Espirales

Http://revistaespirales.com

ISSN 2550-6862

Análisis e impacto del ocio cibernético en las organizaciones

Elizabeth Salinas de Rolando, Guillermo Rolando Farfán, Guillermo Rolando Farfán

Resumen

El ocio cibernético o ciber ocio se describe brevemente como el mal uso del internet en los lugares de trabajo. Siendo el internet un recurso vital hoy en día para las organizaciones, se vuelve necesario tratar este tema, a pesar que ha sido poco abordada por referentes en tecnología. Este trabajo básicamente consiste en la recopilación y análisis de material bibliográfico. Con los datos recabados, se exponen algunas definiciones y hechos relevantes sobre el ciber ocio. Se detalla de manera resumida algunos peligros, costos y problemas asociados con esta práctica en las organizaciones. Se describen algunas tecnologías de la información desarrollados para hacer frente o para detectar casos de ciber ocio. En contraste, se exponen también varias posturas de diversos autores que están a favor de esta práctica, con el objetivo de llegar a una conclusión y determinar si es imperativo o no, detener el ciber ocio por completo, empleando cualquiera de los mecanismos descritos, o si se deja la posibilidad de que continúe esta práctica total o parcialmente.

Palabras clave

Ocio cibernético, ciber ocio, organizaciones

Texto completo:

45-56

Referencias

RECIBIDO: ENERO 2017 REVISADO JULIO 2017 ACEPTADO MAYO 2017

Análisis e impacto del ocio cibernético en las organizaciones

Elizabeth Salinas[1]

Guillermo Rolando Farfán[2]

[1] Ing. Elizabeth Salinas de Rolando, Mg. – Docente Universidad Tecnológica Empresarial de Guayaquil – esalinas@uteg.edu.ec

[2] Guillermo.rolando@level3.com

RESUMEN:

El ocio cibernético o ciber ocio se describe brevemente como el mal uso del internet en los lugares de trabajo. Siendo el internet un recurso vital hoy en día para las organizaciones, se vuelve necesario tratar este tema, a pesar que ha sido poco abordada por referentes en tecnología. Este trabajo básicamente consiste en la recopilación y análisis de material bibliográfico. Con los datos recabados, se exponen algunas definiciones y hechos relevantes sobre el ciber ocio. Se detalla de manera resumida algunos peligros, costos y problemas asociados con esta práctica en las organizaciones. Se describen algunas tecnologías de la información desarrollados para hacer frente o para detectar casos de ciber ocio. En contraste, se exponen también varias posturas de diversos autores que están a favor de esta práctica, con el objetivo de llegar a una conclusión y determinar si es imperativo o no, detener el ciber ocio por completo, empleando cualquiera de los mecanismos descritos, o si se deja la posibilidad de que continúe esta práctica total o parcialmente.

PALABRAS CLAVE: Ocio cibernético, ciber ocio, organizaciones

ABSTRACT

Cyber leisure or cyber leisure is briefly described as the misuse of the internet in workplaces. Since the internet is a vital resource today for organizations, it becomes necessary to address this issue, although it has been little approached by referents in technology. This work basically consists of the compilation and analysis of bibliographic material. With the data collected, some definitions and relevant facts about cyber leisure are exposed. It briefly summarizes some of the dangers, costs and problems associated with this practice in organizations. It describes some information technologies developed to deal with or to detect cases of cyber leisure. In contrast, several positions are also presented by various authors who are in favor of this practice, with the aim of arriving at a conclusion and determining whether it is imperative or not, to stop the cyber leisure completely, using any of the mechanisms described, or if you allow yourself the possibility of continuing this practice in whole or in part.

KEY WORDS: cyber leisure, cyber leisure, organizations

INTRODUCCIÓN:

En la actualidad, internet no solo ofrece una infinidad de posibilidades para acceder a todo tipo de información, sino también a elementos distractores y de entretenimiento como redes sociales, servidores de reproducción de audio y video, juegos en línea, entre otros. Todo este contenido presente en internet, muchas veces, también está disponible en los ordenadores y/o dispositivos móviles de los trabajadores de las diversas organizaciones, quienes posiblemente usen ese importante recurso estratégico para fines no relacionados con su actividad laboral.

Hoy en día, con el uso de internet y otras tecnologías de información en las organizaciones se puede lograr incrementar la productividad de los empleados. Paralelamente las empresas obtienen beneficios como bajar costos, acortar ciclos de producción y mejorar procesos, sin embargo, el acceso a internet también brinda la oportunidad a un empleado de comportarse mal. (Wang, Tian, & Shen, 2013) En base a lo anterior, las organizaciones deben tomar una crucial decisión: Permitir que los empleados tengan acceso total a internet o aplicar medidas de prevención, restricción, castigo, o simplemente permitir que se siga usando el internet libremente.

El objetivo de esta investigación es detallar los costos y problemas asociados con el uso inadecuado del internet en las organizaciones. Realizar un análisis de las posibles soluciones tecnológicas y organizacionales que se pueden ejecutar para poner un límite o anular por completo el libre acceso y, por último, revisar posturas de diversos autores que apoyan estas prácticas para llegar a una conclusión sobre cómo afrontar ese problema ante la detección de casos de ocio cibernético en una organización.

DESARROLLO

2.1 DEFINICIONES

Varios autores definen el problema con diversos términos. Para Johnson & Indvik (2003) Se emplean 4 denominaciones: cyber leisure, cyberslacking, cyberloafing y cyberbluding; términos empleados para describir actividades que involucran a trabajadores desperdiciando tiempo en internet en lugar de dedicarle tiempo a su trabajo. En castellano el término empleado simplemente es ocio cibernético o ciber ocio. Manrique de Lara (2009) define también el cyberloafing como un acto voluntario de los empleados que usan el internet de

las empresas para actividades no relacionadas con el trabajo. Se aprecia que todos los términos empleados para describir este fenómeno en idioma inglés, conllevan la palabra ocio o sinónimos. Para García-Cueto & Cerro (1990), el ocio se define como: "Todo aquel periodo durante el cual el individuo se desliga de sus obligaciones profesionales, familiares y sociales y procura la realización voluntaria de ocupaciones consideradas a priori satisfactorias y como un fin en sí mismo". Pag. 173.

Johnson & Irvick (2003) proveen una lista de actividades que pueden asociarse con ocio cibernético: Visitas de páginas pornográficas, sitios de noticias, websites de compras o intercambio de productos, juegos en línea, salas de chat, búsquedas de empleos, realizar tareas en horas de oficina, intercambiar correos personales con amigos y familiares. A este criterio, se puede agregar fácilmente las visitas a redes sociales, sitios de reproducción de material audiovisual.

2.2 PROBLEMAS GENERADOS POR EL OCIO CIBERNÉTICO

Desde el punto de vista técnico y organizacional, el ocio cibernético puede ser un tema de mucha preocupación para las organizaciones. Messarra, Karkoulian, & McCarthy (2011) indican que el ocio afecta significativamente a las organizaciones pequeñas. El excesivo uso de los recursos, el desperdicio de ancho de banda y la exposición a virus, puede generar lentitud en la operación y deterioro del rendimiento de la red.

Es importante destacar que la actividad de cyberloafing genera muchos costos asociados por pérdidas de eficiencia; o gastos en las organizaciones para impedir que se genere esta práctica. Para Gunia, Corgnet & Hernan-Gonzalez (2014), ya para el año 2001, las organizaciones empezaron a implementar sistemas de monitoreo para controlar a sus empleados, generando toda una industria de monitoreo y seguridad de alrededor de $300 millones. En Estados Unidos, las pérdidas generadas por la improductividad laboral causada por cyberloafing son cercanas a $178 billones al año, pérdidas que incluyen el consumo excesivo del ancho de banda, exposición a riesgos de seguridad y algunas veces, problemas legales por fraudes y acoso sexual (Wang, Tian, & Shen, 2013). Según Messarra, Karkoulian & McCarthy (2012), el costo por una hora de ocio cibernético de 1000 usuarios de internet en USA, es

aproximadamente $35 millones al año. Johnson & Indvik (2003) afirman que las corporaciones en el continente Americano gastan aproximadamente $3.5 billones en acceso a internet, de los cuales, $ 1 billón se le atribuye al uso de internet para actividades de ocio cibernético, generando un grave problema de nivel multibillonario.

De acuerdo con Messara et. al. (1014), Los problemas no son solo para los empleados. Los empleadores se ven afectados por las prácticas de ocio cibernético. Esto se debe a que los empleadores son los dueños de las computadoras y de la red de las organizaciones, por lo tanto, cualquier actividad de cyberloafing ejecutada por sus empleados, muchas veces, prácticas ilegales como las descargas de material con derechos de autor, puede ocasionar severos problemas con la ley. Igual criterio se observa en Young & Case (2004), los empleados pueden incluso, subir el material ilegal descargado a los servidores de las organizaciones, enviar mails ofensivos a sus compañeros trabajadores, que pueden terminar en denuncias por acoso. Johnson & Irvick (2003) condensan los problemas asociados con cyberloafing de la siguiente manera: "Hay tres importantes razones por las cuales las compañías deben preocuparse por sus empleados: 1) pérdida de productividad 2) líos legales y 3) desperdicio de ancho de banda". Pag. 56.

Con respecto a la pérdida de productividad por mal uso del internet en horarios de trabajo, Galletta & Polak (2003) afirman que los trabajadores destinan alrededor de 5.8 horas a la semana en actividades no relacionadas a internet en el trabajo y 4.6 horas de uso de internet en el trabajo a la semana, dando un total de 10.4 horas a la semana, o el 25% de una semana laboral de 40 horas. Según Lim & Chen (2012), al consultar a varios empleados sobre el tiempo aceptable para realizar cyberloafing, el resultado fue 1 hora 15 minutos al día, mientras que el uso del internet para fines no relacionados al trabajo, fue de 55 minutos; cifra muy superior a un estudio realizado 3 años antes, donde el tiempo era 38 minutos. Este aumento es debido a la creciente penetración del internet y al constante desarrollo de nuevas aplicaciones.

Deshacerse de los empleados que realizan cyberloafing puede ser una solución lógica y sencilla, sin embargo, para Young & Case (2004), Despedir empleados que abusan del internet en el trabajo puede crear nuevos problemas como un aumento de la rotación laboral, una disminución de la moral de los trabajadores y pérdidas de productividad.

2.3 MÉTODOS PARA DETENER OCIO CIBRERNÉTICO

Para Wang, Tiang & Shen (2013), existen dos métodos comunes para detener o prevenir el cyberloafing: 1) Políticas internas para el correcto uso del internet y 2) Monitoreo electrónico. Las políticas internas varían de acuerdo a las organizaciones, las cuales deberían bastar para desalentar o prevenir el uso inadecuado del recurso internet. Las políticas del correcto uso de internet deben estar incluidas entre los valores de la organización. Dichas políticas deben ser explicadas y detalladas a los trabajadores, junto a los otros códigos de conducta internos, donde se indique expresamente que el uso del internet es para uso comercial, investigativo, financiero entre otros temas relacionados a la actividad laboral. También, se debe aclarar que toda organización tiene el pleno derecho a monitorear toda actividad en internet, incluyendo los correos electrónicos.

En cuanto a los métodos electrónicos de monitoreo y prevención, existe infinidad de mecanismos para bloquear el acceso, total o parcialmente, o simplemente monitorear las actividades de los empleados. Una de las más sencillas y económicas, de acuerdo a Longe & Longe (2005), sería la instalación de software de filtrado web en cada una de las computadoras de una organización. Estos programas previenen el contenido web no deseado y funcionan de acuerdo a la detección de ciertas palabras clave, las cuales son identificadas y relacionadas con el sitio que se visita, con el fin de no bloquear sitios web no relacionados con la temática que se desea filtrar. Ejemplo: bloquear pornografía y no bloquear sitios educativos o médicos.

Otro mecanismo válido, pero no tan efectivo, consiste en solicitar al proveedor de servicio de internet que bloquee el tráfico indeseado. La ventaja de este método radica en que se reduce la gestión del personal de sistemas o del empleador a cambio del cobro de un valor mensual. Sin embargo, se tiene una gran desventaja: No se tiene control del contenido o del tipo de filtrado. Los proveedores de internet básicamente bloquean contenido pornográfico. Y si se desea agregar otras categorías específicas para bloquear, es posible que este método no sea el más adecuado (Saxena, 2013)

Se puede usar soluciones más avanzadas y centralizadas con firewalls o en los ruteadores para prevenir acceso a ciertos sitios web. Si la organización posee equipamiento cisco o similares, es posible filtrar tráfico indeseado de entrada

con la aplicación de listas de acceso o ACL (Hochmuth, 2002) . La gran mayoría de las empresas posee firewalls y proxys servers basados en Linux. La opción más versátil de filtrado web y, por ende, más extendida por el mundo es la opción de firewall por medio de netfilter/iptables, las cuales son soportadas por todas las distribuciones actuales de Linux. Dicha solución está pensada para pequeñas y medianas organizaciones con personal IT limitado. (Martínez Molina, Pacheco Meneses, & Zúñiga Silgado, 2009).

Para los casos de proxy servers basados en Linux, se tiene la opción de instalar los paquetes Squid Guard o Dans Guardian, los cuales ofrecen un sinnúmero de opciones como el re direccionamiento de sitios web, un registro de sitios visitados y recurrentes, filtrado por frases o palabras clave, filtrado por IP mediante el uso de listas negras, entre otros. Estos paquetes son open source para usos no comerciales. En caso que se desee dar uso comercial, tanto para Squid como para Dans, se debe comprar una licencia directamente con el desarrollador. (Saxena, 2013)

2.4 POSTURAS A FAVOR DEL OCIO CIBERNÉTICO

Existen muchos estudios que tienen una visión distinta del ocio cibernético. En unos casos, es visto de forma positiva y en otros, como una señal de sucesos internos que deben ser atendidos de forma inmediata. El cyberloafing puede ser muy constructivo cuando ayuda a los empleados y a las organizaciones, sin embargo, puede ser muy perjudicial cuando evita que los empleados sean productivos (Ozler & Polat, 2012).

En términos generales, basados en investigaciones sobre las desviaciones de conducta en los lugares de trabajo, evidencia empírica sugiere que los empleados tienden a tener mala conducta cuando son tratados injustamente o cuando sus cargas laborales están desbalanceadas. El uso inadecuado del internet, es en definitiva una alerta clara de que algo está ocurriendo al interior de una organización. (Lim & Chen, 2002). Para Henle & Blanchard (2008), el cyberloafing constituye un buen mecanismo para lidiar con situaciones estresantes en los sitios de trabajo. Sin embargo, si el mal uso del internet se vuelve constante, es posible que los empleados tengan problemas internos o conflictos de roles. Para los mismos autores, una organización que detecta cyberloafing debe inmediatamente aplicar medidas anti estrés para sus empleados y corregir cualquier problema interno.

Por el contrario, el cyberloafing que se produce con moderación, el cual consiste en pasar breves períodos de tiempo en actividades no relacionadas al trabajo, puede generar una importante válvula de escape al aburrimiento, la fatiga, el estrés. También se produce un incremento en la satisfacción en el trabajo, incremento en la creatividad, y en términos generales, se tendría empleados más felices. (Ozler & Polat, 2012).

Una buena medida para disminuir el abuso del internet y el cyberloafing podría ser incrementar la carga laboral. Empleados ocupados incurrirán con menor frecuencia a cometer cyberloafing. Sin embargo, se debe tener cuidado con la carga laboral que se le impone al empleado; ya que puede ocasionar una importante elevación del estrés, lo cual llevaría nuevamente al empleado a incurrir en cyberloafing. (Henle & Blanchard, 2008)

Messarra et. al. (2012) indican que eliminar bruscamente el internet de las organizaciones puede traer consecuencias muy negativas. Cuando se limita o elimina el acceso a internet en una organización, disminuirá la moral de los empleados. Por una parte, los empleadores sienten que se desperdicia tiempo y recursos. Y los empleados, en cambio, no aceptan la idea de ser monitoreados y controlados. Lim & Chen (2012) sostienen, mediante un estudio realizado en Singapur por medio de encuestas, que los empleados creen que el ciber ocio les ayuda a hacer mejor su trabajo y que, por el contrario, si se aplican restricciones, volvería menos interesante su trabajo.

Whitty (2004) afirma que usar internet para propósitos privados es algo muy cotidiano. Equivale a usar el teléfono como modo de comunicación. Dado que el teléfono o el email comparten similitudes en cuanto a su uso en las organizaciones, se puede establecer una analogía con el recurso internet de las organizaciones, el cual puede ser utilizado brevemente para usos privados en los sitios de trabajo sin ninguna afectación a la productividad.

CONCLUSIÓN

El trabajo realizado demuestra que el ocio cibernético es un hecho real que tiene muchos factores de origen y muchas maneras de ser evitado. Sin embargo, luego de analizar las posturas en contra, dando cifras y enumerando los problemas que enfrentan las organizaciones, versus los posibles beneficios

que trae a los empleados, se concluye que la práctica de ocio cibernético no debe evitarse por completo. La afectación a la moral de los empleados y la sensación de sentirse vigilados, puede crear un efecto contrario al esperado. Aplicando las soluciones tecnológicas descritas, se puede bloquear el acceso a sitios potencialmente peligrosos, que contengan pornografía, juegos en línea, descargas ilegales de material audiovisual con derechos de autor, entre otros. Y permitir el acceso al contenido restante. Adicional a esto, la redacción de una política de uso de internet en las organizaciones complementaría la tarea, manteniendo a los empleados informados, capacitados y advertidos de posibles sanciones en caso de detección de abuso del internet para fines no relacionados al trabajo.

Cabe resaltar, que, aunque el tema del ocio cibernético no ha sido tratado tan ampliamente, se encuentra mucha literatura desarrollada especialmente por psicólogos y profesionales expertos en recursos humanos quienes tratan el tema y lo desarrollan en función de sus áreas; tratando de explicar el por qué se da el ocio y las formas de medirlo mediante encuestas. La información técnica relacionada al tema es escasa. Los métodos tecnológicos son múltiples y muy variados, pero no existe un mecanismo especializado para cyberloafing. El bloqueo, filtrado y monitoreo son funciones genéricas de muchos firewalls, proxys y ruteadores. En este sentido, y es deber de cada organización, aplicar las medidas necesarias o hacer caso omiso y permitir el cyberloafing sabiendo que puede la omisión a este problema, puede traer consecuencias como las descritas en este artículo.

REFERENCIAS BIBLIOGRÁFICAS [1]

[1] García-Cueto, E., & Cerro, V. (1990). Características individuales y tipo de ocio. Psicothema, 173-177.

Gunia, B., Corgnet, B., & Hernan-Gonzalez, R. (2014). Surf's Up: Reducing Internet Abuse without demotivating employees. Academy of Management Annual Meeting Prodeedings, 932-937.

Henle, C., & Blanchard, A. (2008). The Interaction of Work Stressors and Organizational sanctions on Cyberloafing. XX(3), 383-400.

Hochmuth, P. (2002). Cisco steps up LAN security efforts. Network World, 19, 10.

Johnson, P., & Indvik, J. (2003). The organizational benefits of reducing cyberslacking in the workplace.

Lim, V. K., & Chen, D. J. (2012). Cyberloafing at the workplace: gain or drain on work? Behaviour & Information Technology, 243-253.

Lim, V., & Chen, D. (2002). The IT way of loafing on the job: Cyberloafing, neutralizing and Organizational Justice. Journal of Organizational Behavior, 675-694.

Longe, O. B., & Longe, F. (2005). The Nigerian Web Content: Combating Pornography using Content filters. Journal of Information Technology Impact, 59-64.

Manrique De Lara, P. Z. (2007). Relationship between Organizational Justice and Cyberloafing in the workplace: Has "anomia" a say in the Matter?

Martínez Molina, K. J., Pacheco Meneses, J., & Zúñiga Silgado, I. (2009). Firewall - Linux: Una solución de seguridad informática para PYMES (pequeñas y medianas empresas).

Messarra, L. C., Karkoulian, S., & McCarthy, R. (2011). To restrict or not to restrict personal internet usage on the job. Education, Business and Society: Contemporary Middle Eastern Issues, 253-266.

Ozler, D. E., & Polat, G. (2012). Cyberloafing Phenomenom in Organizations: Determinants and impacts.

Saxena, S. (2013). Content Filtering using Internet Proxy Servers.

Wang, J., Tian, J., & Shen, Z. (2013). The effects and moderators of cyber-loafing controls: an empirical study of Chinese public servants.

Whitty, M. (2004). Should filtering software be utilised in the Workplace? Australian Employees Attitudes toward internet usage and Surveillance of the Internet in the Workplace.

Young, K., & Case, C. (2004). Internet Abuse in the workplce: New Trends in Risk Management.