Artículo de Revisión / Review Paper

El teletrabajo y la seguridad de la información empresarial

Teleworking and security of business information

J. J. Chaverra Mojica[1], H. de J. Restrepo Vélez[2], J. F. Pérez García[2]

Recibido: 15 de abril de 2015

Aceptado:4 de junio de 2015

Resumen

El presente artículo, pretende abordar los retos a los que se enfrentan los equipos de seguridad de la información en las empresas que han adoptado la modalidad de teletrabajo, y describir los problemas y oportunidades del medio actual, teniendo como guía la normatividad vigente y las buenas prácticas sugeridas en las metodologías que abordan el teletrabajo y lo formulan como alternativa de modernización en las empresas y de bienestar para el empleado, y además, posibilitan la implementación de políticas en materia de seguridad de la información, enfatizando la importancia de esta dentro de la sociedad actual y de la economía del conocimiento.

Palabras clave: teletrabajo, información empresarial, seguridad de la información.

Abstract

This article aims to address the challenges that face the information security teams in the enterprises that has adopted the teleworking, and describe the problems that are taken in the current environment, taking as a guide the current regulations and the good practices

1 MsC en Ingeniería de Sistemas,Tecnológico de Antioquia-Institución Universitaria. jjchaverra@tdea.edu.co.

2 Especialización en Seguridad de la Información. Tecnológico de Antioquia.

suggested in the methodologies that deals with teleworking and formulate it alternately to the modernization in the enterprises and employee welfare, and furthermore, enable the implementation of policies on information security, emphasizing the importance of this in today's society and the knowledge economy.

Keywords: teleworking, business information, information security.

1. Introducción

La seguridad de la información hace parte de las actividades específicas que se necesitan en las organizaciones para poder garantizar la continuidad del negocio, la privacidad y el uso indebido de los activos de información, los riesgos y las amenazas son de todo tipo y se materializan siempre que no se tienen los controles necesarios para evitarlos. En algunas organizaciones existen controles físicos y acuerdos legales tanto internos como externos, gestión de riesgos, inventario de activos, seguridad en páginas web. Todas estas políticas de seguridad, se deben aplicar de igual manera a la modalidad del teletrabajo, teniendo en cuenta que se incrementan los riesgos dadas las condiciones de movilidad y lejanía de la empresa.

Este artículo pretende realizar un análisis de la situación actual del teletrabajo en Colombia y algunas empresas locales, basado en un estudio detallado de las técnicas de protección de datos y las políticas más implementadas en términos de seguridad de la información, sustentadas en documentación indexada y fuentes confiables, además de las experiencias en el campo y con la participación en procesos similares que permiten la observación y conocimiento de las herramientas utilizadas en el teletrabajo. Se hablará tanto de los riesgos, como de las actividades más efectivas de mitigación en materia de aseguramiento de la información de las empresas que han adoptado y han sido pioneras de dicha modalidad y que por ende poseen fallas en su sistema de gestión de riesgos de la seguridad de la información o no lo han establecido en su totalidad.

2. Descripción del problema

El teletrabajo es una modalidad de trabajo empresarial, donde los empleados desempeñan sus labores en casi su totalidad por fuera de las instalaciones de la empresa, valiéndose de las nuevas tecnologías que le permiten desempeñarse en un ambiente virtual similar al de su empresa, sin desplaza-

mientos de largas distancias, con versatilidad en el uso de las tecnologías, y el aprovechamiento de los recursos disponibles para no dejar de ser productivo y continuar con el crecimiento personal y de la empresa. Si se interpretan los términos de modernización, avance tecnológico, evolución laboral, sostenible, amigable con el ambiente, podemos asociarlos todos con el teletrabajo y encontramos que estos son los beneficios principales que reciben las empresas que adoptan esta modalidad, además de los rendimientos económicos para la empresa, el bienestar laboral para los empleados y el bien manifiesto que recibe el entorno aledaño.

El trabajo desde casa o cualquier otro lugar ajeno a las instalaciones de la empresa, tiene como componente primordial el uso de las *TIC's* (tecnologías de la información y las comunicaciones) cuyo uso es primordial en las empresas y la sociedad actual. La habilidad de acceder, adaptar y crear nuevo conocimiento usando las TIC's es crucial para la inclusión social hoy en día [1]. Las redes y el internet de banda ancha con gran capacidad de transmisión de datos y video, el software de conexión remota a escritorios virtuales, entre otras, ha provisto de muchas ventajas en la implementación del teletrabajo en las empresas, sin embargo, existen barreras y retos para llevar a cabo esta actividad de una forma segura, sin que se presenten percances que afecten el desempeño particular del empleado y la disponibilidad de la información. La posibilidad de verse en situaciones inseguras o que potencializan los riesgos de pérdida de la información se incrementan en la práctica del teletrabajo.

Con la salida del trabajador de su entorno físico, salen documentos de la organización que pueden ser confidenciales y a los cuales es más difícil proteger [2]. Dado el uso de conexiones remotas por parte de empleados y organizaciones, como el envío de información a través de internet o el tratamiento de alguna información sensible en un servidor, la importancia de la seguridad en cada punto de entrada y de destino aumenta sustancialmente. Por esto se evidencia la necesidad de establecer unas reglas que permitan un funcionamiento seguro y confiable del teletrabajo [3].

La información constituye un bien intangible de la empresa, da un valor agregado a la capacidad competitiva de la empresa mediante la detección de oportunidades de negocio [4] y por ende su protección debe ser una de las actividades primordiales en cada proceso que se lleve a cabo dentro de la empresa y esta debe ser objeto de un estudio de riesgos detallado. "La socie-

dad actual está inmersa en una revolución que centra su poder en función de la posesión y la capacidad de uso de la información disponible" [5].

3. El teletrabajo en Colombia

En Colombia las empresas que tienen políticas enfocadas hacia el teletrabajo en su mayoría pertenecen al sector TIC (Tecnologías de la información y la comunicación), Tales como UNE, ETB, CISCO, Citrix, Huawei, Telefónica, IBM entre otras, en su mayoría multinacionales. Otras del sector de gobierno incluyen e impulsan en su plan de mejoramiento y modernización esta modalidad. Las pruebas piloto permiten obtener unas experiencias para facilitar alcanzar una meta establecidas de número de personas vinculadas al teletrabajo.

Colombia ha sido hasta ahora uno de los pocos países que a nivel mundial ha reglamentado el teletrabajo mediante la ley 1221 DE 2008, la cual en su artículo tercero define la política pública de fomento para el teletrabajo, en la cual para el cumplimiento de esta ley se designan a diferentes Ministerios y a otras entidades fundamentales para este proceso como lo son el SENA y la DIAN que ayudaran a su desarrollo y acompañamiento. En el fomento del teletrabajo se deben tener en cuenta los siguientes componentes: Infraestructura de telecomunicaciones. (Mejores Prácticas de seguridad informática), acceso a equipos de computación, aplicaciones y contenidos, divulgación y mercadeo, capacitación, incentivos, evaluación permanente y formulación de correctivos cuando su desarrollo lo requiera. Es de anotar que en esta ley se establecen las normas y disposiciones con las que se promueve y reglamenta esta modalidad de trabajo, las cual deben tener muy en cuenta las empresas u organizaciones que quieran implementarla [6].

4. La normatividad.

Con el uso creciente de las telecomunicaciones en las empresas, es también creciente la actividad de fraudes, robo de información en la red y la increíble creatividad de estos ataques: la protección de la información supedita un reto inmenso en materia de colaboración tanto gubernamental como del sector privado, las leyes se deben aplicar con mayor rigor. Sin embargo, la defensa es muy difícil debido a la globalización de los sistemas de informa-

ción, y por ende, la dificultad radica en la diferencia en la legislación mundial acerca de la "*actividad hacker*"; termino necesario para describir un sin número de riesgos y vulnerabilidades existentes en la red mundial y la explotación de los mismos, por parte de individuos o de sistemas. La información, los negocios y su producto monetario que poseen las empresas y los individuos se ven comprometidos constantemente por individuos que toman control generalmente con ayuda de redes de computadores, además de software malintencionado, accediendo a información que no les pertenece, violando la privacidad, robando la identidad y afectando las finanzas mundiales.

El teletrabajo como realidad social, merece que el derecho le preste atención, que lo regule, que lo institucionalice, tal como ya ha comenzado a suceder en la Unión Europea [7].

Es así que la reforma a las leyes ha permitido el tratamiento de delitos informáticos, como ocurre con la ley 1273 de 2009. Los delitos informáticos y los ciberdelitos son dos modalidades diferentes reconocidas. La primera en un sentido más amplio mediante el uso de sistemas informáticos, provocando la lesión o el peligro para los bienes jurídicos o individuales, sean patrimonio económico, libertad, intimidad y el buen nombre. Y la segunda cubre las conductas punibles realizadas con fines ilícitos, sin consentimiento, orientadas a la creación, procesamiento, almacenamiento, adquisición, transporte, divulgación, daño, falsificación, interceptación, manipulación y ejecución automática de bases de datos o información digitalizada reservada, secreta de naturaleza personal, privada o semiprivada, empresarial, comercial o publica que ponga en peligro la confidencialidad, la integridad y la disponibilidad de los datos o información [8].

Existen normas internacionales cuyo objetivo es brindar metodologías y guías de buenas prácticas a las empresas de cómo gestionar la seguridad de la información. Estas normas son la ISO 27001 e ISO 27002. La norma ISO 27002 en su versión 2013 está compuesta por 14 dominios, 35 objetivos de control y 114 controles e incluye en el dominio 6: Organización de la seguridad de la información, y también dos puntos sobre los dispositivos para la movilidad y el teletrabajo, las políticas para dispositivos móviles y las políticas para el teletrabajo. Hay que hacer énfasis en que la principal forma de proteger la información en esta modalidad de trabajo, es creando unas políticas claras que contemplen algunos o varios ítems de los que se listan

a continuación según las necesidades de las organizaciones y que vienen incluidas en la nueva versión de las normas expuestas, siendo muy importante la documentación de estas normas siguiendo unas características básicas y métodos de aplicación con una visión general de los posibles problemas de seguridad y las soluciones propuestas.

El primero nos muestra las políticas de dispositivos móviles que debería considerar una organización, tales como: el registro de los dispositivos móviles, los requisitos de protección física, la restricción de instalación de software, los requisitos de las versiones de software de los dispositivos móviles y para la aplicación de parches, la restricción de la conexión a los servicios de información, los controles de acceso, técnicas criptográficas, protección contra software malicioso, desactivación, eliminación y bloqueo a distancia, copias de seguridad, uso de servicios web y aplicaciones web.

El segundo punto habla de las políticas para el teletrabajo, que deben implantarse como apoyo a las medidas de seguridad de la información teniendo siempre en cuenta, La seguridad física existente del sitio de teletrabajo, el entorno físico de teletrabajo propuesto, los requisitos de seguridad de las comunicaciones, las amenazas de acceso no autorizado a la información, por amigos o familiares. Los acuerdos de licencia de software, la protección contra software malicioso y los requisitos de firewall, la provisión de acceso al escritorio virtual que impide el procesamiento y el almacenamiento de información sobre equipos de propiedad privada.

Más aun, la norma propone algunas actividades de control para las actividades del teletrabajo, definiendo a este como un método que permite al personal trabajar desde un lugar fijo por fuera de las instalaciones de la organización, ya sea el domicilio o un centro de negocios o similar y por las condiciones de movilidad se aborda el uso de los dispositivos portátiles y las comunicaciones móviles. Ambos con un componente común que son los riesgos al trabajar fuera del perímetro seguro de la organización. De hecho propone contemplar la seguridad física del entorno, separar el entorno profesional y el privado, la propiedad de los equipos, provisión y aseguramiento del equipo informático y de las comunicaciones, mantenimiento de los equipos, monitorización y supervisión, aseguramiento de los datos, licencias de software, gestión de incidentes de seguridad y continuidad del negocio [9].

5. La tecnología (TIC)

El conjunto de infraestructura, dispositivos, aplicaciones, y contenidos permiten ahorro de tiempo, aumento en la productividad, e incentivos económicos, evidenciados en ahorro en gastos operacionales de cada empleado. La infraestructura permite las operaciones básicas de la empresa, los dispositivos permiten la conexión entre el trabajador y la empresa. La elección de la tecnología adecuada es un desafío más de tantos que se conocen para permitir alcanzar las metas organizacionales. Estas tecnologías deben adaptarse a cada perfil de teletrabajador y no al contrario, además debe estar disponible en cualquier momento o situación por difícil que se presente [10].

Para atender esas necesidades de comunicación y acceso a la información, el teletrabajo tiene relación con varias tecnologías, que constituyen grupos de soluciones, algunas existentes desde tiempo atrás y otras más evolucionadas, que proporcionan básicamente mayor velocidad de conexión. Los ya conocidos sistemas de redes cableados, inalámbrico y satelitales en conjunto con las infraestructuras de centros datos, se unen a nuevos paradigmas como el de la computación en la nube, Tanto de tipo privadas, públicas o hibridas, con servicios como: SaaS (software como servicio), PaaS (Plataforma como servicio) e IaaS (Infraestructura como servicio).

BYOD. (*Bring your own device*) traiga su propio dispositivo: Trabajo mediante el dispositivo que más se acomode a sus necesidades de movilidad y disponibilidad. Es propiedad del empleado.

BYOA. (*Bring your own application*) traiga su propia aplicación: utilización de las aplicaciones que cada quien considere adecuadas para su trabajo, con o sin consentimiento del área de tecnología.

BYOI. (*Bring your own identity*) traiga su propia identidad: permite que la autenticación digital sea gestionada por un tercero, lo que en el ámbito empresarial puede ser conocido como "IDaaS" (*Identity as a Service*), identidad como servicio [11].

Es muy importante no perder el rumbo en lo que respecta a estas tecnologías, necesitan especial atención, ninguna empresa puede estar lo suficientemente protegida y pronto se verá en actividades riesgosas por su uso, que es muy común en las empresas y por ende en el teletrabajo que supone riesgos que deben ser tratados especialmente. [12].

6. Seguridad de la información

Garantizar la confidencialidad, disponibilidad e integridad de la información, la intimidad y el buen nombre tanto para las personas, como para las empresas es un derecho adquirido en la sociedad, es la preocupación principal de empleados y dirigentes, todos los esfuerzos se deben dirigir a la protección de los activos en las organizaciones. En la modalidad de teletrabajo el empleado tiene una gran responsabilidad para ayudar en este compromiso, no solo de palabra, sino en la práctica aplicando el uso aislado de las herramientas tecnológicas utilizadas en su trabajo, de aquellas que involucran a los demás miembros de la familia o visitantes ocasionales del hogar, por esto su educación en materia de seguridad de información es primordial para el buen desarrollo de sus actividades dentro de un entorno que presenta vulnerabilidades que deben ser identificadas, y para esto se deben conocer conceptos básicos en seguridad de la información, como por ejemplo, *las amenazas para los datos*, destacando entre estas las averías a los discos duros, los errores humanos, los fallos de software, los virus Informáticos, los accesos malintencionados, los fallos eléctricos, los robos y algunos otros de carácter externo como los incendios, las inundaciones y los terremotos. Se debe conocer el *valor de la información* y dar importancia a la protección de los datos personales con prácticas seguras de navegación para evitar el fraude y el robo de información, navegando directamente desde la dirección de las páginas web de entidades bancarias, sin acceder a estas desde vínculos o correos electrónicos, y asegurarse que los sitios utilizan tecnologías seguras. Mantener a salvo la identidad electrónica, protegiendo con contraseñas seguras el acceso a cuentas de correo y el chat, con combinaciones entre mayúsculas/minúsculas y números o caracteres especiales, en lo posible utilizando contraseñas diferentes para cada sitio. No realizar operaciones bancarias en sitios públicos o conectados a redes inalámbricas de acceso libre. Tener cuidado con los correos electrónicos de origen desconocido y cuidarse de entregar los datos personales. Mantener el equipo protegido con antivirus y evitar instalación de software pirata, cerrar siempre la sesión de usuario y ante todo ser precavido en todo momento. A partir de estos conocimientos el teletrabajador en conjunto con los encargados de la seguridad de la información y otros actores del proceso, como administradores de antivirus, redes de datos y monitoreo contando con unas políticas claras al interior de

la organización, todas enfocadas al buen uso y manejo de las herramientas que posibiliten el desempeño del teletrabajador, además de un sistema que permita el tratamiento de los riesgos con sus cuatro enfoques principales: controlar, aceptar, eliminar y trasladar los riesgos [13] se podrá llevar a buen término y mantener de manera adecuada la utilización de los sistemas de información involucrados en la modalidad del teletrabajo.

La probabilidad de pérdida de información y las consecuencias que esto acarrearía para la empresa u organización son una amenaza que no se puede olvidar y desde el campo de la seguridad de la información se debe trabajar en el diseño de un sistema de gestión centrado en la prevención y mitigación de los daños. Por medio de este sistema la organización puede conocer los riesgos que tiene su información y establece la metodología, que debe estar documentada y ser puesta a conocimientos de toda la empresa. Un sistema de gestión de la seguridad de la información (SGSI), en su fase de tratamiento de los riesgos proporciona varias opciones, que pueden ser eliminar los activos que están asociados con el riesgo hallado, lo que puede ser costoso y muy drástico, por lo que siempre es mejor buscar otras medidas, otra opción, es la transferencia del riesgo, ya sea entregando su cuidado a un tercero mediante contratación, o mediante la adquisición de un seguro que cubra los gastos, si se llegara a materializar dicho riesgo. Otra alternativa conocida es la de asumir el riesgo, lo que quiere decir no tomar acciones frente a este, la decisión debe ser tomada por la dirección superior de la empresa. Por último tenemos la acción de mitigar el riesgo, mediante medidas que permitan la protección de la información o el activo en riesgo, cualquier media debe ser documentada y dada a conocer a todos los empleados y dirigentes de la organización.

7. Conclusiones

La evaluación hecha en este artículo sobre el tratamiento que se da a la seguridad de la información en la modalidad del teletrabajo cumple con el objetivo de comunicar, exponer las fallas y las eventuales soluciones al problema. Se evidencia la necesidad de emplear un método práctico para ajustar las políticas existentes de seguridad en la empresa al nuevo modelo, el establecimiento de un sistema de gestión de seguridad de la información, dejando claro que no hay que proponer nada nuevo, las metodologías existen y la

tecnología, con la ayuda de un equipo de trabajo capacitado en colaboración con los empleados y teletrabajadores, permite establecer un ambiente de trabajo que cumpla con las normas básicas de seguridad.

Se proponen métodos y se da a conocer las fallas comunes ya que no es la modalidad de teletrabajo la que afecta la información, es la falta de procedimiento, políticas y métodos de seguridad de la información adecuados los que permiten que se produzcan pérdidas, teniendo en cuenta que el factor más débil es el humano, es necesaria la educación, acompañamiento y retroalimentación constante. La confianza y el apoyo de los superiores de la organización son primordiales para que el ambiente de teletrabajo cumpla con las condiciones adecuadas, tanto en materia de seguridad como de productividad y de bienestar laboral.

La dependencia del teletrabajo de las tecnologías de la información, supeditan a los profesionales en sistemas y de seguridad de la información a una participación activa en el proceso, por esto la actualización constante de procesos, de conocimientos y el compromiso son claves para mantenerse adelante en la continua carrera contra los delitos y eventos de seguridad. Así pues la implementación y ejecución de las políticas parecen una tarea dura pero al final se pueden ver los frutos y el éxito del proceso y las mejoras en seguridad permitirán seguir adelante.

8. Referencias

[1] K. Vermaas and F. Bongers, Broadband in Telework. *Health and Safety:The User Perspective Journal of Internet Commerce*, Vol. 6, No. 2. 2007.

[2] L. Barba, El teletrabajo y los profesionales de la información. *E-prints in library & information science*, Vol. 10, No. 4, pp. 4-13. 2001.

[3] M. Niedzwiedzinski y A. Bakala, Telework and Security. *Systems: Journal Of Transdisciplinary Systems Science*, Vol. 12 No. 1, pp. 43-45. 2007.

[4] N. A. Barreiro, Los costos de oportunidad de la información y la innovación en las empresas. *Ciencias de la Información,* Vol. 34, pp. 23-30. 2013.

[5] M. Rivera, La protección de datos en el entorno laboral. *Revista de derecho, comunicaciones y nuevas tecnologías*, No. 7. 2012.

[6] E. Castillo, Teletrabajo una opción de productividad y eficiencia real para las organizaciones. *Revista Virtual Universidad Católica del Norte*. No. 31. 2010.

[7] M. Rodríguez, El teletrabajo en el mundo y en Colombia. *Revista Gaceta laboral*, Vol. 13, No. 1, pp. 29-42. 2007.

[8] R. Posada, El delito de transferencia no consentida de activos. *Revista de Derecho, comunicaciones y nuevas tecnologías*, N° 8. 2012.

[9] Organización internacional para la estandarización, comisión electrónica internacional *NTC. Tecnología de la información, Técnicas de seguridad, código de prácticas para la gestión de la seguridad de la información.* ISO/IEC 27002:2005. ICONTEC. 2007.

[10] Ministerio de Tecnología de la Información y las Comunicaciones. (2012) *LIBRO BLANCO, El ABC del teletrabajo en Colombia*, Versión 3, pp. 34. 2012.

[11] D. Raths, *The Journal*, Vol. 39, No. 4, pp. 28-32. 2012.

[12] E. Nathan, BYOD Businesses Still Lack Effective Security Policies. *eWeek*, pp. 2. 2012.

[13] R. Gómez, D. Pérez, Y. Donoso y A. Herrera, Metodología y gobierno de la gestión de riesgos de tecnologías de información. *Revista de Ingeniería*. No. 31, pp. 109-118. 2010.