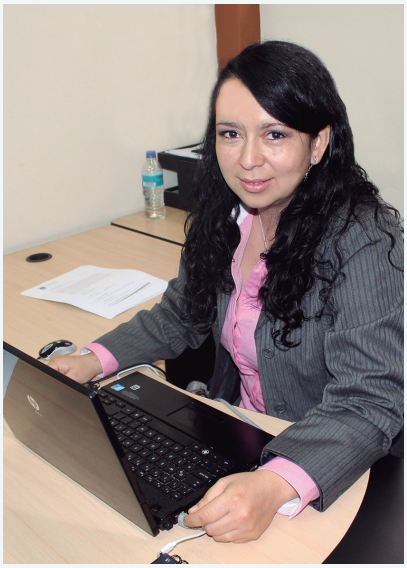
SEGURIDAD INFORMÁTICA… UN FACTOR RELEVANTE EN UNA ORGANIZACIÓN?

Ing. Karina Carrión
Docente Investigadora ITSPN

Se puede entender como seguridad un estado de cualquier tipo de información (informático o no) que nos indica que ese sistema está libre de peligro, daño o riesgo.

Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema cien por ciento seguro.

La seguridad informática es una disciplina que se relaciona con diversas técnicas, aplicaciones, normas, procedimientos y herramientas, que se encargan de asegurar la integridad, disponibilidad, confidencialidad y buen uso de la información de un sistema informático y sus usuarios.



La integridad, disponibilidad y confidencialidad se conocen como principios de la seguridad informática; la integridad se refiere a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático, lo cual asegura que los datos sean precisos, es decir los que se supone que son; la confidencialidad se refiere a la privacidad de la información almacenada y procesada en un sistema informático y garantiza que únicamente los individuos autorizados tengan acceso a esta información; mientras que la disponibilidad se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático lo que garantiza el correcto funcionamiento de los sistemas de información en el momento que un usuario lo requiera.

Seguridad informática comprende las técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados. Estos daños incluyen el mal funcionamiento del hardware, la pérdida física de datos y el acceso a bases de datos por personas no autorizadas.
Las amenazas que debe considerar la seguridad informática son de distintos tipos:

- **Daño en los sistemas.** Para asegurar la disponibilidad de la información debe existir una política de backup que permita contar con una copia de la información, de modo que pueda ser restaurada. También es necesario un procedimiento de contingencia que contemple los distintos casos que se pueden presentar (avería en un servidor, avería en un sistema de almacenamiento, avería en un equipo de comunicaciones,…), e indique los pasos a seguir para restaurar el servicio.

- **Mal funcionamiento del software que procesa la información.** Un software mal diseñado puede poner en riesgo la integridad de la información que recibe y procesa el sistema.
- **Ataques malintencionados.** Provocados por virus, o por personas que intencionadamente buscan destruir o tergiversar la información. Las medidas que se pueden plantear para evitar este tipo de riesgos son de distintos tipos: implementar cortafuegos y antivirus, imponer una política de obligue al uso de contraseñas robustas y que caduquen cada cierto tiempo, entre otros. (D'L Systems, S/F)

¿Por qué es importante la seguridad informática?, es una pregunta que las organizaciones se realizan frecuentemente, abarca toda una serie de riesgos y una amplia gama de amenazas. En la actualidad todas las organizaciones dependen críticamente de sus capacidades tecnológicas de la in-

formación y son potencialmente vulnerables a los ataques, ya sea por querer controlar, corromper la información o destruir la capacidad de éstas para acceder a la información. De acuerdo con los expertos en el área, más del 70 por ciento de las violaciones e intrusiones a los recursos informáticos son ejecutadas por el personal interno, debido a que éste conoce los procesos, metodologías y tiene acceso a la información sensible de una organización, es decir, a todos aquellos datos cuya pérdida puede afectar su buen funcionamiento.

Según Sir Jonathan Evans en una entrevista para la revista KPGM con el tema "El desafío de la seguridad cibernética" (2014)

Compara el modelo tradicional de la seguridad cibernética como un castillo, es decir que tiene un conjunto bastante grande de murallas y fosos alrededor se puede evitar que los chicos malos se suban. Se cree que hay que asumir que en algún momento los chicos malos van a entrar y, por tanto, hay que pensar en dos cosas - ¿cómo identificar la actividad dentro de sus redes y cómo se va a responder?. En caso de que una persona sea una víctima de este tipo de ataques, se necesita planes de contingencia. Al igual que con otras áreas de seguridad, hay una variedad de elementos a considerar. Se tiene el elemento de protección; se tiene que tener la inteligencia de lo que las otras personas están tratando de hacerle; y tiene que ser capaz de gestionar la respuesta cuando se convierte en una víctima. Si todos estos elementos trabajan juntos, entonces se puede tener mucha más confianza de ser capaz de resistir un ataque. Por lo tanto, una buena seguridad cibernética no se trata sólo de tener un muro muy fuerte en el exterior, sino de tener dentro, un sistema inmune y, además, tener la capacidad de recuperarse rápidamente.

En el presente año han salido a la luz diferentes fallos de seguridad cibernética y los expertos en el tema han sugerido nuevos enfoques para afrontarlos.

Según indica la revista Noticias Financieras en uno de sus artículos:"el mundo de la seguridad informática se vio sacudido por la noticia de un ataque masivo al gigante de ventas en línea eBay, que afectó a unos 145 millones de clientes cuya información personal se vio comprometida". (2014).
Esto da lugar a pensar en una realidad vinculada con los ataques informáticos que debe ser tomada en cuenta, pues afecta directamente a las empresas involucrando un costo demasiado alto para ellas.

Estos recientes ataques ponen en sigilo a las organizaciones, las cuales tienen un reto fundamental en la protección de los sistemas y demás activos informáticos, tales como: la información financiera, los datos de clientes, la propiedad intelectual entre otros.

Ahora es relevante considerar otro parámetro: la inversión que se requiere en seguridad. Muchas de las organizaciones no lo hacen, sino hasta cuando les sucede algo; aunque poco a poco la tendencia de prevención va en crecimiento, lo que se busca es tomar medidas necesarias, pues las exigencias en un mundo de hackers, virus, malware, spyware, van en aumento por lo que la seguridad informática es hoy por hoy una prioridad, por lo tanto no se debe tomarlo como un costo, sino más bien como un plus que a la larga va a representar un valor agregado para la empresa.

Frente a estas circunstancias, se debe establecer una estructura de seguridad eficiente que proteja los recursos informáticos sensibles de la organización de las amenazas actuales a las que se enfrentan las organizaciones.

D'L Systems (S/F) en una de sus publicaciones sugiere:

Para fortalecer la confidencialidad:

Encripción o cifrado de datos: Es el proceso que se sigue para enmascarar los datos, con el objetivo de que sean incomprensibles para cualquier agente no autorizado. Los datos se enmascaran usando una clave especial y siguiendo una secuencia de pasos pre-establecidos, conocida como "algoritmo de cifrado". El proceso inverso se conoce como descifrado, usa la misma clave y devuelve los datos a su estado original.

Para fortalecer la integridad:
Software anti-virus: Ejercen control preventivo, detectivo y correctivo sobre ataques de virus al sistema.

Software "firewall": Ejercen control preventivo y detectivo sobre intrusiones no deseadas a los sistemas.

Software para sincronizar transacciones: Ejerce control sobre las transacciones que se aplican a los datos.

Para fortalecer la disponibilidad:

Planes de recuperación o planes de contingencia: Es un esquema que especifica los pasos a seguir en caso de que se interrumpa la actividad del sistema, con el objetivo de recuperar la funcionalidad. Dependiendo del tipo de contingencia, esos pasos pueden ejecutarlos personas entrenadas, sistemas informáticos especialmente programados o una combinación de ambos elementos.
Respaldo de los datos: Es el proceso de copiar los elementos de información recibidos, transmitidos, almacenados, procesados y/o generados por el sistema.

Existen muchos mecanismos para tomar respaldo, dependiendo de lo que se quiera asegurar. Algunos ejemplos son: copias de la información en dispositivos de almacenamiento secundario, computadores paralelos ejecutando las mismas transacciones, entre otros.

Conclusiones

En un mundo globalizado como el de hoy, interconectados a la red mundial, lo que implica un sinnúmero de enlaces entre varios factores: técnicos, legales, administrativos, entre otros, en los que se tiene grandes ventajas pero a su vez ligadas con enormes peligros que necesaria y obligatoriamente deben ser tomados en cuenta y prevenirlos, para lograr generar confianza en todos los componentes de una estructura organizacional.Esto involucra mejorar en todos sus ámbitos, implica además cambiar el paradigma, la cultura de seguridad debe prevalecer y la meta para lograr el objetivo sería formar personas que sepan y quieran trabajar en este nuevo entorno.

Cumplir también con las políticas de seguridad informática impuestas, las cuales deben establecer los medios de protección necesarios para evitar ataques internos o externos, hasta llegar a un alto nivel de confianza, buscando un equilibrio entre la tecnología, las personas y la información, que permita el crecimiento de una organización.

- **Bibliografía**

- Anónimo. (19 de octubre de 2014). Expertos comparten medidas de seguridad informática. Recuperado el 31 de octubre de 2014, de http://search.proquest.com.bvirtual.epn.edu.ec/docview/1613921685/5219E1F089E64DA6PQ/109?accountid=36685
- Anónimo. (07 de Septiembre de 2014). Seguridad informática, principal preocupación hoy en día:Tata.
- Cinco consejos de un ex hacker para aumentar la seguridad informática: ECUADOR TECNOLOGÍA. (20 de Octubre de 2011). Recuperado el 31 de Octubre de 2014, de http://search.proquest.com.bvirtual.epn.edu.ec/docview/899267972/5219E1F089E64DA6PQ/63?accountid=36685
- D'L Systems. (S/F). Archivo de la categoría: Seguridad Informática y cibernética. Recuperado el 08 de noviembre de 2014, de http://asdlc.wordpress.com/category/seguridad-informatica-y-cybernetica/
- García Rommel. Noticias Financieras. (09 de Julio de 2007). Recuperado el 31 de octubre de 2014, de http://search.proquest.com.bvirtual.epn.edu.ec/docview/465641177/5219E1F089E64DA6PQ/66?accountid=36685
- Global network COntent Services LLC, DBA Noticias Financieras LLC. (Agosto de 2014). Empresas de Latinoamérica procuran mayor análisis predictivo de la seguridad informática. Recuperado el 31 de octubre de 2014, de http://search.proquest.com.bvirtual.epn.edu.ec/docview/1551682094?accountid=36685
- Noticias Financieras. (27 de mayo de 2014). Auge de ciberataques desnudan vulnerabilidades del tradicional enfoque de seguridad informática. Recuperado el 31 de octubre de 2014, de http://search.proquest.com.bvirtual.epn.edu.ec/docview/1528487962/5219E1F089E64DA6PQ/83?accountid=36685
- Revista Enter. (29 de Enero de 2009). Delitos informáticos cuestan un billón de dólares a nivel mundial. Recuperado el 31 de Octubre de 2014, de http://go.galegroup.com/ps/i.do?id=GALE%7CA237253422&v=2.1&u=epn_cons&it=r&p=AONE&sw=w&asid=5a2318fb78ea8c9fecb4ac8a99d81288