajo, tiempo y costo necesario para hacerlo. Para

solucionar este inconveniente se utilizan normativas y buenas prácticas con el fin de proceder con el programa que se adapte a la plataforma actual.

El estudio de muestras es más sencillo que el estudio de la población completa; cuesta menos y lleva menos tiempo. Por último, se ha aprobado, que el examen de una población entera todavía permite la aceptación de elementos defectuosos, por tanto, en algunos casos, el muestreo puede elevar el nivel de calidad.

Una muestra representativa contiene las características relevantes de la población en las mismas proporciones que están incluidas en tal población.

Los expertos en estadística recogen datos de una muestra. Utilizan esta información para hacer referencias sobre la población que está representada por la muestra. En consecuencia, muestra y población son conceptos relativos. Una población es un todo y una muestra es una fracción o segmento de ese todo.

4.8 Tipos de muestras

Se categorizan en dos grandes ramas: las muestras no probalísticas y las muestras probalísticas.

En las muestras no probalísticas, la elección de los elementos no depende de la probabilidad, sino de causas relacionadas con las características del investigador o del que hace la muestra. Elegir entre una muestra probalísticas y no probalísticas depende de los

objetivos de la investigación, en el esquema de las misma y de la contribución que se piensa hacer con ella.

En las muestras probalísticas existe la ventaja de que puede medirse el tamaño del error en las predicciones, son esenciales en los diseños de investigación por encuestas en las que se pretende hacer estimaciones de variables en la población, se miden con instrumentos de medición y se analizan con pruebas estadísticas para el análisis de datos. En las muestras probalísticas todos los elementos tienen la misma probabilidad de ser elegidos.

4.9 Descripción de la población y de la muestra

El trabajo rodea la comprensión de las plataformas y de la gestión de Seguridad de Sistemas del Ministerio para el proceso de la información que se gestiona a través del mismo. La muestra a emplear se obtienen diversas pruebas, así mismo, es posible la gestión de datos dentro de registros manipulados y obtenidos.

4.10 Recolección de la información o datos obtenidos

La información a emplear se obtuvo mediante el compendio de diversa documentación; recopilación de datos, artículos en Internet, análisis de diferentes documentos y sobre todo la experiencia del investigador. Así como la información que se obtuvo de manera

presencial a través de encuestas y reuniones gestionadas durante la evolución o desarrollo del proyecto.

4.11 Procesamiento de la Información

La información se procesó acorde a la situación actual y en la valoración de diferentes normas que se integran al programa propuesto. Así como un análisis de los datos obtenidos en las encuestas, se hizo el uso del procesador de texto de Word y para la tabulación o estratificación de los datos se utilizó la herramienta de Excel en ciertos mecanismos.

Se procedió a agrupar las capturas de procesos con el objetivo de determinar que las mismas correspondan a la integración con la muestra definida. Se tabularon los datos y resultados de cada una de las capturas, procesando los resultados como un procedimiento, una vez realizado este punto, se procede a totalizar cada una de las variables de estudio y se define el proceso para obtención de una nota por variable.

5. Propuesta

5.1 Descripción y Metodología

En esta sección se describe de forma general el proceso de la implementación. Esta propuesta está basada principalmente en mejorar la plataforma tecnológica del Ministerio de Seguridad Pública en cuanto a la gestión y procesos de Seguridad Informática, la propuesta se enfoca en la creación de una nueva área de gestión de seguridad informática por lo cual, se presenta información relevante basada en la investigación para poder desarrollarlo. Básicamente, se extrae la información respectiva de procesos que se ejecutan actualmente y cómo se están cubriendo las brechas de Seguridad Cibernética.

Se realiza un análisis detallado de las plataformas que gestionan la seguridad y se realizan observaciones que pueden tratarse de brechas que no están siendo cubiertas por la gestión actual.

Para este desarrollo se necesita desarrollar cuatro 4 fases, para cada una de ellas se detalla la situación actual y el proceso a seguir para la implementación del programa con ayuda de los marcos y normas expuestas en el Marco Teórico.

5.2 Estructura de Seguridad actual

La topología de red del MSP se ha venido mejorando en los últimos años, sin embargo, la gestión de Seguridad ha sido ambigua, no se cuenta con políticas, controles y metodologías de gestión de Riesgos sobre los activos de la información, así como un análisis de riesgo previo a la adquisición de plataformas de Seguridad, por lo tanto, se denotan los aspectos más importantes del estado actual y se muestra la topología de red del MSP para un mejor entendimiento de la implementación.

Aunado a lo anterior, no existen procesos de gestión de cambios documentados, así como hallazgos de auditorías que puedan corregir malas configuraciones o bien ciertas implementaciones podrían estar relacionadas con problemas continuos y que no hayan sido detectados.

En cuanto a políticas se encontró que únicamente existe un documento general llamado Reglamento de Normas y Políticas de las Tecnologías de Información del Ministerio de Seguridad Publica, decreto ejecutivo que cubre una cierta parte en cuanto a la regulación de seguridad respecta, además no existe recurso humano desempeñando y desarrollando documentación de buenas prácticas y políticas que puedan corregir procesos de seguridad, así como creando líneas base de configuración, cambios, etc.

En cuanto a lo anterior, se conoce que la gestión de Seguridad para toda la plataforma del Ministerio recae sobre el Departamento de Telemática, donde se realizan las instalaciones y

configuraciones de los equipos, sin embargo, no existen líneas base de configuración, así como bancos de datos para consultas de diferentes configuraciones.

Figura 29. Nueva Propuesta de Organigrama de la Dirección de Tecnologías de la Información
Fuente: Elaboración propia basada en las observaciones de la investigación

Con esto se valida que actualmente no existe una sección específica que gestione la seguridad propiamente en el Ministerio de Seguridad Pública, al contrario, las funciones son combinadas con Telemática y algunas otras plataformas como el Antivirus Corporativo y el Directorio Activo se gestionan en el Departamento de Soporte.

5.3 Plataformas de Seguridad actuales

Actualmente, la seguridad del Ministerio de Seguridad recae única y exclusivamente sobre las siguientes plataformas:

5.3.1 Plataforma Firewall NGFW Fortinet 3600C

El cual tiene las siguientes funciones:

1. Firewall Perimetral (Protección servicios en la nube –página web, servidor de correo electrónico, protección sobre sub-red DMZ).
2. Firewall de segmentación entre sub-redes (DMZ, LAN, enlaces dedicados con otras instituciones).
3. Concentrador de sub-redes VPN (comunicación con Delegaciones Policiales).
4. Firewall de filtrado Web para acceso al servicio de Internet, mediante grupos de Internet justificados.
5. Firewall IPS
6. Firewall IDS

El Equipo anterior cuenta con un alto nivel de riesgo por cuanto tiene a su disposición un alto procesamiento de módulos de protección y no cuenta con una contingencia o alta disponibilidad.

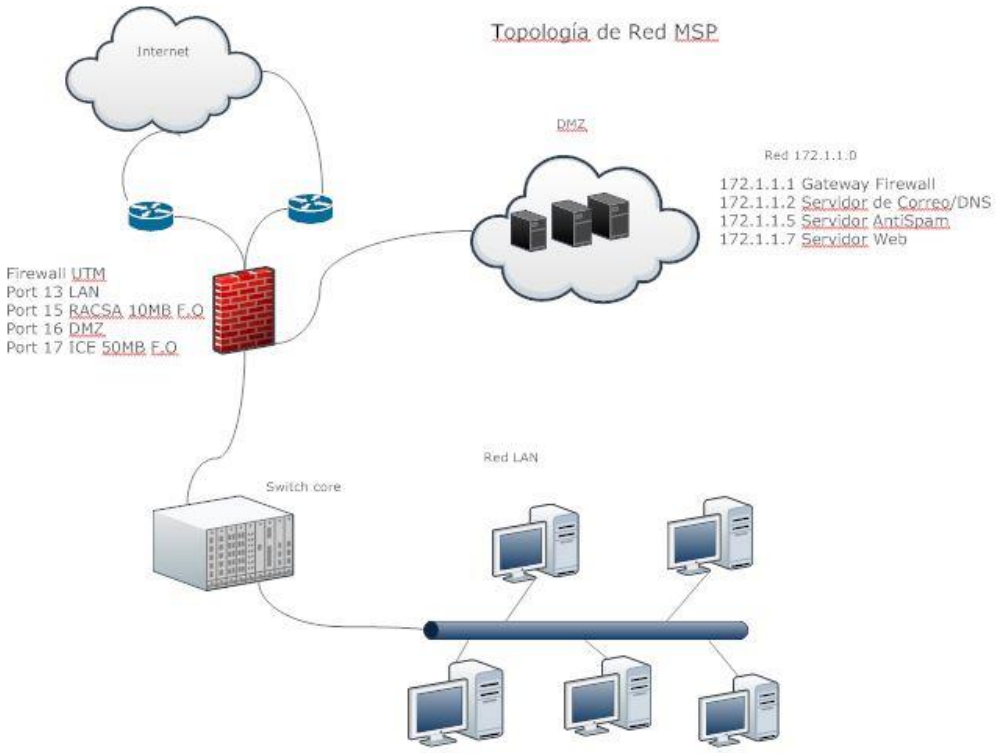

Figura 30. Protección Firewall NGFW-MSP Fortinet 3600C
Fuente: Elaboración propia basada en las observaciones de la investigación

Como lo muestra la figura 34, se denotan las interfaces configuradas en el firewall corporativo, cada interfaz con su respectiva tarea y políticas de filtrado.

En lo que se refiere a la topología de seguridad de red actual, a continuación, las principales políticas de firewall en servicios críticos:

- Corresponde a las políticas de los servidores Web cuyos alias es Servidor_Matina_VM, Correo Electrónico cuyo alias es Servidor_SarapiquiDMZ y DNS cuyo alias es Servidor_SarapiquiDMZ, incluye la interface origen y la interface saliente, además sus respectivos servicios y la acción correspondiente.

En la figura 35 se muestran las políticas de los servidores actuales (extraídas del Firewall Fortinet 3600C).

Figura 31. Política en firewall Interface DMZ a Internet RACSA
Fuente: Políticas extraídas Firewall Perimetral Fortinet 3600C

En este caso, se ha realizado una consulta al dominio www.seguridadpublica.go.cr para validar el respectivo módulo de seguridad, en este caso el https, el cual debería de presentar un certificado a nivel de encripción para la protección del trasiego de datos cuando se accesa a la pagina web del MSP por medio de un navegador web.

Como se logra obervar en la figura 30, el Ministerio no ha implementado una arquitectura de certificados mediante una Autoridad Certificadora, tal como se explica en el capítulo 3.18.3 de este trabajo: *"**Los certificados de servidor** se instalan en un servidor Web y permiten conectar un servicio con el dueño del servicio. En el caso de página Web, permiten garantizar que la dirección URL de la página Web y especialmente su dominio pertenece realmente a tal o cual compañía. También permiten proteger las transacciones con usuarios gracias al protocolo SSL."*

Figura 32. Página Web del Ministerio de Seguridad Pública
Fuente: URL www.seguridadpublica.go.cr

Continuando,con la revisión a nivel de políticas de Firewall, en la figura 37 se muestra la política actual de los servidores DNS y Correo Electrónico del MSP.

Figura 33. Política en firewall del Servidor DNS del MSP
Fuente: Políticas extraídas Firewall Perimetral Fortinet 3600C

Se observan los servicios brindados (DNS, SMTP), así como la opción NAT habilitada, la cual hace referencia a que dichos servidores se publican en Internet a través de una IP Pública perteneciente al pool de RACSA y la cual se menciona en la interface vista en la figura 35.

Todas estas políticas no se encuentran documentadas, para los cambios sobre algunas de ellas no existe una documentación que permita un cambio controlado, dentro del programa se recomienda mantener un inventario, y de ser posible realizar un análisis de riesgo que permita obtener controles reales sobre estas políticas.

En la figura 38 se muestra la política del servidor Web del MSP actual.

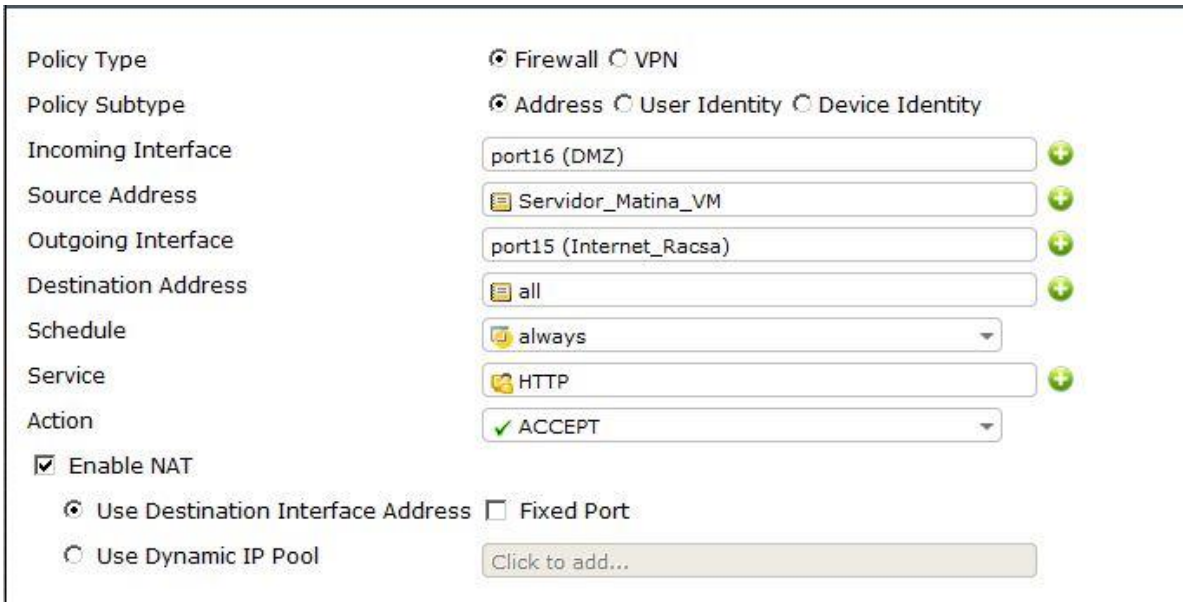

Figura 34. Política en Firewall del servidor web del MSP
Fuente: Políticas extraídas Firewall Perimetral Fortinet 3600C

Se observa el servicio brindado (HTTP), así como la opción NAT habilitada, la cual hace referencia a que dicho servidor se publica en Internet a través de una IP pública perteneciente al *pool* de RACSA y la cual se menciona en la interface vista en la figura 34.

- Corresponde a las políticas inversas (entrante - *inbound*) de los servidores Web cuyo alias es Servidor_Matina_VM, Correo Electrónico cuyo alias es Servidor_SarapiquiDMZ y DNS cuyo alias es Servidor_SarapiquiDMZ, incluye la interface origen y la interface saliente, además sus respectivos servicios permitidos y la acción correspondiente.

En la figura 39 se muestran las políticas (entrantes) de los servidores actuales del MSP.

Figura 35 Política en firewall (entrante - inbound) de los servidores del MSP
Fuente: Políticas extraídas Firewall Perimetral Fortinet 3600C

En este caso se logran observar las políticas en firewall, así como los sensores de protección en modo "default" los cuales no se encuentran revisados ni comparados contra ninguna línea base de protección, así como los objetos de firewall no se encuentran debidamente documentados, bajo un criterio de riesgo.

5.3.2 Plataforma Antivirus Corporativo Kaspersky Endpoint Security

Esta plataforma tiene las siguientes funciones:

1. Servidor Virtual que contiene todas las políticas y grupos de equipos que contienen un cliente de protección instalado.
2. Contiene tareas de escaneos programados en laptops, desktops, servidores
3. Contenedor de firmas de actualización contra protección de malware, rootkits, virus, etc.

5.3.3 Plataforma AntiSPAM –IMSVA Trend Micro

La plataforma Antispam tiene las siguientes funciones:

1. Políticas de filtrado de tráfico de correo malicioso o basura.
2. Actualizaciones con firmas en la nube (TrendMicro).
3. Listas negras de IP's sospechosas.

5.3.4 Plataforma de Directorio Activo (Active Directory)

El Directorio Activo tiene las siguientes funciones:

1. Autenticación de usuario en red o equipo.
2. Recursos que pueden accesar los usuarios.
3. Registro de las acciones de un usuario o grupo en el registro de eventos.
4. La pertenencia a un grupo.
5. Directivas de configuración de seguridad.
6. Configuraciones por medio de GPO's.

5.3.5 Plataforma de Virtual LAN (VLAN)

En cuanto a la plataforma de red virtual, esta tiene las siguientes funciones:

1. Segmentación de sub-redes (Módulo de Recursos Humanos, Módulo de Fuerza Pública, Módulo de Ministro, Módulo de PCD, Módulo de Dirección Informática, Módulo de ENP).
2. Habilitación de puertos y servicios entre recursos compartidos en red.
3. Aislamiento entre módulos.

5.4 Diseño de la estrategia para la creación del Programa de Seguridad Informática

En este apartado, se citan los pasos a seguir para el diseño, así como la estructura.

Para la implementación del programa, es necesario conocer los componentes que pueden fortalecer una Arquitectura de Seguridad, por esta razón se identifican los parámetros siguiendo las ventajas que ofrecen los marcos de trabajo y normas de ciberseguridad.

Aunado a lo anterior, en la recopilación de información se ha realizado un cuestionario para medir la postura de Seguridad actual, este cuestionario se basó en 6 aristas:

- Clasificación y Control de Activos
- Información de Seguridad de Red
- Información de Sistemas
- Análisis de Amenazas
- Control de Accesos
- Información de Servicios

Por lo anterior, para la creación del programa se utilizan las siguientes Normas y marcos de trabajo, con el fin implementar de manera adecuada el Programa de Seguridad.

Normas, marcos de trabajo / Parámetros CS	ISO 27001	COBIT 5	NIST (CS-IC)	B.A.S.E. - A Security Assessment Methodology SANS Institute
Políticas de Seguridad	X	X	X	
Gestión de Riesgos	X		X	
Procesos de Seguridad		X		
Aseguramiento de la información (Proteger activos de la información)		X	X	X

Figura 36 Manta-Propuesta de Normas y Marcos de trabajo a utilizar
Fuente: Elaboración propia basada en las observaciones propias de la investigación

Para lograr implementar el programa la administración superior debe aprobar un departamento específico para el trato de la Seguridad Cibernética, ampliando la estructura de la Dirección de Informática, la cual podría visualizarse de la siguiente manera:

Figura 37. Estructura propuesta para la implementación del programa
Fuente: Elaboración propia basada en las observaciones de la investigación

El Departamento de Seguridad Informática tendrá las siguientes responsabilidades:

- Desarrollar una política de Seguridad, la cual deberá aprobar la alta dirección y publicar un documento de la Política de Seguridad de la Información y comunicar la Política a todos los colaboradores y las partes externas relevantes.
- Revisar la Política de Seguridad de la Información, mediante intervalos planificados (o en caso que se produzcan cambios significativos) para garantizar que es adecuada, eficaz y suficiente.
- Desarrollar un marco de trabajo que sustente un proceso sistemático que logre identificar, evaluar y gestionar el Riesgo de CiberSeguridad.
- Desarrollar un marco de trabajo que permita Identificar, Proteger y Detectar procesos de CiberSeguridad.

- Aplicar las metodologías para la evaluación de la Seguridad de manera constante.

Aunado a lo anterior y como parte de esta propuesta se ha realizado un análisis de Roles y Responsabilidades que deberán de tener los colaboradores que impartirán de manera efectiva a un costo aceptable la base para implementar, desarrollar y gestionar el Programa.

Jefatura del Departamento de Seguridad

Su principal responsabilidad será desarrollar el programa de Seguridad de la Información en el Ministerio de Seguridad Pública, que generalmente incluye la gestión de riesgos de los activos de información, así como aplicar la gobernabilidad de los procesos y controles de Seguridad. Por lo tanto, desempeña un rol importante en la introducción de una metodología apropiada y estructurada para identificar, evaluar y minimizar el riesgo a los recursos de la información, que incluyen los sistemas de TI que respaldan la misión de la organización. En general, la Jefatura del Departamento de Seguridad también actúa como consultor principal en respaldo a la alta dirección para garantizar que estas actividades se realicen permanentemente.

Dentro de las destrezas, certificaciones y atestados recomendablemente deberá tener algún grado de Maestría en la gestión de Seguridad de la Información, certificación CISSP, certificación CISM, con al menos 5 años de laborar en el desarrollo de arquitecturas de seguridad y proyectos de Seguridad.

Profesionales de Seguridad de TI

Tendrán como responsabilidad la administración de módulos de seguridad en plataformas de red de datos, sistemas, aplicaciones y bases de datos; especialistas en computación; analistas de seguridad; consultores de seguridad y su gestión recae específicamente en la implementación y configuración apropiada de los requerimientos de seguridad en los sistemas de TI. A medida que ocurren los cambios en el ambiente de sistemas de TI existe (por ejemplo, expansión de conectividad de red, cambios a la infraestructura existente y políticas organizacionales, estándares o procedimientos, introducción de nuevas tecnologías), los profesionales de seguridad de TI deben de respaldar o utilizar el proceso de gestión de riesgos para identificar y valorar nuevos riesgos potenciales y garantizar la implementación de nuevos controles de seguridad necesarios para defender los sistemas de TI.

Dentro de la destrezas, certificaciones y atestados recomendablemente deberá poseer algún grado universitario, bachiller o Licenciatura, certificaciones en Seguridad y diplomados de Seguridad Informática.

5.4.1 Fases del Diseño para implementación del Programa de Seguridad Informática

El programa cuenta con un conjunto de fases (léase fases como las actividades propuestas para la implementación del programa) que se pueden utilizar en el desarrollo del proceso, para ayudar en la implementación de un esquema de ciberseguridad, de esta forma, se requiere implementar el programa con sus elementos para determinar un conjunto de controles y procedimientos que se integran a la arquitectura de la plataforma.

Es importante tomar en cuenta que actualmente el Ministerio no cuenta con manuales, procedimientos ni flujo de configuraciones ni cambios para realizar este proceso, por lo tanto, la recomendación es iniciar el programa intentando dar un modelo que se adapte a la situación actual, como se logra observar en el punto 1.3 Plataformas de Seguridad actuales, se cuentan como plataformas de protección que han sido desarrolladas de una manera empírica y desordenada, por lo que esta propuesta llegaría con un modelo real de cambio donde la opción más importante es la documentación y adecuación a marcos y normas de trabajo actuales.

Flujo del diseño para la implementación del programa

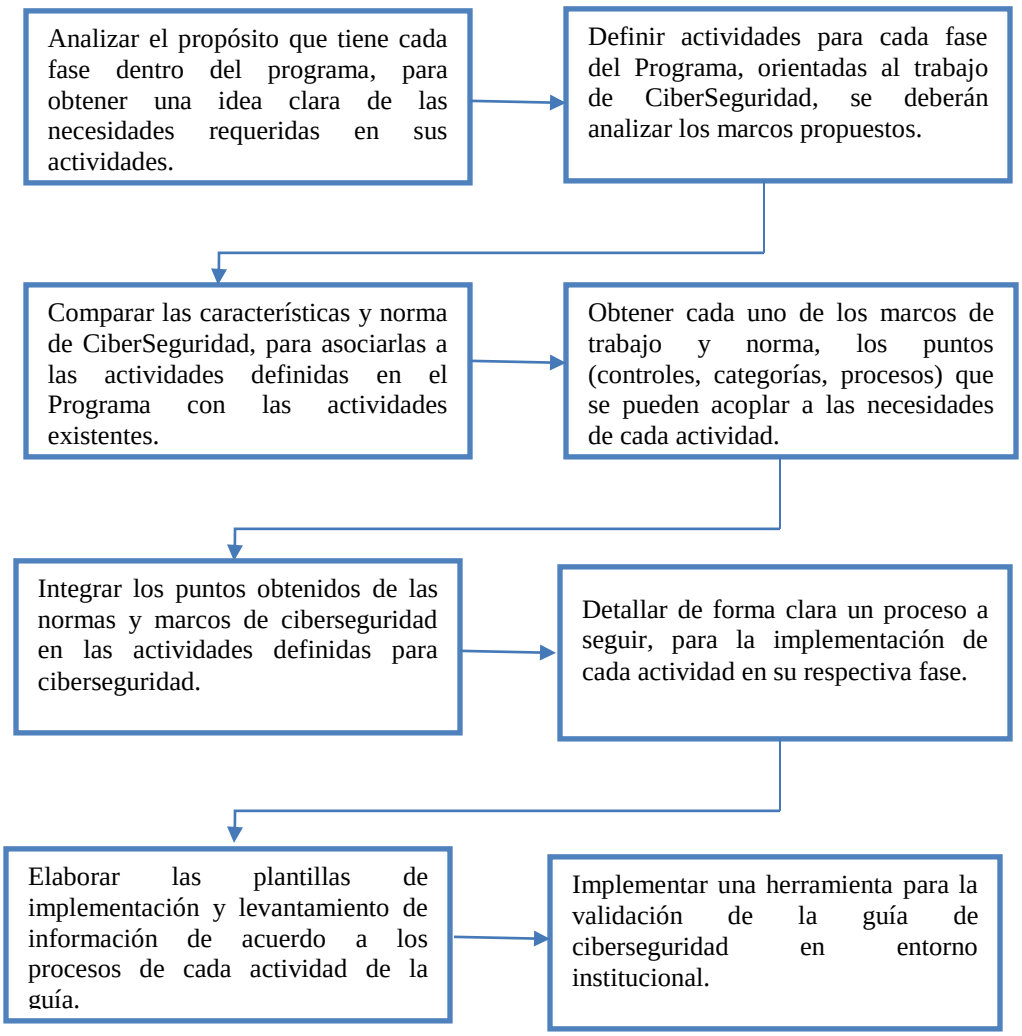

Figura 38. Proceso de elaboración del Programa de Seguridad

Fuente: Elaboración propia basada en las observaciones de la investigación

Para trabajar a través de cada fase del Programa, es importante conocer qué realizará cada una de ellas de acuerdo a las necesidades y requerimientos de CiberSeguridad, además saber qué marcos de trabajo o normas de ciberseguridad se pueden utilizar. Para obtener las características de cada norma y marco de trabajo en la elaboración del modelo de ciberseguridad para el Programa, el cual se muestra en la figura 42.

En cada uno de los puntos de la figura 42 se puede ver que es necesario un estudio para relacionar características de cada norma y marco de trabajo, este estudio valida que dentro de cada una de las actividades definidas encajen los controles, características y procesos orientados a ciberseguridad.

5.4.1.1 Gestión de Requerimientos (Fases)

Este programa trabaja mediante el proceso dinámico la gestión de los atributos del perfil, y los requerimientos de ciberseguridad obtenidos de las partes interesadas para incluirlos en el perfil deseado.

Actividad Fase	Normas y marcos considerados
Creación de una Política de Seguridad Institucional.	- ISO 27001
Creación de un marco (Framework de Seguridad).	- ISO 27001 - NIST (CS-IC)
Gestionar Servicios de Seguridad	- COBIT 5 - NIST (CS-IC)
Evaluación Continua de Seguridad	- B.A.S.E. - A Security Assessment Methodology SANS Institute

Figura 39. Normas y marcos de trabajo considerados para la implementación del programa
Fuente: Elaboración propia basada en las observaciones de la investigación

5.4.2 Fase 1- Implementación de Políticas de Seguridad

Después de la investigación se encontró que no existe una Política de Seguridad que defina directrices de seguridad de la información, por lo que se deben de establecer reglas y normas para la implementación del Programa de Seguridad, las mismas deben de ser desarrolladas en función de la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos cuando lo requieran).

Para la creación de la Política de Seguridad se recomienda trabajar con ISO 27002:2005 del dominio 5. Política de Seguridad 5.1 Política de Seguridad de Información – 5.1.1 Documento de Política de Seguridad de la Información- 5.1.2 Revisión de la Política de Seguridad de la Información.

a) Esta fase hace referencia al Apartado 3.11.1 Establecer el SGSI Léase *"Definir una política SGSI en términos de las características del negocio, la organización, su ubicación, activos y tecnología…"*

Posibles Soluciones para este control:

Ubicación	Descripción	Referencia
SANS.ORG	Define el uso aceptable de equipos y servicios de computación y las medidas de seguridad apropiadas para proteger los recursos corporativos y la información de propiedad de la organización.	Plantilla de Políticas
CENTRO CRIPTOLÓGICO NACIONAL	Los documentos CCN-STIC del Centro Nacional español incluyen normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las TIC en la Administración española.	Series CCN

Figura 40. Posibles soluciones al control para implementación de una política de seguridad
Fuente: Elaboración propia basada en las observaciones de la investigación

5.4.3Fase 2 - Creación de un marco (Framework de Seguridad).

Para el desarrollo del marco de Seguridad se debe enfocar en la propuesta de la NIST, donde indica el alcance que se va a tener y que se debe desarrollar un proceso sistemático para **identificar, evaluar y gestionar el riesgo de ciberseguridad**. En este programa se utilizarán específicamente las siguientes funciones **Identificar, Proteger y Detectar.** Para **(Responder y Recupera**r), pueden ser involucradas durante el desarrollo y madurez del programa.

Cada categoría se divide en sub-categorías y las cuales brindarán especificaciones del proceso a cubrir, así como las referencias informativas para consultar y saber cómo realizar el proceso adecuado para poner en marcha el Programa. A continuación, el identificador de Categorías de cada Función que se implementará.

Identificador Único	Función	Identificador único	Categoría
ID	Identificar	ID.AM	Gestión de Activos
PR	Proteger	PR.AC	Control de Acceso
		PR.DS	Seguridad de Datos
DE	Detectar	DE.AE	Eventos y Anomalías

Figura41. Funciones y categorías únicas de identificación por NIST
Fuente: nist.gov/sites/default/files/documents/cyberframework

Según (NIST.GOV, 2014) **Para Identificar** los activos se deben seguir las siguientes funciones, categorías, sub-categorías, además se brindan opciones como referencia para crear este proceso:

Función	Categoría	Sub-categoría	Referencias Informativas
IDENTIFICAR (ID)	**Gestión de activos (ID.AM):** Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar objetivos de, se identifican y gestionan de acuerdo con su importancia relativa para los objetivos del Ministerio y la estrategia de riesgo de la organización.	**ID.AM-1:** Los dispositivos físicos y los sistemas dentro de la organización son inventariados	· **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: Las plataformas de software y las aplicaciones dentro de la organización son inventariadas	· **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8
		D.AM-3: La comunicación organizacional y los flujos de datos están mapeados	· **COBIT 5** DSS05.02 · **ISO/IEC 27001:2013** A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-5: Los recursos (por ejemplo, hardware, dispositivos, datos y software) se priorizan en función de su clasificación, criticidad y valor	· **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14 · **ISO/IEC 27001:2013** A.8.2.1
		ID.AM-6: Se establecen las funciones y responsabilidades de seguridad cibernética para	· **ISO/IEC 27001:2013** A.6.1.1 · **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11

		toda la fuerza laboral y las partes interesadas de terceros (por ejemplo, proveedores)	

Figura42. Marco de Trabajo para identificación de Activos
Fuente: nist.gov/sites/default/files/documents/cyberframework

Realizando la comparación con la gestión de activos actual, se encuentra lo siguiente:

Clasificación y Control de Activos	
¿Existe un inventario de todos los activos?	☐No ☒ Sí, No está integrada a una base de datos convergente
¿Existe una clasificación de activos críticos?	☐No ☒ Sí, Excel, Archivo Policial,
¿Existe una clasificación de bases de datos críticas?	☐No ☒ Sí, Excel Archivo Policial
¿Se realiza un escaneo periódico de vulnerabilidades y exploits?	☒No ☐ Estaciones de trabajo ☐ Servidores ☐ Red ☐ Aplicaciones Describir el número, fabricante, política..

Figura 43. Validación de gestión de activos actual en MSP
Fuente: Elaboración propia basada en las observaciones de la investigación

Como se logra observar en la figura 46 la gestión de activos no tiene un alcance sobre plataformas críticas, no se ha realizado un análisis de riesgo para identificar los activos, tecnologías y plataformas críticas, por lo tanto, el programa recomienda realizar este proceso.

Por lo anterior, este programa propone identificar activos por criticidad a nivel Gubernamental.

Según (NIST.GOV, 2014) **Para Proteger** los activos identificados previamente, propone seguir las siguiente funciones, Categorías y Sub-categorías, también incluye referencia de marcos y normativas a seguir. Para este proceso incluimos dos Categorías (Control de acceso y Seguridad de datos) a continuación la información**:**

Para el control de acceso:

Función	Categoría	Sub-Categoría	Referencias Informativas
PROTEGER (PR)	**Control de acceso (PR.AC):** El acceso a los activos e instalaciones asociadas está limitado a usuarios, procesos o dispositivos autorizados, las actividades y transacciones autorizadas.	**PR.AC-1:** Las identidades y las credenciales se administran para dispositivos y usuarios autorizados	· **COBIT 5** DSS05.04, DSS06.03 · **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 · NIST SP 800-53 Rev. 4 AC-2, IA Family
		PR.AC-2: El acceso físico a los activos es gestionado y protegido	· **COBIT 5** DSS01.04, DSS05.05 · **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 · **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
		PR.AC-3: El acceso remoto se gestiona	· **COBIT 5** APO13.01, DSS01.04, DSS05.03 · **ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-17, AC-19, AC-20
		PR.AC-4: Los permisos de acceso se gestionan, incorporando los principios de privilegios mínimos y la separación	· **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4

		de funciones	· **NIST SP 800-53Rev. 4** AC-2, AC-3, AC-5, AC-6, AC-16
		PR.AC-5: La integridad de la red está protegida, incorporando segregación de red cuando sea apropiado	· **ISO/IEC 27001:2013** A.13.1.1,A.13.1.3, A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-4, SC-7

Figura44. Marco de trabajo para protección de Activos según NIST
Fuente: nist.gov/sites/default/files/documents/cyberframework

Para Seguridad de los Datos:

Función	Categoría	Sub-Categoría	Referencias Informativas
PROTEGER (PR)	**Seguridad de datos (PR.DS):** La información y los registros (datos) se manejan de acuerdo con la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-1:** Los datos almacenados están protegidos	· **COBIT 5** DSS06.06 · **ISO/IEC 27001:2013** A.8.2.3 · **NIST SP 800-53 Rev. 4** SC-28
		PR.DS-2: Datos en tránsito están protegidos	· **COBIT 5** APO01.06, DSS06.06 · **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 · **NIST SP 800-53Rev. 4** SC-8
		PR.DS-3: Los activos se gestionan formalmente durante la remoción, las transferencias y la disposición	· **COBIT 5** BAI09.03 · **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 · **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16
		PR.DS-4: Se mantiene la capacidad adecuada para	· **ISO/IEC 27001:2013** A.12.3.1

		garantizar la disponibilidad	· **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
		PR.DS-5: Las protecciones contra fugas de datos se implementan	· **ISO/IEC 27001:2013** A.6.1.2,A.7.1.1,A.7.1.2, A.7.3.1,A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Los mecanismos de verificación de integridad se utilizan para verificar el software, el firmware y la integridad de la información	· **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 · **NIST SP 800-53Rev. 4** SI-7
		PR.DS-7: Los entornos de desarrollo y prueba están separados del entorno de producción	· **ISO/IEC 27001:2013** A.12.1.4 · **NIST SP 800-53 Rev. 4** CM-2

Figura45. Marco de trabajo para protección de Activos según NIST
Fuente: nist.gov/sites/default/files/documents/cyberframework

Realizando la comparación con la gestión de activos actual, se encuentra lo siguiente:

Información de Sistemas	
Cuál es la distribución de sistemas operativos en la institución	Windows, Windows Server, Solaris, CentOS, IOS, Windows 10, Windows 7 pro, WS2008 R2, WS2012 R2, etc
¿Existe un software Antivirus para servidores?	☐No ☒ Sí, Kaspersky, AV, etc
¿Existe un software para la gestión y protección de dispositivos móviles? (MDM, MAM, AV).	☒No ☐ Sí, Fabricante, funcionalidades, etc
¿Cómo se previene a los usuarios la instalación de software potencialmente malicioso (Ej, Usuarios no son administradores, usuarios locales)?	Active Directory , Políticas, sin embargo se requiere mejor gestión en seguridad
¿Existen medidas de seguridad para la protección ante cualquier tipo de fuga de datos (DLP, o IRM)?	☒No ☐ Sí, Fabricante, funcionalidades, etc
¿Existe la integración de auditorías de seguridad con alguna plataforma SIEM?	☒No ☐ Estaciones de trabajo ☐ Servidores ☐ Red ☐ Aplicaciones

	Describir el número, fabricante, logs..
Existe una solución de nueva generación para la detección de malware en las estaciones de trabajo (Ej. FireEye, BlueCoat, Kaspersky,)?	☒No ☐ Sí, Fabricante, funcionalidades, etc
Control de Accesos	
¿Existe una solución para la gestión de identidades?	☐No ☒ Sí, Microsoft, Active Directory
¿Está deshabilitado y/o restringido el acceso para utilizar usuarios locales de administrador por defecto?	☒No ☐ Estaciones de trabajo ☐ Servidores ☐ Red ☐ Aplicaciones Describir el número, fabricante, etc
¿La auditoría de seguridad de las aplicaciones con autenticación local está integrada a alguna herramienta de monitoreo? (Ej. SIEM, NAC, etc.)	☒No ☐ Sí, Fabricante, funcionalidades, etc
¿Se realizan controles periódicos para garantizar el acceso de usuarios coincide con sus responsabilidades?	☒No ☐ Sí, Fabricante, funcionalidades, etc

¿Existen procedimientos de control de acceso a los sistemas sensibles, archivos, directorios (Red de servidores VLAN, DMZ).	☐No ☒ Sí, Herramientas del Sistema Operativo, directivas etc
¿Qué tipo de métodos de conexiones externas se tiene con proveedores? (Ej. Site to Site, VPN, VPN SSL, L2TP).	Por RDP específico
¿Existen controles avanzados de autenticación como doble factor o el uso de certificados para acceso remoto?	☒No ☐ Sí,
Información de Seguridad de Red	
Pueden describir como está segmentada la red, es decir, ZONAS DMZ, zonas de seguridad, puertos habilitados, etc.	Anay to Any entre VPN, DMZ por puertos, NO hay documentación de diagramas de red.
¿Existe muros de fuego en la institución, tiene conocimientos si son NGFW?	☐No ☒ Sí, 160,Fortinet,
¿Disponen de un Sistema de Detección de Intrusiones? (IDS)	☒No ☐ Host based IDS (HIDS) ☐ Network-based IDS (NIDS) ☐ Combinación de ambos Describir el número, fabricante, etc

¿Dispone de un Sistema de Detección de Intrusos (IPS)?	☐No ☒ Sí, 1, fortinet, DMZ etc
¿Existe una solución de análisis avanzado de malware? (Ej. Sandboxing, Honeypot)	☒No ☐ Sí, número, fabricante, zonas etc
¿Existen controles para asegurar el acceso a la red? (NAC)	☒No ☐ Sí, número, fabricante, funcionalidades etc.
¿Existe una red de acceso Wireless? ¿Se encuentra aislada? ¿Controlada?	☒No ☐ Sí, Tipo de conexión, controles
¿Están aseguradas las conexiones desde computadoras portátiles, dispositivos móviles y usuarios remotos a la red interna (VPN)?	☐No ☒ Sí, Clientes SSL, no hay segmentación
¿Hay conexiones dedicadas a redes de otras organizaciones (proveedores, instituciones de Gobierno, etc)? ¿Se encuentran aseguradas?	☐No ☒ Sí, OIJ, Migración, Hacienda, TSE-Todas con FW
¿Existe alguna solución para la mitigación de denegación de servicios? (DDOS)	☒No ☐ Sí, número, fabricante, zonas etc

Figura 46. Validación de Gestión y Protección de activos en Plataforma Tecnológica de MSP
Fuente: Elaboración propia basada en las observaciones de la investigación

Como se logra observar en la figura 49 existen deficiencias y faltan controles documentados que permitan la gestión de Protección de los sistemas, por lo tanto, este

programa recomienda apegarse al Marco con el fin de involucrar procesos de Protección basado en las normas aportadas como referencias por la (NIST.GOV, 2014), para esto se deben de seguir las fases mencionadas en la figura 41.

Continuando con el proceso propuesto por (NIST.GOV, 2014) para **Detectar** eventos y anomalías dentro de la gestión de la seguridad, se deben de seguir las siguientes categorías, sub-categorías:

Función	Categoría	Sub-Categoría	Referencias Informativas
DETECTAR (DE)	**Eventos y Anomalías (DE.AE):** La actividad anómala se detecta de manera oportuna y se entiende el impacto potencial de los eventos.	**DE.AE-1:** Se establece y gestiona una línea base de operaciones de red y flujos de datos esperados para usuarios y sistemas	· **NIST SP 800-53Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Los eventos detectados se analizan para comprender los objetivos y métodos de ataque	· **ISO/IEC 27001:2013** A.16.1.1, A.16.1.4 · **NIST SP 800-53Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Los datos de eventos se agregan y correlacionan de múltiples fuentes y sensores	· **NIST SP 800-53Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: El impacto de los eventos se determina	· **NIST SP 800-53Rev. 4** CP-2, IR-4, RA-3, SI -4

		DE.AE-5: Se establecen los umbrales de alerta de incidentes	· **NIST SP 800-53Rev. 4** IR-4, IR-5, IR-8

Ilustración 47. Marco de trabajo para detección de anomalías y eventos según NIST
Fuente: nist.gov/sites/default/files/documents/cyberframework

El proceso de detección de anomalías y eventos que actualmente gestiona el MSP es el siguiente:

Análisis de Amenazas	
¿Existe alguna solución para el análisis del tráfico web?	☒No ☐ Sí, fabricante, funcionalidades etc
¿Se realiza inspección y validación de tráfico SSL?	☐No ☒ Sí, Por medio de certificado local, Navegación web etc
¿Existe alguna solución para análisis de correo electrónico?	☐No ☒ Sí, TrendMicro, AntiSPAM etc
¿Se realiza análisis de URL's point of click?	☒No ☐ Sí, fabricante, funcionalidades etc
¿Hay alguna solución para la protección ante Amenazas Persistentes Avanzadas?	☒No ☐ Sí, fabricante, funcionalidades etc
¿Hay alguna solución de escaneo de contenido de archivos para detección de amenazas maliciosas?	☒No ☐ Sí, fabricante, funcionalidades etc

Información de Servicios	
¿Qué servicios se publican a Internet ?	Página Web, Webmail, Transportes, Auditoria, Moodle, Portal Web
¿Se cuenta con alguna solución contra las debilidades y vulnerabilidades de las aplicaciones web? (WAF) (Ej. CSS, SQL INJ).	☒No ☐ Sí, Se encuentra en proceso de adquisición
¿Qué tipo de autenticación se utiliza en los servicios web?	Solo correo con HTTPS
¿Qué aplicaciones críticas se utilizan en la institución? ¿Se encuentran aseguradas? (DAM, Active Directory, DNS)	Solo por AV,
¿Hay alguna solución para el control de vulnerabilidades de bases de datos?	☒No ☐ Sí, fabricante, políticas etc

El proceso de detección es sumamente importante, ya que se puede identificar en el menor tiempo posible un incidente de seguridad basado en casos de uso generados por las plataformas existentes y los cuales brindar una mayor visibilidad para puntos de mejora.

5.4.4 Fase 3 – Gestionar Servicios de Seguridad

Una vez creado un marco de Gestión de Seguridad (basado en la NIST) se deben de gestionar los Servicios de Seguridad, para ello se debe basar en el marco de referencia de COBIT 5 específicamente en el Dominio Entrega, Servicio y Soporte (DSS), específicamente en su proceso 05 Gestionar servicios de Seguridad, el cual hace referencia a una Matriz de acción (ver en Figura 12. Matriz RACI DSS05) misma que muestra los Roles y Responsabilidades de esta gestión.

Los roles y responsabilidades para este programa deben ser aprobados y realizar en conjunto un proceso controlado para retomar las plataformas y tecnologías correspondientes.

También es importante obtener las entradas y salidas, por ejemplo, para el proceso de Proteger contra software malicioso (Malware) la salida va ser una política de prevención de software malicioso basadas en las evaluaciones creadas en el marco de Seguridad creado en la fase 2.

La recomendación del programa se basa en la pregunta ¿EL QUE? Se va proteger, una vez obtenido ¿EL CÓMO? En la fase 2.

Basado en (ISACA) Cobit 5 se deben de tomar en cuenta los siguientes procesos:

Proceso	Practica de gestión
Proteger contra software malicioso (Malware)	Ver Anexo 3
Gestionar la seguridad de la red y las comunicaciones	Ver Anexo 4
Gestionar la seguridad de los puestos de usuario final	Ver Anexo 5.
Gestionar la identidad del usuario y acceso lógico	Ver Anexo 6
Gestionar el acceso físico a los activos de TI	Ver anexo 7
Gestionar documentos sensibles y dispositivos de Salida	Ver Anexo 8
Supervisar la infraestructura para detectar eventos relacionados con la seguridad	Ver Anexo 9

Ilustración 48. Proceso Dominio Entrega, Servicio y Soporte (DSS) COBIT 5
Fuente COBIT 5 Proceso Catalizadores

5.4.5 Fase 4 – Evaluación Continua de Seguridad

Para esta fase ya se han logrado crear políticas, el marco de trabajo de seguridad y la gestión de seguridad, ahora se requiere contar con líneas base para dar una gestión continua

de seguridad, para esto, se deben enfocar en (Braunton, 2005), el cual indica fácilmente cómo mantener el entorno en términos de patrones de acceso, rendimiento, configuraciones de hardware, servicios, aplicaciones, etc.

Para (Braunton, 2005) deben de existir la siguiente línea base con el fin de cubrir este proceso:

Línea Base (Baseline)	Práctica de Gestión
Línea base de estaciones de trabajo (Workstation Host System Baseline)	Ver Anexo 10.
Línea de base de Red (Network Baseline)	Ver Anexo 11.
Línea base de Servidores (Server Host Baseline)	Ver Anexo 12.

Figura 49. Baseline según (Braunton, 2005)
Fuente: https://www.sans.org/reading-room/whitepapers/auditing/base-security-assessment-methodology-1587

Como se puede observar en la siguiente imagen el programa tiene como base 4 pilares específicos, los cuales se desarrollan de una manera ordenada y siguiendo los pasos expuestos en cada fase.

Figura50. Pilares del Programa
Fuente: Elaboración propia basada en las observaciones de la investigación

6 Conclusiones y Recomendaciones

6.1 Conclusiones

1. Todos los objetivos propuestos en esta propuesta se cumplen satisfactoriamente.
2. El Desarrollo del programa queda sujeto a una aprobación por parte de la administración superior de la Dirección de Tecnologías de la Información.
3. La Documentación para el desarrollo de este programa es fundamental, se deben de seguir los procesos propuestos.
4. Las normas y marcos utilizados en este programa se encuentran en constante actualización con las últimas tendencias de Seguridad Cibernética.
5. Este programa se diseñó específicamente para la plataforma tecnológica del Ministerio de Seguridad Pública y su gestión de Seguridad sobre activos tecnológicos.
6. Esta investigación ayudará a mejorar la gestión de la Dirección de Tecnologías de la Información respecto al manejo y trasiego de información de manera adecuada dentro de la Institución.
7. Esta propuesta tiene como propósito principal la administración de la Seguridad de TI a un nivel apropiado dentro de la Institución, de manera que las acciones de administración de Seguridad estén en línea con los requerimientos del Ministerio de Seguridad Pública.

8. Este documento busca realizar configuraciones en la plataforma de TI, los planes de acción del riesgo de la información y la cultura sobre la Seguridad en la Información a un plan global de Seguridad de TI.
9. Esta propuesta busca concientizar a los altos Jerarcas del Ministerio de aprobar un proceso de Seguridad tal y como se propone en este documento.
10. Otro propósito de esta investigación es crear el programa de Seguridad Informática mediante las normas generales y gestionar y asegurar que la información sea accedida sólo por aquellos que de acuerdo a sus funciones y responsabilidades tiene una necesidad legítima, que esté protegida contra modificaciones no planeadas, realizadas con o sin intención y que esté disponible cuando se requiera.

6.2 Recomendaciones

1. Se recomienda implementar este programa en un plazo de 12 a 24 meses de manera paulatina y siguiendo a cabalidad cada fase propuesta.
2. Se recomienda aprobar dos plazas para la contratación de recurso profesional capacitado para implementar este programa.
3. Se recomienda adquirir plataformas tecnológicas de Seguridad basadas en los procesos e identificación de activos críticos que menciona este programa.
4. Se recomienda adquirir una consultoría basada en este programa y desarrollarlo conforme se estipula, esto en caso de no aprobarse el nuevo departamento de Seguridad Informática.
5. Se recomienda capacitar a los profesionales que actualmente gestionan la seguridad cibernética en el Ministerio de Seguridad Pública para que sea posible la implementación de este programa.
6. Se recomienda aplicar este programa una vez aprobado a todos los niveles de la Organización, y que acceden, ya sea internamente o externamente, a cualquier activo de información del Ministerio independiente de su ubicación.
7. Se recomienda aplicar a este programa a toda la información creada, almacenada, procesada, capturada, transformada, protegida y destruida en el soporte institucional, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

8. Se recomienda aplicar esta propuesta a todos los Programas del Ministerio de Seguridad Pública, Dirección General de la Fuerza Pública, Policía de Control de Drogas, Escuela Nacional de Policía, Dirección General de Guardacostas, Dirección General de Vigilancia Aérea, etc.
9. Se recomienda que la creación de este modelo tenga como prioridad definir un Alcance Institucional, una Clasificación de activos Institucional, Gestión de Riegos y Evaluación continua de Seguridad.
10. Se recomienda la definición de directrices de Seguridad de la Información, establecer las reglas y políticas para la implementación del programa de Seguridad de la Información en los procesos del Ministerio de Seguridad Pública y que se desarrolle en función de la preservación de la confidencialidad, integridad y disponibilidad de los activos críticos.
11. Se recomienda la definición y creación de directrices como Políticas de Seguridad de la Información, Organización de la Seguridad de la Información, Gestión de los activos de Información, etc.

7. Bibliografía

Braunton, G. (29 de September de 2005). *sans.org*. Obtenido de sans.org: https://www.sans.org

ccm.net. (Agosto de 2017). *ccm.net*. Obtenido de ccm.net: http://es.ccm.net

es.ccm.net. (s.f.). *es.ccm.net*. Obtenido de es.ccm.net: http://es.ccm.net/contents/138-firmas-electronicas

Hernández, Fernandez, & Baptista. (2010). *Metodología de la Investigación.*

ISACA. (s f.) COBIT 5 . En ISACA.

ISACA, C. F. (s f.) CyberSecurity Fundamentals. En ISACA, *CyberSecurity Fundamentals Nexus.*

ISACA-CISM. (2015). *Manual de Preparación para Examen CISM.*

LUCENA LÓPEZ, M. J. (1999). *Criptografía y Seguridad en Computadores. Dpto. de Informática Universidad de Jaén.* . España: Edición virtual.

NIST.GOV. (12 de Febrero de 2014). Framework for Improving Critical Infrastructure Cybersecurity . USA.

Rolf M. von Roessing, V. B. (2014). *Transforming Cybersecurity.* ISACA.org.

8. Glosario de Abreviaturas

ACL *Access List Control* en español *Listas de Control de Acceso*.

ANSI *American National Standards Institute* en español *Instituto Nacional Americano de Normalización.*

ARP *Address Resolution Protocolo* en español *Protocolo de Resolución de Direcciones*.

ARPA *Advanced Research Project Agency* en español *Agencia de Investigación de Proyectos Avanzados de Defensa*.

CLI *Comand Line Interface* en español *Interfaz de Línea de Comandos*.

DNA *Digital Network Architecture* en español *Arquitectura de la Red Digital*.

DNS *Domain Name Server* en español *Sistema de Nombres de Dominio*.

DNSSEC Extensiones de Seguridad para el sistema de nombres de dominio

DoD *Departament of Defense* en español *Departamento de Defensa de los Estados Unidos*.

EIA *Electronic Industries Alliance* en español *Asociación de Industrias Electrónicas.*

FTP *File Transfer Protocol* en español *Protocolo de Transferencia de Archivos*.

HTTP *Hyper Text Transfer Protocol* en español *Protocolo de Transferencia de Hipertexto*.

IANA *Internet Assigned Numbers Authority* en español *Autoridad para la Asignación de Números de Internet*.

ICANN*Internet Corporation for assigned Names and Numbers en español Corporación de*

internet para la asignación de Nombres y Números.

ICMP *Internet Control Message Protocol* en español *Protocolo de Mensaje de Control*.

IEEE *Institute of Electrical and Electronics Engineers* en español *Instituto de Ingenieros Eléctricos y Electrónicos.*

IGRP *Interior Gateway Routing Protocol* en español *Protocolo de Enrutamiento de Gateway Interior.*

IP *Internet Protocol* en español *Protocolo de Internet.*

ISP *Internet Service Provider* en español *Proveedor de Servicio de Internet*.

LAN *Local Area Network* en español *Red de Área Local.*

LLC *Logical Link Control* en español *Control de Enlace Lógico*.

MAC *Media Access Control* en español *Control de Acceso al Medio*

MAN *Metropolitan Area Network* en español *Red de Área Metropolitana*.

NAT *Network Address Traslation* en español *Traducción de Direcciones de Red.*

NCP *Network Control Protocol* en español *Protocolo de Control de la Red.*

PDU *Protocol Data Unit* en español *Unidad de Datos del Protocolo*.

PING *Packet Internet Groper* en español *Rastreador de Paquetes en Redes.*

QoS *Quality of Service* en español *Calidad de Servicio*.

SSL *Secure Sockets Layer en español Capa de conexión segura.*

SNA *System Network Architecture* en español *Arquitectura de Sistemas de Red*.

SSH *Security Shell* en español *Intérprete de Órdenes Seguras*.

TCP *Transmision Control Protocol* en español *Protocolo de Control de Trasmisión.*

TIA *Telecomiunications Industry Association* en español *Asociación de la Industria de las Telecomunicaciones.*

UDP *User Datagram Protocol* en español *Protocolo de Datagrama de Usuario.*

VLAN *Virtual Local Area Network* en español *Red de Área Local Virtual*.

WAN *Wide Area Network* en español *Red de Área Amplia*.

WWW *World Wide Web* conocida en español como *Telaraña de Alcance Mundial.*

Anexo 1. Fuentes buscadas

Fuentes de Información

Motor de búsqueda: Google

URL: https://www.nist.gov/

Fecha de la consulta: 24 de febrero, 2017

Otros parámetros: Búsqueda avanzada que incluyera documentos pdf.

Documentos Extraídos: Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories

Protecting Controlled Un classified Information in Nonfederal Information Systems and Organizations

Motor de búsqueda: Google

URL: https://www.protectivesecurity.gov.au

Fecha de la consulta: 02 de febrero, 2017

Otros parámetros: se utilizó una búsqueda avanzada que incluyera documentos pdf.

Documentos Extraídos:

AustralianGovernmentInformationSecurityManagementGuidelines.pdf

AustralianGovernmentInformationsecurityclassificationsystem.pdf

Motor de búsqueda: Google

URL:http://www.iso27000.es/

Fecha de la consulta: 02 de Marzo, 2017

Otros parámetros: se utilizó una búsqueda avanzada que incluyera documentos pdf.

Documentos Extraídos:

Doc_iso27000_all.pdf

Motor de búsqueda:Google

URL: https://www.researchgate.net/profile/Danilo_Jaramillo/publication/282329839

Fecha de la consulta: 15 de Abril, 2017

Otros parámetros: se utilizó una búsqueda avanzada que incluyera documentos pdf.

Documentos Extraídos:

Definition-of-cybersecurity-businness-framework-based-on-ADM-TOGAF.pdf

Anexo 2 Proceso DSS05 Gestionar Servicios de Seguridad

<table>
<tr><td>DSS05 Gestionar Servicios de Seguridad</td><td>Área: Gestión

Dominio: Entrega, Servicio y Soporte</td></tr>
<tr><td colspan="2">Descripción del Proceso:

Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo a la política de seguridad. Establecer y mantener los roles de seguridad de acceso a la información y realizar la supervisión de seguridad.</td></tr>
<tr><td colspan="2">Declaración del Propósito del Proceso

Minimizar el impacto en el negocio de las vulnerabilidades e incidentes de seguridad de la información.</td></tr>
<tr><td colspan="2">El proceso apoya la consecución de un conjunto de principales metas de TI:</td></tr>
<tr><td>Meta de TI</td><td>Métricas Relacionadas</td></tr>
<tr><td>10 Seguridad de la información , infraestructura de procesamiento y aplicaciones</td><td>• Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública.
• Números de servicios de TI con los requisitos de Seguridad pendientes
• Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicios otorgados
• Frecuencia de la evaluación de seguridad frente a los últimos estándares y guías</td></tr>
<tr><td colspan="2">Objetivos y Métricas del Proceso</td></tr>
<tr><td>Meta del Proceso</td><td>Métricas Relacionadas</td></tr>
<tr><td>7 La seguridad de las redes y las comunicaciones cumple con las necesidades del negocio</td><td>• Numero de Vulnerabilidades descubiertas
• Numero de rupturas (breaches) de cortafuegos</td></tr>
<tr><td>8 La información procesada , almacenada y transmitida en los dispositivos de usuario final está protegida</td><td>• Porcentaje de individuos que reciben información de concienciación relativa al uso de dispositivos de usuario final.
• Número de incidentes que impliquen dispositivos de usuario final
• Numero de dispositivo de usuario final no autorizado detectados en la red o en el entorno.</td></tr>
</table>

9	Todos los usuarios están identificados de manera única y tienen derechos de acceso de acuerdo con sus roles en el negocio	• Promedio de tiempo entre los cambios y actualizaciones de cuentas. • Numero de cuentas (con respecto al número de usuarios/empleados autorizados).

Figura51. Gestionar Procesos de Seguridad COBIT 5
Fuente: COBIT 5 Procesos - Habilitadores

Anexo 3. Proteger contra software malicioso (Malware)

Prácticas de Gestión
DSS05.01 Proteger contra software malicioso (malware) Implementar y mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología de software malicioso (por ejemplo: virus, gusanos, software espía, -spyware-y correo basura).
Actividades
1. Divulgar concienciación sobre el software malicioso, forzar procedimientos y responsabilidades de prevención
2. Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi-automática).
3. Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios.

4. Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando productos de vendedores, y servicios de alertas de seguridad).
5. Filtrar el tráfico entrante, como correos electrónicos, descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos phishing).
6. Realizar formación periódica sobre software malicioso en el uso del correo electrónico e internet. Formar a los usuarios para no instalar software compartido o no autorizado.

Figura 52. Proteger contra Software Malicioso (Malware)
Fuente: COBIT 5 – Procesos - Habilitadores

Anexo 4. Gestionar la seguridad de la red y las comunicaciones

Prácticas de Gestión
DSS05.02Gestionar la seguridad de la red y las comunicaciones Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
Actividades
1. Basándose en el análisis de riesgos y en los requerimientos de negocio, establecer y mantener una política de seguridad de las comunicaciones
2. Permitir solo a los dispositivos autorizados tener acceso a la información y a la red de la empresa. Configurar estos dispositivos para forzar la solicitud de contraseña.
3. Implementar mecanismos de filtrado de red, como cortafuegos y software de detección

de intrusiones, con políticas apropiadas para controlar el tráfico entrante y saliente.
4. Cifrar la información en tránsito de acuerdo a su clasificación.
5. Aplicar los protocolos de seguridad aprobados a las conexiones de red.
6. Configurar los equipamientos de red de forma segura
7. Establecer mecanismos de confianza para dar soporte a la transmisión y recepción segura de información.
8. Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.
9. Realizar pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema.

Figura 53. Gestionar la seguridad de la red y las comunicaciones
Fuente: COBIT 5 – Procesos - Habilitadores

Anexo 5. Gestionar la seguridad de los puestos de usuario final

Prácticas de Gestión
DSS05.03 Gestionar la seguridad de los puestos de usuario final Asegurar que los puestos de usuario final (es decir, portátil, equipo desktop, servidor y otros dispositivos y software móviles y de red) están asegurados a un nivel que es igual o mayor al definido en los requerimientos de seguridad de información procesada, almacenada o transmitida.
Actividades
1. Configurar los sistemas operativos de forma segura.
2. Implementar mecanismos de bloqueo de los dispositivos.
3. Cifrar la información almacenada de acuerdo a su clasificación.
4. Gestionar el acceso y control remoto
5. Gestionar la configuración de la red de forma segura.
6. Implementar el filtrado de trafico de red en dispositivos de usuario final
7. Proteger la integridad del sistema.
8. Proveer de protección física a los dispositivos de usuario final.
9. Deshacerse de los dispositivos de usuario final de forma segura

Figura 54. Gestionar la Seguridad de los puestos de usuario final
Fuente: COBIT 5 – Procesos - Habilitadores

Anexo 6. Gestionar la identidad del usuario y acceso lógico

Prácticas de Gestión
DSS05.04 Gestionar la identidad del usuario y acceso lógico Asegurar que todos los usuarios tengan derechos de acceso a la información de acuerdo con los requerimientos de negocio y coordinar con las unidades de negocio que gestionan sus propios derechos de acceso con los procesos de negocio.
Actividades
1. Mantener los derechos de acceso de los usuarios de acuerdo con los requerimientos de las funciones y los procesos de negocio. Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad de tener y necesidad de conocer.
2. Identificar unívocamente todas las actividades de proceso de la información por roles funcionales, coordinando con las unidades de negocio y asegurando que todos los roles están definidos consistentemente, incluyendo roles definidos por el propio negocio en las aplicaciones de procesos de negocio.
3. Autenticar todo acceso a los activos de información basándose en la clasificación de seguridad, coordinando con las unidades de negocio que gestionan la autenticación con aplicaciones usadas en procesos de negocio para asegurar que los controles de autenticación han sido administrados correctamente.
4. Administrar todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno basándose solo en

transacciones aprobadas y documentadas y autorizadas por los gestores individuales designados.
5. Segregar y gestionar cuentas de usuario privilegiadas.
6. Realizar regularmente revisiones de gestión de todas las cuentas y privilegios relacionados.
7. Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistema de TI (aplicaciones de negocio, infraestructura de TI, operaciones de sistema, desarrollo, y mantenimiento), son identificables unívocamente. Identificar unívocamente todas las actividades de proceso de información por usuario.
8. Mantener una pista de auditoria de los accesos a la información clasificada altamente sensible.

Figura 55. Gestionar la identidad del usuario y acceso lógico
Fuente: COBIT 5 Procesos - Habilitadores

Anexo 7. Gestionar el acceso físico a los activos de TI

Prácticas de Gestión
DSS05.05 Gestionar el acceso físico a los activos de TI Definir e implementar procedimientos para conceder, limitar y revocar acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a locales, edificios y áreas debe estar justificado, autorizado, registrado y supervisado. Esto aplicará a todas las personas que entren en los locales, incluyendo empleados, empleados temporales, clientes,

vendedores, visitantes o cualquier otra tercera parte
Actividades
Gestionar las peticiones y concesiones de acceso a las instalaciones de procesamiento. Las peticiones formales de acceso deben ser completadas y autorizados por la dirección de la ubicación de TI, y guardado el registro de petición. Los formularios deberían identificar específicamente las áreas a las que el individuo tiene acceso concedido.
Asegurar que los perfiles de acceso están actualizados. El acceso a las ubicaciones de TI (salas de servidores, edificios, áreas o zonas) debe basarse en funciones de trabajo y responsabilidades.
Registrar y supervisar todos los puntos de entrada hacia las ubicaciones de TI. Registrar todos los visitantes de la ubicación, incluyendo contratistas y vendedores.
Instruir a todo el personal para mantener visible la identificación en todo momento. Prevenir la expedición de tarjetas o placas de identidad sin la autorización adecuada.
Escoltar a los visitantes en todo momento mientras estén en la ubicación. Si se encuentra a un individuo que no va acompañado, que no resulta familiar y que no lleva visible la identificación de empleado, se deberá alertar al personal de seguridad.
Restringir el acceso a ubicaciones de TI sensibles estableciendo restricciones en el perímetro, tales como vallas, muros y dispositivos de seguridad en puertas interiores y exteriores. Asegurar que los dispositivos registren el acceso y disparen una alama en caso

de acceso no autorizado. Ejemplos de estos dispositivos incluyen placas o tarjetas llave, teclados (keypads), circuitos cerrados de televisión y escáneres biométricos.
Realizar regularmente formación de concienciación de seguridad física.

Figura 56. Gestionar el acceso físico a los activos de TI
Fuente: COBIT 5 Procesos - Habilitadores

Anexo 8. Gestionar documentos sensibles y dispositivos de salida

Prácticas de Gestión
DSS05.06 Gestionar documentos sensibles y dispositivos de salida Establecer salvaguardas físicas apropiadas, prácticas de contabilidad y gestión del inventario para activosde TI sensibles, tales como formularios especiales, títulos negociables, impresoras de propósito especial o credenciales (*token*) de seguridad.
Actividades
1. Establecer procedimientos para gobernar la recepción, uso, eliminación y destrucción de formularios especiales y dispositivos de salida, dentro, en y fuera de la empresa
2. Asignar privilegios de acceso a documentos sensibles y dispositivos de salida basados en el principio del menor privilegio, equilibrando riesgo y requerimientos de negocio.
3. Establecer un inventario de documentos sensibles y dispositivos de salida, y realizar regularmente conciliaciones.

4. Establecer salvaguardas físicas apropiadas sobre formularios especiales y dispositivos sensibles.
5. Destruir la información sensible y proteger dispositivos de salida (por ejemplo, desmagnetizando soportes magnéticos, destruir físicamente dispositivos de memoria, poniendo trituradoras o papeleras cerradas disponibles para destruir formularios especiales y otros documentos confidenciales).

Figura 57. Gestionar documentos sensibles y dispositivos de salida
Fuente: COBIT 5 Procesos - Habilitadores

Anexo 9. Supervisar la infraestructura para detectar eventos relacionados con la seguridad

Prácticas de Gestión
DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad Usando herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes.
Actividades
1. Registrar los eventos relacionados con la seguridad, reportados por las herramientas de monitorización de la seguridad de la infraestructura, identificando el nivel de información que debe guardarse con base en la consideración de riesgo. Retenerla por un período apropiado para asistir en futuras investigaciones.
2. Definir y comunicar la naturaleza y características de los incidentes potenciales

relacionados con la seguridad de forma que sean fácilmente reconocibles y sus impactos comprendidos para permitir una respuesta conmensurada
3. Revisar regularmente los registros de eventos para detectar incidentes potenciales.
4. Mantener un procedimiento para la recopilación de evidencias en línea con los procedimientos de evidencias forenses locales y asegurar que todos los empleados están concienciados de los requerimientos.
5. Asegurar que los tiques de incidentes de seguridad se crean en el momento oportuno cuando la monitorización identifique incidentes de seguridad potenciales.

Figura 58. Supervisar la infraestructura para detectar eventos relacionados con la seguridad
Fuente: COBIT 5 Procesos - Habilitadores

Anexo 10. Descripción de Línea Base-Estaciones de Trabajo

Descripción de Línea Base-Estaciones de Trabajo		Herramientas	Plataformas
Información del Sistema	¿Cuál es la configuración del hardware y los componentes del sistema? ¿Qué servicios se instalan, cómo se configuran? ¿Qué aplicaciones están instaladas? Etc	**WINMSD**- Herramienta nativa en la plataforma Windows que puede generar un archivo de información del sistema que se puede almacenar localmente o archivado en un par de formatos.	NAC (Network Access Control)
NTFS y Permisos sobre Archivos del Sistema	Los permisos en las estaciones de trabajo son tradicionalmente más permisivos para uso general por el personal de la organización. ¿Los permisos son demasiado permisivos? ¿Pueden permitir a los usuarios básicos instalar aplicaciones o control total sobre archivos o directorios criticos del sistema?	**File Explorer [Ficha Seguridad],** Regmon, Regedit / Regedt32, AccessEnum - enumera y o edita archivos NTFS y permisos de registro y / o recursos compartidos	FIM (File Integity Monitoring)- Antivirus Corporativo

Service Packs, Parches y Archivos de actualización	¿Está el SO actualizado con todos los Service Packs y cualquier corrección de host aplicable? ¿Existen trajes de aplicación de proveedores o productos como Office o Internet Explorer que requieran parches? ¿Está el motor antivirus y la firma actual?	**LANGuard, Nessus** - herramientas de exploración que revelarán qué protocolos de servicio y puertos son ofrecidos por el dispositivo. **Microsoft Baseline Security Advisor, HFnetCheck, sitio de Windows Update** - herramientas de validación de parches / service pack diseñadas específicamente para la plataforma de Windows que puede comprobar que un host cumpla con los parches / service packs más recientes.	NeWT Vulnerability Scanner
Comunicaciones, Procesos y Puertos del Sistema	¿Cuáles son las comunicaciones normales de punto final de la estación de trabajo? ¿Qué comunicaciones de puertos están saliendo y qué entrantes? ¿Está la estación de trabajo con conocimiento o sin saberlo alojando un servicio que está prohibido o debería estar en un servidor administrado, etc?	**Nmap, LANGuard, SuperScan, Nessus** - exploran las herramientas que revelarán qué protocolos del servicio y los puertos son ofrecidos por el dispositivo. **TCPView, utilidad útil TDIMon** que, a través de una GUI amigable, mapas en tiempo real las conexiones TCP de un ordenador host.	NAC (Network Access Control)

Figura 59. Descripción de Línea Base-Estaciones de Trabajo
Fuente: SANS.org

Anexo 11. Descripción de Línea Base-Red

Descripción de Linea Base-Red		Herramientas	Plataformas
Enumeración de Equipos	¿Cuántos y qué hosts / dispositivos están conectados en la red? Cuántos y qué son; Estaciones de trabajo, Servidores, Impresoras	Nmap, Amap, LANGuard, SuperScan, Nessus - las herramientas de exploración que se pueden dar una gama de IP para escanear y que tratará de identificar cualquier dispositivo en la red que responde. Nmap es particularmente rápido (versión Linux) y precisa en la identificación del host.	NAC (Network Access Control)
Configuraciones Switches	¿Sabe qué Switch / conmutador de puertos conectar y qué otros dispositivos de red, terminan los hosts de red o están desocupados? ¿Tiene y mantiene una matriz de puertos que mapea los puertos a los hosts y qué velocidades deben configurarse?	Diagrama manual y / o hoja de cálculo completa que representa los hosts de la red y los puertos a los que están conectados.	En las grandes empresas que involucran dispositivos administrados y cientos de hosts, es necesario un conjunto de administración. Con los dispositivos no administrados, documentar la configuración es un proceso manual

Configuraciones Routers/Firewall's	¿Cuáles son las configuraciones del Router? ¿Cuál es la subred IP de la red interna y cuál es su dirección WAN externa (Internet)? ¿Qué protocolos están configurados para enrutar / filtrar / bloquear? ¿Qué listas de control de acceso (ACL) existen que controlan el flujo de tráfico? ¿Qué subredes tiene el dispositivo abierto para fines de administración? Telnet Http Ssh ¿Es un router que combina firewall, DHCP y servicios de punto de acceso inalámbrico? En caso afirmativo, ¿están adecuadamente asegurados los servicios WAP?	Nmap, LANGuard, SuperScan, Nessus - exploran las herramientas que revelarán qué protocolos del servicio y los puertos son ofrecidos por el dispositivo.	Las grandes empresas normalmente tendrán un "Router" fronterizo", que es el dispositivo perimetral entre la red de la organización e Internet, estas herramientas pueden utilizarse para evaluar los protocolos de servicio por estos dispositivos tanto externos como internos.
Patrones de Tráfico	¿Cuál es el volumen normal y el patrón de tráfico de red? ¿Cuándo son los altos y bajos picos de uso y valles? ¿cuál es el volumen normal de tráfico entrante y saliente a través del router fronterizo / dispositivo o dispositivos de distribución? ¿A qué fuente y destinos circula el tráfico? ¿Cuáles son algunos de los tiempos de respuesta esperados entre hosts o dispositivos de red? ¿Puedes decir cuando están experimentando volúmenes normales o están en condiciones de sobrecarga, etc?	Microsoft Netmon, Ethereal, Wireshark - sniffers que cuando se coloca adecuadamente en la red puede grabar y guardar sesiones de todo el tráfico en la red, en tiempo real o para análisis posterior. CMD herramientas de línea de comandos - varias herramientas de línea de comandos de DOS como ping, traceroute, arp, netstat, nbtstat para determinar las configuraciones IP y tiempos de respuesta muy básicos.	Scrutinazer

Figura 60. Descripción de Línea Base-Red

Fuente: SANS.org

Anexo 12. Descripción de Línea Base-Servidores

Descripción de Linea Base-Servidores		Herramientas	Plataformas
NTFS y Permisos sobre Archivos del Sistema	Los servidores recién puestos en producción, si se dejan en su configuración predeterminada, pueden ser muy inseguros. Independientemente de la configuración, el permiso NTFS debe estar documentado para que los cambios se puedan identificar si se producen. Además, los permisos NTFS deben modificarse con frecuencia para garantizar la funcionalidad de una aplicación determinada.	**File Explorer [Ficha Seguridad],** Regmon, Regedit / Regedt32, AccessEnum - enumera y o edita archivos NTFS y permisos de registro y / o recursos compartidos	FIM (File Integity Monitoring)- Antivirus Corporativo- Hardening com Firewall de Windows y aplicando plantillas por GPO en Directorio Activo
Service Packs, Parches y Archivos de actualización	¿Está el SO actualizado con todos los Service Packs y cualquier corrección de host aplicable? ¿Existen suites de aplicaciones o servicios (IIS, SQL Server, servidores de correo) que requieran parches? ¿Está el motor antivirus y la firma actual?	LANGuard, Nessus - herramientas de exploración que revelarán qué protocolos de servicio y puertos son ofrecidos por el dispositivo. Microsoft Baseline Security Advisor, HFnetCheck, sitio de Windows Update - herramientas de validación de parches / service pack diseñadas específicamente para la plataforma de Windows que puede comprobar que un host cumpla con los parches / service packs más recientes.	WSUS (Windows Server Update Ss¿ystem)

Control de aplicaciones en Servidores	¿El sistema operativo tiene instalado un agente que comprueba las aplicaciones instaladas, son aplicaciones vulnerables? ¿Son aplicaciones legítimas?	Antivirus Corporativo	Antivirus Corporativo

Figura 61. Descripción de Línea Base-Servidores
Fuente: SANS.org

Anexo 13. Minuta Seguridad Informática, MSP.