Responsabilidad legal del gerente de seguridad de la información

Sara Gallardo M.

La hiperconectividad de hoy obliga a las empresas a trascender la infraestructura tecnológica, para evaluar la importancia de la gestión de la seguridad, el perfil de quien la desempeña, además del alcance e impacto de las funciones adquiridas.

Walter Pinzón

María Conchita Jaimes

Rafael Gamboa

Juan Carlos Reyes

Los permanentes desarrollos de la tecnología informática, en particular todos los relacionados con la hiperconectividad, obligan a las empresas a repensar las condiciones que rodean su negocio para lograr competir y no desaparecer.

Dentro de ese proceso evolutivo, un estudio adelantado por la firma Internacional Data Corporation (IDC), advierte que para el año 2010 el 40% de la fuerza laboral a nivel mundial estará conectada en exceso; habrá 10 dispositivos conectados a la red por cada usuario y unas necesidades de soporte para cerca de cinco mil millones de puntos de conexión.

La misma investigación pudo determinar en un 64% el grado de hiperconectividad actual de la fuerza de trabajo en Latinoamérica, frente al 50% en Europa, el 44% en Norteamérica y el 59% en Asia Pacífico.

Frente a ese panorama, la seguridad de la información cobra un papel fundamental en el ambiente de negocios, que va mucho más allá de los riesgos inherentes a la vulnerabilidad y el buen funcionamiento de la infraestructura tecnológica.

Debería tratarse de un asunto prioritario para la alta gerencia de cualquier organización, en el sentido de evaluar el papel que desempeña el responsable de esa seguridad; su perfil profesional; la posición jerárquica que ocupa dentro de la empresa; además del alcance y la responsabilidad legal de sus funciones.

De ahí que la revista ***Sistemas***, siempre atenta a los temas más actuales y de mayor trascendencia, hubiera dedicado el foro de esta edición al debate de tales inquietudes con distintos expertos del sector informático del país.

Los invitados Walter Pinzón, Gerente de la Secretaría General del Banco Colpatria; Rafael Gamboa, abogado de la firma Bernate y Gamboa; María Conchita Jaimes, directora ejecutiva RAS de Ernst & Young; y, Juan Carlos Reyes, director de Investigación y Desarrollo de Séltika - Seguridad de la Información, fueron recibidos por los anfitriones: Francisco Rueda, director de la revista Sistemas; Jeimy J. Cano miembro del Consejo de Redacción y moderador del foro; Beatriz E. Caicedo, directora ejecutiva de la Asociación Colombiana de Ingenieros de Sistemas (ACIS); y, Sara Gallardo, editora de la publicación.

Acto seguido, el moderador abrió el debate con la formulación de la primera pregunta para los expertos convocados.

Jeimy J. Cano
¿Qué se entiende por responsabilidad legal del Gerente de Seguridad de la Información?

Walter Pinzón
Gerente de la Secretaría General
Banco Colpatria

Desde la perspectiva jurídica, siempre que hablemos en temas legales sobre responsabilidad debemos abordar necesariamente tópicos tales como obligaciones y reparación de perjuicios. Una primera aproximación es considerar la responsabilidad del gerente, quien tiene como obligación observar una serie de lineamientos para cumplir con la ley y las normas paralegales (en el sentido de que en el tema de seguridad de la información se trataría de autorregulación por no haber normatividad específica). Cuando por acción u omisión una persona con la responsabilidad de administrar la información de una empresa transgrede uno de esos lineamientos, deberá responder en las diferentes formas que establece la ley.

Rafael Gamboa
Abogado
Bernate & Gamboa

Parto de la definición de la XXII edición del Diccionario de la Real Academia de La Lengua, que define la responsabilidad como "deuda u obligación de reparar o satisfacer por sí o por tercera persona a consecuencia de un delito de una culpa o de otra causa legal". Otra acepción se refiere a la "causa u obligación moral que resulta para alguien del posible yerro en cosas o asuntos determinados; y, por último, la "capacidad existente en todo sujeto activo de hecho para reconocer y aceptar las consecuencias de un hecho realizado libremente". De cara a tales definiciones lo que se observa es que hay una causa generadora de un perjuicio y va a ser precisamente ese perjuicio el que va a tener que ser resarcido. Existen una causa, una consecuencia, un perjuicio y un nexo causal, que van a generar la responsabilidad por acción u omisión.

Juan Carlos Reyes
Director de Investigación y Desarrollo
Séltika - Seguridad de la Información

Desde un punto de vista más práctico –no soy abogado-, quienes están involucrados en la gerencia de administración de la seguridad, manejan conceptos

técnico-administrativos y su responsabilidad legal no viene directamente de ellos, sino que está atada a la responsabilidad contractual que cualquier empleado en forma independiente debe tener con respecto al cargo desempeñado dentro de la organización. Cada uno de los empleados tiene sus propias responsabilidades y de esa manera tendrán que cumplir con ellas. Ahora bien, el tema particular de seguridad de la información es un poco más complejo, en la medida en que involucra aspectos tales como la privacidad que puede afectar asuntos personales de los empleados de una compañía o de los objetivos de negocio de la misma. En el caso del gerente que nos ocupa, su obligación es mantener todos los esquemas de seguridad dentro de la empresa y, desde ese punto de vista, dicho cumplimiento se podría relacionar con algún tipo de imputación adicional que se le pueda hacer por un hecho o incidente de seguridad específico.

Francisco Rueda
Director Revista Sistemas

¿Quiere decir que la responsabilidad del gerente de seguridad de la información está sujeta al tipo de contrato firmado con la empresa para la cual trabaja y no de él como profesional? ¿No se trata de un cargo muy especial y delicado? Es decir, ¿no se trata de un cargo con un perfil muy especial y muy distinto a los demás dentro de la organización?

Walter Pinzón

El concepto de Juan Carlos Reyes es parcialmente cierto. La responsabilidad no solo obedece a unas obligaciones de tipo contractual o a una vinculación laboral. El gerente de seguridad de la información puede ser considerado un administrador, equiparado a un vicepresidente, no es ni siquiera una gerencia media. Y, en esa medida, sus responsabilidades y obligaciones van mucho más allá. Tanto así que su contrato termina, pero su responsabilidad legal, administrativa y financiera permanece.

Rafael Gamboa

Efectivamente, la responsabilidad excede los términos del contrato laboral para convertirse en extracontractual, así lo determina la clasificación jurídica. En esa medida, la responsabilidad tiene que ver con actos, hechos u omisiones. No importa cuál hubiera podido ser la causa, lo importante es que se haya inferido un perjuicio. La responsabilidad es todo lo contractual; existen

temas laborales, civiles, comerciales, tributarios y penales que no pueden ser contemplados en el contrato, pero que sí definitivamente exceden el tema contractual.

Jeimy J. Cano

¿Existe algún estándar o buena práctica que se pueda seguir o recomendar para apoyar al Gerente de Seguridad de la Información en estos temas?

Walter Pinzón

El único estándar está contemplado en las reconocidas prácticas de Gobierno Corporativo y en el sector financiero al que pertenezco, es donde se exigen las mejores a los administradores. Es una preocupación nacional e internacional, estatal como institucional. Con relación a esas prácticas hoy en día existe un Código País elaborado por la Superfinanciera de Colombia. Existen los documentos:"Libro Verde", el White Paper, las recomendaciones establecidas por parte de la OECD (Consejo de Ministros de Estados Europeos). Hay muchos Códigos que contienen prácticas de Buen Gobierno, en ellos podemos encontrar principios que debe tener en cuenta el Administrador, los que debe tener el Presidente de una empresa, cuáles son las responsabilidades específicas de una Junta Directiva, etc. Se pueden tomar diferentes recomendaciones de estos documentos, de estos Códigos y con estos se puede elaborar un documento específico que puede servir a un gerente de seguridad de la información.

Rafael Gamboa

A lo largo del foro mencionaré algunos principios del derecho que creo son aplicables a las varias áreas, entre otras a este tema específico de responsabilidad legal de seguridad de la información. En lo que se refiere a las buenas prácticas, se trata de un principio de derecho en el sentido de que nadie está obligado a lo imposible. Quiere decir que se debe hacer el mejor esfuerzo para materializar la no obligación o la imposibilidad o exigibilidad de hacer todo lo posible. En otras palabras, se materializa en lo que va a quedar registrado en el gobierno corporativo. Es decir, un manual específico sobre el mejor esfuerzo. De ahí los primeros interrogantes, tales como: ¿usted qué hizo?, ¿qué dejó de hacer? Dicho manual específico del área de tecnología y que no se aplica a otras áreas, debe ser desarrollado y actualizado en forma permanente, en la medida en que tecnológicamente, no es lo mismo decir nadie está obligado a lo imposible, porque ese imposible hoy es posible por la facilidad de las herramientas y avance. En tal sentido, las buenas prácticas existentes en el gobierno corporativo, tienen que ver con la materialización del sentido común de la gerencia, rodeada de una permanente asesoría.

Walter Pinzón

A los principios enumerados por el doctor Gamboa, agregaría la prudencia; el

principio que debe tener en cuenta un buen hombre de negocios para el desarrollo de esa actividad, al que va ligado también la pericia. Principios repito, previstos en Códigos de Buen Gobierno. Se habla en términos legales de la diligencia y el cuidado que debe tener un buen hombre de negocios de cara a la gestión (o sea la responsabilidad que tiene un administrador en el desarrollo de su labor). Y al gerente de la seguridad de la información se le puede exigir más allá, debe tener la suma diligencia o cuidado que un hombre de negocios emplearía en la Administración de sus negocios importantes, Pero aquí destaco que a este administrador al momento de vinculársele a la empresa se le debería advertir acerca de la responsabilidad que implica su cargo y los riesgos que este conlleva.

Juan Carlos Reyes

Por supuesto, el común denominador es el Código de buen gobierno, eso es indiscutible. Sin embargo, la pregunta es ¿cuál es el objetivo o qué es lo que persigue un gerente de la seguridad de la información? El tema del buen gobierno es un tema genérico, perfectamente aplicable, pero en el caso específico de seguridad de la información debe orientarse a cuál es el resultado que se les exige o cuál es el objetivo que se persigue más bien detrás de la gestión de un gerente de seguridad de la información. Para eso también hay otras buenas prácticas que todos conocemos desde el punto de vista técnico, como ISM3, ISO27001, COBIT, etc.; todo ese conjunto de normas que van a ayudar a que esa gestión de seguridad de la información sea más eficaz. Sin embargo, en donde deberíamos centrar la discusión de la responsabilidad legal del gerente de seguridad de la información es qué casos debe atender de manera puntual y cuál es el objetivo que persigue el gerente de seguridad de la información.

Jeimy J. Cano

¿En qué casos debe responder legalmente el Gerente de Seguridad de la Información? ¿Ante una falla de seguridad? ¿Ante una pérdida de continuidad que impacte a terceros? ¿Cuáles serían los casos?

Walter Pinzón

Siempre que se causa un perjuicio se debe reparar. No basta con que la empresa sufra una pérdida económica por culpa del gerente. Si se le llega a causar un perjuicio a un proveedor o a un cliente y que amerite un detrimento patrimonial para la empresa, es decir que la empresa se vea obligada a responder por la falla de un funcionario, en este caso el gerente de seguridad de la información, debe responder. Pero si se trata de una falla de seguridad o de continuidad que impacte el presupuesto ¿qué sucede? Por lo general, cuando hay pérdidas de información, estas se manejan dentro de la empresa, se hace un acuerdo en el sentido de no llevarlas al Tribunal y se cuida de no informarlas a los medios de comunicación. Y es ahí cuando se debe analizar el tema

del riesgo. El más importante para una organización es el riesgo reputacional que puede hacer desaparecer una compañía de la noche a la mañana. Una empresa que no brinde confianza en sus sistemas no sirve, es imposible confiar en una firma que tiene fugas de información y fallas de tal índole. El otro asunto es el tema operacional, no de pérdida patrimonial, sino de una falla en la operación que más adelante pueda causar un detrimento.

Rafael Gamboa

El asunto vital es la responsabilidad contemplada en la ley. Quien causa un perjuicio, debe responder. Por ejemplo, atropellar a una persona en un accidente de tránsito. En tales casos se trata de un homicidio culposo; es decir, un daño causado sin intención. A la luz de la ley el tema de la intencionalidad es importante porque implica una graduación de la pena, pero el punto que busca defender la ley, es resarcir un perjuicio. Entonces el perjuicio se causa por acción o por omisión, siempre que se cause se va a responder. Un punto bien importante que no se debe perder de vista, es que si un empleado causa un perjuicio frente a las funciones que tiene dentro de la empresa, será la empresa la que deba responder, sin perjuicio de que la compañía pueda perseguir al empleado que causó el daño. La razón de poder perseguir al empleado es que si bien fue la empresa la que causó el perjuicio, este perjuicio fue ocasionado por una persona de carne y hueso y es ella la que deberá en últimas responder. Otro aspecto relevante para mencionar es ¿hasta dónde es prudente llegar? Es decir, ¿hasta dónde voy a tensionar la pita?, ¿hasta dónde puedo llegar?, ¿hasta dónde puedo irme sin caer en lo ilegal?, ¿hasta dónde puedo realizar una actividad técnica, jurídicamente no perfecta, pero impecable? Y ahí viene el tema del riesgo que mencionaba Walter. Riesgo que digamos se materializó en lo que sucedió con EnroN. Esta empresa hace un par de años -y de hecho fue casi el detonante en todo este tema de riesgo corporativo-, tensionó mucho la pita y se reventó con todas las consecuencias conocidas, de donde surgió el tema de la creación de un gobierno corporativo, de un manual de buenas prácticas. Para resumir, el

En opinión de los asistentes al foro, el riesgo reputacional es muy importante para una organización, porque la puede hacer desaparecer de la noche a la mañana.

gerente de seguridad de la información debe responder siempre que se cause un perjuicio.

Walter Pinzón

Debe responder cuando se genere una pérdida, para la empresa, para terceros, etc. ¿Cuáles serían los casos en relación con el Gerente de Seguridad de la Información? Yo tengo un caso debido a fuga de información. Más que fuga se trata del uso indebido que puede hacer el gerente de seguridad de la información. Todas las áreas de una empresa son muy importantes, pero la que administra la tecnología, la que tiene el cerebro informático y procesa los datos, lo es más. Y para el custodio de esos datos, de esa información, la responsabilidad es mayor. Del uso indebido que se pueda dar de esa información se puede acarrear una responsabilidad penal. No solamente frente al perjuicio económico, va contra su libertad. Eso está previsto en las normas penales. Pongo otro caso sobre falla en controles. Si fallan los controles por descuido o falta de diligencia de este administrador y se perjudica a la empresa, a los clientes o a un tercero, responde. Un caso de conflicto de interés: en donde se quiera privilegiar intereses personales frente a los intereses de la empresa; por ejemplo, aprovechando este gerente el conocimiento que ha adquirido de la empresa en la cual labora para constituir su propia compañía: a primera vista esto no presenta nada que implique actividad ilegal o falta de ética, el punto es que se apropie para sí de información privilegiada, confidencial o de secretos industriales y luego los utilice en su propia empresa.

Jeimy J. Cano

Por ejemplo, en el caso de tener un documento privado almacenado en una memoria USB, que puede empezar a circular una vez yo conecte ese dispositivo a un computador, puede comprometer la confidencialidad del mismo.

Juan Carlos Reyes

Se trata de un claro ejemplo de detrimento patrimonial, frente al cual el empleado debe responder. Pero así mismo, la empresa tiene que pensar en proteger a sus gerentes de seguridad de la información. Que no solo se trate de las obligaciones contractuales, sino del cumplimiento de esos modelos de seguridad que se definen dentro de la organización y que a pesar de no tener vigencia legal o jurídica, sí se convierten en normas o "leyes" que deben cumplirse al interior de la organización. Unas políticas estándar que se deben respetar y cumplir, las cuales forman parte de la función del gerente de seguridad de la información. Un comentario adicional tiene que ver con la posibilidad de que el cargo de la gerencia de seguridad de información nunca llegue a existir. Hoy en día existen los oficiales de seguridad de la información en ciertos casos específicos, pero la tendencia es que se conforme un área de seguridad en las diferentes compañías que involucra seguridad

física, ambiental, industrial y de la información. De esa manera tenemos que ver es que el gerente de seguridad de la información se convierte en una persona con un nivel de importancia tal como el gerente de seguridad física. El gerente de seguridad física es el responsable de que nadie se le salte el muro, de que nadie se lleve una cámara o cosas así por el estilo. En el plano informático, de que haya algún incidente similar relacionado con la información; lo mismo es la responsabilidad del gerente de seguridad de la información en su ámbito.

Jeimy J. Cano

Si se quiere redactar un Código de buenas prácticas de responsabilidad legal para la gerencia de seguridad de la información ¿cuáles puntos o temas clave debería contener?

María Conchita Jaimes
Directora Ejecutiva RAS
Ernst & Young

Las responsabilidades de la gerencia de seguridad de la información deben ser dictaminadas por la alta gerencia de la compañía con base en los requerimientos de protección de su negocio frente a riesgos de seguridad de la información. La gerencia de seguridad es un facilitador que debe ayudar a los directivos de la empresa en el cumplimiento de todas las políticas sobre la seguridad de la información. En tal sentido, la responsabilidad de la gerencia de seguridad debe estar dada hasta velar por el cumplimiento de esa normativa establecida y solo debe existir sanción cuando se omiten algunas de las actividades contempladas e impuestas por la compañía.

Walter Pinzón

Uno de los aspectos relevantes en temas de prácticas de Buen Gobierno, es el relacionado con el control y el manejo de la información: qué se genera, quién la genera, cómo se administra, a quién se entrega, cómo se entrega. En fin, es necesario establecer en un capítulo, las políticas y herramientas concernientes a efectuar una adecuada gestión de riesgos sobre la información de la compañía. Debe contener un capítulo dedicado al tema de conflicto de interés que prevea y prevenga eventos tan comunes como que por ejemplo las personas al frente del área de información, aceptan invitaciones de los grandes proveedores de tecnología a nivel mundial, con todos los gastos pagos a diferentes países. Otros temas que deben ser considerados la autorregulación y un apéndice de casos para

ilustrar buenas prácticas. Es decir, el Código debe contemplar aspectos de ética, integridad y conducta.

Rafael Gamboa

Es necesario redactar un Código de buenas prácticas de responsabilidad legal para evitar un proceso judicial o en caso de llegar a él, disponer de los mejores argumentos. Un instrumento que contemple lineamientos muy precisos sobre las responsabilidades y la manera de actuar del gerente de seguridad de la información. Dicho Código no podrá ser el mismo para todas las áreas de una empresa, debe ser hecho a la medida de la actividad realizada, es decir, debe contemplar un objeto específico. Así mismo, debe ser un Código vivo, activo, de actualización, de preferencia; algo así como una bitácora que contenga todas las modificaciones de que ha sido objeto y el por qué de ellas. El gerente de seguridad de la información deberá documentar y sustentar muy bien sus argumentos a la hora de responder por sus acciones, basado en los términos del Código previamente establecido. Dicho trabajo debe hacerse en conjunto con las áreas jurídica, de seguridad y de tecnología, con el propósito de documentar procedimientos, formas de funcionamiento y acordar que la mejor defensa dentro de un eventual proceso judicial, se da solo en la medida en que el Código tenga altos estándares en aspectos jurídicos, tecnológicos y gerenciales; se podrá tener un Código "fuerte", ya que existe un principio legal que nadie está obligado a lo imposible y esta imposibilidad se refleja en exigencias que sobrepasan buenos estándares de cuando ocurre el incidente.

Juan Carlos Reyes

Estoy de cuerdo con la necesidad de un Código de conducta, un Código que rija de alguna manera a los gerentes de seguridad; sin embargo, para que eso sea viable hay que partir de lo que es la esencia de la seguridad de la información y vuelvo otra vez al escenario un poco tecnológico. ¿Por qué la esencia? Porque si vemos las estrategias de la seguridad de la información implican primero mucho trabajo y segundo mucha inversión. Y ¿cuál ha sido la solución para poder priorizar o para poder enfocar de una manera inteligente ese esfuerzo y esa inversión que hay que hacer en seguridad? Trabajar en temas como el famoso análisis de riesgos, la clasificación de la información, la respuesta a los incidentes y los planes de continuidad. Esos son cuatro puntos específicos de la norma ISO 27001, que por ejemplo en el caso de la clasificación de información lo que se busca es que se establezcan controles y se invierta ese esfuerzo y ese dinero en proteger la información que realmente es confidencial. Es importantísimo disponer de un Código de conducta para el gerente de seguridad de la información, totalmente alineado con lo que ha sido el verdadero riesgo en seguridad que presenta la empresa. De hecho me atrevería a decir que el Código de conducta termina siendo

casi un control en respuesta al análisis del riesgo (del riesgo que representa el gerente como activo de información). Parte del tratamiento de ese riesgo que se identifique sobre el gerente de seguridad de la información. ¿Por qué? Porque el gerente en sí mismo es un riesgo. Así como uno siempre dice el administrador de la plataforma o del servidor o lo que sea es la persona que tiene el acceso y es la principal sospechosa en el caso de un eventual fraude o algo así por el estilo, pues el gerente de seguridad también tiene mucho poder en sus manos y eso es parte de lo que se debe tener en cuenta dentro del análisis de riesgos. Entonces esta persona es muy poderosa y que como tal debe ser, debe atenerse a ciertas prácticas y a ciertos Códigos de acuerdo a su función.

Jeimy J. Cano

El tema de la gerencia de seguridad de la información es un asunto espinoso y tiene que ver de manera directa con la confianza. El problema es pasar de los controles tecnológicos a la confianza corporativa. Es decir, las métricas de seguridad no debe estar fundamentadas en un estándar como el ISO 27002, en la medida en que dicho estándar detalla una serie de controles para la operación de la seguridad, pero no construir lo que finalmente busca la alta gerencia: confiabilidad de sus operaciones. Esta solo es una plataforma básica para operar la seguridad, pero que no

El problema es pasar de los controles tecnológicos a la confianza corporativa , enfatizaron Walter Pinzón, Rafael Gamboa y Juan Carlos Reyes.

contempla claramente el tema de la confianza. Aspecto que hemos pasado por alto. En este sentido, una compañía contrata una persona con ciertas características y competencias, ciertos recursos y habilidades para que brinde una seguridad mínima, considerando que el riesgo cero no existe. Tarde o temprano se registrará algún incidente, cuyo tamaño dependerá de la calidad de la gestión.

María Conchita Jaimes

La alta gerencia es la que dice hasta dónde el gerente de seguridad de la información asume el riesgo y dentro de ese contexto, debe elegir los sistemas más apropiados para controlar el manejo de la información en aras de atender interrogantes tales como: qué asuntos atiende, qué transfiere, hasta dónde va su responsabilidad, qué no cubre, cuáles seguros debe contratar, qué debe transferir, a quién le debe transferir el riesgo y cómo lo debe manejar, entre otros. Con relación al Código de buenas prácticas de responsabilidad legal estoy de acuerdo en que se requiere establecer los parámetros que regulen la responsabilidad. Pero ese Código en las compañías no lo hay, no existe. Existen políticas de seguridad pero en la mayoría de los casos no se aplican o no están respaldadas por sanciones que obliguen al cumplimiento. ¿Cómo hacer para que todo el esquema de seguridad montado en la organización funcione? La respuesta es el establecimiento de un gobierno de seguridad de la información que imparta directrices y las haga cumplir.

Jeimy J. Cano

Estados Unidos y Europa han adoptado una posición un poco diferente frente al tema de cumplimiento. El trato relacionado con la sanción es claro, sin embargo se abre una posibilidad diferente que busca establecer niveles de cumplimiento. Si la organización cumple, por ejemplo, con el 80% de lo establecido en la regulación, recibe un reconocimiento público, pero si está por debajo de ese porcentaje en términos de cumplimiento, se toman las respectivas acciones, junto con las observaciones y ajustes. Lo que se busca con la medida es incentivar los niveles de cumplimiento de las normas, por reto y desafío, y no por sanción y multas.

María Conchita Jaimes

Con relación al riesgo ¿por dónde se empieza a manejar la información? Es necesario hacer un análisis de riesgos, como principio, esencia y corazón de cualquier sistema de seguridad. A partir de ese estudio, la compañía debe decidir de los riesgos contemplados cuántos cubre y cuántos no. Y sobre los que decidió cubrir, establecer que tipo de controles va a utilizar para minimizar los riesgos prioritarios; definir en dónde va a actuar con base en otros sistemas adicionales. De esa forma, el gerente de seguridad de la información velará por un esquema preestablecido

por la empresa. Eso no quiere decir que la gerencia de seguridad no tenga la responsabilidad de estar actualizado en los todos los riesgos relacionados con el sistema de seguridad de la información. Y ese entorno se debe construir porque la gerencia de seguridad es el motor principal para establecer el sistema de gestión de la seguridad de la información.

Walter Pinzón

Todo lo que se refiera a políticas de seguridad informática no debe quedar en letra muerta y ese mismo Código debe prever un tema de medidas disciplinarias, como llamada de atención, suspensión, sanción, hasta llegar a otras instancias, inclusive de carácter penal. En esa medida, debe quedar clara que la responsabilidad que puede llegar incluso hasta la privación de la libertad.

Jeimy J. Cano

¿Cómo ven ustedes la evolución de la responsabilidad legal de los Gerentes de Seguridad Informática? ¿Hacia qué debemos estar preparados?

Juan Carlos Reyes

Hay que partir del análisis del riesgo para poder establecer esa responsabilidad legal. Es necesario adelantar una serie de procesos metodológicos, no necesariamente ISO 27001, sino muchas otras formas, para saber cómo debe funcionar la responsabilidad legal, la cual debe trascender de la misma manera como esta opera para cualquier vicepresidente de una compañía. Estamos acostumbrados a que la seguridad de la información es un tema de carácter tecnológico, cuando las dificultades a las que se pueden ver enfrentados los directivos de una organización pueden residir en una mala gestión de la gerencia de seguridad de la información. Así se debe enfocar la responsabilidad de este gerente, en la medida en que es la persona que tiene el negocio de una forma más completa en sus manos.

Rafael Gamboa

El tema disciplinario es optativo para la empresa, en la medida en que puede acudir a otras instancias de carácter civil, penal, procesal o de la jurisdicción propiamente dicha. En cuanto a la responsabilidad, cada vez es más creciente, toda vez que el uso de los medios electrónicos se populariza más y más y la información se conserva en ellos. El gerente de seguridad de la información ya no actúa en una república independiente del conocimiento, su función es más amplia y más conocida. Su labor está mucho más vigilada y no tiene la misma autonomía de otras épocas, cuando la tecnología era ajena a las áreas de la organización diferentes a la suya. Hoy en día el gerente de seguridad de la información será el equivalente a un vicepresidente comercial o de medios, como parte integrante de una gran cadena dentro de la empresa. Por otra parte, el gerente de seguridad de la información debe estar vigilado, toda vez que el enemigo más peligroso para cualquier empresa está en su interior. Y en

su caso, nadie conoce mejor el negocio. En resumen, el gerente de seguridad de la información tendrá una función más relevante, será un eslabón de vital importancia dentro de cualquier compañía.

Walter Pinzón

Este administrador debe prepararse para asumir la misma responsabilidad que tiene un miembro de primer nivel de la empresa. Debe ser consciente de que sus actos u omisiones lo pueden llevar a responder en determinados casos, no solo de manera económica; eventualmente, podría estar respondiendo de manera administrativa (ser vetado para trabajar en el sector); comercial (que le impongan multas); civil (que le instauren demandas para reparación de perjuicios); y, hasta penal (le instauren denuncias en su contra)

María Conchita Jaimes

La evolución de la responsabilidad legal de los gerentes de seguridad informática se basa en si se trata de gestión u operación. Hoy en día las compañías tienen la tendencia a asegurar la información en una forma más operativa que en términos de gerencia. Creen que disponer de una infraestructura tecnológica garantiza el no acceso a la información y a los controles del sistema y asimilan las funciones de su protección a las tareas operativas del jefe de seguridad. En la medida en que la seguridad tenga una función de gestión, es decir, de coadministración, el gerente de la información va a tener que responder por temas legales. Se trata entonces de que las compañías adquieran conciencia sobre la vulnerabilidad de la información y su vital importancia dentro del negocio, para que le den más importancia al cargo de seguridad de la información y regulen en forma clara el cumplimiento de las funciones inherentes a esa posición.

Sara Gallardo

¿Desde cuándo se habla de gerencia de seguridad de la información? ¿Ese gerente es la misma persona que dirige el área de informática dentro de una empresa?

Jeimy J. Cano

Con base en los resultados de la encuesta anual de ACIS sobre el tema de seguridad de la información podemos concluir que en el año 2000 no se manifestaba con claridad la figura de la gerencia de seguridad de la información, función que se identificaba como propia del área de tecnología, agobiada con todo tipo de funciones y luchando por tener recursos propios. Dos o tres años más tarde -2003- surge la necesidad de nombrar un gerente de seguridad de la información, diferente a la persona responsable del tema de tecnología. No obstante, todavía no existe una marcada diferencia. El estudio realizado por la Asociación Colombiana de Ingenieros de Sistemas (ACIS) muestra solo un ligero aumento en el uso y nombramiento de personas en dicho cargo.