# Los CISO´s opinan

*Desde su criterio y práctica, se refieren a la realidad de la seguridad de la información en el país.*

Cinco Jefes de Seguridad de la Información –Chief Information Security Officer- de las más reconocidas organizaciones del país, dieron respuesta a las siguientes inquietudes planteadas:

***1. La computación en la nube se ha convertido en una realidad emergente en las empresas colombianas. En este contexto y sabiendo que necesariamente las organizaciones se migrarán a la nube, ¿cuáles son las consideraciones de seguridad de la información en la que el CISO no se puede equivocar, para balancear la necesidad natural de mejorar la ecuación de costos de la empresa, frente al uso de la TI y el aseguramiento de la información clave de la compañía?***

***2. Las redes sociales se han convertido en un fenómeno concreto del empoderamiento de las personas, frente al uso de la información. En este escenario ¿cuáles recomendaciones de seguridad de la información se deben tener en cuenta para limitar la fuga y/o pérdida de la información o deterioro de la imagen corporativa? ¿Cuáles son las soluciones procedimentales, éticas o tecnológicas?***

***3. Los activistas de las redes, los grupos emergentes como Anonymous y otros similares reclaman atención sobre sus declaraciones o actividades. En tal sentido, cualquier empresa puede ser susceptible de acciones "activistas informáticas" que impacten la operación de alguno de sus sistemas. ¿Cuál debe ser la posición de un CISO frente a esta amenaza social informática?***

***4. Cada vez más las organizaciones entregan su operación a terceros confiables, los cuales tienen a cargo la información de negocio de las empresas; de ahí que sea necesario incluir dentro del modelo de seguridad de la información tales actores. En esa dirección, ¿cuál debe ser la posición del CISO ante las iniciativas internacionales de certificación en seguridad de la información de estos terceros, en torno a referentes como la ISO/IEC 27036-Guidelines for security of outsourcing?***

***5. Las soluciones móviles son una clara exigencia de las organizaciones y los procesos de negocio, así como la demanda incremental de los individuos en las empresas, para el uso de sus dispositivos móviles personales. Considerando los riesgos propios del uso de estas tecnologías frente al tratamiento de la información, ¿cuáles son las recomendaciones del CISO para mitigar el riesgo y mantener la movilidad en la empresa?***

**Empresas Públicas de Medellín E.S.P.**
**Manuel Humberto Santander Peláez**
*Arquitecto Seguridad de la Información*
manuel.santander@epm.com.co

1. Las siguientes:

- Las políticas de seguridad de la información no son negociables, pues se trata de la declaración de la gerencia

sobre el uso aceptable de la información y son de obligatorio cumplimiento, para cualquier solución que sea brindada en el marco del desarrollo normal del proceso informático en la compañía.
- El CISO nunca puede ir en contra de los objetivos estratégicos de la organización. Siempre debe encontrar una solución que minimice los riesgos a los cuales está expuesto el negocio y que permita que queden en un nivel aceptable, de acuerdo con lo definido en el proceso de gestión de riesgos corporativo. En caso de no existir solución factible para la empresa, es importante obtener la aprobación para incurrir en el riesgo por parte del comité de seguridad y de los dueños de los activos de información afectados.
- El proceso de monitoreo debe incluir especial atención en estos riesgos para proceder a detectar riesgos materializados en el acto, de tal manera que el impacto para el negocio sea mínimo.

2. Las siguientes:

- Normativas: debe establecerse claramente un reglamento de propiedad de la información que contemple la posesión de la propiedad con respecto a la información generada en las dependencias de la empresa y las respectivas responsabilidades civiles, disciplinarias y penales en las que se incurren, en caso de la violación del mismo.
- Tecnológicas: Debe existir un buen sistema DLP en sitio, que permita bloquear proactivamente cualquier intento de fuga de información correspondiente a activos de información críticos dentro de la organización.

3. Esta amenaza siempre ha existido, solo que por primera vez es visible y podemos observar cómo el concepto de asonadas y manifestaciones de grandes grupos de personas ya se trasladó al ámbito virtual, con los respectivos impactos equivalentes. Simplemente, debe ser considerada dentro del análisis de riesgos y mitigada en forma adecuada, de acuerdo con el contexto y el entorno empresarial.

4. De acuerdo con mi experiencia, las compañías que prestan los diversos servicios de *outsourcing* en Colombia, apenas están empezando a incursionar en tener sus propios sistemas de gestión de seguridad, tanto para procesos internos como externos. Si el negocio considera valiosa la tercerización de uno o más procesos de operación, el CISO está en la obligación de exigir la seguridad requerida a la empresa, en términos del sistema de gestión de seguridad interno, del cual el tercero formaría parte integral. Aunque el estándar ISO 27036 todavía está en desarrollo, es posible incluir dentro del contrato de prestación de servicio, la obligación estricta en el cumplimiento de los objetivos de control de ISO27002 y asegurar la eficacia requerida mediante los indicadores definidos por la norma ISO27004.

5. Las siguientes:

- Los dispositivos móviles son una extensión del perímetro de red de la empresa. Por lo tanto, dichos equipos deben incorporar todas las medidas para salvaguardar la confidencialidad, integridad, disponibilidad, trazabilidad y no repudio de la información, tales como suites de protección *endpoint* contra *exploits* y *malware*, cifrado de información y autenticación fuerte, entre otros.
- Los protocolos de transmisión deben contar con las características de seguridad necesarias para garantizar el no repudio de las transacciones realizadas desde ellos.

**ATH S.A.**
**Javier Díaz Evans**
*Director de Seguridad de la Información*
jdiaz@ath.com.co

1. Es importante resaltar que la Seguridad de la Información debe estar un paso al frente de las iniciativas o soluciones tecnológicas que puedan apalancar a la organización. Dentro de estas soluciones esta la Nube. Su implementación dependerá de las necesi-

dades de la organización y existen soluciones para un grupo específico de usuarios, procesos transversales, actividades de soporte, estratégicas o misionales; nubes públicas o privadas, entre otros. La función de seguridad es garantizar que se pueda utilizar sin afectar o impactar a la organización. Adjunto los elementos claves frente al control de dicho servicio:

- Gestione un inventario de los servicios en la nube: Existen 2 grandes riesgos el primero que no se tenga controlada la adquisición de servicios en la nube y el segundo que no podamos detectar el uso de nuevos servicios.
- Incluir clausulas de seguridad en los contratos: No solo para estos contratos sino para todos hay fallas en la inclusión de clausulas de seguridad, se debe tener claridad de la identidad de quienes proveen el servicio, muchas veces se termina dependiendo de un proveedor único.
- Análisis de Seguridad del Proveedor: La gestión del proveedor es una actividad fundamental la ausencia de monitoreo y seguimiento de los acuerdos establecidos es un riesgo muy crítico para las organizaciones. Es fundamental incluir las cláusulas de derecho a auditar.
- Cumplir con las leyes y regulaciones: Se debe verificar si los datos que se van a enviar a la nube están autorizados por leyes. La privacidad o la regulación de ciertos datos pueden prohibir esta práctica.
- Protección de Datos: En la nube puede fugarse información o perder control de su clasificación, resguardo, destrucción, etc.
- Actualización de la arquitectura de seguridad: la organización debe soportar el uso seguro de los servicios en la nube. Elementos a
- considerar: conexiones seguras, federación de usuarios, uso de sistemas de prevención de fuga de información.
- Gestión de Incidentes, Crisis y Continuidad: Se asume que en la nube se eliminan los problemas de continuidad de la información, esto es un error.
- Adicionalmente la investigación y los temas forenses se vuelven complicados.

2. Las redes sociales pueden ser una herramienta efectiva de colaboración y de apoyo para tareas claves dentro de la organización. Adicionalmente, no podemos seguir haciendo caso omiso sobre cómo operan en la actualidad nuestros colaboradores. Estas herramientas son su interacción con el mundo, su uso no afecta la productividad y el no tener estos servicios puede ser un motivo de inconformismo o rechazo a la organización. Adjunto algunas recomendaciones:

- Normas de conducta y uso adecuado de las herramientas. Seguridad de la Información no puede continuar atajando o poniendo límites a las acciones de las personas. Debemos orientar las actuaciones de nuestros colaboradores, dejando claro lo que está bien y lo que está mal y estableciendo políticas de uso adecuado de los recursos.
- DLP: los sistemas de prevención de fuga de información son fundamentales. Importante que la organización defina claramente los niveles de sensibilidad de la información y dentro de estos se encuentre la información privada.
- Control de contenido: Estas herramientas exponen claramente a la organización y a las personas a riesgos de código malicioso y acceso a contenido no autorizado.

3. Es importante que las áreas de seguridad entiendan que el ciberespacio presenta amenazas que impartan no solamente los criterios de la información como son Confidencialidad, Integridad y Disponibilidad, otros impactos como la reputación la pérdida de mercado, la disminución de la confianza de nuestros clientes son hoy en día las que más nos están afectando. Debemos reforzar nuestros procedimientos de emergencias y respuesta a incidentes, alistarnos para reaccionar a lo que no conocemos.

Nuestra organización ha desarrollado un modelo de Ciberseguridad que consta de 4 elementos claves:

- Cibergobierno y acuerdos recíprocos.
- Inteligencia de Seguridad.

- Conocimiento de nuestras falencias.
- Planes de respuesta.

El Cibergobierno nos ayuda a tener la capacidad de incluir a otras organizaciones dentro del esquema de Ciberdefensa y se establecen acuerdos con estos, para compartir conocimiento y apoyarnos en estrategias de respuesta.

4. Todos los esfuerzos que podamos hacer son bienvenidos, pero recomiendo aunque se incluyan elementos como certificaciones del proveedor; hacer un seguimiento, control y monitoreo constante del cumplimiento de los requerimientos de seguridad por parte del proveedor.

5. El consumo o uso de los dispositivos personales para actividades de negocio es una realidad. Las áreas de seguridad deben tener clara la forma de proteger la información cuando se implementen estos lineamientos dentro de sus organizaciones. Se deben definir varios controles, los cuales enumero a continuación:

*Administrativos*:
- Establecer la política.
- Definir el uso adecuado de los dispositivos personales.
- Definir qué tipo de dispositivos son aceptables.
- Establecer un proceso para la autorización y aprobación del uso de los dispositivos personales.
- Licenciamiento, cumplimiento de leyes y regulaciones, etc.

*Técnicos*:
- Definir la arquitectura de seguridad para el uso de dispositivos personales.
- Establecer la forma segura de acceder a las aplicaciones y datos. Ej.: Sandbox, segregación lógica de negocio y personal, aplicación de todos los controles de negocio y pérdida de privacidad.
- Métodos de borrado seguro de información.

**Organización Terpel S.A.**
**Carlos Alberto Zambrano Smith**
*Director de seguridad Informática L.A.*
carlos.zambrano@terpel.com

1. La computación en la nube almacena múltiples riesgos de seguridad y tiene características particulares que hacen necesaria una evaluación de ese contexto frente a la integridad de los datos, la recuperación y la privacidad. De la misma manera, un análisis de las cuestiones legales, toda vez que cada país administra su propia apreciación en la protección de la información, de la cual no hay una única ley estándar en torno a las exigencias de la privacidad de los datos y la ubicación de la misma, a nivel contractual.

Los clientes deben exigir transparencia en el modelo de despliegue, principalmente en la categoría de sus datos en las zonas Pública, Privada, Híbrido y Comunidades.

No podemos dar la espalda, pero las tendencias de las empresas por el nivel de costos y flexibilidad administrativa, hace que la computación en la nube sea atractiva, de ahí que los responsables de la seguridad informática deben buscar un equilibrio entre la operación del negocio y la protección de la información.

Este servicio todavía está en la búsqueda de la madurez del equilibrio entre seguridad de la información y operación del negocio. En consecuencia y desde mi punto de vista, basado en las prácticas del entorno de la pérdida de imagen por la fuga de información, es importante que el cliente no exponga su información sensible o del *core* estratégico de la organización, sino que use el modelo tipo "Escalera"; es decir, ir llevando a la empresa a medida que los proveedores del servicio de computación en la nube respondan a factores tales como:

- Cumplimiento a las leyes de protección de la información.
- Trazabilidad de los datos y el monitoreo de ambas partes (clientes-proveedores).
- Modelo de responsabilidad de la recuperación de datos en los diferentes escenarios.

El CISO debe definir los lineamientos a los proveedores del servicio sobre el uso adecuado y responsable de la información del cliente, basado en los siguientes criterios:

- Los datos confidenciales fuera de la empresa traen consigo un nivel de riesgo, toda vez que los servicios en manos de terceros obvian los controles físicos, lógicos y de personal. Debe obtener la mayor información posible acerca de las personas que manejan sus datos. Y pedir a los proveedores que suministren de manera permanente información específica sobre la contratación y la supervisión de los administradores de privilegiados, y los controles sobre el acceso.
- Los proveedores tradicionales de servicios están sujetos a auditorías externas y la seguridad de verificación. Los proveedores de computación en la nube deben convertir la tranquilidad de los clientes en el uso de controles tradicionales emergentes, con el objeto de dar trazabilidad a los datos. Aquel proveedor que no acepta este tipo de revisión está dentro de los llamados proveedores sin marco jurídico, en el ámbito de protección de la información.
- Cuando se utiliza la nube, es probable que no se sepa con exactitud dónde están almacenados sus datos. De hecho, usted ni siquiera sabe en qué país se almacenarán. Hay que pedir a los proveedores que se comprometan a almacenar y procesar los datos en determinadas jurisdicciones, de acuerdo con las exigencias de las leyes de protección de los datos y marco legal de la privacidad. Este punto es fundamental en las cláusulas del contrato. Servicios, almacenamiento y leyes deben ser acordes.
- Posiblemente, los datos sin importa la naturaleza del negocio, están almacenados de una manera compartida con múltiples clientes. El cliente debe establecer un mecanismo de separación o instrumento lógico a lo denominado segregación de datos.
- Frente a la recuperación, un proveedor de la nube debe establecer políticas y procedimientos a nivel contractual y en programas de simulaciones, para responder por lo que ocurrirá con sus datos y el servicio, en caso de un desastre o un riesgo materializado. Además, estudio de análisis de vulnerabilidad, test de penetración u otros mecanismos con reporte al cliente, sobre los hallazgos y el nivel de protección de los datos.
- Es complejo un estudio forense informático o investigación sobre un evento de los datos del cliente. Al proveedor de la computación en la nube se le debe exigir todo el apoyo en las investigaciones, de las cuales debe poseer herramientas de trazabilidad y niveles estándares de seguridad, en el acompañamiento de dicha investigaciones.
- En conclusión, dentro de este mar de mercado es imprescindible tener en cuenta que, no todos los proveedores de computación en la nube, dicen ser lo que son. Es muy importante saber elegir.

2. Cada día Internet se convierte en una herramienta operativa y estratégica del negocio y, por ende, las redes sociales son un ente similar a un asesor comercial, en donde se exponen los productos e incluso la imagen de la compañía. Es un atractivo instrumento para los intereses en la expansión de mercado.

Actualmente, la forma de expandir haciendo uso de las 3Cs (comunicación, cooperación, comunidad), es útil para lograr los objetivos de mercadeo y a nivel comercial. Sin embargo existen riesgos tales como:

- Suplantación de identidad.
- Phising.
- Ingeniería Social.
- Vulnerabilidades.
- Publicidad no deseada.

Uno de los casos más sonados es el uso de la red social *Twitter*, que evidenció su utilización para capturar máquinas y convertirlas en Zombis para ser controlada por Bonet.

En otros países se denomina “rumorología”, es decir, daño contra la imagen, son programas maliciosos.

Por lo anterior, es claro que en las redes sociales cualquiera sea su contexto -me enfoco a nivel industrial y comercial- la información privada debe estar fuera de su alcance.

El aporte del CISO es ayudar a construir un perfil netamente público, que contemple liberar en Internet información masiva de carácter no confidencial ni sensible y, solo para la comunidad. Así mismo, fortalecer la política de gestión de la protección de la información, para determinar que los recursos informáticos de la organización son propiedad de la misma y que su adecuada administración es responsabilidad del usuario final. Política que también contempla el uso limitado de las redes sociales exclusivamente en las comunidades controladas y aprobadas por el negocio. De igual manera, esa política debe establecer los términos del control para el acceso a las mismas, por parte de los funcionarios de la compañía.

A esto se suma que los equipos informáticos deben poseer herramientas tecnológicas de monitoreo, trazabilidad y protección, ante cualquier evento en el uso de estas redes.

Recordemos que el objeto no es la prohibición, sino la limitación más una buena cultura de los usuarios, a través de la concientización y buenas herramientas de protección.

Un aspecto vital que se debe tener en cuenta es que toda información privada, en las redes sociales es pública y, en consecuencia, los usuarios de la comunidad perteneciente a tales redes renuncian a la privacidad. Y, es ahí cuando el CISO debe focalizar su esfuerzo en la protección de la información clasificada como sensible, privada y confidencial.

3. Existe una relación con las respuestas de las preguntas anteriores basada en el impacto. No obstante, hay un contexto especial sobre estos ciberactivistas, cuyo objetivo principal es hacerse escuchar sobre cualquier evento de interés público y socioeconómico. Lo vital es que estos grupos publican de manera directa las vulnerabilidades -se evidencia cuando es exitoso el nivel de ataque-, de las empresas y sus intereses, que son aprovechados por atacantes de otros principios y con objetivos distintos.

Sin perder el marco de la protección de la información, el CISO debe evaluar cuál es la posición de la empresa sobre el mercado y el entorno social, en donde este último es fundamental de cara a los intereses que aporta la compañía hacia el cliente externo. Una vez identificadas esas variables, se inventarían los diferentes aspectos que la sociedad acepta o rechaza, tales como precios de productos masivos, sector de empresas de energías o de servicios públicos, precios de consumidores, servicios del gobierno, empresas de tecnología, compañías de no aceptación nacional, bancos y otros de naturalezas similares que impactan en la sociedad y pueden llamar la atención a estos grupos activistas. El paso siguiente es evaluar el apoyo de la plataforma tecnológica, estableciendo qué tan vulnerables son ante una negación de servicios, divulgación de informaciones sensibles o críticas, pérdidas de imagen, etc. Recordemos que cualquier persona puede ser miembro de estos grupos de manera directa e indirecta -¿clientes internos?-. En conclusión, el objeto es mitigar el riesgo considerando los siguientes lineamientos:

- Hacer estudio constante mediante el test de penetración, con el fin de identificar variables de vulnerabilidades y definir planes de acciones oportunas.
- Contar con un sistema de centro de operación de seguridad (SOC) que realice monitoreo y trazabilidad de los registros de las plataformas tecnológicas sensibles, en el aspectos de la información tales como web, correos electrónicos y sistemas de operación del negocio.

- Las plataformas tecnológicas deben dar cumplimiento a las normas estándares de seguridad sobre los servicios y desarrollos.
- En ningún caso garantiza prevenir un ataque -mitigar es el principal logro-. Sin embargo, las compañías deben contar con una matriz de escalamiento DRP (Plan de recuperación desastre) o un BCP dentro del marco de recuperación de plataforma, cuando este se vea afectado de cara a la prestación de los servicios hacia el cliente externo e interno.
- Definir claramente políticas de gestión de la protección de la información, con medidas que logren establecer madurez en la organización.

Las empresas conviven con estas redes de activistas y no podemos ignorarlo ni pensar que estamos exentos; lo que debemos es convivir con buenos controles de seguridad y un programa constante de validación que aporte a la mitigación, ante cualquier evento en los sistemas de información.

4. La información es un activo vital para la estrategia, operación y continuidad de las empresas. En consecuencia, debe existir un método claro, documentado y con unos objetivos de seguridad paralelo a las evaluaciones de riesgos.

Al involucrar la transferencia de una función del negocio a un proveedor externo, no solo debemos establecer la relación cliente-tercero a través de las condiciones de servicios (SLA), sino, ir más allá de esta relación en el tratamiento adecuado, integral, de disponibilidad y, sobre todo, en la confidencialidad de los datos.

A pesar de que la gestión y operación en el tratamiento de los datos y de los servicios está en manos del proveedor, la responsabilidad sigue siendo del CISO. De ahí que a nivel contractual debe quedar plasmado que el cliente, a través de las áreas responsables, tenga el rol de administración del outsourcing con el objeto de establecer métodos claros de trazabilidad, monitoreo y auditoría de los servicios que presta el tercero y la integridad de los datos.

Sin embargo el CISO debe ser estratégico desde el punto de vista del negocio en donde debe dar respuestas dentro de la compañía sobre cuál es la madurez de la empresa al entregar sus servicios al outsourcing; cuál es el nivel de criticidad de su operación, entre otros aspectos.

Si no existe claridad en tales aspectos, no es oportuno tercerizar y el CISO establece frente a las directivas los criterios de los diferentes riesgos. En caso contrario, es decir, si los aspectos señalados son claros, se le facilitan al CISO los diferentes controles que debe aplicar, con el objeto de generar trazabilidad y estructurar el monitoreo de los servicios a prestar por parte del outsourcing.

En este orden de ideas y de acuerdo con la naturaleza y el tamaño de la empresa, el proveedor de *outsourcing* debe poseer certificaciones de normas o estándares de seguridad con el objeto de lograr la confianza entre las partes, además de proporcionar una línea entre los recursos y el valor de la cadena del negocio.

5. Siendo los dispositivos móviles una herramienta de flexibilidad para los directivos, en el sentido de tener acceso a la información de la empresa e incluso a aprobaciones de pagos o actividades financieras, la gestión de la protección de la información se ha convertido en un "verdadero dolor de cabeza" para los líderes de la seguridad informática. En una de las investigaciones en el campo tecnológico, llega a mezclarse la necesidad con la moda del uso de estos dispositivos, pero a medida que pasan los días crece más la necesidad de tener la información a primera mano, como apoyo instrumental.

Estos dispositivos móviles son de gran de interés para los ciberdelincuentes, toda vez que en sus distintas gamas se bajan aplicaciones gratis las cuales, en su mayoría, son programas maliciosos encaminados a robar información, contraseñas y

otros datos de interés de la organización.

El CISO debe definir en los dispositivos móviles los alcances y las limitaciones en su uso. La mejor alternativa es crear conciencia en los usuarios sobre su administración.

Con el fin de mitigar los riesgos se debe crear una cultura asociada con los compromisos de la gestión de la protección de la información, que permita lograr la madurez. En otras palabras, que el usuario sea consciente del uso netamente profesional del dispositivo móvil.

En forma paralela, se deben implementar herramientas de seguridad de los móviles, con el objeto de hacer trazabilidad y bloquear de manera inmediata cualquier evento que afecte la integridad de los datos corporativos.

Los profesionales de seguridad de la información deben definir controles sobre:

- Acceso al correo corporativo.
- Acceso a los aplicativos corporativos.
- Almacenamientos y edición de documentos laborales. Que el usuario no use el dispositivo con fines no relacionados con el negocio.

**Deceval**
**Francisco Pacheco Alfonso**
*Director de Seguridad de la Información*
fpacheco@deceval.com.co

1. Las herramientas de hardware y software de seguridad informática de una u otra manera son algo claras, lo que indudablemente no lo es tanto, son las medidas de disponibilidad, aseguramiento de las condiciones de los productos, las medidas contingentes de los servicios ofrecidos y las alternativas para migrar a otros proveedores o volver a las condiciones individuales con que contaban las compañías, antes de tomar la decisión de ir a la nube.

Con respecto a la confidencialidad de la información considero que las empresas deben empezar a tomar soluciones de encripción de datos, que les permitan hacer todo el ciclo (grabación, procesamiento, copia y recuperación) de una manera natural y no quedar dependientes de los servicios ofrecidos.

2. Particularmente, considero que no es conveniente integrar las redes corporativas con redes sociales, toda vez que es incierto todo lo referente a la seguridad en este tipo de redes. De otra parte, para nadie es un secreto que las redes sociales son un mecanismo utilizado por los atacantes para hacer ingeniería social previa, antes de decidir tomar sus objetivos.

Por ahora, las redes sociales deben tomarse como mecanismos para hacer publicidad complementaria de la empresa, pero no integrada a su red corporativa. Es decir, tenerlas cerca, pero lo suficientemente lejos para no verse afectada.

3. Indudablemente, el trabajo de los CISO hoy en día, se debe centrar en la creación de alternativas contingentes para los diferentes servicios de Infraestructura tecnológica, complementada con procedimientos de atención y respuesta ante incidentes presentados, detectados o con alta probabilidad de ocurrencia.

4. Es la misma problemática que se tiene con un empleado contratado de manera directa e indefinida; lo único que lo diferencia es un tercero que funge como intermediario sobre quien gira todo el peso del contrato. Considero que el modelo de seguridad sugerido por la BS7799 (ISO 27000) cubre de manera adecuada este aspecto.

5. WIFI (AP) debe ser integrado con el Directorio Activo, aspecto que restringe y cierra la gran vulnerabilidad del uso de estos elementos. Por otro lado, se deben buscar alianzas con las TICs que permitan integrar elementos propios de seguridad informática de la red corporativa, como: filtros de contenido, IPS de Red, FW de Aplicación, entre otras, cuando se utilicen este tipo de tecnologías móviles.

**Cámara de Comercio de Bogotá**
**Andrés Ricardo Almanza Junco**
*Coordinador de Seguridad de la Información*
andres_almanza@hotmail.com

1. En este sentido es muy importante tener presente que las relaciones contractuales son los elementos claves con los cuales las ecuaciones se balancean; hoy por hoy tenemos diferentes propuestas de prestación de servicios en la nube, plataforma como servicio, software como servicio o infraestructura como servicio. Cada una con unas consideraciones de seguridad para tener presentes desde el punto de vista de la tecnología, metodología con la cual se pueda llevar a cabo una estrategia clara de protección.

Pero ellas tienen en común una propuesta a la que muchos responsables tanto de TI como de Seguridad de la información, no hemos prestado la respectiva atención, y son las relaciones contractuales que deben ser definidas en cada uno de esos escenarios, en los cuales el receptor del servicio debe tener claramente definido qué esperar del mismo, máxime con las crecientes necesidades de abaratar los costos empresariales de TI, y una creciente e implacable avalancha de amenazas tecnológicas que las organizaciones hoy poseen.

Por tanto es necesario aprender sobre cuáles deben ser las consideraciones y qué definir como parte de los acuerdos contractuales para garantizar una adecuada prestación de servicios de esta naturaleza, cumpliendo con nuestras necesidades.

2. La sociedad digital es algo que las organizaciones han visto como mecanismos de expansión de sus operaciones. Se ha escuchado decir que muchas de las redes sociales son potencializadas como parte de los propios CRM para convertir ese enfoque como parte de las estrategias de marketing, y relacionamiento con el cliente. En este sentido pienso que son muchas las acciones por emprender, dado que las responsabilidades frente a la protección de la información, va más allá de la misma tecnología. Así que tener una posición clara de la organización, frente al uso y su presencia en los medios sociales, es uno de los primeros pasos, para que de una manera controlada la organización entienda los riesgos que pueden ser asumidos por tener una postura frente al uso de los medios sociales.

Por otro lado, las medidas tecnológicas necesarias sumadas a un análisis claro de la información de la entidad encaminado de manera factible y con un balance en la prestación de los servicios de las redes sociales, para controlar cuáles contenidos de información se pueden o no manejar en los medios sociales.

Y, en tercera instancia, un esfuerzo continuo e intenso por tratar de hacer entender a todos y cada uno de los miembros de la entidad, la forma en cómo son responsables de la postura frente al uso responsable de los medios sociales, de tal forma que la información de la organización, no sufra frente a estos nuevos riesgos a los que las organizaciones se exponen.

3. Muchos en este sentido, menosprecian el "hacktivismo" y las actividades de las comunidades de *hackers*, que ya no corresponden a un reto consciente al intelecto, existen demasiadas motivaciones que en muchos casos tienen un orden social. La postura de monitoreo y seguimiento cercano a estos movimientos, debería estar dentro de las estrategias de protección de la información, para poder estar preparado y saber qué hacer; no para evitarlo, porque realmente es poco probable evitar un ataque de estas magnitudes. Es necesario que hagamos seguimiento consciente, disciplinado y continuo de los diferentes movimientos "hacktivistas", de tal manera de poder direccionar los esfuerzos en cuanto a una situación no deseada que pueda llegar a presentarse

4. Los terceros como buenos jugadores en la prestación de servicios de TIC's que las

organizaciones utilizan, deben ser adaptados al modelo de protección de la información que la empresa posee. Es por esa razón que debemos preocuparnos porque existan mecanismos claros con los cuales podamos integrar de manera segura a los terceros, dentro de la operación del negocio. Un estándar internacional como la ISO/IEC 27036 es un excelente mecanismo que permitirá a las organizaciones homogeneizar la forma de transferir la seguridad corporativa hacia nuestros terceros, de tal manera que procuren garantizar el cumplimiento de un modelo propuesto frente a la información de la entidad.

5. Nuevas tecnologías, sinónimos de nuevos riesgos, que acrecientan el panorama de protección de la organización, estrategias móviles, así como estrategias BYOD (bring your own device), son escenarios que no podemos desconocer, que requieren de nosotros los esfuerzos necesarios, para saber cuáles deben ser los mecanismos de protección necesarios. Requiere de nosotros estudiar la necesidad de la movilidad, de quién y por qué, abordar este tipo de estrategias.

En primera instancia, demanda de los CISO's la responsabilidad de tener un marco metodológico construido en la entidad en los temas de la protección de la información; tener definidas unas políticas de uso de la tecnología; así como de las responsabilidades de todos y cada uno de los miembros de la empresa frente a la información, sin importar el medio que se utilice para ella.

Es necesario que los CISO's comprendan de una manera clara el flujo de la información y el negocio, para advertir de manera clara cuáles son los escenarios posibles de uso, pero también de riesgos al involucrarse en estrategias de esta naturaleza.

Requieren del CISO un esfuerzo de trabajo conjunto con las áreas de TI, Control Interno, Riesgos, de tal forma que se articulen los trabajos para poder integrar este tipo de estrategias en la consecución de un negocio. Demandan del CISO un esfuerzo total frente a la forma en cómo estas tecnologías serán entregadas a los usuarios. Es necesario que el CISO pueda hablar todos los lenguajes de la entidad, el de los usuarios comunes y corrientes que demandan estas tecnologías, entender el lenguaje del negocio que busca de cualquier manera una expansión y disminución en los costos de la operación. Entender además, el lenguaje del riesgo y control al que la entidad se debe enfrentar, para con ello construir la estrategia con la cual se pueda abordar este tipo de iniciativas, en donde todas las partes interesadas se sientan cómodas y se logre el objetivo propuesto.