La importancia de tener Instituciones Educativas ciberseguras post pandemia

David Julián Gurumendi Párraga

Abstract

Cyber-attacks refer to computer crimes that have shown great growth as a result of the pandemic, in 2021. According to Kaspersky Latam portal, cyberattacks grew by 24% (Kaspersky, 2021), the reason is due to confinement. Companies had to opt for Home Office, as well as Educational Institutions, which began their Distance Learning activities, thus remaining unprotected and vulnerable to malware attacks, phishing among others. This scientific article proposes to describe the current situation of cybersecurity among Educational Institutions in Ecuador, as well as, the safety measures they must take to protect their information.

Keywords: *Cybersecurity, Cyberattack, Malware, Phishing*

La paz como factor crítico de éxito para una educación de calidad

Resumen

Los ataques cibernéticos son delitos informáticos que han demostrado un gran crecimiento a raíz de la pandemia, en 2021 según el portal de Kaspersky Latam, los ciberataques crecieron un 24% (Kaspersky, 2021), la razón se origina a causa del confinamiento, las Compañías tuvieron que optar por Home Office, al igual que las Instituciones Educativas, que iniciaron sus actividades de Distance Learning, quedando así desprotegidas y vulnerables a ataques de malware, phishing entre otras. El presente artículo científico plantea describir la situación actual de ciberseguridad en las Instituciones Educativas en Ecuador y las medidas de prevención que deben tomar para proteger su información.

Palabras clave: *Ciberseguridad, Ciberataque, Malware, Phishing*

1. Introducción

Actualmente vivimos en una era digital, en donde no hace falta ni siquiera salir de casa para hacer una compra, pagar algún servicio, recibir o enviar dinero, educarse, entre otras actividades. Los datos se envían con frecuencia a diferentes sitios en donde se desconoce si se cumplen o no con las políticas de privacidad, muchas veces, por hacer transacciones rápidas, los usuarios se dirigen a websites totalmente falsos, sitios que son réplicas exactas, pero que la única intención es hurtar data del usuario.

Según el portal de Educación del Gobierno del Ecuador, en el 2021 de 16.095 Instituciones Educativas, solo 8336, es decir el 51,79% cuenta con conexión a Internet (Educación, 2021). La verdadera incógnita es saber actualmente de esa cantidad, cuántas Instituciones Educativas tienen una buena cultura de ciberseguridad, y que tanto invierte el gobierno y accionistas privados en mantener la información a salvo con el software y hardware necesario para sus Instituciones, respectivamente.

El portal de Kaspersky menciona que los países con más ataques cibernéticos, exactamente ataques de phishing, se dan en Brasil con un 15,37%, y en el segundo lugar se encuentra Ecuador con el 13,36%, seguidos de países como: Chile, Colombia, Venezuela y República Dominicana, el promedio de ataques en los diferentes dispositivos electrónicos ascendió a 20 por cada hora.

Las Instituciones Educativas son víctimas a diario de amenazas recibidas por correos electrónicos, correos que suelen llegar disfrazados de “suspensiones de cuentas”, “recuperación de contraseñas”, “alertas de infracciones falsas” entre otros, es por eso que debemos empezar desde la educación cibernética hasta el licenciamiento de nuestros equipos y cuentas, de tal manera que los usuarios puedan estar menos vulnerables ante algún ataque.

El Ecuador se encuentra en el puesto número 63 según el Índice Nacional de la Seguridad Cibernética o NCSI, por sus siglas en inglés (National Cyber Security Index) (NCSI, 2022), aunque, comparado con otros años, el ranking no es malo, es importante que el País inicie un plan de acción que permita que la ciberseguridad sea una cultura desde muy temprano, a través de cursos, charlas o capacitaciones, y así los jóvenes puedan reflexionar sobre lo vulnerable que estamos en esta era digital.

2. ¿Por qué es importante que las Instituciones Educativas estén ciberseguras?

Tener fugas de información o brechas de seguridad en cualquier entidad, ya sea esta pública o privada, trae consigo diferentes pérdidas, no solo monetarias, sino también suplantaciones de identidad, robo de data importante, imposibilidad de acceder a los sistemas informáticos etc.

En las Escuelas, Colegios y Universidades también existe data que hay que proteger, y más importante, la integridad de los menores, como sus nombres, direcciones, edad, y otros registros que las academias suelen almacenar en sus bases de datos. Adicionalmente, en el sector privado, los sistemas informáticos suelen guardar información confidencial como: el número de la tarjeta, tipo de tarjeta, banco emisor y cuenta por los débitos recurrentes a pensiones.

Por lo anteriormente expuesto, es de vital importancia que las Instituciones Educativas se preparen ante estos posibles ataques o riesgos:

2.1. Phishing o Fraude cibernético

Según el libro “Cómo protegerte del Phishing” del Autor Juanjo Ramos, el Phishing es un tipo de ingeniería social que

consiste en recibir un mensaje fraudulento por parte de un atacante, por ejemplo, recibir un email bancario solicitando datos personales como claves o números de tarjeta, de esta manera la persona es engañada y/o manipulada a entregar su información. (Ramos, 2022)

2.2.Malware

Un malware es un programa malicioso que se utiliza para infectar un equipo, de tal manera que su información se pierda y toda la data quede corrompida o inutilizable.

2.3.DOS o Ataque de denegación de servicios

Este tipo de ataque es usado para impedir el servicio de un grupo de computadoras o servidores, también para impedir el correcto de servicio de una red, normalmente el ataque consiste en sobrecargar o saturar los equipos para que los usuarios finales tengan problemas

2.4.Ransomware

Este tipo de delito informático es similar al malware, la diferencia es que los archivos e información son encriptados con la finalidad de pedir un rescate por la recuperación de los mismos.

3. ¿Cómo una Institución Educativa puede mitigar riesgos cibernéticos y proteger su información de atacantes?

Los centros educativos pueden iniciar con un plan de capacitación ya sea presencial o virtual, que permita a los colaboradores y estudiantes identificar posibles amenazas, es importante que el acompañamiento lo haga un experto en seguridad, para que pueda resolver todas las dudas que puedan surgir.

Optar por adquirir herramientas de cybersecurity e learning también es una buena opción, debido a que el avance puede ser progresivo en el tiempo disponible de cada estudiante y colaborador.

Crear políticas que puedan ser socializadas con todos y a la cual se le de estricto cumplimiento, estas pueden ser:

- Usar antivirus licenciado y no crackeado
- Usar un antimalware (Hay soluciones de antivirus en las que esto ya viene incluido)
- Política de creación de contraseñas y renovaciones periódicas
- Crear respaldos de información con cierta periodicidad
- Mantener los equipos con contraseñas de administrador.

Es de vital importancia recalcar que un principio clave para todo tipo de organización es que, los Directivos o Accionistas deben comprender y aceptar que los delitos informáticos son un riesgo del cual ninguna organización está libre, por lo tanto, esto lo convierte en un objetivo, mantenerse libre de atacantes es un problema de todos, no solo del administrador de la seguridad.

A nivel de TI se deben mantener las siguientes recomendaciones:

- Mantener la documentación importante respaldada y fuera del alcance de los usuarios
- Mantener los sistemas operativos, aplicaciones y sus componentes de software en su última versión,
- Manejar una correcta política de usuarios, roles y permisos
- Servidores, plataformas de gestión de usuarios, correos y demás, deben mantenerse con contraseñas distintas, mínimo 8 caracteres que incluyan mayúsculas, minúsculas, números y letras.
- Instalación de endpoints en todas las estaciones de trabajo, oficinas, laboratorios y demás.

- Contar con una red totalmente identificada y segmentada a través de vlans.
- Contar con un firewall con sus debidas políticas y webfilter

Todas estas aristas mencionadas, disminuirán considerablemente los ataques de delincuentes informáticos y permitirán mantener a salvo las Instituciones educativas y las organizaciones en general.

4. Conclusión

Si bien somos un país con un índice de ataques medio – alto, podemos mejorar los números exigiendo un enfoque constante en esta materia, que hoy en día es tan importante. El realizar campañas ayudará a que las personas puedan desarrollar una cultura correcta en el manejo de la información y también, puedan identificar posibles riesgos y amenazas en internet.

Es importante mencionar que, para que el objetivo se cumpla, todos los directivos, funcionarios, docentes, y estudiantes deben ser parte del cambio, deben estar totalmente comprometidos con esta cultura que se empieza a desarrollar en las Instituciones, y que tiene como finalidad u objetivo, la prevención de pérdidas que muchas veces son irrecuperables.

Las políticas que deben ser socializadas son de vital importancia para las Instituciones Educativas, ya que estas son las que van a ayudar a concienciar a la Comunidad sobre todos los riesgos que implican no seguirlas.

Referencias

Educación, M. d. (2021). *Ministerio de Educación*. Obtenido de <https://educacion.gob.ec/datos-abiertos/>

Kaspersky. (21 de 8 de 2021). *Kaspersky Latam*. Obtenido de <https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/>

NCSI. (29 de September de 2022). *NCSI*. Obtenido de NCSI: <https://ncsi.ega.ee/country/ec/>

Ramos, J. (2022). Cómo protegerte del Phishing. En J. Ramos, *Cómo protegerte del Phishing*.