¿Por qué se hace necesario invertir en Ciberseguridad?

Claudio Escobar, Master in Business Engineering (MBE), Universidad de Chile. Académico FEN-UAH.

Desde mediados de los años 80, con la aparición de la interfaz gráfica en los computadores personales, se comenzó a masificar el uso de diversas tecnologías en varios aspectos de la vida cotidiana.

Esa tendencia ha continuado hasta nuestros días, siendo prácticamente imposible poder encontrar alguna organización, por pequeña que sea, que no emplee algún tipo de sistema o software para registrar información.

Nos encontramos pues, en lo que los expertos denominan la cuarta revolución industrial (o industria 4.0), en la cual almacenar, gestionar, analizar y usar información en formato digital es clave para poder ser competitivo.

Esta realidad conlleva una serie de ventajas, pero también presenta una variedad de desafíos. Entre los más importantes se puede mencionar la necesidad de generar una política de seguridad que abarque todos los aspectos asociados a resguardar la información generada y recibida por las organizaciones. Tal es la importancia que tiene la información en el día a día de las organizaciones que es considerada, por muchos expertos, como el principal activo que pueda llegar a tener una empresa o institución.

La información dentro de una organización se puede clasificar en base a varios criterios, pero existe un relativo consenso en distinguir al menos las siguientes categorías: ***crítica***, sin la cual la organización difícilmente podría seguir operando; ***sensible***, que contiene datos estratégicos de la organización y/o datos personales (involucra temas legales si se llega a filtrar dicha información); ***valiosa***, se refiere a aquella que es útil para la organización, pero podría perder valor en el futuro; y ***pública***, esta in-

formación podrías ser accesible incluso por personas externas a la organización.

En base a lo anterior queda de manifiesto que es indispensable que las organizaciones inviertan para aumentar los niveles de seguridad de la información, pero, ¿qué es precisamente seguridad de la información ?[1] Básicamente se refiere a las tecnologías, procesos y políticas diseñadas para proteger los datos de una organización y sus respectivos sistemas de información en cuanto al acceso, uso, interrupción, modificación o destrucción de datos de forma no autorizada. La seguridad de la información tiene 3 pilares, conocidos en la literatura especializada sobre el tema, como la *Triada de la Información* o CIA (Confidencialidad, Integridad y Accesibilidad o Disponibilidad).

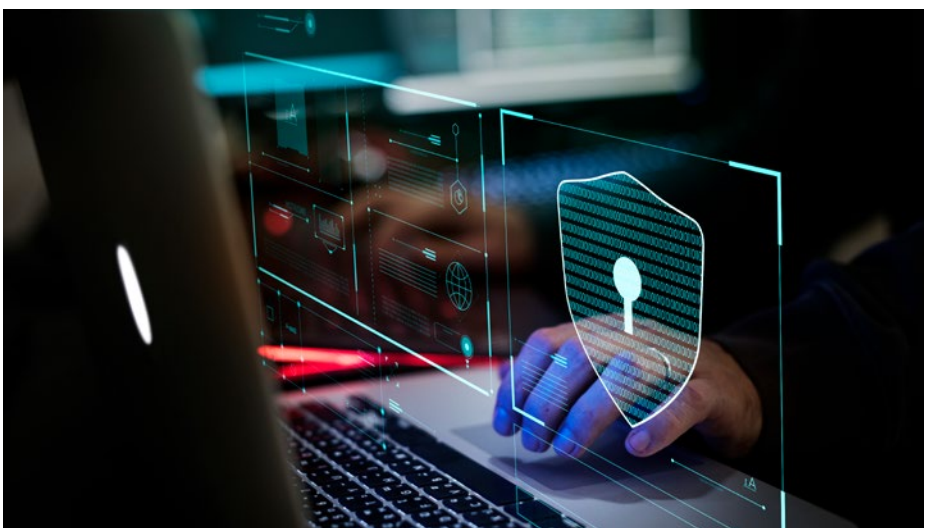
> *Según un reportaje publicado La Tercera, el 81% de las empresas en Chile no cuentan con presupuesto suficiente para su estrategia de ciberseguridad. Esto podría explicar, en gran medida, porque existen tantas vulnerabilidades respecto a brindar niveles mínimos de seguridad de la información"*

La Confidencialidad es la propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización. La Integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. Su objetivo es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados. La violación de integridad se presenta cuando un empleado, persona externa, programa o proceso (por accidente o con mala intención) modifica o borra datos importantes para la organización. Por último, la *Accesibilidad o Disponibilidad* es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. La disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

Recientemente, en nuestro país, han ocurrido un par de eventos que involucraron graves fallas en protocolos de ciberseguridad. El primero de ellos afectó al *Estado Mayor Conjunto de la Defensa de Chile* (EMCO). En base a la información brindada, se declaró que el grupo hacktivista[2] centroamericano Guacamaya aprovechó vulnerabilidades de la plataforma de correo electrónico empleado por EMCO (Microsoft Outlook) para acceder, sin consentimiento, a una serie de emails y a sus documentos adjuntos. Este ataque atentó contra la confidencialidad de la información, puesto que los datos sustraídos (cerca de 400 GB) fueron puestos a disposición de cualquier persona al ser publicados en diversos sitios de internet.

El segundo evento afectó al *Poder Judicial*, en este caso los atacantes aprovecharon una vulnerabilidad del obsoleto sistema operativo Windows 7 para acceder a poco más del 1% de los computadores empleados en las distintas reparticiones que conforman el Poder Judicial. En dicho ataque los hackers contaminaron los equipos con un tipo de ransomware[3], lo que generó que los archivos quedaran cifrados y sin poder acceder a sus contenidos. Este ataque atentó contra la accesibilidad de los datos, ya que no hubo filtración de información como en el caso de EMCO, pero se impidió el acceso a toda la información contenida en dichos computadores.

Además de los casos mencionados anteriormente, son muchos más los eventos que han ocurrido en nuestro país, tanto a nivel



(1) Joyanes Aguilar, Luis. Sistemas de información en la empresa. Alfaomega, 2015.
(2) Agrupación de hackers que emplean herramientas tecnológicas de forma no violenta y con fines políticos.
(3) Tipo de virus que cifra (encripta) archivos de cualquier formato dejándolos inutilizables por parte del usuario que quiera acceder a ellos.

público como privado, pudiendo mencionar además los ataques a *Banco Estado, SERNAC* y la *Comisión Nacional de Acreditación*. Ante esta realidad podríamos preguntarnos si en Chile existe una cultura organizacional que contemple la ciberseguridad como una inversión y no como un gasto. Invertir en seguridad de la información implica varias cosas: contar con personal calificado para las tareas asociadas a este tema, debería haber un equipo multidisciplinario para tales fines; contar con un encargado de seguridad de la información (CSO - Chief Security Officer); diseñar y aplicar políticas de seguridad que abarquen tanto el acceso físico como remoto a información digital y en papel; y finalmente incorporar tecnología idónea para prevenir los distintos tipos de ataques que se puedan realizar sobre la información. Estos ataques se pueden clasificar en dos grandes categorías: Pasivos, en los cuales los atacantes no alteran información y se limitan a monitorizar los sistemas para así obtener información de forma no autorizada (vulnerando la confidencialidad); el segundo tipo es el ataque Activo, donde se realiza algún tipo de modificación o eliminación de datos y/o se busca inutilizar de alguna forma los sistemas de información para impedir el acceso a la información. El primer tipo de ataque es el más difícil de detectar, tomando según algunos estudios, más de 40 días en ser detectados.

En el caso de EMCO llama la atención principalmente dos cosas: ¿Por qué se utilizó el correo electrónico como mecanismo para compartir información sensible y restringida? Un buen protocolo de seguridad debiese prohibir expresamente que información clasificada sea enviada de esa forma. Además, la información fue enviada sin cifrar (encriptada), otro fallo más que pudo ser evitado si existiesen políticas claras al respecto. En el Poder Judicial llama la atención que aún existieran computadores empleando Windows 7, sistema operativo cuyo soporte caducó en enero de 2020, y que cuenta con

varias vulnerabilidades detectadas ¿Tampoco tienen una política de ciberseguridad que regule la actualización de software?

Según un reportaje publicado en el diario La Tercera[4], el 81% de las empresas en Chile no cuentan con presupuesto suficiente para su estrategia de ciberseguridad. Esto podría explicar, en gran medida, porque existen tantas vulnerabilidades respecto a brindar niveles mínimos de seguridad de la información. A esto, se debería sumar un nuevo fenómeno que va en alza y que abre otra gran vulnerabilidad. Los empleados suelen emplear algún tipo de dispositivo propio para realizar todas o algunas de las funciones propias de su cargo. A este fenómeno se le conoce como BYOD (Bring Your Own Device – Trae Tu Propio Dispositivo). Trabajar de esta forma reporta beneficios tanto para la organización como para la persona que hace uso del dispositivo, pero en cuanto a términos de seguridad genera una serie de inconvenientes, pues es difícil estandarizar protocolos de seguridad cuando se trabaja con distintos tipos de tecnología. Además, es importante mencionar que parte de la información de la organización queda almacenada en dispositivos que no son parte de esta ¿Se puede controlar lo que pasará con esa información? La posibilidad de poder controlar lo que pase es realmente baja.

En el sector público se han realizado algunos intentos por mejorar los estándares en ciberseguridad. El Ministerio del Interior y Seguridad Publica creó un Equipo de Respuesta ante Incidentes de Seguridad Informática[5] (CSIRT). Esta unidad tiene dentro de sus principales objetivos: A*dministrar un Sistema de Cooperación Nacional e internacional en materias de ciberseguridad, con el objetivo de reducir el riesgo y articular la respuesta a éstos cuando su materialización sea efectiva y Promover buenas prácticas en materia de ciberseguridad en la Administración Gubernamental*. Ciertamente no basta con tener el CSIRT, pero es un avance y una iniciativa, que, de ser bien aprovechada, podría determinar un camino en conjunto a seguir por todos los estamentos públicos y aumentar los estándares de seguridad. OE

(4) https://www.latercera.com/piensa-digital/noticia/el-81-de-las-empresas-no-cuentan-con-presupuesto-suficiente-para-su-estrategia-de-ciberseguridad/RJELSDPLINCGTDAQNNR4UP4IWQ/
(5) https://www.csirt.gob.cl/