Julio 20 - 2019

Seguridad de la información, *una medida que debe ser adoptada por las empresas en el ambiente actual de la Hiper - conectividad hostil.*

Oscar R. Sierra Bautista.

Oscar.sierra01@est.uexternado.edu.co

Universidad Externado de Colombia - Facultad de Contaduría – Especialización en Administración de riesgos Informáticos.

***Resumen*:** Este articulo presenta una corta reseña de la evolución de la información y explica él crecimiento tecnológico actual que no da otra opción más que estar hiper - conectados a los sistemas informáticos y esto hace necesario que el modelo de implementación de un sistema de gestión sea parte de la estrategia empresarial para el cumplimiento normativo vigente, y para lograr una mitigación de riesgos aceptable sin dejar a un lado la necesidad y el énfasis de generar una cultura de seguridad que no vaya en contravía de la productividad empresarial.

Palabras Clave: Seguridad de la información, estrategia empresarial, riesgos, seguridad informática.

Information security, *a measure that must be adopted by companies in the current environment of hostile Hyper connectivity.*

Abstract: This article presents a short review of the evolution of information security and explains the current technological growth that gives no choice but to be hyper-connected to computer systems and this makes it necessary that the implementation model of a management system is part of the business strategy for regulatory compliance, and to achieve acceptable risk mitigation without leaving aside the need and emphasis on generating a security culture that does not run counter to business productivity.

Keywords: Information security, business strategy, risks, computer security.

Introducción.

En la antigüedad el manejo de la información se realizaba de formas mas simples, pero con mayores riesgos de perdida; la información importante y/o confidencial se guardaba en libros bajo llave o en un archivo al que solo tenían acceso ciertas personas que tenían las llaves y de alguna u otra manera llevaría un registro en papel de los ingresos y consultas o modificaciones realizadas a los documentos confidenciales. De esta manera menos personas tenían conocimiento de la ubicación de la información, sin embargo, una vez descubierto era fácil su acceso por los pocos controles de seguridad.

Por un momento vale la pena ir al pasado y recordar cuando la televisión era uno de los medios "sino el más" avanzado tecnológicamente, las conversaciones se realizaban a través de sistemas análogos con puntos de conexión cableada a largas distancia, y el trabajo de oficina estaba totalmente conformado por documentos físicos, libros, formatos, cartas, manuales, informes etc. Lo que hacía las zonas de archivo en las empresas de gran extensión.

Con el pasar del tiempo fueron apareciendo los sistemas informáticos que ayudaban a realizar algunas tareas básicas, reduciendo los tiempos de las tareas repetitivas, con nuevas funciones para llevar un registro digital de los datos de las empresas, como inventarios, facturas, clientes, y demás información importante para el registro y control de la operación. De esta manera las empresas mismas fueron demandando mas y nuevas funcionalidades a los sistemas que se tenían en aquel entonces, y en un par de décadas se comenzaron a distribuir sistemas informáticos de manera masiva, al punto de llegar al hogar para realizar labores generales de las familias en el procesamiento de información y con la intención de proveer una conexión a una red mundial de información, el ahora llamado "servicio de Internet". Hoy en día es el medio utilizado por todos para realizar tareas de consulta, registro en sitios, enviar mensajes, subir información, realizar compras y comunicarnos con otras personas, empresas, culturas y países.

Con base en lo anterior y a la demanda actual que el mismo uso de las comunicaciones genera por los usuarios y/o empresas se está generando una revolución tecnológica, que algunos autores como ***(Claus SchWab.2016)*** le han llamado "La *cuarta Revolución Industrial*".

Esta revolución se genera por la dependencia actual de las máquinas y de los seres humanos a estar permanente conectados a los sistemas de información como el correo electrónico, las redes sociales, plataformas de chat y de intercambio de archivos lo que en resumen se puede llamar "**hiper – conectividad**" que obliga a todas las personas a estar conectadas para interactuar con otras de manera personal o profesional sin dejar opción alguna, lo que se puede considerar como un método **"Hostil".**

Todas estas plataformas y sistemas guardan información de los usuarios, y registros de cada acción y movimiento que se realiza en sus sistemas, así que dicho esto puede preguntarse *¿Qué información tienen estas plataformas?*

Toda la información que los usuarios han utilizado para registro, como números de cedula, teléfono, dirección y otra información personal en las redes sociales como amigos, familia, fotos y videos son

almacenadas en los sistemas informáticos de estas plataformas sin contar la información básica que ya reposa en las bases de datos de las entidades gubernamentales.

Ahora con el entendido de lo que sucede con la revolución actual tecnológica, se debe incluir un elemento muy importante y es la seguridad de la información que ha venido preocupando a las empresas debido a las cifras de los casos de ataques informáticos, ejecutados para el robo, daño de información y para el espionaje a nivel mundial. Todo esto converge en el gran valor que tiene el poder de tener la información, no solamente con la finalidad de llevar a cabo delitos informáticos con los datos de tarjetas de crédito, patentes, formulas de productos, estrategias de empresas y su información confidencial de negocio si no a otro nivel llamado **"Ciberguerra"** y este termino se puede entender fácilmente analizando que esta revolución tecnológica cambiará a futuro el armamento militar, por los ataques informáticos, de empresas, de unos estados con otros, etc., con la intención de desestabilizar su economía, sus sistemas de alimentación eléctrica, materia prima, hospitalaria y demás acciones que puedan producir Caos.

"La Estrategia cibernética busca generar poderosas armas que permitan de ser necesario una ofensiva y agredir a los enemigos causando los mayores daños, a mayores daños mayores beneficios" (Marin, Nieto, Huertas, & Montenegro, 2018, pág. 254).

El momento actual de la información y la tecnología marca la necesidad de urgencia de aplicar métodos y normas de seguridad que permitan controlar los delitos informáticos y a su vez mantener el buen tratamiento de la información. "Un marco de seguridad de la información es una serie de procesos documentados que a menudo se personalizan para resolver problemas específicos de seguridad de la información" (Cárdenas Solano, Martínez Ardila, & Becerra Ardila, 2016, pág. 937).

La Información Personal.

Ahora bien, no solo basta con implementar un marco de seguridad de la información en las empresas y tomar normas de referencia aplicadas a esta necesidad como ISO/IEC 27000 y su familia o NIST, para mantener la integridad, confidencialidad y disponibilidad de la información; se debe crear una cultura de seguridad de la información, que haga parte de la conciencia de las personas en el manejo de la información corporativa y en el manejo de la información personal.

"Los usuarios de las redes sociales aceptan invitaciones de otros usuarios que no conocen en el mundo real" (Cortes Martinez, y otros, 2016, pág. 120), la época actual mantiene al ser humano con la necesidad constante de estar conectado a la Internet y las nuevas generaciones quieren compartir momentos de la vida y sus emociones en los medios digitales para buscar el aprecio y la aprobación de quienes pueden ver su información. De esta manera se vuelve más común el análisis de los comportamientos de las personas, las tendencias y dentro de esto, los riesgos de suplantación de identidad, robo de información, extorsión y grooming. Ahora es normal preguntarse *¿Con quién comparto mi información?*

"Los administradores de las plataformas (Redes Sociales) no tienen información sobre los antecedentes criminales. Como resultado los delincuentes pueden tener acceso a la información

personal de los usuarios" (Cortes Martinez, y otros, 2016, pág. 124), Hay que tener en cuenta que para ingresar a la red social es necesario registrarse y esto no garantiza que otras personas registradas no sean delincuentes, por lo que se hace importante tener sumo cuidado con la información que se sube a estas plataformas y los permisos y controles aplicados para el público que pueda ver el contenido.

La Información Corporativa.

La protección de la información corporativa debe estar enmarcada en un sistema de gestión de seguridad de la información (SGSI) el cual se implementa bajo normas creadas para este fin, de las cuales se resalta ISO/IEC 27000 que describe de manera completa los lineamientos de auditoría y control del (SGSI) para empresas.

Es importante tener en cuenta que un sistema de seguridad de la información no es únicamente los controles tecnológicos que se puedan implementar para mitigar los riesgos. "Hay que considerar que la protección de la seguridad de la información a través de sus políticas no se lleva únicamente por medio de una perspectiva tecnológica, es necesario tener una visión amplia a través de un enfoque interdisciplinario donde el factor humano juega un papel fundamental" (Altamirano Yupanqui & Bayona Oré, 2017, pág. 113).

Implementación del Sistema de Seguridad de la Información (SGSI).

El primer paso para la implementación de un (SGSI) es aceptar que existen riesgos potenciales que pueden vulnerar la información de la empresa y de los clientes, y esta conciencia no debe estar únicamente en los departamentos de tecnologías de la información (TI), sino que debe descender desde de la alta dirección y permear a las demás áreas de los riesgos que se pueden presentar.

Un aspecto muy importante que complementa la idea anterior es que a menudo se cree que un proyecto de (SGSI) es un proyecto únicamente de las áreas de TI. "El proyecto (SGSI) es de toda la organización y como tal requiere la aprobación y el apoyo de la dirección para avanzar en su adecuada implementación" (Valencia Duque & Orozco Alzate, 2017, pág. 77). De esta forma también hay que lograr que la organización incluya los temas de seguridad de la información en su estrategia empresarial de tal manera que los controles y la cultura que se fomente no actúe en contra de la productividad del negocio, pero que si mantenga las buenas prácticas y lineamientos que demande el SGSI para mitigar los riesgos y la incertidumbre ante cualquier evento.

"En el momento de formular una estrategia empresarial se debe tomar en consideración, la gran cantidad de variables que inciden en la evolución de la empresa, y por tanto se debe dar lugar a acciones que permitan "Navegar" entre toda la turbulencia e incertidumbre que rodea la organización empresarial" (Martínez Moncaleano, 2018, pág. 210).

Una vez que la dirección empresarial este de acuerdo con el SGSI es necesario identificar los activos de información que son importantes para la operación de la empresa, estos pueden ser equipos tecnológicos, aplicativos como también y de manera muy importante los documentos que por su clasificación deben tener un tratamiento de riesgo especial.

El archivo general de la nación *(Colombia)* generó una guía para la clasificación de la información y en apoyo a los procesos de gestión documental y a lo establecido en la ley 1712/2014, su decreto reglamentario 103/2015 y normas relacionadas. Esto ayuda a tener una idea clara de la manera en la que se debe tener una clasificación de la información de acuerdo con su confidencialidad para realizar una mejor gestión del riesgo.

"Una vez identificados los riesgos y sus impactos sobre los activos de información relevante para la empresa es necesario identificar o diseñar las medidas de mitigación de estos y asegurar la efectividad" (Camacho Morales, Cano Martínez, Neira Rueda, Ovalle Leguizamón, & Villamil Salazar, 2013, pág. 153).

(Valencia Duque & Orozco Alzate, 2017, pág. 78) afirman los siguientes pasos para el establecimiento de las prioridades de la organización para desarrollar un SGSI:

1. Obtener la aprobación de la dirección para iniciar el proyecto.
2. Definir el alcance, los límites y la política.
3. Realizar el análisis de los requisitos de seguridad.
4. Realizar la valoración de Riesgos y planificar su tratamiento.
5. Diseñar el SGSI.

Para complementar la afirmación de las prioridades se debe tener en cuenta que es necesario fomentar una cultura organizacional de seguridad de la información y una cultura en los individuos donde cada uno se vea como custodio de sus datos y, por tanto, responsable por su adecuado tratamiento. (Camacho Morales, Cano Martínez, Neira Rueda, Ovalle Leguizamón, & Villamil Salazar, 2013).

El ser humano es el eslabón más débil en los procesos de seguridad de la información por esta razón los nuevos ataques informáticos y de ingenia social van enfocados a su comportamiento, por esto la importancia de hacer el énfasis correcto en las estrategias de sensibilización que promueva una cultura. "Las organizaciones independientemente de su naturaleza están sometidas a constantes cambios, incertidumbres y la manera de enfrentar estas situaciones será el reflejo de los valores, creencias y normas existentes en su cultura, de allí la importancia de cómo se administre" (Londoño Vargas, 2013, pág. 13).

Por ultimo y no menos importante dentro del diseño del SGSI es la inclusión de los temas normativos vigentes (legales) que apliquen al manejo de la información *Ej. Habeas Data.* Y en los cuales es definitiva la comunicación con el área jurídica de la empresa quien se encargará de que el diseño cumpla con las leyes vigentes frente a las auditorias y a la materialización de los riesgos de cualquier activo de información.

Conclusión.

Actualmente las actividades diarias de los seres humanos obligan de una u otra manera a estar conectados a los sistemas de información públicos y/o privados sin dejar ninguna opción diferente a la de tomar conciencia de la revolución tecnológica de hiper – conectividad hostil, que advierte la necesidad de adoptar sistemas de gestión de seguridad de la información para lograr mitigar los riesgos, y dar cumplimiento a las leyes vigentes, todo enmarcado en la necesidad de mantener una cultura de seguridad.

Referencias.

Abril, A., Pulido, J., & Bohada, J. A. (2013). Análisis de Riesgos En Seguridad De La Información. *Revista Ciencia, Innovación y Tecnología*, 39 - 53.

Altamirano Yupanqui, J. R., & Bayona Oré, S. (2017). Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Expplican su Cumplimiento. *Revista Ibérica de Sistemas y Tecnologías de Información.*, 112 - 133.

Camacho Morales, J. P., Cano Martínez, J. J., Neira Rueda, M. G., Ovalle Leguizamón, V. C., & Villamil Salazar, M. P. (2013). La Información Reservada en el ordenamiento juridico Colombiano: Reflexiones Práctica e Implicaciones para el Derecho Disciplinario. *Revista Derecho Penal y Criminología*, 145 - 185.

Cárdenas Solano, L. J., Martínez Ardila, H., & Becerra Ardila, L. E. (Noviembre de 2016). Gestión de Seguridad de la Información: Revisión Bibliográfica. *El profesional de la información*, 931-948.

Cortes Martinez, F. R., Herrera Candelaria, A. D., Ramírez Lozano, M. A., Rodriguez Zuñiga, A. R., Martínez Peláez, R., & Parra Michel, J. R. (2016). Después de presionar el botón enviar, se pierde el control sobre la información personal y la privacidad: un caso de estudio en México. *Revista Ibérica de Sistemas y Tecnologías de Información.*, 115 - 128.

Londoño Vargas, K. S. (2013). *Estrategias de Sensibilización que Promueva una CUltura Organizacional de Calidad.* Obtenido de Universidad Militar Nueva Granada: https://repository.unimilitar.edu.co/bitstream/handle/10654/10874/Londo%F1oKatherinStefanie2013.pdf;jsessionid=692E4F07002D7C189007BE9AA179D967?sequence=1

Marin, J., Nieto, Y., Huertas, F., & Montenegro, C. (2018). Modelo Ontológico de los Ciberdelitos : Caso de estudio Colombia. *Revista Ibérica de Sistemas y Tecnologías de Información.*, 244 - 257.

Martínez Moncaleano, C. J. (2018). Teoria del Caos y Estrategia Empresarial. *Revista de la Facultad de Ciencias Ecónomicas y Administrativas. Universidad de Nariño.*, 204 - 2014.

Valencia Duque, F. J., & Orozco Alzate, M. (2017). Metodología para la implementación de un sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *Revista Ibérica de Sistemas y Tecnologías de Información.*, 73 - 88.

Velasco Melo, A. H. (2008). El Derecho Informático y La Gestión De La Seguridad De La Información, Una Perspectva Con Base En La Norma ISO 27001. *Revista de Derecho*, 333 - 366.