SEGURIDAD INFORMÁTICA PARA EL TELETRABAJO EN EMPRESAS PRIVADAS EN COLOMBIA

Bustos Guáqueta Carlos Andrés
Cundinamarca, Universidad Piloto de Colombia
Bogotá, Colombia
ingcarlosbustos83@gmail.com

RESUMEN: *El artículo a continuación sugiere parámetros básicos para implementar seguridad informática para los trabajadores y empresas privadas en Colombia que emplean el teletrabajo como una opción para la continuidad en sus negocios y beneficios para los empleados. Esta guía sugiere como tratar temas en la seguridad de equipos de cómputo y sistema operativo, seguridad en las comunicaciones, seguridad de la información y seguridad de los recursos humanos.*

PALABRAS CLAVE: *Empresas privadas Colombia, seguridad informática, teletrabajo.*

ABSTRACT: *The article then suggests basic parameters to implement security for workers and private companies in Colombia that use telecommuting as an option for business continuity and employee benefits. This guide suggests how to deal with security issues in computer equipment and operating system, communications security, information security and safety of human resources.*

KEYWORDS: *Colombia private companies, computer security, teleworking.*

1. INTRODUCCIÓN

El mundo de los negocios continua en constante crecimiento y evolución esto se debe a la tecnología, el 90% de los ejecutivos en USA trabajan fuera de la organización, 34% de la fuerza laboral en USA no tiene oficina, Colombia no es ajena a esta cifra, según el estudio realizado por Flurry [1] Colombia tiene un 278% en aceptación de nuevas tecnología y activación de dispositivos móviles prevaleciendo a países como Vietnam, Turquía y Ucrania. Es poco probable el no pensar que iniciativas BYOD no serán adoptadas por la mayoría de empresas nacionales, ya que prácticamente seria ir en contracorriente a una tendencia mundial.
El Gobierno Colombiano mediante el MinTic ha realizado numerosos proyectos el más reciente www.teletrabajo.gov.co para incentivar la adopción del teletrabajo, para empresas y gremios todavía no consideran un modelo firme para las organizaciones. Colombia, continúa realizando esfuerzos para posicionar el teletrabajo como una opción válida para solucionar varios problemas estructurales como la movilidad en las ciudades capitales y aumentar la productividad entre los trabajadores. Entonces, ¿por qué las empresas en Colombia no adoptan definitivamente el teletrabajo?

Se considera varias posibles razones:

- Existe temor y dudas por la seguridad de la información, ya que no cuenta una metodología de protección, a pesar de existir una guía de implementación de teletrabajo para Colombia como el Libro Blanco del teletrabajo V3.0 no es muy específica a la hora de presentar mecanismos de protección de la información.

- Los empresarios exploran varias limitantes como la resistencia al cambio, la modificación de la cultura organizacional, contar con herramientas para controlar la productividad y una mayor apropiación de las TIC en las compañías.

- El teletrabajo es voluntario, tanto para el funcionario como para la entidad. Por lo tanto las direcciones de talento humano deben revisar el respectivo manual de funciones y competencias laborales e identificar las actividades y cargos susceptibles de realizarse a través del teletrabajo.

- Cumplimiento mínimo de las Tic, ya que no todos los trabajadores cuenta con los equipos o conectividad que permita su óptimo desempeño en sus funciones en este caso la empresa no le es conveniente invertir en infraestructura para dotar particularmente a sus empleado.

Por ende este artículo sugiere parámetros básicos para implementar seguridad informática para los empleados y empresas en Colombia que optan por el teletrabajo.

2. PROCEDIMIENTO SUGERIDO DE ASEGURAMIENTO

2.1 POLÍTICAS O NORMAS DE SEGURIDAD PARA LA EMPRESA

Es muy importante definir la política o normas de seguridad interna de la empresa con el fin de estandarizar el modo y las condiciones bajos las cuales los directivos desean que se desarrolle el trabajo.

Según el tamaño, necesidad y naturaleza de la empresa se podrán definir las siguientes políticas que cubran por lo menos los siguientes ítems:

- Procedimiento de solicitud voluntario y autorización de teletrabajo
- Perfiles de usuarios que podrán optar por el teletrabajo y definir los permisos de acceso remoto.
- Procedimiento de conexión remota alterna en caso de fallos
- Posibilidad de utilizar equipos personales (BYOD) para el teletrabajo y su medida de seguridad.
- Política para el almacenamiento de la información de la empresa equipos personales o medios extraíbles.
- Procedimiento para proteger físicamente los accesos a los equipos de cómputo de la empresa.
- Cláusulas de responsabilidad de la información a custodio por el empleado bajo teletrabajo

Es recomendable ajustar el anterior listado guiándose con los controles de la norma NTC-ISO/IEC ISO27001 la correcta aplicación de los controles debe garantizar usos aceptables de seguridad.

2.2 EQUIPOS DE CÓMPUTO Y SISTEMAS OPERATIVOS

Los equipos provistos por la empresa o equipos de uso personal debe cumplir con parámetros mínimos de seguridad pero en ocasiones no cumplen estos parámetros por lo tanto deben ser catalogados como equipos no confiables aunque las amenazas actuales hacen prácticamente imposible poder considerar un equipo totalmente seguro; para esto se puede establecer una línea base para determinar la confiabilidad del equipo de cómputo
Los requerimientos mínimos para asegurar un equipo de cómputo son:

2.2.1 Equipos de confianza

- Proteger el acceso de la maquina mediante una contraseña en BIOS
- Sistema operativo y aplicaciones actualizadas
- Software antivirus
- Perfiles de usuario para sin privilegios para instalación de software y modificación de configuraciones.
- Configuraciones seguras para los navegadores de internet
- Bloqueo automático por inactividad.
- Software anti malware, antispyware, antirootkit
- Control de acceso sólido.
- Cifrado de disco duro.
- Verificación periódica de la las reglas de seguridad del equipos
- Restricción de navegación global de internet.

2.2.2 Equipos no confiables

- En caso de tener múltiples perfiles de usuario en el sistema operativo, debe existir un perfil protegido con contraseña robusta y la información que contiene este perfil no debe ser accedida por otros perfiles en la misma máquina.
- En lo posible emplear arranque dual el cual permite dos sistemas operativos en la misma maquina uno destinado para actividades de teletrabajo y el segundo para fines personales.

2.3 PROTECCIÓN FÍSICA

Los modelos de trabajo actual emplean en gran parte ordenadores portátiles, tablets, teléfonos inteligentes con notables ventajas de portabilidad pero con una alta posibilidad de perder el dispositivo o ser robados lo cual es necesario establecer medidas para este tipo de equipos.

2.3.1 Protecciones antirrobo

Emplear dispositivos de anclaje como candados o guayas de seguridad que permita asegurar el dispositivo normalmente los mecanismos más robustos son muy grandes y aparatosos en su uso, la recomendación más importante es el sentido común y no desatender el equipo de cómputo.

2.3.2 Seguimiento y borrado remoto

Emplear software clientes para localización geográfica o el borrado remoto de la información; este software permite hacer recuperación de datos de forma remota por esta razón es importante valorar los términos y condiciones del software de acceso remoto y el acceso que puedan tener sobre la información e dispositivo

2.3.3 BYOD (Bring Your Own Device)

Se ha convertido en tendencia esta modalidad donde las empresas optan por reducir costos y la administración de los equipos de cómputo permitiendo al empleado mezclar su vida laboral y personal con el objetivo de aumentar la productividad. Este modelo lleva a importantes problemas de seguridad ya que no existe administración o control por el departamento TI por esto se debe realizar un análisis de riesgo, antes de implementar este modelo se deben tomar medidas técnicas y organizativas así:

- Políticas de seguridad indicando el uso adecuado de los equipos y de la información.
- Cláusula de responsabilidades en el manejo de la información de la empresa.

2.4 COMUNICACIONES

La infraestructura en las comunicaciones brindan grandes beneficios en la disponibilidad de aplicativos y de la información de las compañías, pero este denota riesgos en las seguridad ya que los métodos de acceso en las redes sugieren miles de conexiones que pueden ser vectores de ataque hacia la compañía
La seguridad en las comunicaciones debe estar dirigida en combatir o contrarrestar una o varias amenazas ya sea inmediato, latente o potencial que pretendan atentar con los principios de confidencialidad, disponibilidad e integridad de la información.

La creación de un modelo de seguridad para las comunicaciones debe identificar los componentes o características de las redes de comunicación, existen tres tipos de redes.

- Red no controladas
  Este tipo de red es aquella que no puede ser gestionada o controlada por el departamento de TI pero es necesario para lograr una comunicación.
- Red controlada
  Este tipo de red es toda aquella que se encuentra bajo la jurisdicción del departamento Ti de la compañía.
- Red en ámbito protegido
  Este tipo de red se encuentra bajo el mismo concepto de la red controlada pero adiciona componentes criptográficos.

Identificando el tipo de redes de la empresa se debe definir el modelo de arquitectura de comunicaciones y establecer qué tipo de información debe circular en cada una de estas redes, es claro que toda información que sea transferida por medio de redes no controladas debe ser cifrada y contener métodos de criptografía punto a punto mediante configuración de VPN. La configuración de criptografía en las redes controladas y de ámbito protegido será definida por el departamento de seguridad y alta gerencia teniendo en cuenta que los ataques pueden ser originados dentro de la organización.

2.4.1 VPN (Virtual Private Network)

Esta configuración brinda beneficios para los administradores de TI ya que permite una administración centralizada evitando abrir accesos a cada una de las aplicaciones con sus consiguientes riesgos de ataque y sus controles de seguridad.
Otra de las bondades de las redes VPN radica en su robustez y seguridad, para que utilicen autenticación fuerte de doble factor el cual consiste en combinar certificados de seguridad con una autenticación mediante contraseña.

2.5 SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información es el conjunto de medidas técnicas, organizativas y legales que permiten a las empresas asegurar la confidencialidad, integridad y disponibilidad de su sistema de información la definición brindada por el estándar para la seguridad de la información ISO/IEC 27001, aprobado y publicado en Octubre de 2005 por la ISO (International Organization for Standardization) y por la comisión IEC (International Electrotechnical Commission).

La implementación de un Sistema de la Seguridad de la Información (SGSI) exige tiempo y planificación, su objetivo es proteger la información para ellos se debe identificar los activos que deben ser protegido y en qué grado, posterior a esto se debe aplicar un plan PHVA (Planear, Hacer, Verificar y Actuar) este proceso nunca finalizara ya que los riesgos nunca son eliminados, estos son reducidos a puntos aceptables por parte de la alta gerencia.

Al establecer los controles de la familia de la norma NTC-ISO/IEC ISO27000 permite asegurar el activo más importante de una organización como lo es la información.

2.5.1 Copias de seguridad

Las copias de seguridad son generadas y administradas de forma automática por el departamento TI, pero en entornos de teletrabajo no se aplican mejores prácticas en respaldar la información.

El método de backup, varía de acuerdo a la forma de teletrabajo:

- Escritorios remotos
- Perfil móvil, o sincronización automática, mediante software
- Sincronización manual.
- Copias de seguridad offline

2.5.2 Cifrado del disco duro

Proteger la información que se almacena fuera de la empresa se considera la una de las principales preocupaciones a la hora de disponer de teletrabajadores, tal vez porque el robo o pérdida de un equipo portátil es algo que puede ocurrir con una alta probabilidad.
Contra este tipo de fugas de información no es suficiente con poner contraseña de varios niveles sobre el equipo o sistema operativo, ya que si el hardware de almacenamiento es extraído y puesto en otro equipo la información será expuesta inmediatamente. Para prevenir este tipo de amenaza, se sugieren dos soluciones:

- No almacenar nada de información sensible en el equipo y usarlo únicamente online
- Cifrar la información.

Existen diferentes soluciones de cifrado cuya elección

dependerá de las necesidades de seguridad y usabilidad, son las siguientes:

- **Cifrar el disco completo mediante el propio sistema operativo:**

Los principales sistemas operativos disponen de herramientas de cifrado, esto permite una solución rápida y sencilla ya que no requieren software adicional si no tan solo el provisto por el propio sistema operativo.
Es muy importante tener en cuenta que al cifrar el disco duro puede afectar el rendimiento del sistema operativo y mantener la llave maestra en caso de recuperar información del disco duro cifrado.

- **Crear un volumen cifrado:**

Este método permite cifrar la información en un archivo único dando una sensación de mayor seguridad pero puede presentar problemas de compatibilidad con sistemas operativos y problemas al descifrar la información.

2.5.3 Documentación física

Por lo general en un entorno de teletrabajo la información en documentación física es menos susceptible de sufrir ataques pero se deben tomar medidas de seguridad así:

- Almacenar los documentos de acuerdo a su sensibilidad en un lugar seguro mientras no se estén utilizando
- Tomar medidas para el transporte de documentación por medio de contenedores y no perder de vista.
- Establecer el método correcto para destruir la información en papel evitando tirarla directamente al contenedor del reciclaje o designándolo como hojas de borrador para labores domésticas.

2.5.4 Sistemas de almacenamiento on line

Con el avance del big data han surgido múltiples proveedores de almacenamiento on line; dando beneficios en la portabilidad, disponibilidad de la información en diferentes dispositivos, controles de versiones, acceso controlado a otros usuarios, suprime el uso de medios extraíbles, el software de sincronización viene incluido en la mayoría de sistemas operativos. A pesar de todos los beneficios, se deben considerar los peligros de este tipo de almacenamiento.

- Valorar el tipo de información que será guardada en los almacenamientos on line ya que si la plataforma es vulnerable a un ataque podría ser posible acceder a la información por terceros
- La información puede ser accedida por los funcionarios de la empresa o gobierno donde se encuentre alojada la plataforma.
- El cifrado de la información es delegada a la plataforma de almacenamiento lo cual no permite tener control sobre esto.
- La información almacenada en sistemas on line puede incurrir en incumplimientos de normativas o leyes de protecciones de datos
- No descuidar los contratos de prestación de servicio que ofrecen estas plataformas ya que no siempre se comprometen a garantizar la disponibilidad de la información, pudiendo tener fallos técnicos que les dejen sin conectividad durante días, o pudiendo llegar al extremo de cerrar por temas legales con el país donde se aloja la plataforma

2.6 SEGURIDAD DE RECURSOS HUMANOS

Los recursos humanos muy probablemente son el componente más crítico al momento de garantizar las tres características de la seguridad de la información: integridad, confidencialidad y disponibilidad, por lo tanto deben adoptarse controles y prácticas de gestión que ayuden a mitigar el impacto de los riesgos que por este factor se pudieran materializar.

Particularmente uno de los pilares básicos de la norma ISO 27001 hace referencia a la seguridad sujetada a los recursos humanos, que debería enfocarse desde la definición de las funciones y los recursos hasta la finalización de la relación laboral, incluyendo la seguridad en el desarrollo de las funciones de los empleados. Con la definición clara de las funciones se asegura que todo el recurso humano en el modo de teletrabajo de la empresa entienda sus responsabilidades y estén en las condiciones para desarrollarlos; de esta forma se pueden reducir riesgos de fraude y uso inadecuado de los activos de información de la empresa. Esto se puede lograr en gran medida con una adecuada verificación de antecedentes que esté de acuerdo al tipo de información al que va a acceder el empleado.

Adicionalmente es necesario establecer los procedimientos para garantizar que el retiro de la empresa por parte del recurso humano sea controlado garantizando la devolución de todo el equipamiento y la eliminación de las credenciales de acceso a los sistemas. Lo más recomendable es revocar, en primer lugar aquellos accesos a los sistemas más críticos o vulnerables, y además hacer un monitoreo del uso de las cuentas de correo electrónico para garantizar que no se extraiga información confidencial, respetando las consideraciones de privacidad que apliquen. Todo lo relacionado con la finalización de contrato debería estar formalizado para incluir el retorno previo del software, documentos corporativos, equipos, dispositivos móviles, tarjetas de crédito, tarjetas de acceso e información guardada en medios electrónicos.

2.6.1 Ingeniería social

La ingeniería social se logra por medio de manipulación psicológica y habilidades sociales con el objetivo de obtener algún tipo de información sensible o útil de la empresa o empleado.
La ingeniería social tiene diversas formas de actuar:

- Técnicas Pasivas: Basadas en observar y analizar a los empleados, permitiendo crear un perfil psicológico que permite abordar al empleado.
- Técnica no presencial: Se emplea medios de comunicación como teléfono, correo electrónico.

- Técnica presencial no agresiva: Mediante el seguimiento, vigilancia de domicilios, búsqueda en la basura del empleado con el fin de recolectar la mayor cantidad de información.
- Técnica activas: Mediante la suplantación de identidad, personalizaciones de otros empleados y presión psicológica

Para implementar defensas ante amenazas de ingeniera social se debe tener en cuenta los siguientes parámetros:

- Diseñar y efectuar políticas de seguridad las cuales deben darse a conocer a los empleados donde ellos adquieran el conocimiento y compromisos por parte de ellos.
- Las campañas de concienciación es muy importantes mediante aprendizaje estructurado, reuniones menos formales, campañas con pósteres u otros eventos para anunciar las directivas de seguridad. Cuanto más refuerce los mensajes de sus directivas, más exitosa será su implementación.
- Deben existir protocolos reactivos en los procedimientos relacionados con la directiva de seguridad, registrando los posibles ataques de ingeniería social para prevenir posibles ataques en la empresa.
- Si las propuestas de seguridad afectan negativamente a la rentabilidad o a la agilidad comercial de la empresa, es probable se deba evaluar el riesgo. Se debe lograr un equilibro entre la seguridad y la operatividad.

3 CONCLUSIONES

La seguridad informática hoy en día denota una importancia muy grande en las empresas colombianas el cual exige dar a conocer o capacitar a los departamentos TI, desafortunadamente existen un concepto erróneo por parte de los directivos de las compañías donde dan por sentado que el equipo TI que mantiene en marcha la arquitectura en sistemas también aseguran la infraestructura lo cual no sucede realmente así. La clave para desarrollar exitosamente un plan de seguridad informática son la definición de políticas de seguridad claras, de fácil entendimiento y cumplimiento junto a la combinación de estrategias la cual permitan reducir los riesgos a puntos aceptables, desafortunadamente las organizaciones ignoran la interrelación de este proceso y consideran la implementación como un costo adicional el cual no tendrá un retorno de inversión lastimosamente no perciben que la implementación de la seguridad informática e información es de forma preventiva en caso de ser vulnerables a un ataque serán un valor más elevado en la recuperación del ataque.

La implementación de políticas de seguridad informática en organizaciones bajo modalidad de teletrabajo es una solución integral que no solo busca proteger, preservar, administrar de manera eficiente todo tipo de recursos con los que cuenta las organizaciones, sino que también busca dar solución, prevenir, evitar, controlar y minimizar los daños de incidentes que afectan a la organización, por esto, preparar y capacitar al personal en temas asociados a la seguridad informática y cómo hacer frente a incidentes que se llegarán a presentar con el fin de responder de una manera adecuada es una de las principales metas de esta estrategia.
La capacitación del personal es un factor muy significativo ya que el recurso humano lastimosamente es el factor más vulnerable entre todos los activos de una compañía, la capacitación permite que empleado puedan tomar un papel activo dentro de la organización de manera que apliquen el conocimiento con el fin de proteger de una adecuada la información que se le confía.
El teletrabajo es una opción que brinda grandes beneficios a la empresa, el empleado y la ciudad donde se ubica la compañía; pero exige grandes retos en seguridad el combinar conceptos de seguridad de la información e informática podrá controlar y minimizar los riesgos en el modelo de teletrabajo.

4 REFERENCIAS

[1]. Peter Farago. Flurry Insights Blog (2015, Mar) - China Knocks Off U.S. to Become World's Top Smart Device Market
http://flurrymobile.tumblr.com/post/113381348495/china-knocks-off-u-s-to-become-worlds-top-smart

[2]. Karen Scarfone, Paul Hoffman, Murugiah Souppaya – (2009 Junio) Guide to Enterprise Telework and Remote Access Security - NIST Special Publication 800-46 Revision 1
http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf

[3]. Aaron Dolan (2004 Feb 10). Social Engineering SANS Institute
http://www.sans.org/reading-room/whitepapers/engineering/social-engineering-1365

Autor
Carlos Andrés Bustos Guáqueta
Ingeniero de Sistemas
Est. Especialización en Seguridad Informática
Seminario de Gestión de la Seguridad y el Riesgo
Universidad Piloto De Colombia
Junio 2015