Algo básico de la seguridad híbrida

DOI: 10.29236/sistemas.n167a2

Daniel Jiménez, MBA, CPP®, PSP®, CHSS, ESRM, WVP&IP

Hablar de seguridad es un criterio muy amplio a nivel organizacional, pero también es algo especifico, que ayuda a las corporaciones a protegerse de diversas amenazas que conduzcan a múltiples tipos de pérdidas. Hoy el concepto debe ser visto de manera mucho más holística e inclusiva en cuanto al alcance corporativo; cada una de las aristas relacionada con la seguridad deben ser incluidas como parte de las responsabilidades del encargado de esta área en las compañías; seguridad de la información, seguridad informática, cumplimiento, investigaciones, manejo de crisis y emergencias, seguridad ocupacional, seguridad física y muchas otras que pueden convertirse en parte esencial dentro de los diferentes negocios, tendrían que integrarse a manera de factor diferencial de este hombre o mujer que no

solo tenga conocimientos de seguridad física.

Podría cuestionarse entonces, ¿por qué el gerente de seguridad tiene responsabilidades de protección de la información? Y el fondo de la respuesta radica en que su principal responsabilidad es evitar y ejercer control de las pérdidas, pero que en última instancia no lo hará de forma aislada o a manera de silo dentro de la facilidad sino que, con el concurso de un oficial de protección de la información, para que junto a este, logre alcanzar su objetivo de evitar y/ o prevenir las pérdidas, para ver de manera visible la adecuada gestión de los riesgos en las diferentes áreas, como las mencionadas en la parte superior de este escrito.

Además de esto, es significativo entender que la protección de activos dentro de las diferentes estructuras organizacionales se logrará de manera exclusiva con la integración de ***las personas; los procedimientos y el uso de la tecnología*** adecuada, todo esto basado en un excelente diseño que atienda las necesidades de las empresas y para que su efectividad se pueda apreciar en todo su esplendor, se necesita disponer de varios elementos en perspectiva, así:

El primero de ellos, un enfoque sistémico de gestión de riesgos, que deje apreciar aspectos como las diferentes condiciones internas y externas, y su integración para definir los contextos en los que trabajará la organización. Además de ello, la extensión de esas autopistas en las cuales se estará moviendo la evaluación de esos riesgos, y que se complementará con la definición de los criterios.

Entender y conocer cómo la valoración de riesgos define e identifica, analiza y evalúa los diferentes riesgos, para que de esa manera la misma organización logre comprender ¿qué se va a proteger? y ¿de qué se va a proteger?; y como complemento de esto dentro de ese enfoque sistémico, definir las opciones de tratamiento de riesgo.

Pero como lectores estaremos pensando, se está hablando de manera académica de lo que es parte del proceso de la gestión del riesgo y es totalmente cierto, porque no se debe perder como lo mencioné anteriormente, la perspectiva y, si pensamos en dejar de lado la aplicación de este sencillo procedimiento, pues difícilmente vamos a tener resultados alineados con un enfoque sistémico y metodológico.

Obviarlo nos lleva a entender el porqué nuestro mercado aparece infestado de una cantidad de personas que se auto endilgan la etiqueta de especialistas, simplemente porque han realizado un curso de formación como auditor en diferentes estándares, normas y otras iniciativas, sin tener en cuenta las responsabilidades que conlleva

el mismo título de especialista, además de que no es cuestión de autodeterminación, sino de reconocimiento por parte de un tercero con autoridad para definir la ***"especialidad de una persona"***, que es quien reconoce ante la comunidad la pericia y experiencia junto con el uso del conocimiento, en una ciencia o disciplina, que se pueden convertir en sendas vulnerabilidades dentro de la organización por su misma condición.

Como segundo aspecto, el manejo técnico de la disciplina que se logra, además de experiencia, con una educación, capacitación, entrenamiento y desarrollo a diferentes niveles, de pregrados y postgrados.

Ahora, desde lo relacionado con el ser humano y su conocimiento, el segundo gran aspecto que nos ocupa para hablar de la seguridad hibrida tiene que ver con los procedimientos, los que deben estar articulados con el mismo objeto del negocio, y enfocados al cumplimiento de las políticas que desarrollen o pretenden alcanzar la misionalidad dentro de ese planeamiento estratégico trazado por la empresa para la vigencia que determine.

El verdadero sentir de estos procedimientos radica directamente en la capacitación y disponibilidad de estos para que se puedan materializar, mucho más, cuando hablamos de asuntos relacionados con la protección de activos de la información y las medidas de protección sobre estos. Algo que nos dejó la pandemia generada por el COVID 19, fue la enseñanza asociada con las contramedidas que, desde el área responsable de controlar el flujo y la seguridad de la información, se iniciaron y que perdurarán en el tiempo; mucho más hoy como parte esencial para evitar las pérdidas dentro de múltiples compañías que transan sus operaciones haciendo uso de diferentes infraestructuras de TI y redes externas.

Tal como lo mencioné anteriormente, un correcto diseño teniendo en cuenta el Diseño Base de Amenazas o Amenaza Base del Diseño (DBT por sus siglas en inglés) permitirá que la infraestructura de protección o su planeamiento sea modular y adaptable a las diferentes amenazas que migren con el tiempo manteniendo un esquema siempre operativo y funcional, para proteger no solo los activos tangibles e intangibles sino que también a la misma facilidad, por lo que este se convierte en un factor decisivo para esta tercera parte, que tiene que ver con la seguridad hibrida y que es el uso de la tecnología.

Sabiendo y conociendo, nuestras vulnerabilidades, amenazas, habiendo identificado los riesgos y las opciones de tratamiento de los riesgos, lo que nos resta es transpolarlas con las diferentes contramedidas, para lo cual es imperioso que se sepa y conozca más allá de lo básico; muchos de los responsa-

bles de la protección de activos de una empresa recomendarán “se requiere una cámara en esta esquina, un molinete y lector biométrico en la entrada, un radio de tales características, un vigilante armado”, pero cuando se trata de justificar el porqué de estas recomendaciones, sus argumentos se diluyen como humo, dejando en evidencia su subjetividad ante el conocimiento de los conceptos ya señalados; por lo mismo, es necesario que las recomendaciones de uso de tecnología estén orientadas en principio a atacar o mitigar los riesgos identificados desde el punto de vista de protección de la organización, para que en función de ello, se logre entender la seguridad como una herramienta eficaz, eficiente y efectiva bajo un enfoque no solo sistémico y metodológico, sino con un resultado costo efectivo para todas las partes interesadas.

Para concluir, es necesario mencionar que la necesidad de las estructuras corporativas está orientada al cumplimiento de sus objetivos, independientemente de cuál sea su objeto social; y para ello, dentro de la protección de activos se requiere hacer uso de elementos y herramientas que dejen ver la manera costo efectiva de gestionar los riesgos de seguridad a diferentes niveles (estratégicos, tácticos/misionales y operativos), además que la seguridad es uno de los instrumentos que se pueden emplear a nivel organizacional para esa gestión de los riesgos en todos los grados.

***Daniel Jiménez**. MBA, CPP®, PSP®, CHSS, ESRM, WVP&IP*