Apagón Informático: importancia de la ciberresiliencia*

Andrés Martínez López
Coordinación de Seguridad de la Información
Dirección de Sistemas y Servicios Institucionales
Universidad Nacional Autónoma de México
Ciudad de México, México
andres.martinez@unam.mx

Adriana Cruz García
Coordinación de Seguridad de la Información
Dirección de Sistemas y Servicios Institucionales
Universidad Nacional Autónoma de México
Ciudad de México, México
adriana.cruz@unam.mx

***Abstract*—The increasing relevance of products and services in Information Technology has generated a significant impact across all sectors of contemporary society. Service continuity has become a crucial aspect for organizations, highlighting the importance of proper risk identification and management, as well as the implementation of effective contingency plans. This research focuses on the analysis of a recent incident that caused large-scale outages, related to a failure in an update of a product from the cybersecurity company Crowdstrike that affected Windows operating systems, impacting key sectors such as banking, healthcare, and aviation. Through a rigorous methodological framework, strategies for maintaining effective control are examined, and guidelines for risk assessment are presented, considering the relevance of these mechanisms in cyber resilience. Additionally, international efforts in cybersecurity are evaluated, and the hypothesis is posed on how a comprehensive approach to implementing these measures could have altered the impact of the aforementioned incident. This analysis provides a critical and reflective point of comparison for organizations both within and outside the technology industry, emphasizing the urgent need to strengthen cyber resilience in an interconnected world.**

***Index Terms*—cyber resilience, risk assessment, contingency plans, service continuity, international efforts**

I. Introducción

La importancia de los productos y servicios en Tecnologías de la Información (TI) hoy en día impacta en gran medida a todos los sectores de la sociedad. La continuidad del servicio es crucial para cualquier empresa por lo que la adecuada identificación y gestión de riesgos, así como un apropiado plan ante desastres se vuelve fundamental para mitigar, en el mayor grado posible, el impacto ante cualquier incidente que pueda presentarse en el futuro.

En los últimos años, uno de los principales desastres que ha afectado a nivel mundial múltiples empresas como bancos, hospitales, aerolíneas, etc, ha sido la interrupción en el servicio de sistemas operativos Windows a causa de una actualización lanzada por la empresa de ciberseguridad Crowdstrike. Las metodologías para mantener un control organizado y guías para realizar un correcto análisis de riesgos toman importancia cuando incidentes como el mencionado ocurren e impactan a nivel mundial.

El tema principal de está investigación es exponer los mecanismos adecuados para una ciberresiliencia que permita minorizar el impacto ante incidentes, así como destacar los esfuerzos realizados a nivel internacional en materia, lo anterior con el objetivo de cuestionar ¿Qué hubiera pasado si se tuvieran estos esfuerzos permeados en su totalidad en Crowdstrike? ¿El impacto sería el mismo? De esta forma otorgar un punto de comparación y reflexión a organizaciones dentro y fuera de la industria tecnológica.

II. Apagón Informático

A mediados de julio de 2024 ocurrió un incidente informático a nivel mundial que afectó a equipos con sistema operativo Windows a causa de una actualización lanzada por la empresa de ciberseguridad Crowdstrike que afecto a diversas organizaciones más allá del sector tecnológico. CrowdStrike es una empresa de ciberseguridad que ofrece productos y servicios contra ransomware y malware principalmente a grandes organizaciones. En palabras de George Kurtz Fundador y CEO de CrowdStrike “La interrupción del servicio se debió a un defecto detectado en una actualización de contenido de Falcon para hosts de Windows” [1] fallo que dejaba inoperable al equipo de cómputo. El programa Falcon basa su funcionamiento en la nube lo que le permite brindar protección parcialmente automatizada en la que los clientes no intervienen para instalar o actualizar contenidos de software [2].

Fig. 1: Línea de tiempo. (Elaboración propia con base a la informacion obtenida de [3])

Artículo revisado por:
M. en C. Carlos R. Tlahuel Pérez - Coordinador de Seguridad de la Información
Ing. Julio César Roldán Elorza - Jefe de Departamento de Respuesta a Incidentes

Como se puede observar en “Fig. 1”. En el intervalo de dos días se lanzó el parche de actualización defectuoso, se identificó el problema y se mostró una solución por parte de Crowdstrike, sin embargo, dicha solución requería de la intervención manual en cada uno de los activos afectados por parte de los clientes, en el que al menos 8.5 millones de dispositivos se vieron afectados [3], debido a esto y al tipo de infraestructura de las empresas, es posible que hayan tardado varias horas e incluso días en poderse recuperar de este desastre y que a pesar de ello “dependiendo del entorno, podrían surgir problemas potenciales a partir de esto” [2].

III. Mecanismos para la Ciberresiliencia

A. Gobernanza

La gestión de incidentes de seguridad informática se ha convertido en una parte crucial para quienes trabajan con tecnología digital. Manejar estos incidentes de manera efectiva es una tarea complicada, ya que requiere una planificación detallada y la asignación de recursos significativos. La prevención derivada de los análisis de riesgo, al anticipar y comprender los riesgos potenciales, las organizaciones pueden implementar medidas preventivas efectivas que reducen la probabilidad de que ocurran incidentes y minimizar sus consecuencias, en los casos en que la prevención no sea posible, la respuesta adecuada, oportuna y eficaz será fundamental para asegurar la continuidad del negocio de forma metodológica, sin embargo, lo esencial es lo que se aprende a partir del incidente.

La correcta Gobernanza de TICs es una forma de mantener un control sobre los recursos, existen diferentes guías y/o normas a las que una organización puede apegarse, como ejemplos se encuentran: ITIL [4], [5], COBIT [6], [7], ISO/IEC 27000 [8], [9], Marco de ciberseguridad del NIST [10], por mencionar algunos. Estos marcos no solo permiten mantener un control organizado, sino que a su vez involucra a la seguridad de la información y la respuesta a incidentes.

B. Respuesta a Incidentes

Las fases del ciclo de vida de la respuesta a incidentes de acuerdo con el Marco de ciberseguridad del NIST [10], constituyen etapas fundamentales que orientan a las organizaciones en la gestión eficaz de incidentes de seguridad. Estas etapas son esenciales para reducir el impacto de los incidentes y para restablecer la normalidad operativa con la mayor celeridad posible. Las fases constan de:

- Preparación: Identificar herramientas y recursos para prevenir incidentes, realizar evaluaciones de riesgo periódicas, mantener sistemas actualizados y seguros, y monitorear continuamente la seguridad. También es clave asegurar el perímetro de la red, implementar software contra malware en todos los niveles de la infraestructura, y capacitar a usuarios y personal de TI en políticas y estándares de seguridad.
- Detección y Análisis: Documentar los incidentes detalladamente es crucial para identificar patrones comunes y manejar la situación de manera efectiva. Esto permite perfilar redes y sistemas, conocer los comportamientos normales, y mantener registros históricos. Al ocurrir un incidente, debe priorizarse según su impacto funcional, impacto en la información y capacidad de recuperación. El equipo de respuesta debe informar a las personas adecuadas, asegurarse de que todos cumplan con sus roles, y proporcionar actualizaciones de estado a las partes relevantes.
- Contención, Erradicación y Recuperación: Dentro de la contención se desarrollan y establecen cursos de acción con base en estrategias y procedimientos de remediación previamente definidos que eviten el agotamiento de recursos o daños mayores. La recuperación debe llevarse a cabo en fases: primero, implementando cambios prioritarios y rápidos, y luego concentrándose en ajustes a largo plazo y en el mantenimiento continuo.
- Actividad posterior al incidente: El aprendizaje y la mejora continua requieren informes que faciliten el conocimiento y la actualización de políticas y procedimientos al identificar errores o pasos faltantes. Además, es esencial revisar periódicamente la documentación y los procedimientos del equipo de respuesta.

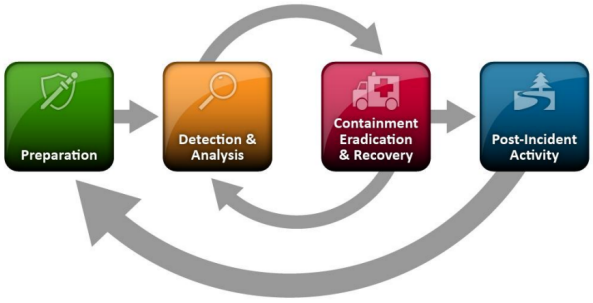

Fig. 2: Ciclo de vida de Respuesta a Incidentes (P. Cichonski, Computer Security Incident Handling Guide)

C. Análisis de riesgos

Acorde al NIST [11] para llevar a cabo un análisis de riesgo se tiene que evaluar el nivel de amenaza al que se enfrenta una entidad ante un posible evento o situación. Este análisis se basa en dos aspectos clave: los efectos negativos que se producirían si el evento ocurriera y la probabilidad de que dicho evento tenga lugar, con el fin de prever pérdida de confidencialidad, integridad o disponibilidad de datos. Para dar seguimiento, se pueden utilizar diversas guías o normas como referencia para mantener un análisis de riesgo estructurado, tales como la metodología del NIST [10] y la Guía para la Gestión de Riesgos de Seguridad de la Información perteneciente a la ISO/IEC 27005:2022 [8]. Ambas guías proporcionan directrices para:

- Evaluación del Riesgo: Este proceso incluye la caracterización del sistema, la identificación de amenazas y vulnerabilidades, la evaluación de los controles existentes y la estimación de la probabilidad e impacto de las amenazas.

- Mitigación o Tratamiento del Riesgo: Se enfoca en la reducción del riesgo mediante la implementación de controles adecuados. Acorde a un análisis de costos y beneficios los riesgos pueden asumirse, evitarse, reducirse o transferirse.
- Análisis y Evaluación: Consiste en desarrollar y aplicar estrategias para medir la efectividad de las acciones de tratamiento del riesgo. Estos ajustes pueden involucrar cambios en redes, políticas y tecnologías en el entorno actual. Dependiendo del análisis, se pueden adoptar las siguientes medidas:
  - Mantener el plan actual si el riesgo está bajo control.
  - Activar el plan de contingencia si el plan original resulta ineficaz.
  - Re-planificar si ninguno de los planes es adecuado o si emergen nuevos problemas.
  - Cerrar el riesgo si la probabilidad y el impacto son extremadamente bajos y están bien establecidos.

IV. Legislación en materia

Hasta el momento se han mencionado normas o guías para la gobernanza, seguridad, análisis de riesgos y respuesta a incidentes ante los recursos de TI, sin embargo, las compañías no están obligadas a cumplir alguna de estás y solo son tomadas acorde a los beneficios o nivel de madurez de las organizaciones. Dentro de esta sección solo se vislumbra un primer esfuerzo de carácter obligatorio, como lo es la Ley de la Ciberresiliencia. Esta ley, propuesta para su implementación en la Unión Europea, surge a raíz de la preocupación por las enormes pérdidas, que ascienden a billones de euros, causadas por ataques cibernéticos exitosos. Sus objetivos se fundamentan en asegurar que los productos digitales sean comercializados con un enfoque prioritario en la seguridad a lo largo de todo su ciclo de vida, e incentivar a los usuarios sobre la ciberseguridad al utilizar dichos productos [12].

Dentro del reglamento propuesto [13] se consideran cuatro objetivos específicos:

1) *Garantizar que los fabricantes mejoren la seguridad de los productos con elementos digitales desde la fase de diseño y desarrollo y a lo largo de todo el ciclo de vida.*
2) *Garantizar un marco de ciberseguridad coherente y facilitar su cumplimiento por parte de los productores de equipos y programas informáticos.*
3) *Mejorar la transparencia de las características de seguridad de los productos con elementos digitales.*
4) *Permitir a las empresas y a los consumidores utilizar productos con elementos digitales de forma segura.*

La Ley de Ciberresiliencia ofrece múltiples beneficios al estandarizar las normativas, simplificar los procedimientos y reducir los costos asociados con el cumplimiento y la gestión de incidentes. Esta legislación no solo mejora la seguridad cibernética, sino que también protege los derechos de los usuarios y fortalece la reputación de las empresas. En conjunto, estos factores hacen de la Ley de Ciberresiliencia un avance crucial en la protección y fortalecimiento de la infraestructura cibernética crítica.

Además, su impacto no se limita a la Unión Europea, sino que, al implementarse, podría ser adoptada globalmente, promoviendo un mayor orden y cohesión en la gestión de la ciberseguridad a nivel internacional. Esta adopción global facilitaría la creación de un marco regulatorio más uniforme y eficaz, que ayudaría a enfrentar los desafíos cibernéticos de manera más coordinada en todo el mundo.

V. Permeabilidad de la ciberresiliencia - Crowdstrike

Se han mencionado algunos de los marcos que pueden ser utilizados por las organizaciones para prevenir riesgos y mitigar el impacto a través de controles. De igual forma se expuso la propuesta de la Ley de Ciberresiliencia para implementarse en la Unión Europea, sin embargo, en el continente americano, en específico Norte América, no se ha mostrado ningún reglamento o ley que obligue a las empresas (de esta región) como Crowdstrike a seguir directrices y marcos en ciberseguridad que garanticen la calidad a lo largo de todo el ciclo de vida de un producto o servicio, pero sobre todo que fortalezcan su ciberresiliencia al tener la cabida de "anticipar, resistir, recuperarse y evolucionar para mejorar sus capacidades frente a condiciones adversas, estrés o ataques a los recursos informáticos" [14].

Dicha ciberresiliencia debe ir acompañada de los mecanismos mencionados en las secciones anteriores, incidentes como los sufridos por Crowdstrike vislumbra un débil acoplamiento a estos, en específico dentro del análisis de riesgos ya que para realizar una evaluación cuantitativa del riesgo cibernético, es esencial analizar incidentes cibernéticos históricos a partir de fuentes verificables y llevar a cabo un análisis basado en evidencia que permita identificar, reconocer y valorar los factores que determinan su frecuencia, así como su grado de impacto. [15] compañías como Trend Micro, McAfee y Symantec se han visto involucrados en incidentes similares al ocasionado por Crowdstrike por lo que no es el primero en su tipo y muy probablemente volverá a pasar como lo menciona Rik Ferguson, vicepresidente de inteligencia de seguridad de Forescout [19]. Los incidentes acaecidos en las otras compañías tuvieron que haber sido tomados en cuenta para poder desarrollar estrategias de recuperación ante desastres más eficientes ajustándose al servicio ofrecido mediante la nube.

Más del 95% de las grandes corporaciones informan que una hora de interrupción continua en herramientas tecnológicas pueden resultar en costos que superan los $100,000 dólares en un año [16]. Retomando la cronología de lo sucedido en la actualización perjudicial en los sistemas operativos Windows, pasaron al menos 78 minutos para que Crowdstrike emitiera una solución [17] aunado al tiempo de recuperación de cada compañía afectada al tener que ingresar de forma manual a sus sistemas para implementar la solución. Convirtiéndose en perdidas significativas no solo para Crowdstrike sino para todas las empresas que se vieron afectadas por este incidente, pérdidas que buscan reducir leyes como la Ley de Ciberresiliencia en la Unión Europea.

VI. Conclusión

Los marcos para fortalecer la ciberresiliencia en cualquier organización es fundamental para poder actuar de forma eficaz y expedita ante cualquier incidente que pueda presentarse a futuro, sin embargo, también es esencial en el desarrollo de estrategias ante recuperación de desastres mejor afinadas a cada sector considerando múltiples eventos históricos y características tanto tecnológicas como de cualquier otro ámbito que ayude a definir de manera clara los riesgos y se minimice el impacto o daño ante un incidente.

La falta de múltiples niveles de conciencia situacional restringe la capacidad para gestionar y mitigar incidentes de manera efectiva, ya que las organizaciones tienden a concentrarse únicamente en sus problemas inmediatos, adoptando una perspectiva introspectiva. Aunque intentan entender el panorama general, a menudo carecen del conocimiento necesario para compartir información y colaborar con otros sectores fuera y dentro del sector tecnológico. El problema se agrava porque la gestión de incidentes a menudo se percibe como una estructura jerárquica de arriba (dirección) hacia abajo (cliente), cuando en realidad debe desarrollarse de manera ascendente, involucrando a diversas organizaciones de respuesta con diferentes ubicaciones geográficas y funciones durante un incidente cibernético significativo. [18]

Así como, la correcta implementación y ejecución de marcos y normas, ayuda a cada organización de forma individual a tener una guía para poder fortalecer sus capacidades, el desarrollo de leyes y directrices se vuelve imperativo para prever perdidas en todos los niveles de un proceso, negocio, organización o nación, en que las diferentes y principales compañías en Tecnologías de la Información deberán de coadyuvar no solo en la creación de este tipo de leyes, sino que a su vez, también a nivel tecnológico para desarrollar productos y servicios que garanticen la calidad y funcionamiento a fin de reducir la probabilidad de suscitarse un incidente como el de Crowdstrike.

Referencias

[1] G. Kurtz, "To our customers and partners," crowdstrike.com, Aug. 07, 2024. https://www.crowdstrike.com/blog/to-our-customers-and-partners/

[2] Linder, "What actually happened inside the CrowdStrike update to cause a worldwide IT breakdown?," ABC News, Jul. 20, 2024. https://www.abc.net.au/news/2024-07-20/what-happened-crowdstrike-global-outage-explainer/104122582

[3] "CrowdStrike Outage Timeline and Analysis — BitSight," Bitsight. https://www.bitsight.com/blog/crowdstrike-outage-timeline-and-analysis.

[4] "ITIL 4: Las mejores prácticas en Gestión de Servicios de TI," Itil Mx, Aug. 11, 2020. https://www.itil.com.mx/

[5] Á. Guzmán, "ITIL v3 - Gestión de Servicios de TI," Dialnet, 2012. https://dialnet.unirioja.es/servlet/articulo?codigo=4001967

[6] R. Y. Pratama and S. Umaroh, "An IT Asset Governance model design using COBIT 2019 and ITIL V4 framework at BKU Itenas," E3S Web of Conferences, vol. 484, p. 02006, Jan. 2024, doi: 10.1051/e3sconf/202448402006.

[7] L. P. López and J. Carlos, "Importancia de las Tic y Cobit 5, para 'las empresas de hoy' y para el nuevo rol del 'auditor interno,'" Seria Apuntes De Clases, Jan. 2018, [Online]. Available: http://repositorio.ucb.edu.bo/xmlui/handle/20.500.12771/115

[8] "Information Security Cybersecurity and Privacy Protection - Guidance on Managing Information Security Risks [ISO/IEC 27005:2022]." [Online]. Available: https://plataforma-aenormas-aenor-com.pbidi.unam.mx:2443/pdf/CEN/77898

[9] "Modelo de gestiónde los servicios de Tecnologíade Informaciónbasado en COBIT, ITIL e ISO/IEC 27000," RevistaTecnológica ESPOL –RTE, vol. 30, no. 1, May 2017, [Online]. Available: https://rte.espol.edu.ec/index.php/tecnologica/article/view/581/356

[10] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology," Aug. 2012. doi: 10.6028/nist.sp.800-61r2.

[11] CSRC Content Editor, "risk - Glossary — CSRC." https://csrc.nist.gov/glossary/term/risk

[12] "Ley de ciberresiliencia," Configurar El Futuro Digital De Europa, Sep. 15, 2022. https://digital-strategy.ec.europa.eu/es/library/cyber-resilience-act

[13] "Propuesta de reglamento del Parlamento Europeo y del Consejo, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales Y por el que se modifica el Reglamento (UE) 2019/1020," EUR-Lex, Sep. 2022, [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

[14] incibe, "Metodología de evaluación de indicadores para la mejora de la ciberresilencia," Feb. 2023. [Online]. Available: https://www.incibe.es/sites/default/files/contenidos/guias/IMC/imc_01_metodologia-evaluacion_2023.pdf

[15] K. Palsson, S. Gudmundsson, and S. Shetty, "Analysis of the impact of cyber events for cyber insurance," The Geneva Papers on Risk and Insurance Issues and Practice, vol. 45, no. 4, pp. 564–579, Jun. 2020, doi: 10.1057/s41288-020-00171-w.

[16] K. Sicard, "The need for Disaster recovery and incident Response: Understanding Disaster Recovery for Natural Disasters versus Cyber-Attacks," Kennesaw Journal of Undergraduate Research, vol. 6, no. 2, Jan. 2019, doi: 10.62915/2474-4921.1167.

[17] Warren, "Inside the 78 minutes that took down millions of Windows machines," The Verge, Jul. 23, 2024. [Online]. Available: https://www.theverge.com/2024/7/23/24204196/crowdstrike-windows-bsod-faulty-update-microsoft-responses

[18] "Preparing for Cyber Incidents with Physical Effects on JSTOR," www.jstor.org, [Online]. Available: https://www.jstor.org/stable/26427372

[19] R. Ferguson, "It has happened before, and it'll happen again," Linkedin, Aug. 2024. https://www.linkedin.com/posts/rikferguson_it-has-happened-before-and-itll-happen-activity-7220156690233450496-Ecvz (consulatado Sep. 10, 2024).