Importancia de la Ciberseguridad en las organizaciones del Ecuador y en nuestro trabajo

¿Por qué es importante la Ciberseguridad en las organizaciones del Ecuador y en nuestro trabajo?

La información comprende para toda organización del Ecuador, sea ésta pública o privada, con o sin fines de lucro, y con independencia de su misión y visión, su activo más importante. Así, por ejemplo, bases de datos de clientes, números de cuentas bancarias, información personal y médica, son tan sólo unos cuantos ejemplos de la información que las organizaciones ecuatorianas manejan diariamente en el ciberespacio y que son de vital importancia para su giro de negocio.

Ante las múltiples amenazas y escenarios a los que la información está expuesta en el mundo moderno virtual, la Ciberseguridad es simplemente imprescindible para poder resguardarla garantizando primordialmente su confidencialidad, integridad y disponibilidad; pues una brecha de seguridad en la misma implicaría su dominio público y un daño en la reputación e imagen de la organización.

Pero la Ciberseguridad en el Ecuador y en el perfil de un profesional de Tecnologías de la Información abarca mucho más que este aspecto. En primer lugar, en mi criterio, la Ciberseguridad tiene un rol fundamental porque con el paso del tiempo las organizaciones ecuatorianas buscan cada vez más poder modernizarse y es común que se planteen como meta la automatización de procesos de negocio a través de herramientas tecnológicas y software.

Tareas comunes que antes eran realizadas en el país en papel, hoy en día han sido llevadas a portales web, sistemas informáticos u otros medios para integrarlos en el ciberespacio, de manera que puedan ser empleadas por los clientes de las organizaciones de manera sencilla desde cualquier lugar que se encuentren. Pero este hecho también ha conducido a que se creen nuevas vulnerabilidades a las cuales se encuentra expuesta la información empleada.

Por otra parte, en el Ecuador es común cada vez más que las organizaciones cuenten con su propia infraestructura tecnológica para la conexión hacia sitios remotos e Internet, además del uso de PLCs (*Programmable Logic Controllers*) y sistemas SCADA (*Supervisory Control And Data Acquisition*). Esto demanda que los controles de Ciberseguridad sean de responsabilidad de los profesionales de tecnologías de la información que pertenecen a dichas organizaciones. Por lo tanto, garantizar que la información empleada en el ciberespacio sea secreta, íntegra y se encuentre siempre disponible, es de suma importancia y resulta, en mi opinión, una tarea compleja pues demanda de conocimientos y profesionales preparados para poder asumirla.

Es de igual manera importante notar que Ecuador no es un productor de tecnología, por lo que las organizaciones hacen uso a diario de soluciones tecnológicas importadas. La realidad es que en las organizaciones del Ecuador muchas veces no se cuenta con el conocimiento o el know-how para implementar medidas de seguridad en el uso de estas soluciones en el ciberespacio, exponiéndola a múltiples amenazas.

Aunque este hecho puede ser obvio muchas veces pasa desapercibido. Pero existe, de manera análoga, otro factor que no es tan notable y por el cual la Ciberseguridad en el Ecuador es de suma importancia. Este factor comprende el uso cada vez más creciente de protocolos de comunicaciones en el ciberespacio relativamente nuevos, y por lo tanto no seguros.

Es decir, las organizaciones en el Ecuador con el fin de modernizar sus plataformas tecnológicas incluyen muchas veces soluciones que hacen uso de protocolos relativamente nuevos en la industria y que requieren de otras capas de seguridad al ser empleados en el ciberespacio. Un ejemplo podría ser el protocolo OpenFlow, el cual no posee mecanismos de autenticación ni cifrado de información, y que ha sido empleado en redes definidas por software por varias organizaciones en el país, exponiendo a la información a varias amenazas.

Pero existe un factor muy relevante que destaca de los demás y que en mi criterio comprende el aspecto de Ciberseguridad en el que más esfuerzo y recursos se debe invertir: los escenarios de interconexión de sistemas tecnológicos con varios tipos de dispositivos a través de una red pública llena de amenazas como Internet.

Y es que en la actualidad las organizaciones en el Ecuador hacen uso de varios tipos de sistemas tecnológicos en sus giros de negocio, los cuales además brindan a través de puntos de acceso información a ser empleada por un sin número de dispositivos como computadores, teléfonos móviles, asistentes digitales personales, televisores, consolas de videojuegos, entre muchos otros. El Internet de la Cosas (IoT – *Internet of Things*) ha ayudado a acelerar en el Ecuador este escenario, haciendo común que inclusive dispositivos como relojes o gafas de sol puedan emplearse en el ciberespacio.

El problema radica en que estos dispositivos poseen características computacionales limitadas, por lo que no es factible en muchos escenarios proteger la información de la que hacen uso al interconectarse hacia los sistemas informáticos a través de Internet, utilizando mecanismos como los empleados en un computador tradicional. Sin embargo, su uso en las organizaciones ecuatorianas crece de manera exponencial y es cada vez mayor, por lo que es imprescindible invertir esfuerzo y recursos que permitan precautelar la seguridad de la información que estos dispositivos manejan en su interconexión hacia distintas plataformas por redes públicas.

Esto es un gran reto, ya que involucra varias tecnologías y no tan sólo una. Es decir, un escenario sumamente heterogéneo demanda de un mayor esfuerzo y de un mayor nivel de conocimiento, pues una misma vulnerabilidad podría requerir ser mitigada de diferentes maneras. De ahí la importancia de este aspecto en la Ciberseguridad en el Ecuador.

En conclusión, al ser la información un recurso tan importante y a la vez tan expuesto a múltiples amenazas, hace que la Ciberseguridad para las organizaciones en el Ecuador sea imprescindible para la mitigación de los riesgos que su uso en el ciberespacio e Internet involucra. De igual manera, dado que los escenarios de Ciberseguridad son cada vez más complejos por las múltiples amenazas y la heterogeneidad por el uso de varias de tecnologías, demanda del pensamiento crítico y preparación de los profesionales en esta rama para poder salvaguardar la información.

Firmado electrónicamente por:
DAVID FABIAN
CEVALLOS SALAS