¿Qué es la seguridad informática?

Por Gustavo Sain

@grsain

La seguridad en las organizaciones tiene sus orígenes a principios de siglo XX y tenía como objetivo proteger las instalaciones físicas frente a los conflictos sociales y laborales de la época. La misma estaba orientada a salvaguardar las propiedades y personas contra el robo, fuego, inundación, contrarrestar huelgas y felonías y, de forma amplia, todos los disturbios sociales que puedan poner en peligro el progreso e incluso la vida del negocio. Con la irrupción de las computadoras como herramienta laboral y doméstica, la aparición de Internet y la World Wide Web y la consecuente expansión de redes informáticas corporativas, los datos y la información digitalizada adquieren un valor mayor para las organizaciones, tanto así como el uso de las tecnologías de la información y la comunicación en el seno de las mismas.

Para Álvaro Gómez Vieites se puede definir a la **seguridad informática** como cualquier acción que impida la ejecución de operaciones no autorizadas sobre un sistema informático o red de computadoras. En líneas generales, comprende el conjunto de medidas preventivas, de detección y corrección destinadas a proteger los recursos informáticos de una organización. De los diferentes factores que inciden en la seguridad informática, se podría definir como los más importantes **la confidencialidad, la autenticidad y la integridad** (la tríada CIA, Confidenciality, Integrity, Availability)**.** La confidencialidad hace alusión a la garantía de que cada mensaje transmitido por las redes de comunicaciones o almacenado en un sistema informático pueda ser leído por su legítimo destinatario, garantizando las medidas de seguridad apropiadas para ese objetivo. La autenticidad, en cambio, refiere a la identidad del creador de un mensaje o documento es legítima, tanto así como la

autenticidad de un equipo al cual uno se conecta dentro de una red para brindar un determinado servicio. Por último, la integridad está relacionada con la garantía de que los contenidos de un documento no hayan sido alterados desde su creación o durante su transmisión en red. Otros factores que hacen a la seguridad informática son la *disponibilidad*, la *autorización*, *auditabilidad*, *anonimato* y *certificación*.

La seguridad informática es entendida como un **proceso**, no un producto terminado a implementar en los sistemas o redes de una organización en tanto que tiene que ser constantemente monitoreado y evaluado permanentemente. Este proceso incluye reducir la posibilidad que se produzcan incidentes de seguridad, facilitar la rápida detección de los incidentes de seguridad, minimizar el impacto en el sistema de información, conseguir la rápida recuperación de los daños experimentados, revisión y actualización de las medidas de seguridad implantadas (auditoría).

El objetivo de la seguridad informática es la de mitigar los efectos de las amenazas y vulnerabilidades mediante una serie de **controles preventivos, disuasivos, detectivos, correctivos y recuperativos.** Los controles preventivos y disuasivos se realizan antes de que se produzca un incidente de seguridad, con el objetivo de evitarlo. Los controles detectivos buscan detectar el incidente una vez que se está produciendo, mientras que los controles correctivos y recuperativos tiene lugar una vez que se produjo el incidente y su objetivo es tratar de salvar un sistema informatico de los daños y la información que este contiene.

Asimismo los controles pueden diferenciarse en **controles físicos, controles técnicos y controles administrativos.** Los controles físicos incluyen medidas de protección física tales como cerraduras electrónicas, sistemas de acceso biométrico, cámaras de seguridad etc. Los controles técnicos o lógicos son aquellas medidas tecnológicas tales como la seguridad de las aplicaciones y del sistema operativo de

una computadora, por ejemplo. Por último, están los controles administrativos son aquellos que hacen a la política de seguridad de una organización.

Los diferentes planos donde actúa la seguridad informática son el **técnico**, el **legal**, el **humano** y el **organizativo**. En cuanto al aspecto más importante, el técnico, incluye el nivel físico (hardware) como el nivel lógico (software) y comprende la ejecución de las medidas de seguridad implementadas por una organización para la protección de los sistemas informáticos y sus redes de comunicación. En cuanto al aspecto legal, el mismo hace alusión a las diferentes normativas legales o administrativas que obligan a las organizaciones a adoptar medidas de seguridad específicas. El aspecto humano, en cambio, alude a la sensibilización, capacitación de personal que desempeña funciones relacionadas con el mantenimiento de los sistemas informáticos. Por ultimo está el plano organizativo, que refiere al diseño e implementación de las políticas de seguridad de una organización tales como los planes, las normas y los procedimientos, entre otros.

El **proceso de análisis y gestión de riesgos** de un sistema informático comprende una etapa de evaluación de los sistemas y redes de una organización y tiene como objetivo la implementación de un plan para la implantación de medidas de seguridad basado en la evaluación de los posibles riesgos y amenazas que pueden afectar a un sistema informático. Algunos conceptos que son centrales en este proceso y resultan importantes en el campo de la seguridad informática son los de *recursos del sistema, amenazas, vulnerabilidad, incidente de seguridad, impacto y riesgo.*

Uno de ellos son los **recursos del sistema**, que son aquellos activos que debe proteger la organización. Entre ellos figuran el hardware (computadoras, impresoras escáneres, etc.), el software (sistemas operativos, programas de gestión, herramientas de programación, etc.), elementos de comunicaciones (como cableado, puntos de

acceso a la red, líneas de comunicaciones), locales y oficinas, las personas que utilizan y se benefician del sistema y la imagen y reputación de la organización.

Las **amenazas** son eventos accidentales o intencionados que puede ocasionar algún daño al sistema informático y ocasionar pérdidas materiales o financieras o de otro tipo. Existen diferentes tipos de amenazas; naturales (incendios, inundación, tormenta, fallas eléctricas, explosiones, etc.); agentes externos (ataques de una organización criminal, sabotajes, disturbios y conflictos sociales, robos, estafas, virus informáticos, etc.); y agentes internos (descuidos del personal, errores involuntarios en el manejo de herramientas, sabotaje por parte de empleados descontentos, entre otras).

Una **vulnerabilidad** es una debilidad que presenta un sistema informático que puede permitir que las amenazas causen daños en los mismos y así producir pérdidas para la organización, mientras que un **incidente de seguridad** es un evento que puede producir una interrupción de los servicios brindados por un sistema informático y/o posibles pérdidas materiales o financieras. El **impacto** es la medición y valoración de un daño que podría producir en una organización un incidente de seguridad, mientras que el **riesgo** es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un determinado impacto en la organización.

Asimismo existen tres conceptos fundamentales para las organizaciones en términos de seguridad informática, los mismos son los de **políticas, planes y procedimientos.** Una política de seguridad de una organización comprende los principios y líneas de acción fundamentales que sirven de base para la seguridad de los sistemas informáticos y definen las responsabilidades para las cuestiones técnicas y organizativas. Un plan de seguridad, en cambio, incluye al conjunto de decisiones que

definen las acciones futuras y los medios a utilizar para tal fin, mientras que los procedimientos de seguridad son tareas y operaciones a ejecutar de acuerdo a las políticas de seguridad de la organización. En el caso de estos últimos, los mismos generan registros y evidencias que facilitan el seguimiento, control y supervisión de funcionamiento.

Una dimensión de la seguridad informática es la **seguridad física de las instalaciones**, es decir, los lugares donde se ubican las computadoras en una organización. Los mismos deben poseer requisitos mínimos, que incluyen medidas como la protección frente a incendios, explosiones, inundaciones, accesos no autorizados, etc.; la selección de elementos de construcción internos tales como puertas, ventanas, paredes, suelos y techos, centrales eléctricas, elementos de comunicaciones etc.; y la definición de áreas dentro de la organización, tales como áreas públicas, áreas con acceso restringido, etc., entre otras.

Por último la organización realiza **auditorías de seguridad** periódicas para comprobar la correcta implementación de la política de seguridad que incluye medidas tales como el análisis de posibles vulnerabilidades del sistema informático empleando herramientas de software para localizarlas automáticamente; la revisión de la instalación y configuración de equipos de seguridad tales como antivirus, cortafuegos, etc.; y la realización de pruebas de intrusión, entre otros.

**Especialista en cibercrimen, asesor de la Dirección Nacional de Política Criminal del Ministerio de Justicia y DDHH de la Nación y profesor universitario.*