CONTEXTO DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Yeny Yovana Segura Mancipe
yysegura@hotmail.com
Universidad Piloto de Colombia

Abstract **–** This article shows a context on the management of information security incidents: existing international and national initiatives to safeguard the confidentiality, integrity and availability of information in organizations, national regulatory framework and the ISO/IEC 27035:2011 standard**.**

Resumen **–** En este artículo se muestra un contexto sobre la gestión de incidentes de seguridad de la información: iniciativas internacionales y nacionales existentes para salvaguardar la confidencialidad, integridad y disponibilidad de la información en las organizaciones, marco normativo nacional y la norma ISO/IEC 27035:2011**.**

Índice de Términos **–** Incidente, información, gestión de incidentes, seguridad de la información, tecnologías de la información**.**

I. INTRODUCCIÓN

El vertiginoso desarrollo de las tecnologías de la información y de las comunicaciones ha traído consigo innegables beneficios para las personas y las organizaciones, así como riesgos asociados a la seguridad de los sistemas de información y la información en sí misma. Es por eso que hoy en día, la seguridad se ha convertido en parte fundamental de la gestión de las organizaciones, convirtiéndose en un reto asegurar la infraestructura tecnológica, las aplicaciones y la información, de tal manera que el sistema continúe ejecutándose correctamente bajo un ataque malicioso.

En el marco de la gestión de la seguridad de la información se debe desarrollar la gestión de incidentes de seguridad, de tal manera que le permita a las organizaciones responder adecuadamente a estos incidentes y así proteger la confidencialidad, integridad y disponibilidad de la información, principal activo de las organizaciones.

II. MOTIVACIÓN DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD

Las estadísticas presentadas por organizaciones expertas en seguridad informática a nivel internacional, son dicientes frente a la cantidad e impacto de los incidentes de seguridad.

El informe ESET Security Report 2017, muestra cuáles fueron los principales incidentes de seguridad en las empresas durante el año anterior, éste contó con la participación de más de cuatro mil ejecutivos y profesionales de TI de Argentina, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay y Venezuela.

El informe muestra como los códigos maliciosos se han posicionado como la principal causa de incidentes de seguridad en las compañías de la región, con un importante crecimiento en 2016 al obtener el 49% de las respuestas afirmativas en las encuestas.

Debido a la proliferación del *ransomware* (secuestro de información en el ámbito digital), en esta ocasión ESET cuenta con una categoría de incidentes exclusiva para este tipo de *malware*, en razón a que el cifrado de archivos con fines de extorsión merece una mención aparte debido a las repercusiones que ha tenido para las organizaciones en el último tiempo. Es importante señalar que, en su primera aparición como una categoría de incidentes, el *ransomware* se posicionó en el segundo lugar de los resultados de las encuestas con un 16%, desplazando al *phishing* hacia la tercera posición con 15%.

En el siguiente gráfico se muestra cuáles fueron los principales incidentes de seguridad que afectaron a las empresas latinoamericanas durante el año 2016:

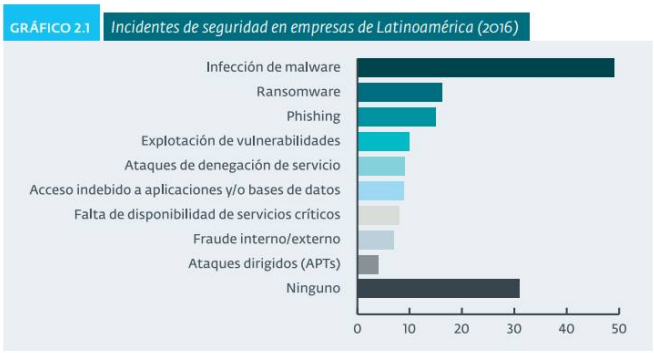

Fig. 1. Incidentes de seguridad en empresas de Latinoamérica [6].

III. INICIATIVAS INTERNACIONALES Y GLOBALES

A. Convenio sobre la ciberdelincuencia

El convenio sobre la ciberdelincuencia es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en internet, mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones; este fue elaborado por el Consejo de Europa con la participación activa de los estados observadores de Canadá, Japón y China.

El convenio sobre la ciberdelincuencia, adoptado el 23 de noviembre de 2001 en Budapest, tiene como principal objetivo el que figura en el preámbulo: aplicar una política penal común encaminada a la protección de la sociedad contra el cibercrimen, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional.

Es un instrumento internacional que tiene como fin armonizar el derecho sustantivo y dar herramientas esenciales en la investigación de los delitos que se cometen por vías informáticas. Es el primer convenio internacional sobre delitos informáticos y es visto como el estándar mundial sobre la materia y tiene los siguientes objetivos:

- Mejorar los instrumentos de cooperación internacional.
- Armonizar el derecho sustantivo, no limitarlo.
- Creación de instrumentos procesales comunes.
- La instauración de una red permanente de contactos

Los países miembros se comprometen a tipificar como delitos, dentro de sus respectivas legislaciones, distintas acciones criminales cometidas por medios informáticos: acceso ilícito, interceptación ilícita, interferencia en los datos, interferencia en el sistema, abuso de los dispositivos, falsificación informática, fraude informático, delitos sobre pornografía infantil y delitos sobre infracciones de la propiedad intelectual.

B. Directrices de la OCDE para la seguridad de sistemas y redes de información: hacia una cultura de seguridad

La Organización para la Cooperación y el Desarrollo Económico (OCDE) consiente que, dada la creciente interconexión, los sistemas y las redes de información son más vulnerables, ya que están expuestos a un número creciente, así como a una mayor variedad de amenazas y de vulnerabilidades. Esto hace que surjan nuevos retos que deben abordarse en materia de seguridad.

Por lo anterior, establece las siguientes directrices que aplican para todos los participantes de la nueva sociedad de la información y sugieren la necesidad de tener una mayor conciencia y entendimiento de los aspectos de seguridad, así como de la necesidad de desarrollar una "cultura de seguridad":

1) Concienciación: Los participantes deberán ser conscientes de la necesidad de contar con sistemas y redes de información seguros, y tener conocimiento de los medios para ampliar la seguridad.
2) Responsabilidad: Todos los participantes son responsables de la seguridad de los sistemas y redes de información.
3) Respuesta: Los participantes deben actuar de manera adecuada y conjunta para prevenir, detectar y responder a incidentes que afecten la seguridad.
4) Ética: Los participantes deben respetar los intereses legítimos de los otros.
5) Democracia: La seguridad de los sistemas de información y redes debe ser compatible con los valores esenciales de una sociedad democrática.
6) Evaluación del riesgo: Los participantes deben llevar a cabo evaluaciones de riesgo.
7) Diseño e implementación de seguridad: Los participantes deben incorporar la seguridad como un elemento esencial de los sistemas de información y redes.
8) Gestión de la Seguridad: Los participantes deben adoptar una visión integral de la administración de la seguridad.
9) Reevaluación: Los participantes deben revisar y reevaluar la seguridad de sus sistemas de información y redes y hacer las modificaciones pertinentes a sus políticas, prácticas, medidas y procedimientos de seguridad.

Estas directrices pretenden dar respuesta a un ambiente de seguridad cada vez más cambiante, a través de la promoción del desarrollo de una cultura de seguridad, esto es, centrándose en la seguridad del desarrollo de sistemas y redes de información, así como en la adopción de nuevas formas de pensamiento y comportamiento en el uso e interconexión de sistemas y redes de información.

IV. INICIATIVAS NACIONALES

A. Lineamientos de política de ciberseguridad y ciberdefensa

En el año 2011, el Gobierno Nacional aprobó el Documento CONPES 3701 en el cual establecieron los lineamientos de política de ciberseguridad y ciberdefensa. Este documento establece las medidas que deben adoptar las entidades que tengan acceso al manejo de la información para contrarrestar el incremento de las amenazas informáticas, dentro de las cuales se establecieron normas técnicas y estándares nacionales e internacionales, así como iniciativas internacionales sobre protección de infraestructura crítica y ciberseguridad. El gobierno nacional a través del CONPES 3701 de 2011 definió la creación de tres grupos orientados a proteger a los cibernautas y los sistemas de información nacional, así:

- Grupo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT
- Comando Conjunto Cibernético de las Fuerzas Militares
- Comisión Intersectorial, en la cual participan de una manera integrada el Ministerio de Defensa Nacional, Ministerio de Justicia y del Derecho, Ministerio de Tecnologías de la Información y las Comunicaciones y otras entidades como el SENA, el Consejo Superior de la Judicatura, la Comisión de Regulación de Comunicaciones y la Agencia Nacional de Inteligencia.

B. Política nacional de seguridad digital

En abril del 2016 se aprobó el Documento CONPES 3854 de Seguridad Digital Integral, en el que se estableció la implementación en cinco ejes:

1) Establecer un marco institucional claro en torno a la seguridad digital, basado en la gestión de riesgos.
2) Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital.
3) Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos.
4) Fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos.
5) Impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional.

Dentro del CONPES 3854 se manifestó que la política de Ciberseguridad y Ciberdefensa adoptada por Colombia, debe ser complementada para responder adecuadamente a los nuevos tipos de incertidumbres e incidentes digitales y, adicional a lo anterior, se puso en evidencia que Colombia dispone de un marco normativo nacional disperso en torno a la seguridad digital que comprende leyes, decretos y otros actos expedidos bajo condiciones diferentes a las actuales, por lo cual se creó la política nacional de seguridad digital.

Para cumplir con los objetivos establecidos en los frentes expuestos en la Política Nacional de Seguridad Digital se establecieron diferentes estrategias. En concreto, para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital a nivel nacional e internacional, se planteó la búsqueda de la adhesión de Colombia a diferentes convenios internacionales, dentro del cual se resaltó el Convenio de Budapest.

C. Proyecto de Ley para adherir al Convenio de Budapest

El Gobierno Nacional, en cabeza de la Cancillería y los Ministerios de Justicia, Defensa y Tecnologías de la Información y las Comunicaciones (TIC), presentó al Congreso de la República un proyecto de ley para que Colombia se adhiera al Convenio de Budapest, que busca construir una política mundial común contra la ciberdelincuencia.

El proyecto de ley inició su trámite legislativo en la Comisión Segunda del Senado y una vez cursados los cuatro debates en el Congreso, pasará a revisión de la Corte Constitucional y posteriormente a sanción presidencial. Luego, la Cancillería hará oficial la adhesión al convenio que le permitirá a Colombia no solo avanzar en temas de cooperación internacional contra delitos informáticos, sino también fortalecer las leyes y regulaciones nacionales contra el ciberdelito en todos los niveles.

El Convenio de Budapest facilita la adopción de medidas para detectar y perseguir, tanto en territorio nacional como en área internacional, a los posibles ciberdelicuentes. En esa medida, se prevé la creación de una red que opere 24 horas de los 7 días de la semana, para garantizar una rápida cooperación internacional que reaccione frente a algún tipo de incidente. En consecuencia, en casos que suponen el uso ilícito de las redes de comunicación, el convenio permite investigar y judicializar estos crímenes para que Colombia no se convierta en un paraíso donde los ciberdelincuentes extiendan sus redes.

D. Guía para la gestión y clasificación de incidentes de seguridad de la información

La Guía para la gestión y clasificación de incidentes de seguridad de la información elaborara por el Ministerio de Tecnologías de la Información y las Comunicaciones, está destinada para las entidades públicas de orden nacional y entidades públicas del orden territorial, así como proveedores de servicios de gobierno en línea, y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de TI en el marco de la Estrategia de Gobierno en Línea.

La guía está basada en mejores prácticas y documentos de uso libre por parte del NIST (National Institute of Standards and Technology – (Computer Security Incident Handling Guide), y en los lineamientos recomendados en la Norma la ISO IEC 27001 – 2013, numeral 16 de la misma, para la gestión de incidentes.

Para definir las actividades de esta guía se incorporaron componentes definidos por el NIST alineados con los requerimientos normativos de la NTC–ISO–IEC 27035-2013 para la estrategia de gobierno en línea.

El objetivo principal del Modelo de gestión de incidentes de seguridad de la información es tener un enfoque estructurado y bien planificado que permita manejar adecuadamente los incidentes de seguridad de la información.

La gestión de incidentes de seguridad de la información involucra los siguientes procesos:

- Planificación y preparación para la gestión del Incidente
- Detección y análisis.
- Contención, erradicación y recuperación.
- Actividades Post-Incidente.

Se recomienda a las entidades crear un equipo de atención de incidentes de seguridad en cómputo CSIRT o un grupo que haga sus veces, quienes se encargaran de definir los procedimientos a la atención de incidentes, realizar la atención y manejar las relaciones con entes internos y externos.

V. MARCO NORMATIVO NACIONAL

Colombia ha impulsado leyes orientadas a proteger la información en sus diferentes medios, los datos personales, el comercio electrónico, etc. En la siguiente tabla se muestra la normatividad nacional relativa a la seguridad de la información:

TABLA I
MARCO NORMATIVO NACIONAL

Marco Normativo Nacional		
Norma	**Objeto**	**Tema**
Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.	Comercio electrónico y firmas digitales
Ley 594 de 2000	Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones	Ley General de Archivos, criterios de seguridad
Ley 679 de 2001	Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución.	Pornografía infantil, responsabilidad ISPs
Ley 962 de 2005	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.	Simplificación y racionalización de trámite. Atributos de seguridad en la información electrónica de entidades públicas
Ley 1150 de 2007	Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con recursos públicos.	Seguridad de la información electrónica en contratación en línea
Ley 1266 de 2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.	Habeas data financiera, y seguridad en datos personales
Ley 1273 de 2008	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.	Delitos Informáticos y protección del bien jurídico tutelado que es la información
Ley 1341 de 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.	Tecnologías de la información y aplicación de seguridad
Ley 1437 de 2011	Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo.	Procedimiento administrativo y aplicación de criterios de seguridad
Ley 1480 de 2011	Por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones.	Protección al consumidor por medios electrónicos. Seguridad en transacciones electrónicas
Decreto Ley 019 de 2012	Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la administración pública.	Racionalización de trámites a través de medios electrónicos. Criterio de seguridad
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.	Ley estatutaria de Protección de datos personales
Ley 1621 de 2013	Por medio de la cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia y cumplir con su misión	Ley de Inteligencia, Criterios de seguridad

Marco Normativo Nacional		
Norma	**Objeto**	**Tema**
	constitucional y legal, y se dictan otras disposiciones.	
Ley 1712 de 2014	Por medio de la cual se crea la Ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.	Transparencia en el acceso a la información pública

Fuente: autor.

VI. INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Un incidente de seguridad de la información, de acuerdo a la norma ISO 27001, es un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones de negocio y amenazar la seguridad de la información, es decir, pueden afectar la confidencialidad, la integridad y la disponibilidad de la información.

La norma ISO/IEC 27035, presenta las siguientes categorías de incidentes de seguridad de la información:

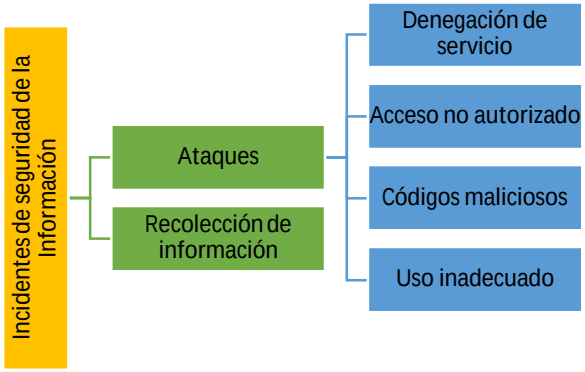

Fig. 2. Categorías de Incidentes de Seguridad de la Información.
Fuente: autor.

A. Denegación del servicio

Los ataques de Denegación de Servicio (DoS) y Denegación de Servicio Distribuida (DDoS), son incidentes de seguridad que hacen que un sistema, servicio o red dejen de operar a su capacidad prevista, provocando la denegación de servicio a los usuarios legítimos del sistema afectado. Existen dos tipos de incidentes de denegación causados por medios técnicos: eliminación y agotamiento de recursos.

A continuación, se presentan algunos ejemplos típicos de incidentes de denegación del servicio:

- Envío masivo de paquetes TCP para llenar el ancho de banda de red con tráfico de respuesta.
- Envío de datos en un formato inesperado, a un sistema, servicio o red, con la intención de hacerlo colapsar o interrumpir su operación normal.
- Apertura de múltiples sesiones autorizadas con un sistema, servicio o red particular, con la intención de agotar sus recursos

Estos ataques se realizan con frecuencia por medio de *botnets*, un grupo de robots de software (códigos maliciosos) que funcionan de forma autónoma y automática. Los *botnets* pueden comunicarse con miles de computadores afectados.

Algunos incidentes técnicos de denegación del servicio pueden ser causados accidentalmente, por ejemplo, una mala configuración realizada por un operador o por incompatibilidad del software de la aplicación, pero la mayoría de las veces estos incidentes son deliberados.

A continuación, se describen los métodos más frecuentes de denegación del servicio:

Ataque Reflector: en un ataque reflector un servidor envía múltiples solicitudes con una dirección IP falsificada a un servicio en un servidor intermedio (Por lo general se usan servicios basados en protocolo UDP). El servidor responde a la petición empleando la dirección falsificada, de esta forma el servidor que responde es quien aparece como ejecutante del ataque y por esa razón se denomina el reflector (espejo). El ataque de DDoS puede tener como objetivo el servidor cuya dirección fue falsificada o el servidor que actúa como el reflector.

Ataque amplificado. Al igual que un ataque por reflector, se emplea una petición con una dirección IP falsa a un servidor intermediario. A diferencia del ataque por un reflector, el objetivo será emplear toda una red como elemento intermediario para el ataque. La intención es emplear una petición ICMP o UDP a una dirección de *broadcast* para que muchos servidores respondan a la misma, como la dirección es falsa toda la red responderá al servidor que será víctima del ataque.

Ataques *Flood*. En un ataque por inundación, un servicio o recurso se hace indisponible iniciando una elevada serie de solicitudes de conexión incompletas. Este tipo de ataque satura al receptor imposibilitándolo para atender nuevas conexiones.

Los incidentes de denegación del servicio causados por medios no técnicos, que dan como resultado pérdida de información, servicios y/o aplicaciones pueden ser causados por:

- Violaciones a las medidas de seguridad físicas, presentando como resultado robo o daño intencionado y destrucción de equipos

- Daño accidental al *hardware* por incendio o por inundación
- Condiciones ambientales extremas, por ejemplo, altas temperaturas
- Mal funcionamiento de sistemas, o sobrecarga
- Cambios no controlados en el sistema
- Mal funcionamiento en el software o hardware

B. Acceso no autorizado

Esta categoría de incidentes consiste en intentos reales no autorizados, para acceder o utilizar incorrectamente un sistema, servicio o red. Algunos ejemplos de incidentes de acceso no autorizado provocados técnicamente incluyen:

- Intentos por recuperar archivos de contraseñas
- Ataques por desbordamiento de búfer para obtener acceso privilegiado a un objetivo, por ejemplo, administrador del sistema
- Aprovechamiento de las vulnerabilidades del protocolo para secuestrar o dirigir equivocadamente las conexiones de red legítima
- Intentos de elevar privilegios a recursos o información

Los incidentes de acceso no autorizado causados por medios no técnicos, que dan como resultado la divulgación o modificación de información, o mala utilización de servicios de información, pueden ser originados por lo siguiente:

- Violaciones a las medidas de seguridad física, dando como resultado acceso no autorizado a la información
- Sistemas operativos mal configurados o que operan, en forma deficiente, debido a cambios no controlados en el sistema
- Mal funcionamiento del software o del hardware

El acceso no autorizado se logra cuando se explota una vulnerabilidad del sistema operativo o de una aplicación, cuando se obtienen usuarios o claves o mediante ataques de ingeniería social. Los atacantes usualmente obtienen acceso limitado a partir de la vulnerabilidad y mediante ese acceso buscan elevar su nivel de privilegios de acceso.

Algunos ejemplos de acceso no autorizado incluyen:

- Comprometer la cuenta del superusuario de un servidor controlador de dominio
- Adivinar o romper *password*
- Ver o copiar información sensible sin tener autorización como registros de nómina, información de hoja de vida médica, números de tarjetas de crédito
- Ejecutar programas para exploración o indagación de redes como *sniffer* o *scanners*, para observar nombres de usuario o claves
- Usar un *filesystem* compartido para distribuir software ilegal o copias ilegales de software
- Usar un computador desatendido sin la debida autorización

En la legislación colombiana, el acceso no autorizado, está tipificado como delito penal, así lo señala el Código Penal Colombiano, en su Artículo 269A: "Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes".

C. Códigos maliciosos

Los códigos maliciosos hacen referencia a un programa o parte de éste insertado en otro programa, con la intención de modificar su comportamiento original, usualmente para realizar actividades maliciosas como robo de información y de identidad, destrucción de información y de recursos, denegación de servicio, etc. Los ataques con códigos maliciosos se pueden subdividir en cinco categorías: virus, gusanos, troyanos, códigos móviles y combinaciones de éstos. Hace algunos años los virus se crearon para atacar cualquier sistema vulnerable, en la actualidad los códigos maliciosos se usan para realizar ataques dirigidos.

De acuerdo con la publicación de ESET, el *ransomware* ha sido uno de los códigos maliciosos que más relevancia ha tenido en los últimos tiempos, afectando a usuarios y empresas de todo el mundo. El *ransomware* (secuestro de información) es el término genérico para referirse a todo tipo de software malicioso que le exige al usuario del equipo el pago de un rescate.

Este tipo de *malware* suele dañar el equipo y los datos que este contiene; puede haber cifrado los documentos y exigir el pago de un rescate para desbloquear el acceso a ellos. Los códigos que actúan de este modo se conocen como *filecoder* (codificador de archivos). El más popular es *Cryptolocker*.

Posibles modos o vías de infección:

La forma de infección más usual es a través de la apertura de archivos adjuntos de correos electrónicos no solicitados, o al hacer clic en vínculos que aseguran provenir de entidades bancarias o de empresas de mensajería. También se encontraron versiones de *cryptolocker* que se distribuyeron a través de redes *peerto-peer* (P2P) para compartir archivos, haciéndose pasar por claves de activación para programas populares de software como Adobe Photoshop y Microsoft Office.

Si el equipo se infecta, Cryptolocker busca una amplia gama de tipos de archivos para cifrar y, una vez que terminó el trabajo sucio, muestra un mensaje donde exige una transferencia electrónica para descifrar los archivos.

El uso de código malicioso está contemplado como delito penal en Colombia, así lo señala el Código Penal Colombiano en su artículo 269E: "Uso de software malicioso. El que, sin

estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes".

D. Uso inadecuado

Este tipo de incidentes ocurre cuando un usuario transgrede las políticas de seguridad del sistema de información de la organización. Estos incidentes no son ataques en el sentido estricto de la palabra, pero con frecuencia se reportan como incidentes y los debería gestionar el ISIRT. Ejemplos de incidentes de seguridad de uso inadecuado son:

- Descargar e instalar herramientas para piratería informática
- Usar el correo corporativo para asuntos personales
- Usar recursos corporativos para crear un sitio no autorizado
- Usar actividades entre colegas para adquirir o distribuir archivos piratas

Otras situaciones que se consideran incidentes de seguridad de uso inapropiado incluyen:

- Descarga e instalación de software ilegal
- Descarga o acceso a material relacionado con pornografía, terrorismo, segregación racial, etc.
- Uso del correo electrónico para enviar correo masivo no deseado
- Envío de correos intimidatorios, ofensivos o agresivos
- Uso de servicios de archivo compartido para intercambiar música, vídeos, software o todo material protegido por derechos de autor.
- Transferir información de propiedad de la organización sin autorización a terceros.

E. Recolección de información

Esta categoría de incidentes incluye las actividades asociadas con la identificación de objetivos potenciales y el entendimiento de los servicios que funcionan en dichos objetivos. La meta es identificar:

- La existencia de un objetivo y comprender la topología de la red circundante, y con quien se comunica rutinariamente el objetivo
- Las vulnerabilidades potenciales en el objetivo o en el ambiente de red, que pudieran ser aprovechadas.

Ejemplos típicos de ataques para recolección de información por medios técnicos incluyen:

- Volcado de registros de sistemas de nombres de dominio para el dominio de internet del objetivo
- Envío masivo de paquetes TCP para encontrar sistemas que estén activos
- Sondeo del sistema para identificar el sistema operativo del equipo
- Escaneo de los puertos de red disponibles en un sistema para identificar los servicios y la versión del software de estos servicios
- Escaneo de uno o más servicios que se conocen que son vulnerables, a través de un rango de direcciones de red.

Los incidentes de recolección de información pueden ser generados por medios no técnicos, tales como:

- Violaciones a las medidas de seguridad física, que dan como resultado acceso no autorizado a información, y robo de equipos para almacenamiento de datos que contienen datos importantes.
- Sistemas operativos mal configurados o mal funcionamiento del hardware o el software, que da como resultado personal interno o externo que obtiene acceso a información para la que no está autorizado.

VII. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La norma ISO/IEC 27035 proporciona a las organizaciones un enfoque estructurado y planificado para:

- Detectar, reportar y evaluar incidentes de seguridad de la información
- Responder a incidentes de seguridad de la información y hacer su gestión.
- Detectar, evaluar y gestionar las vulnerabilidades de seguridad de la información
- Mejorar continuamente la seguridad de la información y la gestión de incidentes

Las organizaciones que usan un enfoque estructurado para la gestión de incidentes de seguridad de la información, obtienen los siguientes beneficios:

- Mejora de la seguridad global de la información
- Reducción de impactos adversos para el negocio
- Fortalecimiento del enfoque en prevención de incidentes
- Fortalecimiento de la priorización
- Fortalecimiento de la evidencia
- Contribución a las justificaciones de presupuesto y de recursos
- Mejora de actualizaciones a los resultados de la evaluación y a gestión de riesgos de seguridad de la información
- Mejora en la conciencia en seguridad de la información y el material del programa de entrenamiento
- Suministro de entradas para las revisiones de la política de seguridad de la información

Según la norma ISO 27000:

Evento de Seguridad de la Información: Presencia identificada de una condición de un sistema, servicio o red, que

indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Incidente de seguridad de la información: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones de negocio y amenazar la seguridad de la información.

Equipo de respuesta a incidentes de seguridad de la información – ISIRT: Equipo conformado por miembros confiables de la organización, que cuentan con las habilidades y competencias para tratar los incidentes de seguridad de la información, durante el ciclo de vida de éstos.

Fases de la gestión de incidentes de seguridad

La gestión de incidentes de seguridad de la información consta de las siguientes fases:

1. Planificación y preparación
2. Detección y reporte
3. Evaluación y decisión
4. Respuestas
5. Lecciones aprendidas

Fig. 3. Fases de la gestión de incidentes de seguridad de la información. Fuente: autor.

Fase de planificación y preparación: esta fase incluye las siguientes actividades:

a) Formulación y generación de una política de gestión de eventos, incidentes y vulnerabilidades de seguridad de la información con el correspondiente apoyo de la alta dirección, para asegurar la asignación de recursos y se mantenga una capacidad de respuesta a incidentes.
b) Actualización de las políticas de gestión de riesgos y de seguridad de la información, a nivel corporativo y de TI.
c) Definición y documentación de un esquema detallado de gestión de incidentes de seguridad de la información, que incluya los siguientes aspectos: una escala de clasificación de eventos e incidentes de seguridad de la información, formatos para reportar eventos, incidentes y vulnerabilidades de seguridad, Procedimientos operativos para el ISIRT, con asignación roles y responsabilidades.
d) Establecimiento de un ISIRT con un programa adecuado de formación para sus integrantes
e) Establecer y mantener relaciones adecuadas con organizaciones internas y externas relacionadas directamente con la gestión de eventos, incidentes y vulnerabilidades de seguridad de la información.
f) Establecer, implementar y operar mecanismos técnicos para apoyar el esquema de gestión de incidentes, tales como: auditorías internas, gestión de vulnerabilidades, sistemas de detección de intrusos, software antivirus, entre otros.
g) Diseño y desarrollo de un programa de formación y concientización en gestión de eventos, incidentes y vulnerabilidades, que involucre a todo el personal de la organización.
h) Probar el uso del esquema de gestión de incidentes de seguridad de la información, sus procesos y procedimientos, para poner a prueba el esquema en una situación real, verificar cómo se comporta el ISIRT bajo la presión de un incidente grave (se deberían organizar pruebas periódicas para verificar procesos/procedimientos y para verificar como responde el ISIRT a incidentes complejos severos, mediante el simulacro de ataques, fallas o defectos reales). Es conveniente prestar atención particular a la creación de escenarios simulados que deberían basarse en amenazas de seguridad de la información nuevas y reales.

La política de gestión de eventos, incidentes y vulnerabilidades de seguridad de la información debe estar dirigida a todas las personas que tienen acceso legítimo a los sistemas de información e instalaciones relacionadas.

Fase de detección y reporte: Esta fase involucra la detección de las ocurrencias de eventos de seguridad de la información, la recolección de información asociada con ellas, y el reporte de dichas ocurrencias, por medios humanos o electrónicos. Esta fase también involucra la detección y reporte de vulnerabilidades de seguridad de la información que aún no han sido aprovechadas para causar eventos o incidentes de seguridad de la información. Para la fase de detección y reporte una organización debe asegurar las siguientes actividades:

a) Detectar y reportar la ocurrencia de un evento de seguridad de la información, o la existencia de una vulnerabilidad de seguridad de la información ya sea por el personal o clientes de la organización, o automáticamente con la ayuda de alertas de sistemas de seguimiento de seguridad como IDS/IPS, programas antivirus, *honeypots*, motores de correlación; alertas de seguimiento de redes tales como cortafuegos; análisis de información de registro de dispositivos, servicios, equipos y diversos sistemas; escalamiento de eventos anómalos detectados por el área de TIC y mesas de ayuda, reportes de usuarios y

notificaciones externas como proveedores de servicios de telecomunicaciones, ISIRT nacionales.
b) Recolectar información sobre un evento o vulnerabilidad de seguridad de la información.
c) Asegurar que todos los involucrados en el PoC (Punto de Contacto) registren adecuadamente todas las actividades, resultados y decisiones para análisis posterior
d) Asegurar que se recolecta evidencia electrónica y se almacena en forma segura, y que se hace seguimiento continuo de su preservación
e) Asegurar que el régimen de control de cambios se mantenga y cubra el seguimiento de los eventos y vulnerabilidades
f) Escalar, según se requiera durante toda la fase, para revisión y/o decisiones posteriores
g) Registrar en un sistema de seguimiento de incidentes

Toda la información recolectada de un evento o vulnerabilidad de seguridad de la información debe ser almacenada en la base de datos de eventos/incidentes/vulnerabilidades gestionada por el ISIRT.

Fase de evaluación y decisión: Esta fase involucra la evaluación de la información asociada con las ocurrencias de eventos de seguridad de la información, y la decisión a cerca de si son incidentes de seguridad de la información. Incluye las siguientes actividades:

a) Actividad para que el PoC (Punto de Contacto) evalúe y determine si un evento es un incidente de seguridad de la información posible o concluido, o es una falsa alarma. Se debe identificar: 1) el dominio del impacto, 2) activos, infraestructuras, información, procesos, servicios y aplicaciones afectadas o que se van a ver afectadas, 3) los posibles efectos en los servicios esenciales de la organización.
b) Actividad para que el ISIRT lleve a cabo la evaluación para confirmar los resultados del PoC (Punto de Contacto), ya que el evento sea o no un incidente de seguridad de la información. Se deben tomar decisiones sobre cómo tratar el incidente de seguridad confirmado, por quien y con qué prioridad.
c) Actividad para escalar, según se requiera durante toda la fase, para evaluaciones o decisiones posteriores.
d) Asegurar que todos los involucrados, especialmente el ISIRT, registran adecuadamente todas las actividades para análisis posterior.
e) Asegurar que se recolecta evidencia electrónica y se almacena en forma segura
f) Asegurar que el régimen de control de cambios se mantenga y cubra el rastreo de incidentes de seguridad de la información y las actualizaciones de reportes de incidentes de seguridad de la información
g) Actividad para distribuir la responsabilidad por las actividades de gestión de incidentes de seguridad de la información, a través de la jerarquía de personal adecuada, en donde las acciones de evaluación, toma de dicciones y acciones involucran personal de seguridad y personal diferente de éste.
h) Actividad para suministrar procedimientos formales que debe seguir cada persona notificada, incluida la revisión y corrección del reporte, la evaluación de daños y la notificación del personal pertinente.
i) Actividad para usar directrices para una documentación minuciosa de un evento de seguridad de información
j) Actividad para usar directrices para una documentación minuciosa de las acciones posteriores a un incidente de seguridad de la información
k) Actividad para la actualización de la base de datos de eventos/incidentes/vulnerabilidades

En esta fase la organización debería incluir la evaluación de la información recolectada de las vulnerabilidades de seguridad de la información y las decisiones de cuáles deberían tratarse, quien y con qué prioridad.

Fase de Respuestas: Esta fase busca dar respuesta a los incidentes de seguridad de la información, las respuestas se pueden ejecutar de inmediato, en tiempo real o casi real, y algunas pueden involucrar el análisis forense de seguridad de la información. Las actividades claves en esta fase son las siguientes:

a) Revisión por parte del ISIRT para establecer si el incidente de seguridad de la información está bajo control o no. Si el incidente está bajo control se ejecutan respuestas inmediatas como por ejemplo la activación de procedimientos de recuperación; en caso contrario se activaría la función de manejo de crisis.
b) Asignación de recursos internos e identificación de recursos externos para responder a un incidente
c) En caso de requerirse, llevar a cabo el análisis forense de seguridad de la información.
d) Escalar el incidente según se requiera, para revisiones o decisiones posteriores.
e) Registro de actividades por parte de todos los involucrados, especialmente el ISIRT
f) Recolección y almacenamiento de evidencia electrónica de forma segura
g) Aseguramiento para que el régimen de control de cambios se mantenga y cubra el tanto el rastreo como las actualizaciones de reportes de incidentes de seguridad.
h) Comunicación de la existencia del incidente de seguridad a los dueños de los activos/información/servicios afectados y a organizaciones internas/externas que debería estar involucradas en la gestión y resolución del incidente.

Una vez determinado el incidente de seguridad y acordadas las repuestas al mismo, la organización debe:

a) Distribuir la responsabilidad de las actividades de la gestión de incidentes a través de la jerarquía de personal correspondiente
b) Suministro de procedimientos formales que debe seguir cada persona involucrada

c) Directrices para una documentación minuciosa del incidente, de las acciones posteriores y la actualización de la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información.
d) Actualización de la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información

Una vez que el incidente de seguridad de la información se haya tratado exitosamente, se debería cerrar formalmente y esto se debería registrar en la base de datos de gestión de incidentes de seguridad de la información.

Fase de lecciones aprendidas: Esta fase se lleva a cabo cuando los incidentes de seguridad de la información se han solucionado y contempla el aprendizaje acerca de cómo los incidentes y vulnerabilidades se han manejado y tratado. Las actividades claves de esta fase son:

a) Realizar el análisis forense de seguridad de la información, según se requiera
b) Identificar lecciones aprendidas de incidentes y vulnerabilidades de seguridad de la información
c) Revisar, identificar y hacer mejoras a la implementación de controles de seguridad de la información
d) Revisar, identificar y hacer mejoras a los resultados de la revisión por la dirección y a la evaluación de riesgos, como resultado de las lecciones aprendidas
e) Examinar la eficacia de los procesos, procedimientos, reportes y estructura organizacional para responder a la evaluación y recuperación de cada incidente, y con base en las lecciones aprendidas identificar y hacer mejoras en el esquema de gestión de incidentes de seguridad de la información.
f) Actualizar la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información
g) Comunicar y compartir los resultados de la revisión dentro de una comunidad de confianza

VIII. COBIT 5

Existen otros marcos de referencia que abordan el tema de la seguridad de la información, uno de ellos es COBIT 5, un marco de negocio para el gobierno y la gestión de TI en las organizaciones, que en su dominio de entrega, servicio y soporte contempla el proceso gestionar los servicios de seguridad (DSS05), cuyo objetivo es minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información, a través de las siguientes prácticas de gestión:

DSS05.01 Proteger contra software malicioso (malware)
DSS05.02 Gestionar la seguridad de la red y las conexiones
DSS05.03 Gestionar la seguridad de los puestos de usuario final
DSS05.04 Gestionar la identidad del usuario y el acceso lógico
DSS05.05 Gestionar el acceso físico a los activos de TI
DSS05.06 Gestionar documentos sensibles y dispositivos de salida
DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad

A continuación, se detallan las prácticas específicas que conforman el proceso de administrar servicios de seguridad:

La protección contra malware (virus, gusanos, spyware, herramientas de escaneo, herramientas de acceso remoto) debe implementarse a través de sistemas de detección de amenazas (por ejemplo, firewalls de última generación), sistemas de detección / prevención de intrusiones (IDS / IPS), eventos de búsqueda (registro) repositorios (por ejemplo, sistemas de información de seguridad y gestión de eventos [SIEM]), capacidades forenses (herramientas) y el mantenimiento de parches de seguridad.

La seguridad de la red debe gestionarse activamente con una estrategia integrada y un conjunto de herramientas a través de capas y topología de red (por ejemplo, listas de control de acceso de interruptor / enrutador [ACL], firewalls, IDS / IPS). Los controles se deben implementar en todos los puntos de entrada, incluidos el correo electrónico, las aplicaciones web, los protocolos de transferencia de archivos, las redes sociales, los mensajes, las aplicaciones en la nube / los puertos de almacenamiento y hardware (USB).

La seguridad del punto final (software antivirus / antimalware, seguridad web / correo electrónico, firewalls) debe implementarse y administrarse para garantizar que las computadoras portátiles, computadoras de escritorio, servidores y dispositivos móviles estén adecuadamente protegidos (medidos contra el valor de la información).

La identidad del usuario y el acceso lógico deben administrarse en base a las necesidades del negocio y a los privilegios mínimos. Una buena práctica es fortalecer los controles en torno a la autenticación (es decir, la identificación del usuario, la contraseña) y la autorización a los recursos confidenciales. Uno debe asegurarse de que el acceso privilegiado o de administrador (por ejemplo, "claves del reino") esté especialmente bien controlado y controlado.

El acceso físico a los activos de TI se debe gestionar con procedimientos para otorgar, limitar y revocar el acceso físico a los sitios de la organización según las necesidades del negocio. El acceso debe estar justificado, autorizado, registrado y monitoreado.

Los documentos confidenciales (por ejemplo, formularios especiales, instrumentos negociables) deben salvaguardarse con los controles apropiados. Los dispositivos de salida (por ejemplo, *tokens* de seguridad) también deben controlarse con una contabilidad precisa.

La supervisión de seguridad de la infraestructura de TI es un componente clave del entorno de control. Se debe considerar un

conjunto de controles y herramientas robustos, como un repositorio de búsqueda (p. Ej., Sistema SIEM), sistemas de agregador de registros centralizados y seguros, herramientas y procesos forenses y software de detección de malware.

IX. CONCLUSIONES

El uso de las tecnologías de la información y las comunicaciones les permiten a las organizaciones obtener entre otros beneficios, la modernización y optimización de procesos, ampliación de mercados, comunicación ágil y eficiente con clientes y proveedores; sin embargo, están expuestas a incidentes que pueden llegar a comprometer la seguridad de la información, generando impactos adversos para el negocio.

Para mejoras de la seguridad de la información y reducir los impactos negativos para el negocio, las organizaciones tanto públicas como privadas deberían adoptar un marco de gestión de incidentes de seguridad de la información. Los incidentes de seguridad siempre estarán presentes, lo que marcará la diferencia, será el grado de preparación y respuesta que se tenga frente a ellos.

REFERENCIAS

[1] Congreso de la República de Colombia. (2017, agosto). Proyecto de Ley por medio del cual se aprueba el «Convenio sobre la Ciberdelincuencia», adoptado el 23 de noviembre de 2001, en Budapest. [En línea]. Disponible en: http://leyes.senado.gov.co/proyectos/images/documentos/Textos%20Radicados/proyectos%20de%20ley/2017%20-%202018/PL%20058-17%20Convenio%20Ciberdelincuencia.pdf

[2] Congreso de la República de Colombia. (2009, enero). Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”. [En línea]. Disponible en: http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

[3] Consejo de Europa. (2001, noviembre). Convenio sobre la Ciberdelincuencia. [En línea]. Disponible en: https://rm.coe.int/16802fa41c

[4] Departamento Nacional de Planeación. (2011, Julio). Documento Conpes 3701: Lineamientos de Política para Ciberseguridad y Ciberdefensa. [En línea]. Disponible en: http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

[5] Departamento Nacional de Planeación. (2016, abril). Documento Conpes 3854: Política Nacional de Seguridad Digital. [En línea]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

[6] ESET. ESET Security Report Latinoamérica 2017. [En línea]. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

[7] Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). GTC-ISO/IEC 27001: Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información (SGSI) - Requisitos. Bogotá D.C., 2006.

[8] Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). GTC-ISO/IEC 27035: Tecnología de la Información - Técnicas de Seguridad - Gestión de Incidentes de Seguridad de la Información. Bogotá D.C., 2012.

[9] Organización para la Cooperación y el Desarrollo Económico (OCDE). (2002, Julio). Directrices de la OCDE para la Seguridad de Sistemas y Redes de Información: hacia una cultura de seguridad. [En línea]. Disponible en: https://www.oecd.org/sti/ieconomy/34912912.pdf

[10] Presidencia de la República de Colombia. (2017, agosto). Sistema Informativo del Gobierno. [En línea]. Disponible en: http://es.presidencia.gov.co/noticia/170816-Gobierno-presento-proyecto-de-ley-para-adherir-al-Convenio-de-Budapest-contra-la-ciberdelincuencia

Autor

Yeny Yovana Segura Mancipe. Ingeniera de Sistemas egresada de la Universidad Cooperativa de Colombia de la ciudad de Villavicencio. Actualmente estudiante de la Especialización en Seguridad Informática de la Universidad Piloto de Colombia en la ciudad de Bogotá D.C.