Resiliencia en la Seguridad Informática

Pinilla, Alexander.
Alexander.pinilla@outlook.com
Universidad Piloto de Colombia

Resumen—La seguridad informática apunta a la protección de la infraestructura computacional y lo que se relaciona con esta; especialmente, la información contenida o circulante. Es por ello que existen estándares, protocolos, herramientas y leyes concebidas para minimizar los posibles riesgos. La protección o seguridad de una organización es cada vez más complicada debido a las amenazas y riesgos actuales, y las medidas de seguridad tradicionales no son suficientes. La administración de las amenazas y riesgos de modo tal que sea posible para las organizaciones gestionar de manera efectiva los ataques y su evolución, es lo que define como resiliencia. La importancia de la inteligencia de seguridad es tener un mayor conocimiento no solo en prácticas para el cuidado de la información, sino también en procesos que reduzcan las posibilidades de ser atacados.

Abstract— Computer security aims at protecting the computer infrastructure and what relates to this; especially, the information contained or circulating. That is why there are standards, protocols, tools and laws designed to minimize potential risks. The safety or security of an organization is increasingly complicated due to current threats and risks, and traditional security measures are not enough. The administration of virtual threats so that possible for organizations to effectively manage attacks and their evolution, is what defines as resilience. The importance of security intelligence is to have a better understanding not only care practices information, but also in processes that reduce the chances of being attacked.

Índice de Términos— Amenazas, ataques, resiliencia, estándares, procesos, seguridad.

Index Terms—Attacks, resilience, processes, security, standards, threats.

I. INTRODUCCIÓN.

Todas las organizaciones sin importar tamaño o sector, tienen riesgos y amenazas que deben afrontar de una manera organizada e inteligente con el fin de garantizar su operación, continuidad, seguridad de sus activos y la seguridad de su información.

La palabra resiliencia, proviene del latín “resilio” que significa rebotar o volver atrás; en sicología, resiliencia es la capacidad del ser humano para sobreponerse a periodos de adversidades que se puedan presentar en la vida. Esta capacidad permite mantenernos en pie y con ganas de seguir adelante tras enfrentar un problema.

En los sistemas de tecnología será la capacidad de una organización, de una infraestructura o de un sistema para soportar y recuperarse ante desastres; con el fin de proveer, proporcionar y mantener en forma aceptable su operación y servicios; de esta forma medir un aspecto tan importante como lo es la disponibilidad, las capacidades con que se cuentan y al final anticiparse, resistir, recuperarse y evolucionar ante futuros riesgos y amenazas.

II. SEGURIDAD INFORMÁTICA.

La seguridad informática como se ha definido por parte de muchos expertos tiene que ver con las condiciones, procesos y metodologías que una organización ha implementado con el fin de protegerse y garantizar la seguridad de sus activos e información confidencial, privada o sensible frente a las amenazas o riesgos; como ataques internos o externos, divulgación, destrucción o modificación.

Por esto la seguridad de la información se enfoca en garantizar y mantener las siguientes características dentro de cualquier organización. [1]

A. *Autenticidad:* Es una prueba de identidad; la garantía de que un mensaje, transacción o intercambio de información es de la fuente que dice ser. El proceso de autenticación puede implicar más de una prueba como una contraseña o tarjeta de acceso o métodos de autenticación biométricos como huellas o escáner de retina.

B. *Confidencialidad:* Se debe comprender que información deber ser protegida, a quién autorizar y

[1] Information Security Resources, [en línea], http://www.sans.org/information-security/

como dar accesos. Especificar qué información debe ser accesible a las personas que deben serlo.

C. Disponibilidad: En estos tiempos la información debe estar disponible 7 x 24, o cuando sea necesario. Los esfuerzos en asegurar accesos se pueden perder si la información no es accesible cuando y donde sea necesario. Se debe garantizar su acceso para cuando se necesite y por el personal autorizado.

D. Integridad: Significa que la información no se modifica durante su almacenamiento o transmisión. Los cambios solo pueden ser posibles con la autorización y métodos de las partes involucradas, teniendo control, registro y auditoria de lo realizado. [2]

E. No Repudio: Se refiere a la seguridad de que alguien o una entidad no podrán negar algo. Es la capacidad para asegurar que las partes en un contrato o comunicación no podrán negar la autenticidad de su firma o envío de un mensaje. [3]

La seguridad informática es un tema en las organizaciones que puede generar un impacto económico y administrativo para su información de datos personales y corporativos. Una cultura organizativa respecto al buen uso de las herramientas digitales disponibles y buenas prácticas permitirá asegurar la protección de la información.

Es normal que las organizaciones implementen y hagan uso de diversas plataformas que se orientan a la mitigación de riesgos informáticos; sin embargo, en la actualidad se encuentran nuevas tendencias para que las organizaciones reconsideren sus buenas prácticas en ciberseguridad donde se debe entender que los riesgos y amenazas están allí y querer eliminarlas es un imposible.

Las organizaciones están invitadas a identificar en qué nivel de seguridad se encuentran y conocer cuáles son sus principales debilidades, no solo prevenir los riesgos, sino hacerse más flexibles ante ellos.

III. CIBER-RESILIENCIA - DESCRIPCIÓN GENERAL.

Según el sitio web oficial del departamento de seguridad nacional de los Estados Unidos de América, define la resiliencia como la capacidad de adaptarse a las condiciones cambiantes y prepararse para resistir y recuperarse rápidamente de una interrupción. [4]

Se trata de la administración de riesgos y amenazas, no de su eliminación. Las organizaciones deben implementar las estrategias de seguridad correctas ahora mismo, reconocer sus necesidades con mayor conocimiento de seguridad por parte de su personal y sus procesos; tomar conciencia de sus niveles de seguridad para conocer sus problemas de seguridad más importantes.

Las organizaciones en los últimos años enfrentan nuevos ambientes en cuanto a seguridad, lo cual de acuerdo a sus negocios pueden verse expuestas a nuevos ataques que ponen a prueba su seguridad; para algunas organizaciones la falta de herramientas, personal sin experiencia en seguridad las puede dejar en inferioridad o expuestas a los ciber-delincuentes que explotarían sus vulnerabilidades y agujeros de seguridad.

Es necesario que las organizaciones sin importar su tamaño o sector cambien su forma de pensar en cuanto a la seguridad de sus activos e información; deben saber utilizar e identificar lo que el entorno actual ofrece para conseguir una postura adecuada y acorde a los riesgos que se puedan presentar. La ciber-resiliencia es un enfoque que utilizará soluciones de seguridad específicas y detalladas con decisiones más rápidas y efectivas para enfrentar nuevos riesgos y amenazas.

Los gobiernos de igual forma conociendo el crecimiento de los riesgos y amenazas en internet han puesto en marcha programas y leyes para proteger a los ciudadanos; ayudar a la economía y de esta forma reducir este tipo de delincuencia.

Nuevas tecnologías como virtualización, la nube y la movilidad, hacen que haya crecimiento en la ciber-delincuencia, pero de igual forma hay crecimiento en la ciber-seguridad; lo cual mantiene el control, seguimiento y vigilancia en estos ambientes.

Algunas soluciones actuales, que tienen las organizaciones para identificar y bloquear amenazas, pueden contener bases de datos robustas, demasiado filtrado, servidores y demás equipos de seguridad de gran variedad. Y se podría pensar que tener y mantener varias capas de seguridad, está brindando más protección; pero por su gran cantidad de registros y alertas, suele suceder que no se prioriza con eficacia y no se responde a los riesgos y amenazas urgentes.

[2] Information Security Concepts, [en línea], http://www.brighthub.com/computing/smb-security/articles/30076.aspx
[3] Nonrepudation, [en línea], http://searchsecurity.techtarget.com/definition/nonrepudiation
[4] Explore Terms: A Glossary of Common Cybersecurity Terminology, [en línea], http://niccs.us-cert.gov/glossary#letter_r

Es evidente que todas las organizaciones se deben replantear su enfoque acerca de la seguridad. Ningún activo de una organización estará libre de un riesgo informático, pero podría ser ciber-resistente. Un equilibrio entre los equipos de TI, equipos de seguridad y líderes de las organizaciones permitirá comprensión, apoyo y protección contra los riesgos informáticos sin obstaculizar sus negocios.

La resiliencia cibernética no pretende eliminar el riesgo; esto es imposible, pero un nivel de riesgo aceptable permite innovar, crear y desarrollar nuevas ideas. Las organizaciones para lograr ciber-resiliencia deberán alejarse de una seguridad fragmentada hacia una que sea integrada para toda la organización, que comparta la inteligencia sobre las amenazas y aproveche todos los servicios de seguridad. Establecer estrategias más sólidas y resistentes de forma proactiva, es estar preparado para proteger, detectar y responder a los riesgos y amenazas emergentes. [5] [6]

IV. ORGANIZACIONES MAS RESILIENTES.

El conjunto de capacidades tales como identificación, detección, cooperación, recuperación y mejora continua en las diferentes organizaciones de cualquier tamaño y sector frente a los distintos riesgos y amenazas, definen su disposición para construir y mantener la resiliencia. Como meta y objetivo para la organización es encontrar las capacidades preventivas de gestión y respuesta para la recuperación, mejora y continuidad.

Los múltiples ataques cibernéticos buscan interrumpir los servicios que brinda una organización, explotando sus vulnerabilidades y accediendo a sus activos e información, lo cual pone en riesgo sus intereses y la confianza depositada por sus clientes. Conseguir la resiliencia con las capacidades mencionadas, para que la organización sea capaz de medirla eficientemente con la metodología correcta, para garantizar la protección de sus activos, datos y sistemas.

Para una organización, tener la capacidad de recuperación requiere el reconocimiento de que debe prepararse desde ahora para hacer frente a los impactos graves de amenazas futuras que no se puede predecir ni prevenir. La gestión actual o tradicional de riesgo es insuficiente para hacer frente a los impactos no previstos en el ciberespacio o sus entornos. Es por eso que la gestión del riesgo empresarial debe ampliarse para la capacidad de recuperación.

Un equipo, formado por profesionales de seguridad experimentados, donde se incluyen empleados, inversionistas, clientes y otros, será la fuerza con las iniciativas de seguridad. La Resiliencia como equipo será el encargado de asegurar la comunicación necesaria entre todos los actores, con el fin de establecer un plan integral y concertado de recuperación. [7]

Un ataque cibernético o del entorno, de gran impacto para cualquier organización puede ser catastrófico. Desafortunadamente, no existe una fórmula para evitar los ataques y las violaciones a pesar de los mejores esfuerzos de una organización para su protección. Muchas organizaciones aún carecen de las más sofisticadas tecnologías y la experiencia que necesitan para hacer frente a las nuevas amenazas y riesgos más avanzados. Pero para minimizar un potencial ataque, las organizaciones deben cambiar su forma de pensar acerca de la seguridad; pensar en términos de no eliminar los riesgos o amenazas sino de crear resiliencia.

Para crear resiliencia, las organizaciones deben empezar por cambiar su conversación sobre los riesgos y amenazas. Es importante alinear TI y el negocio y, fomentar debates regulares y productivos para identificar los beneficios y riesgos asociados con una estrategia. Encontrar y utilizar un lenguaje común. La parte directiva y seguridad de TI deben aceptar que la organización se verá tentada a tomar riesgos y amenazas con el fin de tener éxito, entonces debe tomar decisiones inteligentes e informadas sobre cómo gestionar los riesgos y amenazas.

La alta dirección debe tomar un papel más activo en el establecimiento y supervisión de un programa de seguridad. En una organización resiliente, la alta dirección toma las decisiones y es en última instancia responsable de su cumplimiento. Como resultado, estos altos directivos deben ser educados sobre los riesgos y amenazas que la organización enfrenta y asumir la responsabilidad de hacer frente a estos.

Las organizaciones, deben pasar de una mentalidad policial a una que promueve las estrategias impulsado además por las personas, procesos y tecnología. Al cambiar la cultura en torno a la información digital y fomentar el aprecio por una estrategia que abarca la preparación, prevención, detección, respuesta y recuperación, las organizaciones obtendrán verdadera

[5] Ciber-resiliencia, [en línea], http://www.symantec.com/es/mx/page.jsp?id=cyber-resilience
[6] ¿Su organización cuenta con ciber-resiliencia?, [en línea], https://www.youtube.com/watch?v=ZnTTm2NgcQo
[7] Cybersecurity: The increasing threat to brand reputation, [en línea], http://www.securityinfowatch.com/article/11489898/cyber-risk-increases-threat-to-brands

resistencia y la capacidad de responder y recuperarse rápidamente de un ataque.

Una organización sin una visión completa de su propio entorno y un panorama de amenazas actual, será fácil para un atacante. Para lograr la resiliencia, las organizaciones necesitan una mejor inteligencia de seguridad. La inteligencia de seguridad es la información y datos sobre vulnerabilidades y amenazas, que se analizan y permiten la priorización de acciones para maximizar la reducción de riesgos. Una mejor y mayor inteligencia de seguridad permite una mejor toma de decisiones empresariales, mejores procesos de organización, una mayor protección contra los ataques cibernéticos, al igual que una mejor preparación para cuando ocurran, con el fin de brindar resultados de negocios más resistentes y ágiles. Una organización puede orientarse hacia la seguridad multicapa que abarca personas, procesos y tecnología.

En cuanto a las personas; los analistas de seguridad en su evaluación y análisis de los datos deben entender, reconocer un incidente potencial y, a continuación, aplicar su experiencia y habilidad para determinar si el incidente es una verdadera amenaza para la seguridad de una organización y responder adecuada e inteligentemente. Si algunas organizaciones no tienen personal de TI o este personal no tiene la experiencia o conocimientos, la elección, es un proveedor externo que pueda proporcionar servicios de seguridad especializada.

Educar los empleados de la organización sobre las políticas de seguridad y las mejores prácticas, especialmente en lo que se refiere a la pérdida de datos. Cantidad de pérdida de datos no se produce a través de las acciones maliciosas de un atacante, sino a través de las acciones de los empleados que, sin saberlo ponen datos de la organización en situación de riesgo; como la frecuente transferencia de datos corporativos para aplicaciones en la nube no autorizadas, donde la seguridad, en la mayoría de los casos depende exclusivamente de los proveedores externos. Otros incidentes suelen ser respecto a documentos comerciales utilizados en el correo electrónico desde el lugar de trabajo a sus cuentas de correo electrónico personales, tabletas o teléfonos inteligentes de propiedad personal. Los datos corporativos estando en el dispositivo móvil personal, no están bien protegidos. No se toman las precauciones básicas, como el uso de contraseñas o copias de seguridad.

Estas actividades exponen los datos potencialmente sensibles a un mayor riesgo, que si se mantienen en un dispositivo de propiedad de la organización; y el riesgo puede aumentar si la información no se elimina cuando ya no es necesaria.

Las organizaciones deben desarrollar políticas laborales y de seguridad exigibles a nivel de movilidad que brinden que hacer y no hacer con la información en el lugar de trabajo y cuando se trabaja de forma remota. Definir claramente lo que los empleados pueden y no pueden llevar con ellos cuando salen de la organización.

Riesgos de publicar cierta información en sitios sociales, por ejemplo; se están convirtiendo en la mejor forma para los ciber delincuentes, recopilando información para ejecutar ataques dirigidos o para obtener acceso a los dispositivos corporativos o personales. Otra recomendación es que los empleados deben ser educados sobre cómo utilizar su configuración de privacidad, permisos y los riesgos de la descarga de aplicaciones falsas o gratuitas.

Desde el punto de vista, como un proceso; la resiliencia es un proceso que requiere perfeccionamiento continuo ya que las amenazas y riesgos cambian y, las necesidades organizacionales evolucionan. El proceso puede ser mejor como un marco o guía que debería tener cinco áreas: Preparar e identificar, proteger, detectar, responder y recuperarse. Con el uso de esta guía, las organizaciones pueden evaluar la fuerza de su propia estrategia de seguridad cibernética, en cada una de estas áreas. Prepararse mejor a los ataques, evaluar que vulnerabilidades pueden ser utilizadas y de esta forma determinar las debilidades de seguridad existentes en la organización; o cambios en los procedimientos que se podrían hacer para responder mejor a incidentes cuando son detectados.

Es de vital importancia darse cuenta de que cada paso debe ser evaluado con base a los resultados, en lugar de las listas de comprobación; ya que cada organización tiene sistemas únicos y diferentes necesidades de seguridad. El resultado final debe ser una habilidad mejorada para tomar decisiones de negocios que impactan positivamente en la seguridad de la organización.
Además del desarrollo de una estrategia de seguridad bien pensada que utiliza toda la inteligencia de seguridad disponible y, es lo suficientemente ágil para responder a un panorama de amenazas en constante cambio.

Y en cuanto a la tecnología, las organizaciones implementan una variedad de tecnologías para garantizar su seguridad, pero lo realmente importante es qué tan bien la organización utiliza esas tecnologías; incluyendo la inteligencia de seguridad, en su estrategia de seguridad.

Si la inteligencia de amenaza se pudiese compartir a través de una comunidad, se podría ayudar a preparar una organización para la posibilidad de un ataque. Crear un departamento de TI proactivo con visibilidad de todo el entorno, con el fin de ver patrones de ataques, dan una visión que constantemente evoluciona y responde contra atacantes que se vuelven más avanzados.

Para obtener este nivel de resistencia cibernética, las organizaciones deben correlacionar todos los datos de amenazas recopiladas a través de diferentes puntos de control de seguridad; además de información recopilada a nivel mundial que identifica nuevos patrones de ataques. Aquí es donde el análisis de gran información entra en juego. Se necesita una gran cantidad de datos para ver los patrones que podrían indicar posibles ataques; una gran capacidad de análisis de datos puede conectar los puntos y ver los datos de diferentes ángulos. Sin embargo, el difícil manejo de grandes volúmenes de datos, significa que los esfuerzos de seguridad son predictivos más que basados en un histórico. Proteger la información de una organización es manejar e integrar con inteligencia un marco o guías que deben asegurar que todos los sistemas están utilizando inteligencia consistente y confiable, recolectando y monitoreando para detectar anomalías.

A través de este enfoque, donde se puede detectar rápidamente y solucionar un problema potencial antes de que se extienda, resulta en una reducción de daños y costos. Adicional, el mantenimiento de un ambiente casi libre de riesgos y amenazas protege los clientes y socios de negocio. Será una organización con un objetivo poco atractivo para un criminal cibernético. [8]

V. MODELO DE GESTIÓN DE LA RESILIENCIA – DIVISIÓN CERT-INSTITUTO DE INGENIERÍA DE SOFTWARE – UNIVERSIDAD CARNEGIE MELLON. "CERT RESILIENCE MANAGEMENT MODEL"

La División CERT se encuentra dentro de la SEI, un centro de investigación y desarrollo financiado por el gobierno federal en la Universidad Carnegie Mellon, ubicada en la ciudad de Pittsburgh (Pensilvania); la cual es una de las universidades más destacada en investigación superior de los Estados Unidos en el área de ciencias de la computación y robótica.

La División de CERT está catalogado como un bien de los Estados Unidos en el campo de la ciberseguridad y se reconoce como una organización de confianza, una autoridad dedicada a mejorar la seguridad y la resiliencia de los sistemas y redes informáticas. La División CERT regularmente se asocia con el gobierno, la industria, la aplicación de la ley, y la academia de los Estados Unidos para desarrollar métodos y tecnologías avanzadas con el fin de contrarrestar a gran escala, las amenazas informáticas más sofisticadas.

Esta parte del artículo no pretende ir al detalle de los componentes del **Modelo de Gestión de la Resiliencia** de la división CERT; en su lugar se quiere dar a conocer los lineamientos generales que se manifiestan en este documento y que las organizaciones y sus equipos de trabajo de seguridad deben conocer como herramienta base, para dirigir activamente la recuperación de su organización ante las amenazas y riesgos que se puedan presentar tanto en la actualidad como en el futuro.

En mayo de 2010 se publicó un modelo de gestión de resiliencia patrocinado por el Departamento de Defensa de Estados Unidos, cuyo fin es gestionar la capacidad de recuperación en aquellos entornos donde se presentan riesgos, mejorando sus procesos.

Este modelo pretende brindar las mejores prácticas para las organizaciones en las disciplinas de gestión de la seguridad, la gestión de la continuidad del negocio y la gestión de operaciones de TI; ofreciendo el logro de los objetivos de gestión y apoyo a la capacidad de recuperación de la dirección estratégica de la organización; mejorando la capacidad de una organización para cumplir con sus compromisos y objetivos, con coherencia y previsibilidad en los cambiantes entornos de riesgo y posibles interrupciones. CERT-Resilience Management Model, será de gran utilidad para los equipos de trabajo en las organizaciones responsables de las actividades de seguridad o de continuidad del negocio, como también a los equipos que quieran hace un uso más eficiente de las buenas prácticas como ISO 27000, COBIT, ITIL.

Debido a que siempre habrá amenazas y riesgos nuevos y, aunque conociendo que las organizaciones realizan todo lo necesario para contrarrestarlos, a veces no es suficiente; lo importante es ser capaz de predecir cómo se comportará el futuro cuando haya riesgos en su entorno. La división CERT reconoce que las organizaciones se

[8] The Cyber-Resilient Enterprise: Harnessing Your Security Intelligence, [en línea], http://www.symantec.com/content/en/us/enterprise/white_papers/b-cyber-resilient-enterprise-wp-21332471-en-us.pdf

enfrentan a retos en la gestión de la capacidad de recuperación y su solución para hacer frente a estos desafíos debe tener varios puntos de vista, como:

Considerar que las actividades de gestión para la seguridad, la continuidad del negocio, y las actividades de TI se están centrando hacia un continuo conjunto de prácticas en la gestión de la capacidad de recuperación operacional.

Abordar los temas de métricas, proporcionando medios fiables y objetivos para evaluar la capacidad y una base para la mejora de procesos; por último, la solución debe ayudar a las organizaciones a mejorar los procesos, para cerrar las brechas que en última instancia se traduce en deficiencias que disminuyen la capacidad de recuperación operativa y afectan la capacidad de una organización para alcanzar sus objetivos estratégicos.

Este modelo como mejora de procesos, permite a las organizaciones utilizar una definición de sus procesos, como punto de referencia para identificar el nivel actual de su capacidad de organización, estableciendo un objetivo deseado, apropiado y alcanzable para el rendimiento y la medición de su brecha entre el desempeño actual y el desarrollo de planes de acción para mejorar sus niveles de reacción.

Este Modelo de Gestión de la Resiliencia – CERT, es el primer modelo conocido en el ámbito de la seguridad y la continuidad, el cual proporción a cualquier organización un medio por el cual medir su capacidad para la recuperación operacional y determinar coherentemente cómo se llevará a cabo en momentos de estrés, debido a interrupciones y cambios en sus entornos de riesgo.
CERT-Resilience Management Model v1.0 contiene 26 áreas de proceso que cubren cuatro áreas de gestión de la capacidad de recuperación operativa: gestión empresarial, ingeniería, operaciones y gestión de procesos.

Las prácticas contenidas en estas áreas de proceso están agrupadas desde una perspectiva de gestión; es decir, las prácticas se centran en las actividades que una organización realiza para dirigir activamente, controlar y gestionar la capacidad de recuperación en un entorno de incertidumbre, complejidad y el riesgo.

El Modelo de Gestión de la Resiliencia, no establece específicamente cómo una organización debe asegurar la información; en cambio, se centra en los procesos igualmente importantes de la identificación de los activos de información críticos, la toma de decisiones acerca de los niveles necesarios para proteger y mantener estos activos, la implementación de estrategias para lograr estos niveles, y el mantenimiento de estos niveles en todo el ciclo de vida de los activos en tiempos estables y , más importante aún, en momentos de estrés. En esencia, el enfoque apoya las medidas concretas adoptadas para asegurar la información, haciéndolas más eficaces y más eficientes. [9]

En octubre de 2011, la División CERT publica un documento que es un complemento al Modelo de Gestión de la Resiliencia (CERT-RMM), dirigido a ayudar a los usuarios del modelo a entender la unión entre las áreas del CERT-RMM, los estándares de la industria, y códigos de prácticas que son comúnmente utilizados por las organizaciones en un entorno operativo.

De igual forma el documento ayuda a lograr un objetivo primordial del Modelo de Gestión de la Resiliencia (CERT-RMM), que es permitir a los que lo adopten a que sigan utilizando sus normas y códigos de prácticas preferidas a nivel táctico, mientras que se logra la madurez de gestión y mejora de la capacidad de recuperación operacional a nivel de proceso.

Las normas y códigos de prácticas que se mencionan son de dominio público, aunque algunas pueden tener restricciones de uso y de licencia. Por tal razón, se referencian con sus números originales; la información sobre la obtención de copias de cada norma o código de prácticas se incluye, con el fin de conocer la fuente autorizada. [10]

A. ANSI / ASIS SPC.1-2009

El ANSI / ASIS SPC.1-2009 es la Norma Nacional Americana sobre Resiliencia Organizacional: Seguridad, preparación, y Sistemas de Gestión de Continuidad - Requisitos con orientación para su uso [ANSI 2009]. El documento es publicado por ASIS International y aprobado por el American National Standards Institute, Inc. La norma se ha concebido como un recurso de la organización para fomentar la preparación en previsión de incidentes perturbadores. La norma presenta directrices sobre su interpretación de la gestión de la resiliencia organizacional.[11]

[9] Software Engineering Institute – CERT RMM, http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9479
[10] Software Engineering Institute – CERT RMM, v1.1, http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9849
[11] The ANSI/ASIS SPC.1-2009 can be obtained in PDF from ASIS, [En línea], http://www.ndsu.edu/fileadmin/emgt/ASIS_SPC.1-2009_Item_No._1842.pdf

B. BS 25999

BS 25999 es (BSI) código de la British Standards Institution de la práctica y la especificación para la gestión de la continuidad del negocio. El propósito de la norma es proporcionar una base para la comprensión, desarrollo e implementación de la continuidad del negocio dentro de una organización y para proporcionar la confianza en las relaciones de la organización con los clientes y otras organizaciones.

Hay dos BS 25999 documentos: el código de prácticas, BS 25999-1: 2006 [BSI 2006], y la especificación, BS 25999-2: 2007 [BSI 2007]. [12]

C. COBIT

COBIT es los Objetivos de Control para la Información y Tecnologías [ITGI 2007]. Fue desarrollado por la Asociación de Auditoría y Control de Sistemas de Información (ISACA) y el IT Governance Institute (ITGI) para ofrecer a los administradores, auditores y usuarios de TI, los objetivos de control de tecnología de la información generalmente aceptadas para maximizar beneficios de TI y garantizar una adecuada gobernanza de TI, seguridad, y control. [13]

D. CMMI Capability Maturity Model Integration (CMMI)

Es un modelo de madurez para la mejora de procesos para el desarrollo de productos y servicios. El CMMI para el Desarrollo (CMMI-DEV) representa el dominio de sistemas y software de desarrollo [CMMI 2006]. El CMMI para servicios (CMMI-SVC) está diseñado para cubrir las actividades necesarias para gestionar, establecer y prestar servicios [CMMI 2009]. [14]

E. FFIEC Business Continuity Planning Handbook

Las Instituciones Financieras del Consejo Federal de Examen (FFIEC) publican una serie de folletos que integran la Información del FFIEC. Estos folletos se publican para ayudar a los verificadores de bancos para evaluar las instituciones financieras y los procesos de gestión de riesgos de proveedores de servicios con el objetivo de asegurar la disponibilidad de servicios financieros críticos.

El folleto Plan de Continuidad de Negocios FFIEC [FFIEC 2008] fue utilizado como referencia en este código de prácticas del Modelo de Gestión de la Resiliencia. [15]

F. ISO / IEC 20000-2: 2005 (E)

ISO / IEC 20000 es un estándar y código de buenas prácticas para la gestión de servicios de TI publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional (ISO / IEC). Se basa en (y reemplaza) la anterior norma británica BS 15000. Refleja la mejor guía práctica para la gestión de servicios de TI a lo dispuesto en el marco ITIL (Information Technology Infrastructure Library), además cubre ampliamente otras normas de gestión de servicios.

G. ISO / IEC 24762: 2008 (E)

ISO / IEC 24762, "Directrices para la información y la tecnología de las comunicaciones de servicios de recuperación de desastres" [ISO / IEC 2008a], es parte de las normas de gestión de continuidad de negocio publicadas por ISO / IEC. Puede ser aplicado en la empresa o de proveedores externos en la recuperación de desastres de instalaciones y servicios físicos.

H. ISO / IEC 27005: 2008 (E)

ISO / IEC 27005, "Tecnología de la información - Técnicas de seguridad - Información de gestión de riesgos de seguridad" [ISO / IEC 2008b], es también una derivación estándar británico. ISO / IEC 27005 se basa en BS 7799-3: 2006. La norma describe un proceso de gestión de riesgo específico para la seguridad de la información y el análisis de ese riesgo.

I. ISO / IEC 31000: 2009 (E)

ISO / IEC 31000, "Gestión de riesgos - Principios y Directrices" [ISO / IEC 2009], es otra norma publicada por la ISO / IEC y, como se ha mencionado, es distinta de la norma ISO / IEC 27005. ISO / IEC 31000 se desvía de la norma británica origen de las normas anteriores. ISO / IEC se deriva del documento de Normas y Estándares Australia Nueva Zelanda: AS / NZS 4360: 2004. Esta norma es un conjunto de las mejores prácticas y directrices para el desarrollo de un marco de gestión de riesgos. La orientación es marco organizacional en su alcance y se centra en la gestión del riesgo perceptible y tolerancia al riesgo.[16]

[12] BSI, http://shop.bsigroup.com/
[13] ISACA, http://www.isaca.org/cobit/pages/default.aspx
[14] Software Engineering Institute, http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8091
[15] FFIEC, http://ithandbook.ffiec.gov/
[16] ANSI, http://webstore.ansi.org/

J. NFPA 1600

NFPA 1600 es la Agencia de Protección de Fuego Estándar Nacional de desastres / emergencias y programas de continuidad de negocios [NFPA 2007]. Se centra principalmente en el desarrollo, implementación y operación de los desastres, y los programas de continuidad de negocio de emergencia, incluyendo el desarrollo de diversos tipos de planes relacionados. La edición de 2007 de esta norma se utilizó como referencia y es una actualización de la norma 2004.[17]

K. PCI DSS

PCI DSS es el Payment Card Industry Data Security Standard que evolucionó a partir de los esfuerzos de seguridad por las principales organizaciones de tarjetas de crédito [PCI 2009]. Su objetivo es proporcionar un estándar de seguridad de datos para los comerciantes y proveedores de servicios de pago con tarjetas y procesadores para prevenir el fraude y control de vulnerabilidades. El cumplimiento de la norma se valida a través de evaluaciones realizadas por evaluadores PCI DSS-calificados.[18]

VI. CONCLUSIONES

Todas las organizaciones actuales necesitan una estrategia de resiliencia que se extiende a través de su personal, la tecnología y los procesos. Imaginar un enfoque nuevo basado en los servicios que ofrece con un único punto de vista unificado de todos sus sistemas en sus instalaciones, sistemas de nubes, dispositivos móviles, y redes.

La resiliencia aumenta la confianza empresarial y capacidad. Cuando los empleados están capacitados y conscientes de las políticas de seguridad, las organizaciones están mejor preparadas para las amenazas. Una organización que reúne, consolida y se correlaciona de inteligencia de seguridad es capaz de detectar ataques en tiempo real, responder rápidamente, y prepararse para futuras amenazas siendo más ágil y resistente.

Actualmente, las organizaciones están adoptando formas más abiertas, más conectados para hacer negocios. Este enfoque es esencial para las organizaciones que buscan ser innovadoras y competitivas; pero este enfoque está abierto también a las amenazas nuevas y sofisticadas donde las viejas herramientas de defensa ya no están a la altura de estos desafíos.

La capacidad de recuperación enfatiza la gestión no la eliminación de riesgos. Se reconoce que la seguridad tiene que ir más allá de los sistemas, el software y los departamentos de TI, armar a la gente con la capacidad de reconocer los riesgos, construir los procesos necesarios, aprovechar la inteligencia colectiva de los demás, y tomar medidas preventivas o correctivas.

La capacidad de resiliencia ayuda a las organizaciones a crear un enfoque en la seguridad para identificar las amenazas internas, mantenerse informadas de los asuntos de seguridad externas que amenazan su organización, y tomar medidas contra ellos de forma rápida y efectiva.

REFERENCIAS

[1] Information Security Resources, [en línea], http://www.sans.org/information-security/
[2] Information Security Concepts, [en línea], http://www.brighthub.com/computing/smb-security/articles/30076.aspx
[3] Nonrepudation, [en línea], http://searchsecurity.techtarget.com/definition/nonrepudiation
[4] Explore Terms: A Glossary of Common Cybersecurity Terminology, [en línea], http://niccs.us-cert.gov/glossary#letter_r
[5] Ciber-resiliencia, [en línea], http://www.symantec.com/es/mx/page.jsp?id=cyber-resilience
[6] ¿Su organización cuenta con ciber-resiliencia?, [en línea], https://www.youtube.com/watch?v=ZnTTm2NgcQo
[7] Cybersecurity: The increasing threat to brand reputation, [en línea], http://www.securityinfowatch.com/article/11489898/cyber-risk-increases-threat-to-brands
[8] The Cyber-Resilient Enterprise: Harnessing Your Security Intelligence, [en línea], http://www.symantec.com/content/en/us/enterprise/white_papers/b-cyber-resilient-enterprise-wp-21332471-en-us.pdf
[9] Software Engineering Institute – CERT RMM, http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9479
[10] Software Engineering Institute – CERT RMM, v1.1, http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9849
[11] The ANSI/ASIS SPC.1-2009 can be obtained in PDF from ASIS, [En línea], http://www.ndsu.edu/fileadmin/emgt/ASIS_SPC.1-2009_Item_No._1842.pdf
[12] BSI, http://shop.bsigroup.com/

[17] NFPA, http://www.nfpa.org/
[18] PCI, https://www.pcisecuritystandards.org/

[13] ISACA, http://www.isaca.org/cobit/pages/default.aspx
[14] Software Engineering Institute, http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8091
[15] FFIEC, http://ithandbook.ffiec.gov/
[16] ANSI, http://webstore.ansi.org/
[17] NFPA, http://www.nfpa.org/
[18] PCI, https://www.pcisecuritystandards.org/

Autor

Alexander Pinilla Bustos
Ingeniero de Sistemas, Estudiante de la Especialización en Seguridad Informática.
Actualmente trabajo en: Compuredes S.A.