https://repository.uaeh.edu.mx/revistas/index.php/tepexi/issue/archive

TEPEXI Boletín Científico de la Escuela Superior Tepeji del Río

Publicación semestral, Vol. 8, No. 16 (2021) 6-9

Tepexi

ISSN: 2007-7629

Cómo proteger mis datos en la era COVID-19

How to protect my data in the COVID age

Mónica García-Munguía [a], Silvia S. Moreno-Gutiérrez [b], Héctor D. Molina-Ruiz [c], José L. Alvarado-Reséndiz [d]

Abstract:

Staying at home should not impede to continue taking care of the resources of companies, clients, partners, and employees, so adaptation has been the most recurrent activity in all sectors, which in the vast majority of cases is not. they were ready for a new way of working and protecting information. A rapid and effective implementation strategy is presented to protect information and continue unleashing data power in these times of adaptation due to the COVID-19 pandemic**.**

Keywords:

COVID-19, data, protection

Resumen:

El quedarse en casa no debe ser un impedimento para seguir cuidando de los recursos de las empresas, los clientes, socios y empleados, por lo que la adaptación ha sido la actividad más recurrente en todos los sectores, que en la gran mayoría de casos no estaban preparados para una nueva forma de trabajo y protección de la información. Se presenta una estrategia de implementación rápida y eficaz para la protección de la información y para continuar liberando el poder de los datos en estos tiempos de adaptación debido a la pandemia del COVID-19.

Palabras Clave:

COVID-19, datos, protección

Introducción

La protección de datos personales es un Derecho Humano que está consagrado en nuestra Carta Magna (art. 6, apartado A, fracciones I y II) vinculado a la protección de la privacidad y de los datos de los ciudadanos con el objetivo de bloquear su uso ilícito y vulneración en perjuicio de la dignidad de cada persona.

El COVID-19 trajo consigo el impulso a trabajar un entorno digital ya que surgió la necesidad de trabajar en modalidad home office utilizando aplicaciones y plataformas en línea por lo que los ataques de los delincuentes.

En esta nueva normalidad, donde todos están conectados trabajando a distancia, fluyendo información personal, empresarial, financiera, etc., los ataques cibernéticos se han incrementado; en México a partir de la pandemia el robo de datos incremento en un 300% según la firma Trend Micro empresa de Tecnología y Estrategia de ciberseguridad *(González, 2020)*, siendo los más (comunes el denominado *phishing.*

Para esta estrategia se necesitan conocer dos aspectos importantes:

1. A qué se enfrentan las organizaciones.
2. Qué desean proteger.

En las Tecnologías de la Información y Comunicación (TIC´s) refiriéndose a la seguridad, se tiene otra amenaza que son los ciberdelincuentes y que son expertos en el aprovechamiento de acontecimientos y noticias de impacto mundial que promuevan sus temas, siendo mayores que la pandemia de virus.

[a] Autor de correspondencia, Universidad Autónoma del Estado de Hidalgo, https://orcid.org/0000-0002-0507-3933, Email: monicagm@uaeh.edu.mx.

[b] Universidad Autónoma del Estado de Hidalgo, https://orcid.org/0000-0002-8957-3707, Email: silviam@uaeh.edu.mx.

[c] Universidad Autónoma del Estado de Hidalgo, https://orcid.org/0000-0003-4657-3237, Email: hmolina@uaeh.edu.mx.

[d] Universidad Autónoma del Estado de Hidalgo, https://orcid.org/0000-0003-1473-7727 Email: jose_alvarado4225@uaeh.edu.mx.

Fecha de recepción: 10/02/2021, Fecha de aceptación: 15/02/2021, Fecha de publicación: 05/07/2021

El COVID-19 obligó a todos los negocios y organizaciones a forzar un cambio rápido para el trabajo remoto, obligando el uso de máquinas en el hogar, que difícilmente se encuentran aseguradas, dejando sin uso el equipo de las Tecnologías de la Información (TI) sin o con poco personal. Esta situación ha resultado en una pérdida económica, sin embargo, no se debe permitir que se sumen problemas de violaciones de seguridad a los datos personales.

Cuando las empresas tienen que reaccionar por un tema ajeno y poco común haciéndolo casi inmediatamente, se resalta cuáles son las capas que se dejaron de proteger, se exponen sus vulnerabilidades y se demuestra que no estaban tan seguros como se pensaba teniendo un gran riesgo en la información.

Si se piensa que el COVID-19 ha cambiado la forma en cómo se realiza la seguridad de la información se está equivocado, esta disciplina no cambio debido a que se tuvo que adaptar a esta contingencia permitiendo a los trabajadores realizar home office, distanciamiento social, realizar digitalización de datos, compartir información, logística, etc.

Los paradigmas de seguridad para los temas mencionados ya existían y eran considerados como lo menciona (Delgado y Álvarez 2008) “A mayor volumen de información procesado y transferido informática y telemáticamente, mayor riesgo derivado de su pérdida, alteración o revelación”, lo que se exige ahora es acelerar la adaptación y transformación o conversión a este nuevo entorno y responder a las necesidades que se tenían y que se originaron por la contingencia.

Aquellas empresas que siempre han postergado y han dejado de invertir en la seguridad, el día de hoy están trabajando en la seguridad y revisando que el impacto de no tomar decisiones de seguridad a tiempo les afecte en la continuidad del negocio.

Derivado de lo anterior, surge un conflicto en cuanto a saber el monto de inversión para la seguridad, según Francisco Cayuela citado en el (Universal, 2019), en México las empresas asignan el 5.1 % de su presupuesto en seguridad en Tecnologías de la Información, invirtiendo solo en el cumplimiento de las normas y no en los riesgos; el 80% de las empresas sufrieron un incidente de seguridad en el último año y el 44% no cuenta con una estrategia general de seguridad de la información, de la revista PWC mencionado por (Cadena, 2019), también destaca que las amenazas cibernéticas a las empresas fueron del 18% y los ciberataques por 13.2%, protegiéndose solo de ataques externos y pocos invierten en la seguridad interna.

Todo esto genera conflictos entre los Chief Information Officer (CIO) de las empresas, los jefes de datos, responsables de la protección de datos, los responsables de la seguridad de la información debido a que un CIO su enfoque está centrado en la entrega y disponibilidad de servicios digitales para obtener una ventaja competitiva y satisfacción del cliente cuando el resto se dedica a encontrar riesgos de seguridad y privacidad en esos mismos servicios, teniendo cada uno de ellos funciones diferentes con intereses distintos generando disputas ocasionadas porque no se tiene claro qué es lo que se tiene que cuidar y proteger, determinar los riesgos reales en caso de perder la información, presentado las consecuencias de ello y analizar sí realmente la información se está protegiendo como debe de ser.

Existen nuevas regulaciones donde se le da más poder a los dueños reales de la información como clientes y trabajadores, así también, son necesarios los controles para poder hacer que éstas se cumplan siendo más complejas por lo que los costos para adquirir soluciones a las necesidades de las organizaciones se incrementan, ya que requieren adoptar nuevas funcionalidades.

El COVID-19 mostró que no solo bajar costos es migrar a la nube, sino que exhibió la realidad de las empresas al no poder continuar con su infraestructura que se requiere de una tecnología elástica y flexible que solo este tipo de infraestructura puede ofrecer. El cliente empieza a tener incertidumbre por la información que proporcionó y rastrea algunas de sus redes sociales para conocer si fue hackeado o bien, en sus aplicaciones de streaming como zoom o meet.

Por ello, es necesario contar con una técnica para llevar el control de los datos personales.

Figura 1. Forma de proteger datos en la era COVID-19. Fuente: Holloway (2020).

Para determinar la estrategia para la seguridad, se analizaron las causas por las que se debe adaptar a esta nueva realidad. Según el director de la revista Info Security Magazine (Raywood, 2019), el 69% de los clientes empresariales en Estados Unidos están dispuestos a boicotear una marca sabiendo que dicha empresa no toma en serio la seguridad de los datos; (se sugiere cambiar por “;” punto y coma) el 62% indica que la empresa a la que se le entregaron los datos son los responsables de su uso, por lo que si fueron utilizados con otros fines ajenos a la marca, la culpa de ese mal uso es de ella, después de ese incidente de robo el 83% dejaría de adquirir alguno de sus productos o servicios, como lo sucedido a Facebook tras sufrir un

hackeo masivo aprovechando un fallo de seguridad que afectó a cerca de 50 millones de cuentas (Ollero, 2018) que origino una fuga masiva de usuarios, según Pew Research Center de Estados Unidos, el 25% de los usuarios abandonaron esta red social. Un porcentaje que aumenta hasta el 44% en el caso de los jóvenes teniendo una afectación directa, por lo que un 21% de los clientes no regresarían por fuga de información.

Con respecto a los ataques de phishing en torno a COVID-19 según Jeremy (2020), representan "la mayor colección de ataques tipos unidos por un solo tema que nuestro equipo ha visto en años, si no alguna vez ".

Los usuarios su primordial búsqueda de información es acerca de la pandemia, considerando que el trabajo es en casa y la ciberseguridad es mucho menor que en el entorno empresarial, pueden estar más susceptibles a los ataques de phising abriendo correos de origen supuestamente confiable como el Centro de Control de Enfermedades de los Estados Unidos (CDC) o la Organización Mundial de la Salud (OMS), sí las víctimas hacen clic para descargar una aplicación oficial en un intento de ayudar a encontrar una cura para COVID-19, lo que logra el hacker es que, se instale en el equipo de casa un nuevo ladrón de información apodado RedLine Stealer. Actualmente los señuelos de correo electrónico COVID-19 son para propósitos de entrega de malware o phishing.

El ransomware es otro objetivo final TA505 Locky y ha utilizado recientemente señuelos de coronavirus para entregar descargadores en la computadora de la víctima. Una vez entregados, los atacantes pueden descargar tipos adicionales de malware, incluidos troyanos bancarios y ransomware (Degrippo, 2020). Figura 2.

Figura 2. Señuelo de preguntas frecuentes sobre el coronavirus TA505. Fuente: (Degrippo, 2020).

Existen 3 métodos para ayudar a la protección de datos desde el home office:

- Estar preparados para no caer una ingeniería social,
- Construcción de contraseñas fuertes contraseñas y,
- Actualización de los sistemas operativos.

Además, se debe complementar con la capacitación, tecnología y procesos que garantice a los clientes y empleados el acceso a los foros en línea donde pueden proponer sus preguntas, ser respondidas debiendo elaborar el informe de incidentes en tiempo real.
Degrippo (2020) recomienda defensas en capas en el borde de la red como el firewall específicamente donde se encuentran las bases de datos que contienen la información de los usuarios, una puerta de enlace de correo electrónico, en la nube y en el punto final y controles de acceso más estrictos, especialmente para las VPN.

También es importante democratizar la información, tener corresponsabilidad de los datos que se están resguardando, así como su uso adecuado, considerando que los datos pueden prevenir de las credenciales, de sensores de internet de las cosas, streaming, sistemas biométricos, datos médicos entre otros y que se deben proteger adecuadamente por lo que se debe definir y gestionar políticas para privacidad de datos.

Por lo que se propone la arquitectura de privacidad de datos. Figura 3.

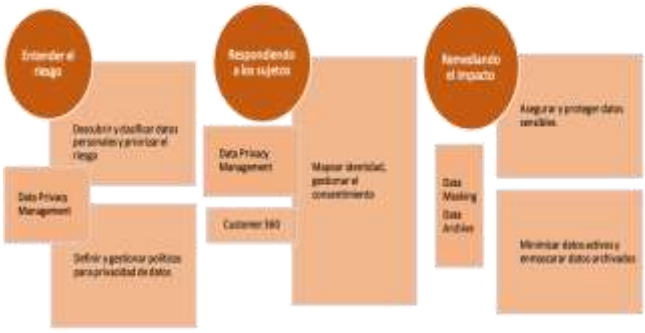

Figura 3. Arquitectura Privacidad de Datos. Fuente Holloway (2020).

Aplicando las dos primeras fases se puede lograr mitigar el riesgo a través de las técnicas de enmascarados y archivos de información.

El demo que proporciona la empresa Informática (2020) denominado Data Privact Management, Figura 4 nos ayuda a la analítica de la seguridad y hacer visible el diagnostico de seguridad de la información, configurando las reglas sobre las que se mide el riego, usuarios, datos críticos, áreas, políticas, etc., haciendo escaneo de toda la infraestructura; con este demo demuestra donde se encuentran los datos sensibles, de acuerdo a las políticas, los departamentos que la manejan, etc., y así determinar el riesgo y mandar alertas de riesgos altos y medios para saber dónde se corrompen las políticas, quien las hizo y a qué hora se presentaron y así

aplicar reglas de enmascarado, realizar reglas de calidad, cambiar procesos, etc.

Figura 4. Data Privact Management. Fuente: Informática (2020).

El posible impacto por fuga de información es también otra de las causas principales para modificar las técnicas de seguridad, por lo tanto, la evolución de la confianza y lealtad del cliente es primordial y estos permitan nuevamente obtener sus datos, a los clientes nuevos darles certeza, cada día se solicitan más datos personales para las nuevas estrategias donde se involucra el Data Science e inteligencia artificial (IA) para trabajar nuevos modelos de negocio.

Es importante hacerles saber que los clientes o empleados son los dueños de su información teniendo cierto control.

Existen recursos para enfrentar el tsunami de riesgo con el tema COVID-19. La seguridad cibernética nacional del Reino Unido Centro (NCSC) proporcionó una guía para asegurar el trabajo a domicilio, y varios proveedores de seguridad, incluidos Trend Micro, SentinelOne, Emsisoft y Coverware están ofreciendo protección gratuita para organizaciones por un período limitado.

Los peligros planteados por muchos en esta etapa del COVID-19 con respecto a las amenazas, son quizás más agudas para aquellas organizaciones no acostumbradas a apoyar al trabajo en casa, considerando que muchas áreas incluso nunca pensaron trabajar así, como la aeronáutica, la defensa, aeroespacial, demostrando que el sector tecnológico y las personas con ese perfil es el rol mejor preparado para asumir el reto.

Mientras el COVID-19 se logra controlar, mitigar o erradicar, este reto ha preparado a las organizaciones a tener las bases para que se cuente con toda la infraestructura y estrategias ante una nueva emergencia mundial, sea de cualquier índole.

Referencias

[1] González, A. (15 de abril de 2020). REFORMA. Obtenido de Consorcio Interamericano De Comunicación, S.A. De C.V., Reforma.Com: https://www.reforma.com/aplicacioneslibre/preacceso/articulo/default.aspx?__rval=1&urlredirect=https://www.reforma.com/crece-300-robo-de-datos-por-covid-19/ar1920142?referer=--7d616165662f3a3a6262623b727a7a7279703b767a783a--

[2] O. Delgado and G. Álvarez, "Seguridad con PGP," 2008. [Online]. Available: http://www.pcworld.es/archive/seguridad-con-pgp

[3] Universal, E. (26 de Julio de 2019). México invierte cada vez más en seguridad empresarial. El Universal. (Holloway, 2020)

[4] Raywood, D. (Abril de 2019). Infosecurity Magazine. Obtenido de Reed Exhibitions Ltd: https://www.infosecurity-magazine.com/

[5] Cadena, J. (2019). Best Partners. Obtenido de Best Partners: https://bestpartners.tech/nota/32310

[6] Ollero, D. (28 de septiembre de 2018). El Mundo. Obtenido de Unidad Editorial Información General, S.L.U: https://www.elmundo.es/tecnologia/2018/09/28/5bae5e88268e3eb1538b45ed.html

[7] Jeremy H, A. F. (16 de marzo de 2020). Proofpoint. Obtenido de Nuevo malware de Redline Password Stealer: https://www.proofpoint.com/us/blog/threat-insight/new-redline-stealer-distributed-using-coronavirus-themed-email-campaign

[8] Degrippo, S. (16 de marzo de 2020). Proofpoint. Obtenido de Información sobre amenazas de malware TA505: https://www.proofpoint.com/us/blog/threat-insight/ta505-and-others-launch-new-coronavirus-campaigns-now-largest-collection-attack

[9] Holloway, C. (2020). Informática LLC. Obtenido de https://www.informatica.com/mx/

[10] Informática. (2020). Informática. Obtenido de https://www.informatica.com/mx/lp/data-privacy-by-design_3582.html?formid=9283&programName=20Q1-M-DPDS-ESO-DGP-NS-NP-NI-IF-EBK-DataPrivacyDesignMexico-0-PT3582-