



GESTION DE LA SEGURIDAD DE LA INFORMACION - MAAGTICSI

Edgar Vásquez | Responsable Gobierno Enterprise



TM

Introducción

El 19 de agosto de 2010, Intel, el mayor fabricante mundial de microchips, anuncia la compra de McAfee. De esta fusión surge *Intel Security* una división de *Intel*

- Cobertura de 125 millones de usuarios
- Más de 180 millones de dispositivos móviles cubiertos con los productos de McAfee
- 5,000,000 en despliegue de productos de McAfee
- Más de 800 patentes de seguridad
- Más de 120 socios con Alianza de McAfee Security Innovation
- 7.497 empleados de Intel de seguridad a nivel mundial *
- 120 países que conforman la huella global de McAfee
- \$ 2.3 mil millones de ingresos anuales +



Intel y McAfee están proporcionando un nuevo modelo de protección de la industria en todas las capas

Esta innovación tecnológica y colaboración está conduciendo a Nuevos productos y las sinergias en Seguridad Informática

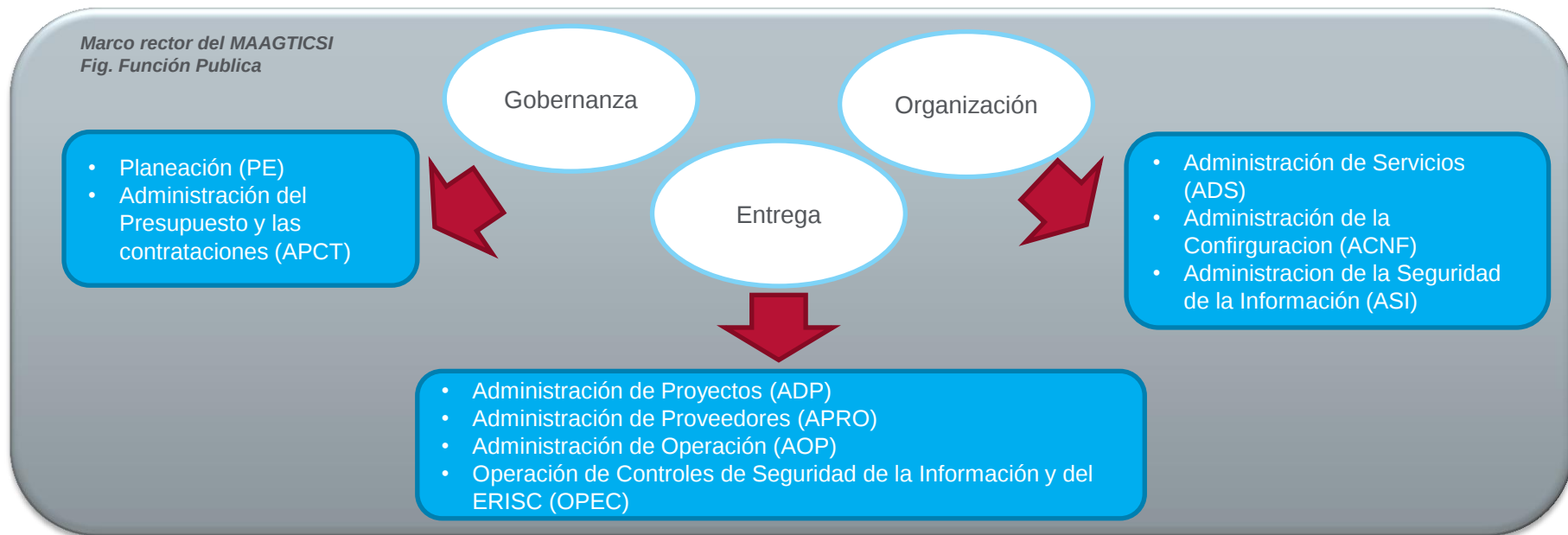
Antecedente

- **2011** El **MAAGTICSI** fue publicado en el año 2011 y es una actualización del MAAGTIC
- **2013** propone dentro de la Estrategia transversal “**Un Gobierno Cercano y Moderno**”, el establecer una Estrategia Digital Nacional para fomentar la adopción y el desarrollo de las tecnologías de la información y comunicaciones (TIC), e impulsar un gobierno eficaz que inserte a México en la Sociedad del Conocimiento
- **2014** Fue publicado en el Diario Oficial de la Federación por la Secretaría de la Función Pública una actualización del MAAGTICSI, en el Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional.

Antecedente

MAAGTICSI

- El manual contiene tres grupos, los procesos necesarios para propiciar la operación ágil y oportuna de las actividades de las TIC (Secretaría de la Función Pública, 2014).



¿Por qué es necesaria la Seguridad de la Información (SI)?

“La seguridad de la información tiene como objetivo proveer la Confidencialidad, Integridad y disponibilidad, además de la autenticación y no repudio durante el ciclo de vida (generación, análisis, almacenamiento, búsqueda, difusión y depuración) de la misma, para alcanzar las metas institucionales siguiendo lo establecido en la EDN, y en la legislación vigente aplicable en la materia”.



Amenazas

México, vulnerable ante amenazas cibernéticas

Nota



México cuenta con instituciones y marcos técnicos de ciberseguridad, pero no tiene una planificación y estructuras orgánicas. EL INFORMADOR / ARCHIVO

Más información

Síguenos en: [f](#) [t](#) [v](#) [p](#)

Internet | OEA | Cibernautas | Virus Informáticos

• En México los costos anuales generados por ciberdelitos en 2014 ascendieron a tres mil millones de dólares

Los delitos e inseguridad en la red día con día adquieren mayor importancia por falta de preparación ante las amenazas

CIUDAD DE MÉXICO (31/MAY/2015) - La creciente adopción de Tecnologías de la Información y Comunicación (TIC) en diversos ámbitos políticos, económicos y sociales en el país genera beneficios y nuevas oportunidades en diversos campos, aunque también abre las puertas para nuevas amenazas.

Al respecto, la consultora The Competitive Intelligence Unit (<http://www.the-ciu.net/>), afirmó que día con día los delitos e inseguridad en la red adquieren mayor importancia, no sólo por el aumento en su recurrencia, sino también por la falta de preparación de los países para responder las amenazas.

DINERO

EN IMAGEN

HACKER

GUÍA PARA [CUIDAR TU QUINCENA](#) [SER MILLONARIO](#) [ESTAR SANO](#) [EN LA MIRA](#)

México es de los países que más spam con virus envía

A pesar de los errores que cometen las organizaciones y el gobierno, la percepción en México es que los diferentes sectores están "algo preparados"

Aristegui

NOTICIAS



TEMAS DEL DÍA

MÉXICO

ENTREVISTAS

MULTIMEDIA

LIBROS

VI

Gobierno de México es vulnerable a ataques cibernéticos: EU

Un Informe de la Secretaría de Defensa apunta que el asunto aún no es considerado como de seguridad nacional, lo que abre las puertas a los hackers para inhabilitar los sistemas de operación del gobierno, servicios públicos, cámaras de vigilancia, vuelos y transporte en general, entre otros.

EL FINANCIERO

HOME

ECONOMÍA

EMPRESAS

NACIONAL

TECH

AFTER OFFICE

NACIONAL

Ataques cibernéticos ponen a prueba al Estado: Policía Federal

Amenazas

<https://wikileaks.org/hackingteam/emails?q=entermas&mfrom=&mto=&title=¬itle=&date=&nofrom=¬o=&count=50&sort=0>



Hacking Team

Today, 8 July 2015, WikiLeaks releases more than 1 million searchable emails from the Italian surveillance malware vendor Hacking Team, which first came under international scrutiny after WikiLeaks publication of the [SpyFiles](#). These internal emails show the inner workings of the controversial global surveillance industry.

Search by Terms in Email Search by Attached Filename Search by Email-ID

You must fill at least one of the fields below.

Search terms throughout whole of email:

You can use [boolean operators](#) to search emails.

For example **sudan rcs** will show results containing both words, **sudan | rcs** will show results with either words, while **sudan !rcs** will show results containing "sudan" and not "rcs".

Mail is From:

Mail is To:

Enter characters of the sender or recipient of the emails to search for.

☒ Advanced Search

Search Show

Acuerdo de Políticas y Disposiciones para la Estrategia Digital Nacional y el MAAGTICSI

“Artículos que hacen referencia en materia de Tecnologías de la Información y comunicaciones, y en la de Seguridad de la Información”



Artículo 26.-

Las Instituciones conforme a lo indicado en el MAAGTICSI, previo al inicio de la puesta en operación de un aplicativo de cómputo, realizarán el análisis de vulnerabilidades correspondiente, el cual preferentemente será realizado por un tercero, distinto a quién desarrolló el aplicativo. El resultado del análisis deberá preservarse para efectos de auditoría



Vulnerability Manager

Auditoría y remediación según prioridad: combina información de vulnerabilidad, gravedad e importancia de los activos para identificar, calificar y enfrentar con rapidez las infracciones y vulnerabilidades de sistemas y dispositivos en red.

Protección activa y pasiva de la red: combina la localización y la monitorización activas y pasivas de la red, y descubre los dispositivos virtualizados, móviles u ocultos que hay en ella.

Prueba de “no vulnerable”: una exigencia importante de los auditores es probar que usted no es vulnerable a las amenazas.

Identificación y correlación de amenazas nuevas: califica automáticamente el riesgo potencial de las amenazas nuevas al correlacionar eventos con sus datos de activos y vulnerabilidades.

Auditoría de políticas y evaluaciones de cumplimiento: define valores de verificaciones de políticas y determina si su organización cumple con las principales regulaciones. Mediante un asistente fácil de usar, le proporciona plantillas para SOX, FISMA, HIPAA, PCI y más.

Generación de informes flexible: categoriza los datos por activo o red y utiliza filtros para seleccionar y organizar los resultados en los informes.



Planeación

- Ejecutar la Planeación del Proyecto
- Dirigir el Taller de Protección de Datos
- Definir los Elementos de Datos y Modelo de Gobierno



Diseño

- Definición de Requerimientos
- Definición de Arquitectura de la Solución McAfee
- Definición de estándares de Implementación



Implementación

- Define security policies
- Develop security business process architecture
- Specify reporting requirements



Operación

- Configuración de Flujo de Trabajo
- Desarrollo de Análisis optimizado de Reglas
- Desarrollo de Programa Análisis de Descubrimientos



Optimización

- Revisión de Configuraciones
- Revisión de Reglas
- Revisión de uso por parte del Cliente



Transferencia de Conocimientos

- La transferencia de conocimientos ocurrirá de manera interactiva durante el tiempo comprometido y cubrirá la configuración y administración de la Solución.



McAfee Data Loss Prevention

Asegurar el éxito y reducir los riesgos

Principales Actividades

Project Management

Recolección interna de las principales fuentes de información

Reunión de Kick Off Kick off meeting

Planeación de Recursos.

Reunión de seguimiento semanal

Entrega de Reportes Semanales

Reunión de Cierre de Proyecto

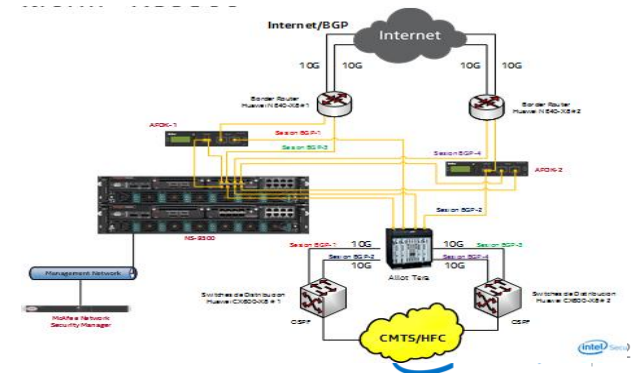
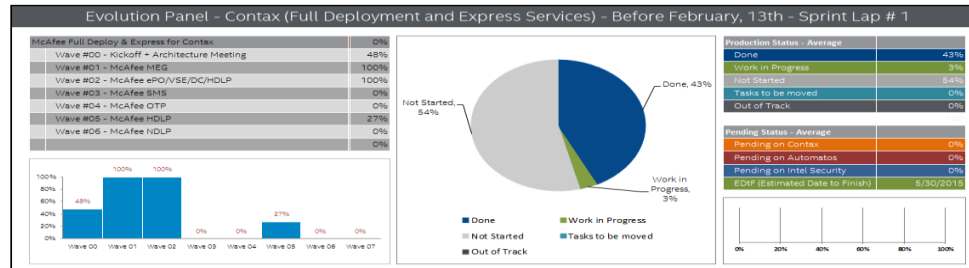
Diseño de Arquitectura

Documentación requerida para cumplir con regulaciones MAAGTICSI

Ingeniería de Detalle

Entrega de Requerimientos

Elaboración y presentación del diseño personalizado de acuerdo al ambiente e infraestructura del cliente.



Artículo 28.- Seguridad de la información considerada de Seguridad Nacional



Las Instancias de Seguridad Nacional observarán las disposiciones siguientes:

I. La información relacionada con la seguridad nacional, generada o custodiada, que pretendan diseminar, deberá identificarse previamente, mediante la asignación de alguno de los niveles de diseminación que a continuación se indican:

a) "AAA": se asignará este nivel cuando se trate de información requerida para el proceso de decisiones políticas fundamentales, esto es, para la adopción de decisiones sobre riesgos y amenazas a la seguridad nacional, por parte del Presidente de la República, previa consideración del Consejo de Seguridad Nacional, cuya revelación no autorizada pueda dañar la integridad, estabilidad o permanencia del Estado mexicano;

b) "AA": este nivel se asignará a la información resultante del ejercicio de atribuciones sustantivas, cuya revelación no autorizada pueda actualizar o potenciar un riesgo o amenaza a la seguridad nacional en términos de la Ley de la materia, o bien, comprometer su operación, las condiciones de seguridad de las instalaciones estratégicas o la integridad física de su personal, y

c) "A": se asignará este nivel a aquella información que derive del cumplimiento de las disposiciones jurídicas en materia de ejercicio del gasto, transparencia y rendición de cuentas, cuya revelación no autorizada pueda comprometer su operación, las condiciones de seguridad de las instalaciones estratégicas o la integridad física de su personal;



McAfee Data Loss Prevention

Bitácora de seguridad: El registro continuo de eventos e incidentes de seguridad de la información que ocurren a los activos de información.

El grupo estratégico de seguridad de la información deberá constatar que, como parte de los mecanismos que se establezcan para el ambiente operativo, se implemente un control para la elaboración y conservación de bitácoras de seguridad para los sistemas identificados como parte de una infraestructura crítica. En estas bitácoras se registrará el usuario, nombre de equipo, dirección IP, hora de entrada y salida del sistema, así como el tipo de consulta o cambios realizados en la configuración de las aplicaciones. Estas bitácoras tendrán un tiempo mínimo de almacenamiento de un año.



Integración Plataformas de Seguridad



McAfee Content Filtering
McAfee Email Gateway
McAfee Firewall
McAfee NSP
McAfee MVM
McAfee ePO



Network Access Control



Servidores Adm de Dominio



Dispositivo RSA



Checkpoint Smart Console



PIX/ASA



Servidores SAP



Servidores AIX



Bases de Datos



Ajuste de parámetros de logs genéricos



Casos de Uso de McAfee SIEM

- Actividad sospechosa generada desde conexiones VPN

The screenshot displays the McAfee SIEM interface. The top section, 'Physical Display', shows a list of 'Triggered Alarms'. The 'Alarm Name' column lists various security events, and the 'Summary' column provides details for each. The 'Assignee', 'Severity', 'Trigger Date', 'Acknowledge Date', and 'Ack' columns are also present.

Alarm Name	Summary	Assignee	Severity	Trigger Date	Acknowledge Date	Ack
ACL - Excessive Firewall/ACL Connections	Signature ID 'ACL - Excessive Firewall/ACL Connections Denied From Single Host' (47-1	Administrator	78	08/05/2015 10:34:00		
GTI - DNS Communication with Malicious	Signature ID 'GTI - DNS Communication with Malicious Host - Event or Flow' (47-40001	Administrator	75	08/05/2015 10:34:04		
Attack - Possible Conficker Worm Activity	Signature ID 'Attack - Possible Conficker Worm Activity' (47-4000152) match found	Administrator	79	08/05/2015 10:34:04		
Suspicious - Events from DataCenters CEMEX	Signature ID 'Suspicious - Events to DataCenters CEMEX' (47-6000026) match found	G-MXOCC SIEM	80	08/05/2015 10:24:00		
Suspicious - Events to DataCenters CEMEX	Signature ID 'Suspicious - Events to DataCenters CEMEX' (47-6000031) match found	e-ragarcia@NO	82	08/05/2015 10:24:00		
Login - Brute Force Login - Source User	Signature ID 'Login - Brute Force Login Attempts from a Single Source' (47-6000022) n	G-MXOCC SIEM	30	08/05/2015 10:23:59		
ACL - Excessive Firewall/ACL Connections	Signature ID 'ACL - Excessive Firewall/ACL Connections Denied From Single Host' (47-1	Administrator	78	08/05/2015 10:23:59		
GTI - DNS Communication with Malicious	Signature ID 'GTI - DNS Communication with Malicious Host - Event or Flow' (47-40001	Administrator	75	08/05/2015 10:14:14		
Suspicious - Events to DataCenters CEMEX	Signature ID 'Suspicious - Events to DataCenters CEMEX' (47-6000031) match found	e-ragarcia@NO	82	08/05/2015 10:13:53		
Suspicious - Events from VPN connections	Signature ID 'Multiple Signatures...' match found	e-ragarcia@NO	79	08/05/2015 10:13:53		
ACL - Excessive Firewall/ACL Connections	Signature ID 'ACL - Excessive Firewall/ACL Connections Denied From Single Host' (47-1	Administrator	78	08/05/2015 10:13:50		
Login - Brute Force Login - Source User	Signature ID 'Login - Brute Force Login Attempts from a Single Source' (47-6000022) n	G-MXOCC SIEM	30	08/05/2015 10:04:08		
Login - Brute Force Login Attempts	Signature ID 'Login - Brute Force Login Attempts with administrator user' (47-6000023	G-MXOCC SIEM	75	08/05/2015 10:04:04		
Suspicious - Events to DataCenters CEMEX	Signature ID 'Suspicious - Events to DataCenters CEMEX' (47-6000031) match found	e-ragarcia@NO	82	08/05/2015 10:03:41		
Active Directory Changes - Suspicious Us	Signature ID 'Active Directory Changes - Suspicious Users' (47-6000026) match found	G-MXOCC SIEM	80	08/05/2015 10:03:40		
ACL - Excessive Firewall/ACL Connections	Signature ID 'ACL - Excessive Firewall/ACL Connections Denied From Single Host' (47-1	Administrator	78	08/05/2015 10:03:39		

The 'Event Details' section is expanded, showing a table with columns: Severity, Rule Message, Event Count, Source IP, Destination IP, Protocol, Last Time, and Event Subtype. The event is categorized as 'Suspicious - Events from VPN connections'.

Severity	Rule Message	Event Count	Source IP	Destination IP	Protocol	Last Time	Event Subtype
6	DCERPC: Frag Length Overly Long	1	10.26.180.183	10.161.200.40	n/a	08/05/2015 10:03:32	untrusted

The 'Event Details' section is further expanded, showing a list of events matching the criteria. The event is categorized as 'Suspicious - Events from VPN connections'.

For Source IP 10.26.180.183 the following event(s) were found within 50 minutes:

- 1 events matched the following criteria:
- Normalization Rule in Exploit, Host Port Scan, Malware, Potential Exploit, Suspicious Activity, Suspicious Packet
- Source IP in 10.16.112.0/21, 10.26.180.0/22

Conclusión

Es muy importante que existan mejores procesos y políticas que permitan un mejor manejo de la información y adoptar las medidas necesarias a través de un **Sistema de Gestión de Seguridad de la Información (SGSI)** basado en el **MAAGTICSI (Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información)**

La Administración Pública Federal y los responsables de la Seguridad de Tecnologías de información tiene un gran reto para poder estandarizar y llevar a cabo estas políticas para la Estrategia Digital Nacional



Muchas Gracias !!!!!

Edgar Vásquez Cruz



Mail: edgar_vasquez@mcafee.com

Web: www.intelsecurity.com