Revista Científica Mundo de la Investigación y el Conocimiento

DOI: 10.26820/recimundo/7.(1).enero.2023.79-86
URL: https://recimundo.com/index.php/es/article/view/1919
EDITORIAL: Saberes del Conocimiento
REVISTA: RECIMUNDO
ISSN: 2588-073X
TIPO DE INVESTIGACIÓN: Artículo de revisión
CÓDIGO UNESCO: 1203 Ciencia de los Ordenadores
PAGINAS: 79-86

Resiliencia en la informática

Resilience in computing

Resiliência em informática

Nelly América Valencia Martínez[1]; Cynthia Maribel Yulán Valencia[2]; Blanca Dania Chipe Valencia[3]

RECIBIDO: 02/12/2022 **ACEPTADO:** 26/01/2023 **PUBLICADO:** 25/02/2023

1. Máster en Docencia de las Matemáticas; Máster en Docencia y Gerencia en Educación Superior; Ingeniera en Sistemas Computacionales; Profesora de Segunda Enseñanza; Facultad de Ciencias Matemáticas y Físicas; Universidad de Guayaquil; Guayaquil, Ecuador; nelly.valenciam@ug.edu.ec; https://orcid.org/0000-0001-6905-3125
2. Máster Universitario en Formación de Profesores de Secundaria de la República del Ecuador (Administración de Empresas y Economía); Ingeniera en Sistemas Computacionales; Unidad Educativa Fiscal Amarilis Fuentes Alcívar; Guayaquil, Ecuador; cynthia_yulan85@outlook.es; https://orcid.org/0009-0002-1472-4766
3. Magíster en Mercadotecnia Mención en Dirección Estratégica y Gerencia de Marcas; Ingeniera en Administración de Empresas Turísticas y Hoteleras; Tecnológico Universitario Argos; Guayaquil, Ecuador; b_chipe@tecnologicoargos.edu.ec; https://orcid.org/0009-0008-2357-4898

CORRESPONDENCIA

Nelly América Valencia Martínez
nelly.valenciam@ug.edu.ec

Guayaquil, Ecuador

RESUMEN

Este artículo, apoyado en revisión documental, a través de una perspectiva literaria pretende dar a conocer la importancia de la resiliencia que ha tenido un auge cada vez mayor en los últimos años. La resiliencia, es un factor trascendental en emprendimientos exitosos que, sin perseverancia ante la adversidad, no hubieran trascendido. “Se debe ser competente ante las adversidades para hablar de resiliencia, no sólo saberlas tolerar”. El avance de la ciencia ha generado un acelerado y desmesurado crecimiento de la tecnología de la información y comunicación TIC, trayendo consigo un sinnúmero de herramientas informáticas que están siendo utilizadas en el ciberespacio por los ciudadanos para actividades financieras, educativas, sociales, de recreación, entre otras; esto a traído la ciberdelincuencia los cuales han detectado vulnerabilidad en las TIC y creando un camino para penetrar los sistemas informáticos cometiendo introducciones y realizando perjuicio.

Palabras clave: Resiliencia, Ciberseguridad, Informática.

ABSTRACT

This article, supported by a documentary review, through a literary perspective aims to publicize the importance of resilience that has had an increasing boom in recent years. Resilience is a transcendental factor in successful ventures that, without perseverance in the face of adversity, would not have transcended. "You must be competent in the face of adversity to talk about resilience, not just know how to tolerate them." The advancement of science has generated an accelerated and excessive growth of ICT information and communication technology, bringing with it countless computer tools that are being used in cyberspace by citizens for financial, educational, social, recreational, among other; This has brought cybercrime, which have detected vulnerability in ICT and creating a way to penetrate computer systems committing introductions and causing damage.

Keywords: Work-Related Risks, Prevention Plans, Risk-Prevention.

RESUMO

Este artigo, apoiado por uma revisão documental, através de uma perspectiva literária, visa sensibilizar para a importância da resiliência, que tem vindo a aumentar nos últimos anos. A resiliência é um factor transcendental em empreendimentos de sucesso que, sem a perseverança face à adversidade, não teria transcendido. "É preciso ser competente face à adversidade para falar de resiliência, e não apenas saber tolerá-la". O avanço da ciência gerou um crescimento acelerado e desproporcionado das tecnologias de informação e comunicação TIC, trazendo consigo uma série de ferramentas informáticas que estão a ser utilizadas no ciberespaço pelos cidadãos para actividades financeiras, educacionais, sociais, recreativas e outras; isto trouxe o cibercrime que detectou vulnerabilidade nas TIC e criou uma forma de penetrar nos sistemas informáticos cometendo introduções e fazendo estragos.

Palavras-chave: Resiliência, Segurança Cibernética, Informática.

Introducción

La importancia del estudio de revisión, busca identificar y analizar la Resiliencia en la informática, esta también se la puede catalogar dentro del dominio de la denominada Resiliencia Empresarial, la misma que, entre otras áreas cubiertas, incluye la Gestión de la Continuidad del Negocio y, por ende, la Planificación de las Contingencias y de la Recuperación de información ante desastres.

Los avances tecnológicos realizados y la experiencia adquirida en la prestación de los servicios han permitido que la resiliencia sea relacionada con la seguridad informática con mayor frecuencia (Clará, 2017).

Definir resiliencia ha sido un continuo problema y aún existe falta de consenso acerca de lo que implica la resiliencia, como sus características y dinámica. El concepto de resiliencia tiene su origen en el término resilio que significa volver atrás, volver de un salto, resaltar, rebotar. Este término pertenece al campo de la física, entendiéndose que es la capacidad que tiene un cuerpo de recobrar su forma primitiva cuando se deja de ejercer presión sobre él.

La resiliencia es una dimensión personal interviniente que se desarrolla a partir de la configuración de factores constitutivos del trasfondo biopsicólogico del individuo, como lo son el temperamento y la capacidad intelectual (Bernard, 2006).

En organizaciones y empresas, la resiliencia ha pasado a formar parte de la naturaleza de las mismas y está implícita en su estructura. Cuando una entidad se etiqueta como resiliente es porque se observa que, ante una serie de sucesos, la organización ha sabido reaccionar y externamente contínua operando como si nada hubiera ocurrido. Muchos expertos en el tema en las organizaciones, utilizan también el termino como sinónimo de sostenibilidad (Joyanes, 2017, p.288).

Mientras que la resiliencia en sistemas tecnológicos es la capacidad que tiene un sistema de resistir y recuperarse ante desastres y perturbaciones. Según el sitio web oficial del departamento de seguridad nacional de los Estados Unidos de América (2023), define la resiliencia como la capacidad de adaptarse a las condiciones cambiantes y prepararse para resistir y recuperarse rápidamente de una interrupción.

El término ha llegado al campo de la ciberseguridad y se utiliza indistintamente como resiliencia y como ciberresiliencia. El glosario de términos de CCN-STIC-401 de España. Define la resiliencia como: “Capacidad de los sistemas para seguir operando pese a estar sometidos a un ciberataque, aunque sea en un estado degradado o debilitado. Así mismo incluye la capacidad de restaurar con presteza sus funciones esenciales después de un ataque”.

El sector de la ciberseguridad y sobre todo las empresas de seguridad utilizan el término ciberresiliencia (cyber- resilience). Muchos de ellos la consideran como la administración de amenazas virtuales de modo tal que sea posible gestionar de manera efectiva los ataques cibernéticos.

El 2021 para Ecuador fue un año de transición digital muchas migraciones a la nube. Por otra parte, tanto usuarios como empresas han tenido que hacer frente a numerosos tipos de amenazas. Es así que el 11 de abril del 2019, el ecuador recibió de los hackers más de 40 millones de ataque, la mayoría a los portales web de entidades públicas, motivo por el cual muchas entidades públicas se vieron afectadas en la atención al público (Cedeño, 2022).

1.1. Resiliencia Informática

La resiliencia informática es la capacidad de un sistema para recuperarse de un fallo y conservar la confiabilidad del servicio cuando este las presenta, su objetivo es asegurar que todas las operaciones comer-

ciales estén protegidas, para que así una amenaza o incumplimiento no afecte todo el negocio (Bernard, 2006).

Esta resiliencia informática permite contar con varios enfoques que posibilitan mantener una entrega continua de las operaciones mientras hay una interrupción, todos estos enfoques en conjunto resguardan el ciclo de vida de los procesos necesarios para planificar, detectar, responder, recuperarse y mejorar después de una limitación asociada con un fallo o un ataque informático.

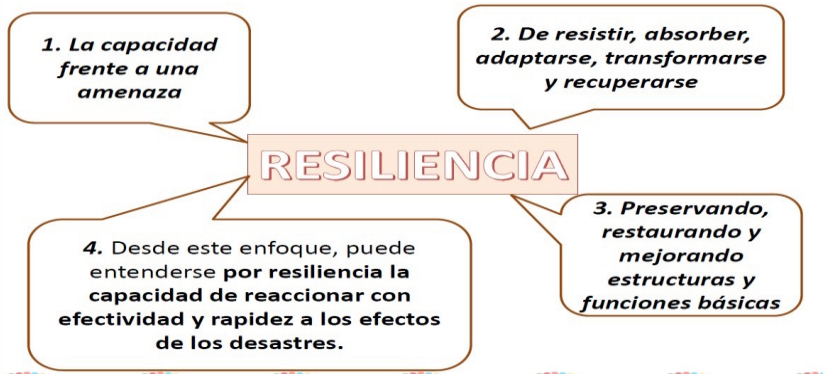

Gráfico 1. Resiliencia

Fuente: Klimsza, (2019)

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.

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 (Vargas, Recalde y Reyes, 2017).

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.

1.2. Importancia de la resiliencia informática

La importancia de la resiliencia informática es mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información manejada por computadora. Esto permite que los componentes del sistema permanezcan inalterados a menos que sean modificados por las personas autorizados.

En la actualidad existe una gran dependencia de la tecnología y computación en la nube, lo que ha hecho que incremente la ciberdelincuencia. Además, debemos sumar a todo esto el cambio en la modalidad de trabajo que se ha venido dando desde el 2020 motivado por la pandemia, pasando a realizar las labores de forma remota y usar mucho más la nube (Cedeño, 2022).

Y es por todo esto que se ha ido incrementando la importancia de la resiliencia informática, pues se enfoca en proteger las fronteras y asegurar las operaciones comerciales para que puedan recuperarse

rápidamente después de un ciberataque, garantizando la protección de la red y los datos de los sistemas TI.

En los últimos años ha sido especialmente relevante para la resiliencia informática, pues muchos proveedores de seguridad han competido para ofrecer nuevas herramientas y procesos de última generación que proporcionen una capa adicional de protección que resguarde los sistemas de las empresas. La clave para que los equipos de seguridad de TI puedan abordar y gestionar mejor los problemas está en los marcos de cifrado, gestión de claves y la resiliencia informática.

1.3. Ventajas de la resiliencia informática

Para Levano et al., (2019), la resiliencia informática tiene distintas ventajas para una empresa, antes, durante y después de un ataque cibernético, entre ellas se mencionan las siguientes:

1. Mejora de la seguridad del sistema: contar con un programa de resiliencia informática permite el desarrollo y diseño de estrategias que se adapten a la infraestructura de TI existente.
2. Cumplimiento de requisitos reglamentarios y legales: Incluir la resiliencia informática contribuye con el cumplimiento de los requisitos legales, lo que ayuda con el sistema de seguridad, como la directiva de Redes y Sistemas de Información.
3. Mejora del equipo de TI: la resiliencia informática mejora los procedimientos diarios dentro del departamento de TI, ayudando a desarrollar un equipo de TI más práctico y visible en todo el medio de trabajo.

1.4. Seguridad informática

La seguridad informática o ciberseguridad es el proceso de prevención y detección de accesos maliciosos a sistemas informáticos y sus recursos por parte de terceros, anónimos e incluso a veces personas pertenecientes a la misma organización.

La ciberseguridad es el resultado del proceso acelerado de la globalización, que ha permitido la continua innovación en la tecnología de la información y comunicación, logrando con ello el uso constante del ciberespacio (Sancho, 2017). Así mismo Cornejo, Verdezoto y Villacís (2019), indican que la ciberseguridad es un conjunto de acciones que persigue la protección de la información de las organizaciones y en general de toda comunidad que está en el ciberespacio.

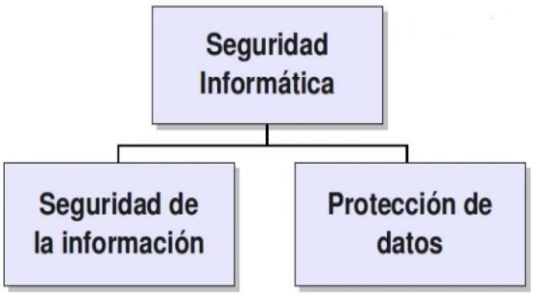

Gráfico 2. Seguridad informática

Fuente: Holguín y Rodríguez, (2020).

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.

Dentro de las amenazas humanas se tienen: Hacker (Persona que busca su superación continúa aprovechando las posibilidades que le brindan los sistemas), Cracker (Hacker dañino), creador de virus e Insider (personal interno de una organización que amenaza de cualquier forma al sistema de la misma) (Hernández, 2012). Mientras que entre las amenazas físicas están: los incen-

dios, instalaciones eléctricas (estátuca, interrupción de suministros de corriente, cableados defectuosos).

Según Painilla (2022) la seguridad de la información se enfoca en garantizar y mantener las siguientes características dentro de cualquier organización:

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.

b. **Confidencialidad:** Se debe comprender que información deber ser protegida, a quién autorizar y como dar accesos.

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.

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.

1.5. Importancia de la seguridad informática

Su importancia se enfoca en la necesidad de impedir las consecuencias que implica el robo de información importante para la empresa, en todas sus áreas. Va dirigida a prevenir las amenazas y los riesgos que puedan correr los sistemas de información internos.

Gráfico 3. Importancia de Seguridad Informática

Fuente: Propia.

En un informe de la Southern New Hampshire University se menciona que un 62% de los encargados de seguridad informática en algunas empresas, indican que se sienten medianamente o nada seguros con los sistemas informáticos de las organizaciones donde se desempeñan, por otro lado, solo el 7% se siente extremadamente seguro en este aspecto.

Esto ha hecho que cada día las compañías incrementen sus esfuerzos, otorgando más fondos de su presupuesto destinado a la seguridad informática, dicha tendencia va impulsada por los expertos en amenazas de ciberseguridad que se basan en los cambiantes ataques informáticos.

Los enfoques que abarca la resiliencia informática son: la seguridad cibernética, gestión de riesgos, continuidad del negocio, recuperación de desastres (Serna, Zenozain y Schmidt, 2017).

Metodología

Para el desarrollo metodológico se empleó revisión documental, la cual permitió la búsqueda, selección y el análisis de la información que se requería para la investigación, siendo obtenidas de fuentes secundarias de artículos científicos, sitios web estatales y trabajos que tienen relevancia en el tema de resiliencia informática.

Se exponen la perspectiva de la resiliencia de la informática desde las definiciones, importancia y ventajas, están también fueron consideradas como la seguridad informática.

Resultados

La ciber-resiliencia aparece en primer lugar en la lista de las cinco prioridades y medidas del documento de Estrategia de Ciberseguridad de la Unión Europea.

Las acciones que se plantean para alcanzar la ciber-resiliencia comienzan por la disponibilidad de productos confiables, a través de la potenciación, el impulso y el reforzamiento de las capacidades nacionales de investigación y desarrollo en ciberseguridad de las TIC.

La adecuada gestión del riesgo, la gestión del cambio y la implementación de medidas preventivas y correctivas en toda su extensión, incluyendo planes de continuidad de negocio y de recuperación frente a desastres, forman una parte capital de las herramientas para aumentar la ciber-resiliencia.

Las tendencias del sector de seguridad de la información y ciberseguridad se centran en servicios en la nube, big data y analytics e internet de las cosas (con todos sus pilares fundamentales: sensores, redes inteligentes y medidores inteligentes, drones).

Desde este 3 de agosto de 2022, Ecuador cuenta, por primera vez, con su Estrategia Nacional de Ciberseguridad (ENC), que permitirá a los ciudadanos acceder a servicios digitales con mayor seguridad y fortalecer la protección de sus datos personales. Además, abre nuevas opciones para generar regulación a fin de proteger a todos los actores de la sociedad de la ciberdelincuencia y fortalece las infraestructuras tecnológicas de las entidades públicas y privadas.

Conclusiones

Todas las organizaciones actuales necesitan una estrategia de resiliencia que se extiende a través de su personal, la tecnología y los procesos.

Una organización con inteligencia de seguridad es capaz de detectar ataques en tiempo real, responder rápidamente, y prepararse para futuras amenazas siendo más ágil y resistente.

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.

La capacidad de resiliencia ayuda a crear un enfoque en la seguridad para identificar las amenazas internas y poder mantenerse informadas de la seguridad externa que continuamente amenazan, así como tomar medidas de forma rápida y efectiva.

Se reconoce que la seguridad tiene que ir más allá de los sistemas, el software y los departamentos de TI.

Los Ciberataques se pueden dar por amenazas de origen o externas y también por las vulnerabilidades del sistema informático, lo cual afecta la integridad, disponibilidad y sobre todo la confidencialidad de la información.

La resiliencia aumenta la confianza empresarial y capacidad, motivo por el cual la empresa y la administración pública deben implementar estrategias para hacer frente a las amenazas cibernéticas.

La Estrategia Nacional de Ciberseguridad en Ecuador abarca a todo el país incluyendo Gobierno Nacional, organismos de control, instituciones judiciales, Gobiernos Autónomos Descentralizados, empresas privadas, entidades académicas y financieras.

Su objetivo es generar un ciberespacio seguro para los ciudadanos, promoviendo agilidad en los procesos y creando confianza a escala internacional para que más empresas inviertan en el país.

Bibliografía

Bernard, M.J. (2016). La resiliencia emprendedora. Cuadernos de Investigación. Papeles de trabajo. Número 2006/05. Escuela de negocios de Emlyon. Francia.

Cedeño, R. (2022). Ciberseguridad y Ciberdefensa: Perspectiva de la situación actual en el Ecuador. Revista tecnológica Ciencia y educación Edwards Deming. 6(1). p 50- 62.

https://www.researchgate.net/publication/357781915_Ciberseguridad_y_Ciberdefensa_Perspectiva_de_la_situacion_actual_en_el_Ecuador_Cybersecurity_and_ Cyberdefense_Perspective_of_the_current_situation_in_Ecuador

Clará, M. (2017). Teacher resilience and meaning transformation: How teachers reappraise situations of adversity. Teaching and Teacher Education, 63, 82-91. https://doi.org/10.1016/j.tate.2016.12.010

Cornejo, Y., Verdezoto, V., & Villacís, A. (2019). Ciberdefensa, Ciberseguridad y sus efectos en la sociedad. International Multilingual Journal of Science and Technology 4(2).

Departamento de seguridad nacional de los Estados Unidos de América (2023). Explore Terms: A Glossary of Common Cybersecurity Terminology. http://niccs.us- cert.gov/glossary#letter_r

Guía de seguridad C C N - STIC-401 (2015). Glosario y abreviaturas. España. https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400- Guias_Generales/401-glosario_abreviaturas/index.html

Hernández, J.C. (2012). "La protección de datos personales en internet y el hábeas data", Revista derecho y tecnología, 13, p. 62

Holguin, J. & Rodríguez, M. (2020). Proactividad y resiliencia en estudiantes emprendedores de Lima. Propósitos y Representaciones, 8 (2), p.367. https://online-journals.org/index.php/i-jet/article/view/18519

Huerta, V. (2015). ALTAIR-SIGVI: Un nuevo sistema para combatir el cibercrimen mitigando las vulnerabilidades. RUIDERAe: Revista de Uniandes de Información (7).

Joyanes, L. (2017). Industria 4.0 La cuarta Revolución Industrial. Alfoamega. Mexico. https://books.google.com.ec/books?id=QyN1EAAAQBAJ&pg=PA288&dq=%C2%BFSu+organiza ci%C3%B3n+cuenta+con+ciber+resiliencia?&hl=es&sa=X&ved=2ahUKEwi85Oz8rvP8AhW4SjABHTE6DU0Q6AF6BAgIEAI#v=onepage&q=%C2%BFSu%20organizaci%C3%B3n%20cuenta%20con%20ciber%20resiliencia%3F&f=false

Klimsza, C. (2019). Avances en los Lineamientos Metodológicos para Aproximarse a la Medición de Resiliencia. Comisión Económica para América Latina y el Caribe (CEPAL)

Levano-Francia, L.; Sanchez, S.; Guillén-Aparicio, P.; Tello-Cabello, S.; Herrera-Paico, N.; & Collantes-Inga, Z. (2019). Competencias digitales y educación. Propósitos y representaciones, 7 (2), 569-588. http://dx.doi.org/10.20511/pyr2019.v7n2.329

Ministerio de Telecomunicaciones y de la sociedad de la información de ecuador, (2023). Estrategia Nacional de Ciberseguridad. https://www.telecomunicaciones.gob.ec/por-primera-vez-ecuador-cuenta-con-su- estrategia-nacional-de-ciberseguridad/

Painilla, A. (2022). Resiliencia. Universidad Piloto de Colombia. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2904/Trabajo%20de%20grado2215.pdf?sequence=1

Sancho Hirare, C. (2017). Ciberseguridad. Presentación del dossier. (20), 8-15. Quito: URVIO, Revista Latinoamericana de Estudios de Seguridad.

Serna Silva, G., Zenozain Cordero, C., & Schmidt Urdanivia, U. (2017). La resiliencia: un factor decisivo para el crecimiento y mejora de las organizaciones. Gestión en el Tercer Milenio, 20(39), 13-24

Vargas, R., Recalde, L., & Reyes, R. (2017). Ciberdefensa y Ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. URVIO. (20), 31-45.

CITAR ESTE ARTICULO:

Valencia Martínez, N. A., Yulán Valencia, C. M., & Chipe Valencia, B. D. (2023). Resiliencia en la informática. RECIMUNDO, 7(1), 79-86. https://doi.org/10.26820/recimundo/7.(1).enero.2023.79-86