Maestría Profesional en Gerencia de Proyectos

Proyecto de Integración

Proyecto Final
Gestión de Riesgos y La Ciberseguridad
Para Proyectos Tecnológicos

Profesora: Vanessa Zamora González.

Estudiante: Rebeca López Sequeira

2016

Gestión de riesgos y la ciberseguridad para proyectos tecnológicos

Resumen

Los avances en las nuevas infraestructuras tecnológicas como el *Internet of Things, Big Data* y el *Cloud Computer* agilizan el desarrollo de herramientas y aplicaciones de uso general para todos los usuarios de la red. Es por esta razón que la investigación del proyecto se enfocó en probar porque es importante la integración de la ciberseguridad en la gestión de riesgos. La justificación se basa en la falta de regulaciones estrictas, para aquellos usuarios que violentan la privacidad y roban datos importantes. Los resultados obtenidos por medio de la encuesta realizada ponen en evidencia la poca información con la que cuentan los usuarios, para asegurarse de obtener un beneficio tecnológico seguro, las conexiones que existen entre las herramientas son cada vez más, y la gran cantidad de servicios disponibles que requieren gestionar los riesgos e incorporar la ciberseguridad con el fin de resolver efectivamente los problemas de seguridad en la red. Por otra parte, se recomienda a todos los usuarios ser precavidos y asegurarse de entender las políticas de privacidad de las herramientas que utilizan, así mismo es importante tomar conciencia de que el desarrollo tecnológico es una gran ventaja que involucra la seguridad como riesgo.

Palabras Claves: Gestión de Riesgo, Ciberseguridad, Ataques, Desarrollo, Tecnología.

Abstract

Latest progress in new technology infrastructures such as the Internet of Things, Big Data and Cloud Computer speed up the development of tools and applications commonly used for all network users. This is the reason why this pushed the investigation of my project was committed to be focused on demonstrating the importance of cybersecurity integration into risk management. The lack of strict regulations for users who violate privacy and steal data has been part of the defense of the project. The results achieved by the survey clearly showed how users are not well informed about how they can safely take advantage of technology. Tools are linked each other more often, and there is a vast choice of available services that require the incorporation of risk management and cybersecurity with the objective of resolving in an effective manner, cyberspace security problematic. Likewise we recommend all users to be alert and make sure they understand

the privacy policies that applications and tools frequently use. It is essential to create awareness that technological development is a great benefit that involves security risks.

Key Words: Risk Management, Cybersecurity, Attack, Development, Technology.

Introducción

A partir de 1990 cuando el internet se incorpora a una sociedad la cual desconocía los efectos positivos y negativos que nacerían a partir de este momento histórico, los proyectos tecnológicos surgen para marcar una nueva era mundial, por lo que las necesidades de las personas, la industria y el comercio se establecieron a partir de la red. Por otra parte, los avances en la seguridad de los sistemas apenas toman fuerza durante los últimos diez años, ya que se han convertido en un punto clave e importante dentro de la infraestructura tecnológica. Una de las razones por las que la seguridad emerge en la red, es porque las amenazas que surgen en esta, desarrollaron un esquema de ataque mucho más inteligente que el de sus inicios, por lo que deben ser tratadas bajo una estrategia de seguridad capaz de monitorear, detener y prevenir cualquier vulnerabilidad en los sistemas.

A pesar de los esfuerzos por alcanzar una plataforma discreta con un enfoque integrado de seguridad, se siguen encontrando fallos de seguridad en el desarrollo de los proyectos, es por ello que la gestión de riesgos y la ciberseguridad requieren unificarse y resolver los problemas de infraestructura.

En este proyecto de investigación se analizará la problemática actual en la ciberseguridad y el impacto a los consumidores, las compañías y el gobierno debido a las prácticas ilegales en la red, también como la gestión de riesgos se trabaja sin considerar la seguridad en la red como su principal riesgo.

Justificación del Trabajo

La investigación científica se basa en como la gestión de riesgos y la ciberseguridad requieren ser combinadas para todos los proyectos tecnológicos, con el propósito de mitigar o eliminar los riesgos asociados con fallas debido a la deficiente infraestructura desarrollada y que por ende, afectan de manera negativa a los clientes, las empresas y los gobiernos.

Problema de Investigación

El problema que se ha observado es que la red se ha convertido en un espacio sin límites y por ello no puede ser explorada del todo. Las políticas o las leyes de cada país desean controlar la red, sin embargo, esto es solo una medida para sancionar las prácticas criminales que atentan con la seguridad en los datos. La raíz del problema se debe a que los proyectos tecnológicos utilizan la red como una herramienta de código abierto para generar mejores productos con múltiples características, sin antes evaluar los riesgos que conllevan estos nuevos sistemas.

El Cloud computer, Internet of Things, Big Data Systems son solo algunos ejemplos de cómo se ha avanzado para utilizar de forma eficiente y precisa la red, pero esto no significa que la seguridad en estos sistemas esté en las mejores condiciones, más adelante se va a explicar con ejemplos como es que los sistemas al servicio del público ocasionan pérdidas en las empresas por desconocer el tema de seguridad u omitir el riesgo por una plataforma tecnológica deficiente.

¿Debe la ciberseguridad ser incluida en la gestión de riesgos para los proyectos tecnológicos?

Objetivos de Investigación

Objetivo General

Investigar la razón por la que la gestión de riesgos y la ciberseguridad se deben integrar en el desarrollo de los proyectos tecnológicos.

Objetivo Específicos

- ✓ Identificar por qué la gestión de riesgos y la ciberseguridad son importantes en los proyectos tecnológicos, con el fin de mejorar la seguridad de las herramientas en línea.

- ✓ Definir la situación actual de la seguridad en la red en diversas soluciones o herramientas tecnológicas, con el fin de presentar evidencia de cómo los usuarios no conocen los riesgos de la red.
- ✓ Identificar los riesgos altos que se presentan en las plataformas y los servicios de la red, con el fin de brindar una mejor seguridad a los usuarios.
- ✓ Determinar la importancia de la seguridad frente a los ataques y las amenazas, con el fin de educar a los usuarios en la utilización correcta de las plataformas tecnológicas.

Revisión Bibliográfica

Los ciberataques son la principal razón por la que algunas empresas como Sony Picture Entertaiment decidieron transferir sus riesgos de la plataforma por medio de una póliza de seguro, es decir están admitiendo que sus debilidades de infraestructura no pueden ser eliminadas a corto plazo, por lo que prefieren evitar demandas o cuestionamientos por medio de su seguro. De ninguna manera están resolviendo su problema de raíz, pero al menos están conscientes de que la ciberseguridad es un elemento importante en su empresa por lo tanto, sus próximos proyectos van a resolver muchos de sus actuales problemas de seguridad. (Van Den Gregory, 2015).

El desarrollo en el área de Internet of Things (IOT) es realmente impresionante y sus beneficios en una sociedad sin criminales cibernéticos sería aún más extraordinaria, pero no es la realidad que vivimos, es un hecho que más y más los ataques cibernéticos aumenten. Por lo que la seguridad en esta área necesita ser muy precisa y proactiva. (Herrero Alcántara, 2016)

McAfee Labs de *Intel Security* publicó un informe donde predice lo que va a pasar con el tema de seguridad para todos aquellos dispositivos que almacenan datos y los nuevos servicios en la nube, el panorama no es el mejor, y aporta otro elemento importante, la integridad de los datos. Este será fuertemente atacado, afectando principalmente los sistemas financieros. Algunas medidas o sugerencias preventivas son el intercambio de inteligencia entre las empresas y proveedores de servicios para proteger mejor la industria. (Gómez, 2015)

En cuanto al área de la seguridad en la nube, dado que se mencionó anteriormente es importante entender porque este nuevo servicio es el blanco perfecto para los ataques. El *Cloud Computing*

ofrece una variedad en la profundidad de datos debido a su flexibilidad y capacidad de espacio en el almacenamiento virtual, a diferencia de un servidor normal o una base de datos, estos tienen un límite de espacio y al mismo tiempo, restringe al usuario en cuanto a los *bytes* de memoria por registro, por el contrario la nube ofrece un servicio dinámico y con fácil acceso, en cuanto a espacio sus costos son altos, pero mientras puedan ser pagados no es un problema, ahora bien la seguridad sí es un tema de discusión, a pesar de que tenemos diferentes tipos o categorías de seguridad entre ellos: la física, respaldos, desarrollo e interfaces estándar y elasticidad. (Dekker Dimitra, 2015)

Los proyectos tecnológicos que incorporen una solución basada en Big Data incrementan el número de usuarios conectados en la red así como el volumen de datos no estructurados que pueden ser procesados dadas las cualidades que ofrece Big Data. La seguridad en esta solución está cambiando, se ha creado una relación con los datos históricos almacenados y las posibles amenazas. (Rossen, 2015)

La tecnología actual se ha vuelto una herramienta muy útil para facilitar los procesos en muchas áreas de la vida, por eso es fundamental que los expertos en ciberseguridad aconsejen y apoyen la idea de que los riesgos a los que nos enfrentamos no son sencillos de manejar, pero las alternativas y desarrollo de nuevas soluciones pueden generar la defensa necesaria para combatir las amenazas en la red. (Manuel Fernández, 2016)

Actualmente la Unión Europea estableció una serie de procesos o procedimientos en materia de seguridad las cuales deben ser adoptadas por aquellas empresas públicas y privadas que utilicen la red para el uso comercial. La idea principal de este tipo de medidas busca hacer conciencia de la importancia en el uso de la tecnológica y como estas dominan el mundo y los que habitan en él. Claramente no es un asunto factible sin la ayuda de los gobiernos y el apoyo de los usuarios (Consejo de la Unión Europea 2016).

Por otra parte América Latina se ha dedicado a implementar los principios del Convenio de Budapest contra el delito cibernético, también surgió la propuesta de mejorar la higiene cibernética, esta consiste en culturizar a las personas y a las empresas para que aprendan a defenderse de futuros ataques. La OEA y el BID se esfuerzan y luchan contra la delincuencia

cibernética promoviendo estrategias sostenibles. Lamentablemente no todos los países se unen a esta campaña por lo que el alance se limita a unos pocos. (Lewis, 2016).

Metodología de la Investigación

De acuerdo con los objetivos planteados anteriormente, la metodología de investigación que se va trabajar es la investigación no experimental descriptiva cuantitativa, esta va a permitir establecer patrones o variables de cómo la tecnología ofrece recursos o herramientas con escasa seguridad.

El diseño de la investigación está basado en el comportamiento de los clientes frente a las nuevas tendencias tecnológicas y cómo las anteriores se han convertido en un estilo de vida. A pesar de los ciberataques, el desarrollo de nuevas tecnologías no se ha visto afectado y cada vez son más las plataformas que ofrecen nuevos productos y servicios a los clientes.

La unidad de trabajo es delimitada a una cantidad que permitió relacionar aquellas características con la investigación, por lo que la muestra es no probabilística. Hernández; Fernández y Batista. (2010). Se trabaja por medio de una encuesta a un grupo específico de usuarios, esto porque se debe enfocar en aquellos clientes o participantes activos de la red y sus productos.

Los datos recolectados se basarán en los resultados obtenidos en la encuesta realizada, como se mencionó antes, la muestra seleccionada es tomada de un grupo de usuarios que con certeza utilizan la infraestructura de *Big Data, Internet of Things* y la nube en sus actividades diarias.

Como parte de los requisitos de la medición de datos están la confiabilidad, la validez y la objetividad, en el caso de esta investigación se utilizaron los requisitos anteriores para garantizar que los resultados tengan una relación lógica con lo que se quiere analizar. Debido a esto los datos mostrarán cómo la seguridad tecnológica es importante para los usuarios de la red.

La estructura de la encuesta se realizará tomando en cuenta preguntas cerradas o limitadas, es decir con respuestas previamente dadas las cuales serán elegidas por el participante, de igual manera se incluyen preguntas abiertas, con la finalidad de recibir otras opciones a la interrogante. El contenido de la entrevista se desarrolló tomando en cuenta cinco áreas de la tecnología que la mayoría de las personas utilizan en la actualidad:

1. La familia: las redes sociales se enfocan en las relaciones personales, los usuarios las utilizan como medio para darse a conocer y estar en contacto con sus familiares, por medio de fotografías, mensajes públicos o privados.
2. El trabajo: los chats, los servicios en línea, los buscadores, son solo algunas de las herramientas con las que se cuenta para transferir datos, encontrar información y realizar transacciones.
3. El dinero: las transacciones en línea como transferencias, los envíos y el recibo de dinero, los negocios, las consultas por medio del chat en línea de los bancos, entre otros.
4. La salud: relojes inteligentes, móviles y sensores para obtener datos de la presión arterial, la temperatura, algunos incluyen un dispositivo para medir el azúcar de la sangre, entre otros.
5. El entretenimiento: aplicaciones, compras en línea, TV, transporte entre muchos otros elementos que se ofrecen para pasar el tiempo y disfrutar, ya sea en grupo o en forma individual.

Lo anterior es solo un ejemplo de cómo los usuarios de la red utilizan la tecnología en sus vidas, por lo que la entrevista se enfocó en validar este hecho y mostrar el porqué la ciberseguridad es un elemento importante y clave en el desarrollo de los proyectos tecnológicos.

Resultados

La encuesta se realizó desde el día 15 hasta el 26 de agosto del 2016, el período se estableció en dos semanas con el fin de permitirle a los encuestados tomar su tiempo, de igual manera lograr obtener la mayor cantidad de respuestas posibles y generar más datos para el análisis.

Esta encuesta se planeó para que un total de ochenta y cinco personas enviaran sus respuestas, sin embargo se recibió solamente la contestación de sesenta y siete personas, es decir un 79% de 100% de la muestra. El grupo seleccionado para la encuesta es de mi trabajo, un departamento de ingenieros en sistemas, ingenieros industriales y administradores, con una mezcla de generaciones, en la mayoría X, *milenials* y algunos *baby boomer*. El único elemento en común que tenemos todos es que trabajamos en el área de informática lo cual hace aún más interesante conocer sus puntos de vista y opiniones con respecto al tema de la ciberseguridad.

La encuesta se realizó de dos maneras distintas, una de ellas fue el envío de la misma por medio de un link a los correos, y la otra fue entregar la encuesta impresa y dejarlos terminar las respuestas, esto porque a algunas personas no les gusta realizar encuestas en línea y otras, sí lo desean así.

La encuesta consta de doce preguntas, entre ellas diez conformadas por preguntas cerradas y solamente dos abiertas, la idea principal de hacerlo de esta manera es porque se obtienen datos extras acerca de qué tanto conocen las personas de los riesgos en la ciberseguridad.

También se recuerda que la encuesta se hizo tomando en cuenta cinco áreas en las que la mayoría de personas se relacionan con la tecnología, por lo que los datos obtenidos reflejan una realidad en el uso de las herramientas de la red.

La primera pregunta es relacionada directamente con el uso de las redes sociales y cómo los usuarios comparten datos e información personal, el 82% de los personas admitieron que efectivamente utilizan la red social como un medio para publicar datos personales, fotografías e incluso sus gustos o preferencias, el otro 18% no lo hace así, podría ser por privacidad y seguridad de su información.

En la siguiente pregunta se quería analizar qué tanto conocen los usuarios de la red sobre la vulnerabilidad en la seguridad y cómo los ciberataques son una realidad en la red. Los resultados fueron que el 73% de los encuestados sí conocían que las redes son enfrentan al menos un millón de ciberataques diarios y solo un 27% no lo sabía, esto quiere decir que una gran parte de los usuarios sí entienden los riesgos que conlleva el compartir datos en la red. En relación con esta pregunta y para darle seguimiento, se quería saber por qué debería ser importante para los usuarios conocer esta información, el 93% contestaron que les concierne porque sus datos al ser robados podrían usarse en su contra para una futura extorsión o robo de dinero, ahora bien el 7% respondió que no sabía qué era un ciberataque, esto último me pareció preocupante, ya que esta palabra si bien es cierto es de la actualidad, existe mucha información al respecto y se debería considerar como un tema de conocimiento universal. Desde otro punto de vista, permitió deducir que siempre habrá una parte de la población de usuarios que no entienden este concepto, sea por educación o bien por desinterés acerca del tema.

Las preguntas número cuatro y cinco están enfocadas en conocer si los encuestados utilizan las plataformas bancarias para hacer consultas, transacciones u otros. El 91% asegura que sí las usan,

ya que es un servicio eficiente, rápido y se ahorran el tiempo de trasladarse a una sucursal bancaria, hacer fila, esperar y finalizar exitosamente el trámite. El otro 9% no ha utilizado la plataforma, ya que no la consideran segura. Revisando las respuestas dadas, se tienen muchos beneficios al usar las plataformas bancarias, los bancos privados y estatales proporcionan la facilidad o el servicio. Desde el punto de vista de los bancos, es menos costoso tener una plataforma bancaria donde se generen transacciones y consultas, que el contar con personal extra en sus bancos haciendo los trámites. Los costos de personal fueron reemplazados por tecnología en otras palabras, esto no quiere decir que se deba descuidar la seguridad de la red, más bien se deben aumentar los esfuerzos para garantizar plataformas seguras y estables para los clientes.

Posteriormente, se evaluaron tres preguntas en cuanto a la mensajería instantánea y su uso en el área del trabajo, al ser una herramienta de fácil manejo, con un tiempo real de envío y recibido, sin costo o si lo tiene es muy bajo en comparación con una llamada, se ha convertido en el medio predilecto de comunicación de todos. El 91 % respondió que sí pertenece a grupos de trabajo creados desde la mensajería, el 9% no lo hace. Por otra parte a la pregunta de que si comparten información del trabajo por la misma vía el 86% dijo que no lo hacen y un 14% al contrario, sí la utiliza con ese fin. Con estos resultados podría ser contradictorio el pertenecer a un grupo de trabajo, si no se habla de información del mismo, el 80% explicó que no comparten datos porque conocen las políticas de confidencialidad de la empresa, sin embargo esto no significa que las sigan como debería ser, me parece sin sentido estar en un grupo del trabajo si no se habla de trabajo, es decir con qué propósito pertenecerían a un grupo de trabajo. Este punto lleva a la conclusión de que no se debería pertenecer a grupos del trabajo, primero se evitarían problemas con la fuga de la información, los empleados no serían amonestados por parte de los superiores, aparte si la mensajería instantánea no es propia de la empresa de trabajo no deberíamos ser obligados a pertenecer a la misma en los grupos de trabajo.

Nuevamente se retoma el tema de los datos personales esta vez para compras de artículos o servicios en línea, el 86% de los encuestados sí efectúan compras en línea, por esta razón comparten sus datos de números de tarjetas en un cien por ciento. La gran mayoría salva su información en las bases de datos de las tiendas en línea favoritas. A la pregunta de qué tanto conocen acerca la seguridad de dichas páginas, el 63% no tenían la menor idea al respecto, o sea no leen los términos y las condiciones que deben ser aceptados *a priori* para una compra, omiten

el hecho de que sus números de tarjetas pueden ser robados, para posteriormente ser usados de manera ilegal en cualquier parte del mundo. Este dato es realmente preocupante si no conocemos el riesgo que se toma como usuarios y el de las tiendas en línea.

Por último se quería conocer si los encuestados utilizan aplicaciones o relojes inteligentes para almacenar sus datos de salud, como por ejemplo su ritmo cardíaco, el 76% contestó que no y el 24% sí los usan. En este caso es probable que con el paso del tiempo aumente el número de usuarios que utilicen esta tecnología, aunque el resultado obtenido tampoco es bajo.

Conclusiones

En el presente trabajo se planteó como objetivo identificar por qué es importante la gestión de riesgos y la ciberseguridad. Efectivamente se comprobó por medio de la encuesta, los usuarios de la red comparten información privada tanto de su persona como de la familia, por varias razones:

1. Confían en la seguridad de la red que utilizan
2. Negligencia
3. Diversión o entretenimiento

La gestión de riesgos debería estar comprometida a mitigar o transferir dichas razones, a través de la ciberseguridad. Los resultados muestran la realidad en la que se vive. Los usuarios de la red compran en línea artículos o servicios, divulgan datos de su familia o trabajo al público, utilizan la libertad de expresión en las redes sociales, tienen un conocimiento escaso en el tema de la seguridad y el compartir información es solo uno de los puntos que ponen en riesgo su propia seguridad en la red.

Es por ello que las plataformas y la infraestructura tecnológica desarrollan gran parte de su esfuerzo en crear paredes de fuego o encriptación de datos. Lo cual no es suficiente para controlar el tráfico de datos, los virus maliciosos, y los grupos dedicados a crear ataques masivos.

En el futuro cercano se van a manejar el 95% de nuestras relaciones por medio de la red, esto sería desde la educación, las finanzas personales, la salud, el entretenimiento y la familia, el punto que une todos estos elementos será la red. Por esta razón la gestión de riesgos sirve para mostrar qué tan importante debería ser nuestra seguridad en las herramientas tecnológicas.

Recomendaciones

Las oportunidades para mejorar la plataforma tecnológica son infinitas, debemos como usuarios de las redes exigir una seguridad que no comprometa nuestra integridad. El futuro de la ciberseguridad es una área amplia y ciertamente difícil de manejar o controlar, sin embargo el identificar los riesgos a tiempo, permitirá generar confianza y estabilidad en el ambiente.

La responsabilidad de la seguridad en la red es compartida entre los usuarios y las empresas que lideran los mercados de la tecnología, por lo tanto las recomendaciones se pueden plantear de la siguiente manera:

1. Ninguna plataforma tecnológica es cien por ciento segura, esto significa que se debe hacer una campaña de educación para los usuarios.
2. Los ciberataques no se eliminan, por el contrario aumentan, por esta razón las empresas que desarrollan herramientas deben prepararse y mitigar los riesgos.
3. Los usuarios deben aprender a poner un límite en lo que comparten en las redes sociales.
4. El comunicar datos de trabajo por medio de mensajería instantánea podría tener como consecuencia una demanda y posteriormente, el encarcelamiento.
5. Comprar en línea es ventajoso siempre y cuando se conozcan los términos y las condiciones de las tiendas en línea.

Estas son algunas recomendaciones que se comparten, de acuerdo con los resultados de la encuesta, en general la gestión de riesgos es un elemento sumamente importante en el desarrollo de las aplicaciones y la infraestructura tecnológica. En la actualidad, los usuarios confían en que la tecnología brinda mayor valor agregado si se emplea en todas las actividades diarias, por lo que podría recomendar como punto final, no utilizar todas las plataformas de la red.

Anexos

Gráfico 1 Pregunta 1

Fuente: Elaboración propia

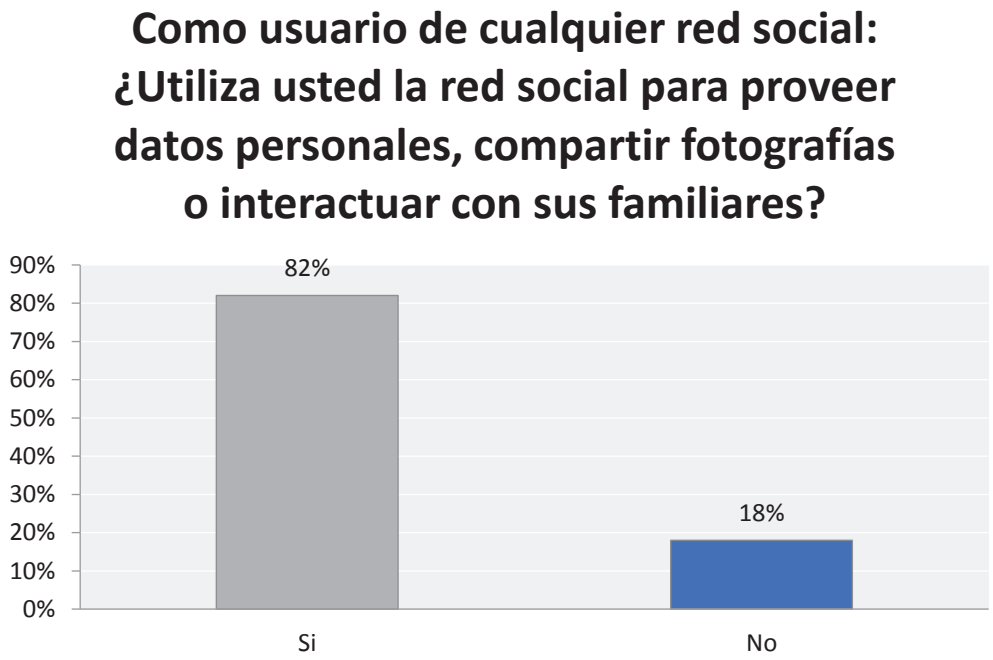
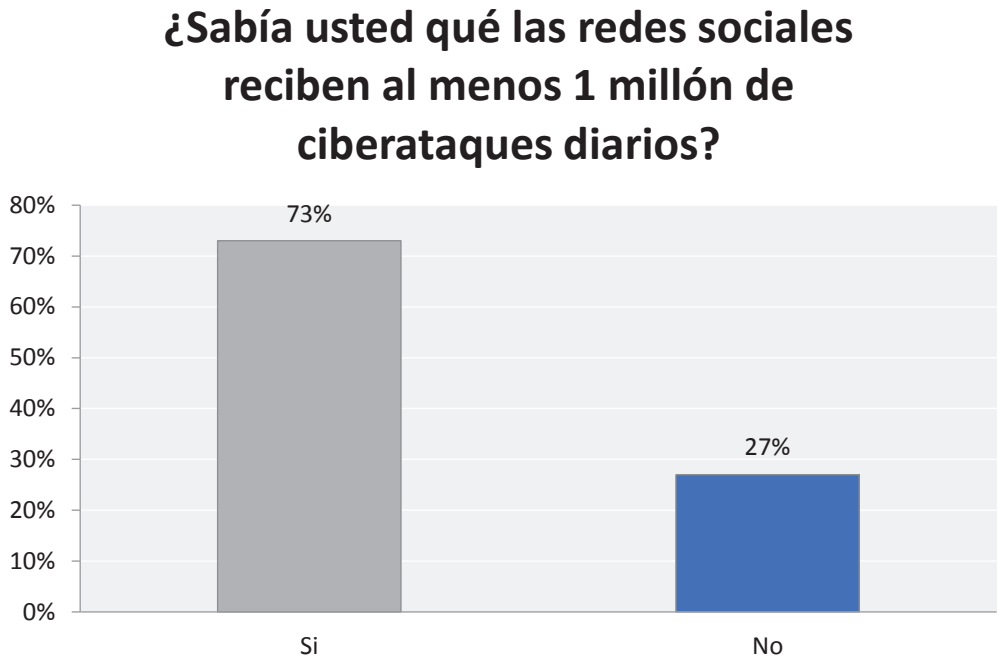
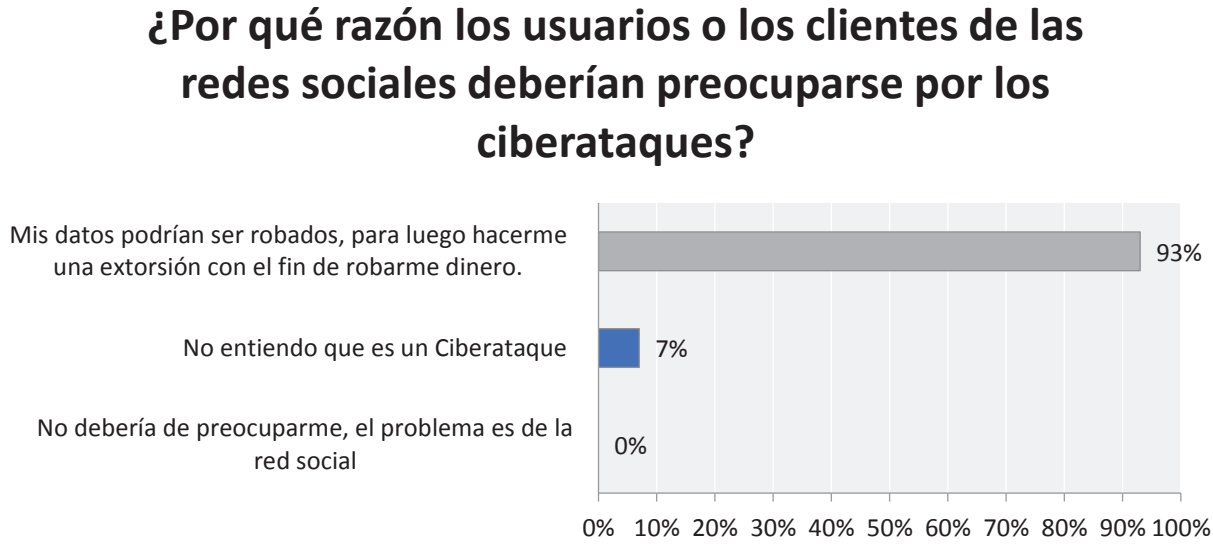


Gráfico 2 Pregunta 2



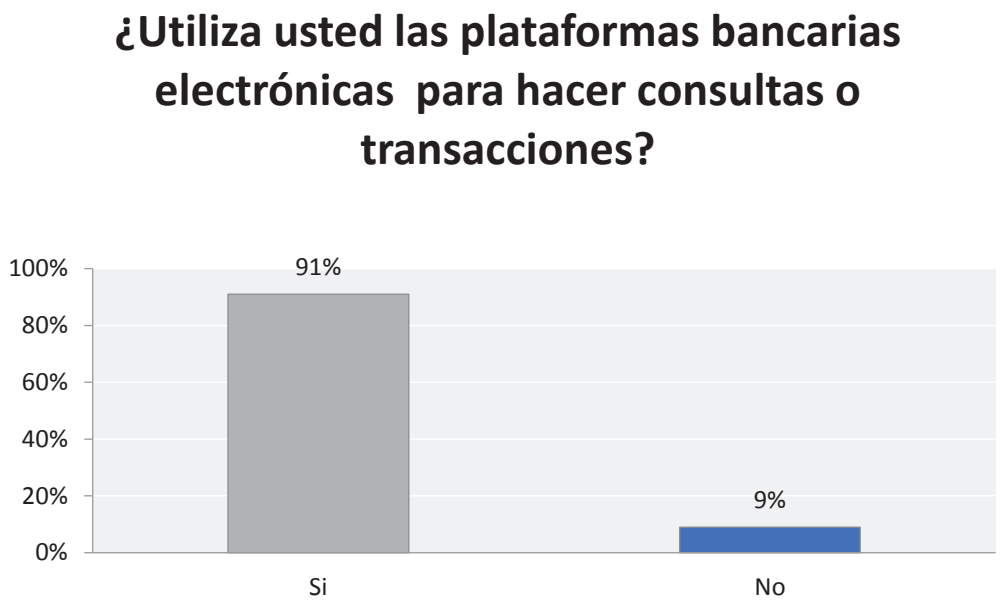
Fuente: Elaboración propia

Gráfico 3 Pregunta 3



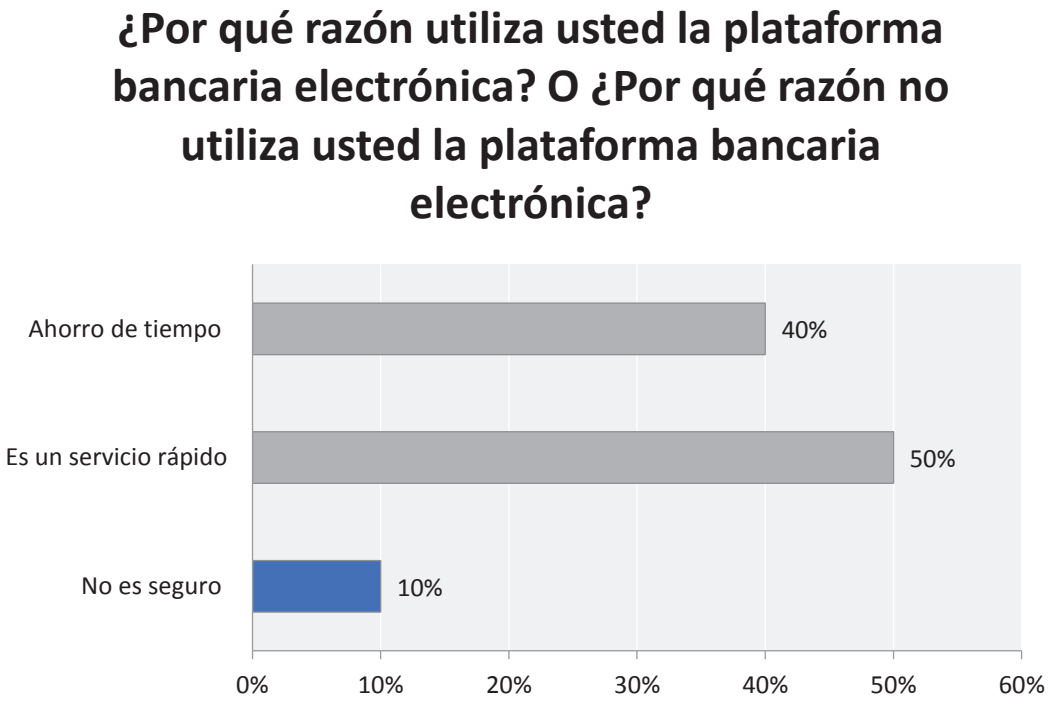
Fuente: Elaboración propia

Gráfico 4 Pregunta



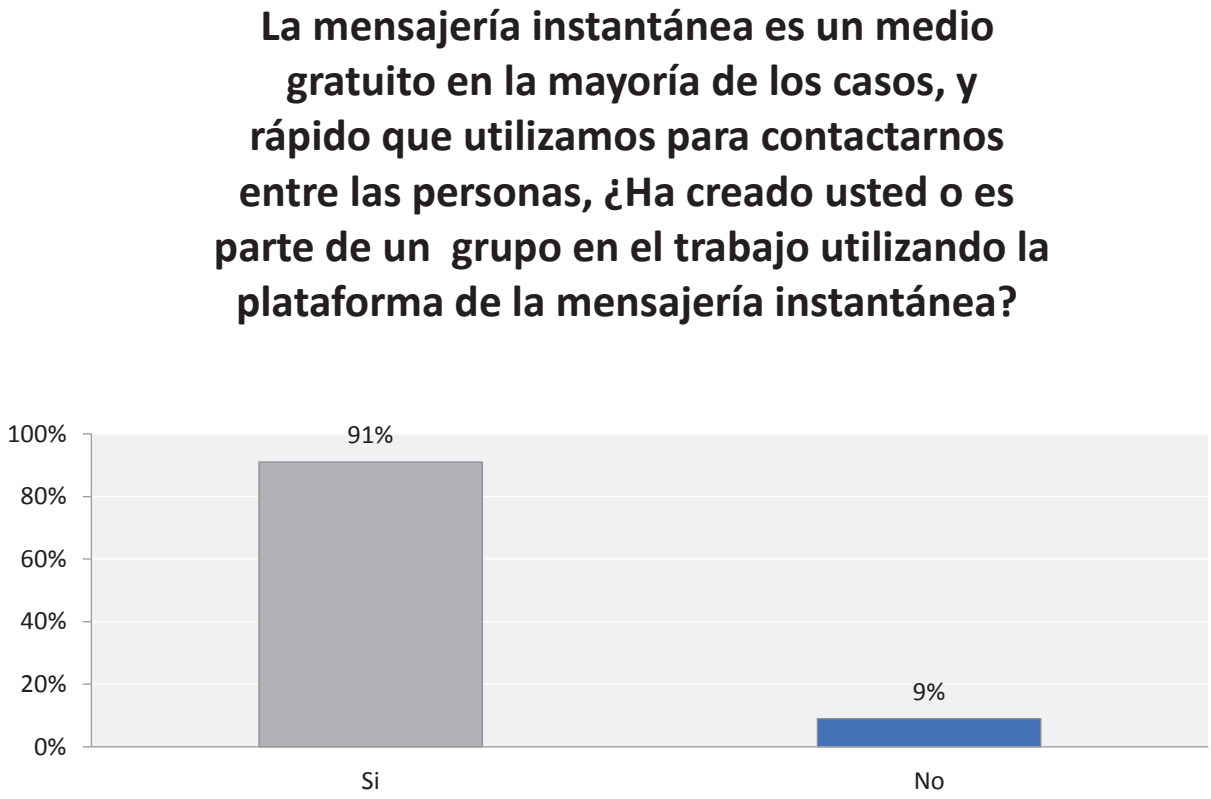
Fuente: Elaboración propia

Gráfico 5 Pregunta 5



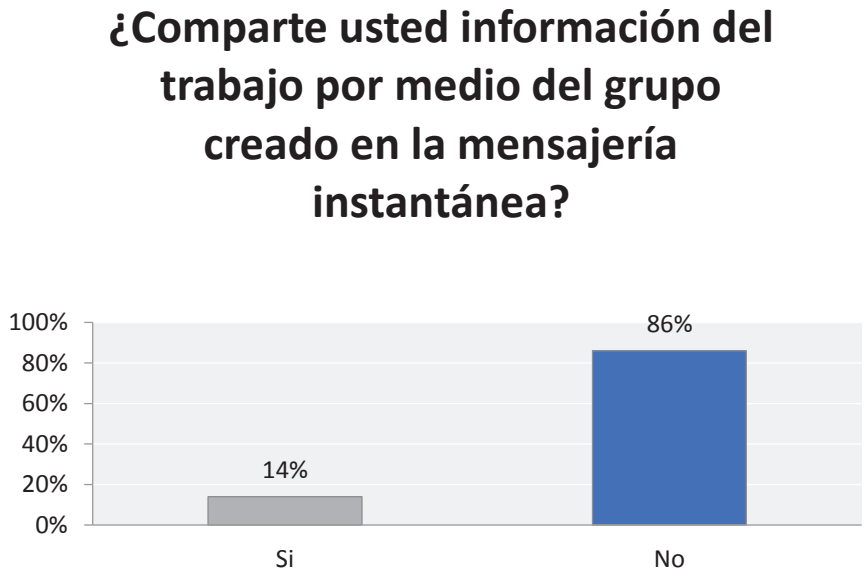
Fuente: Elaboración propia

Gráfico 6 Pregunta 6



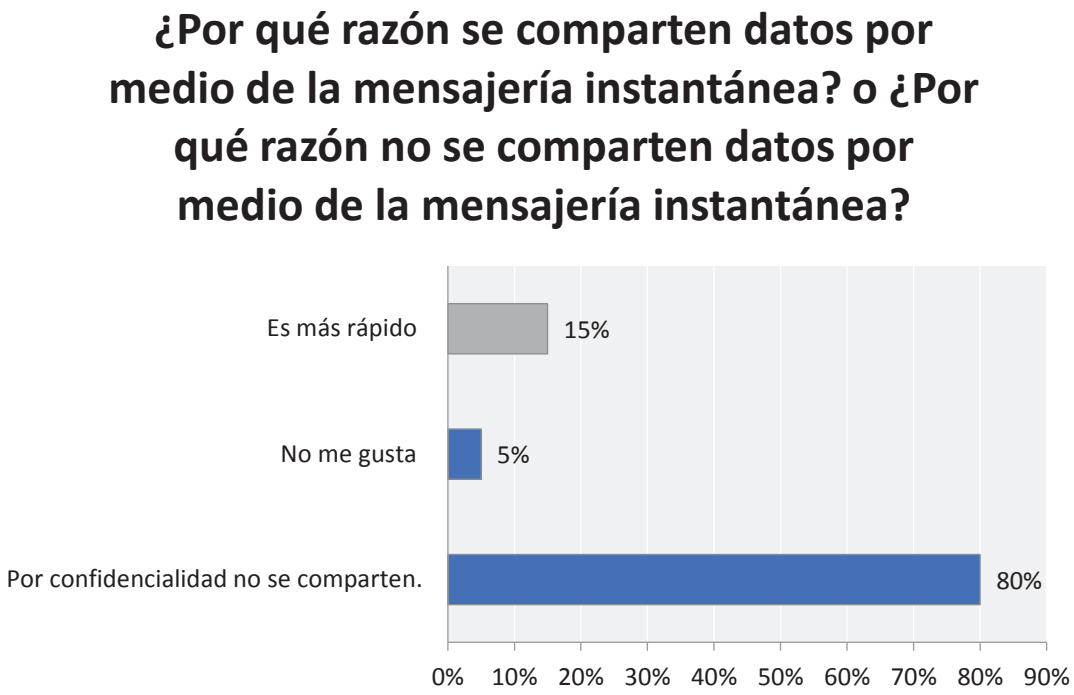
Fuente: Elaboración propia

Gráfico 7 Pregunta 7



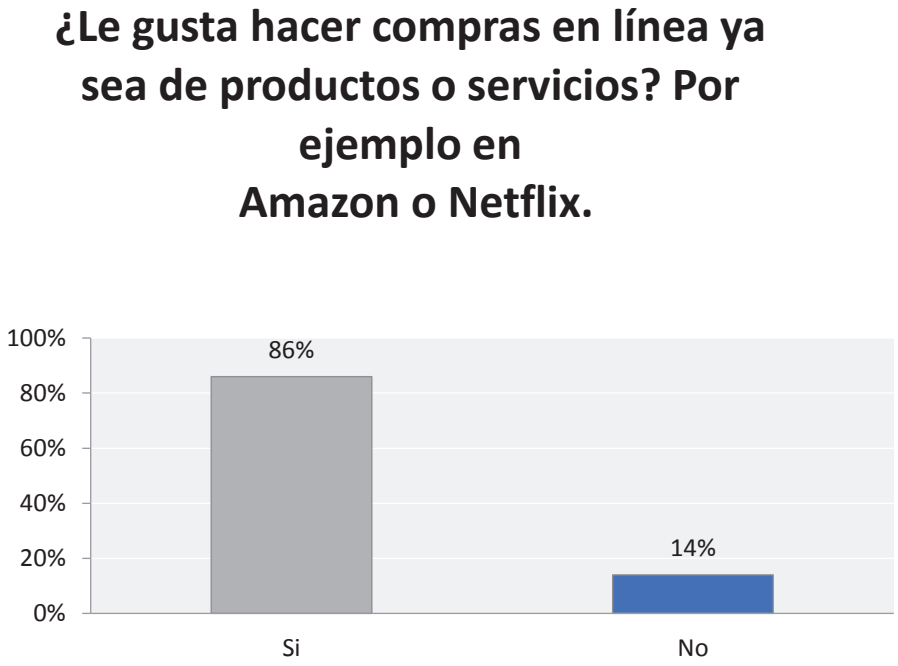
Fuente: Elaboración propia

Gráfico 8 Pregunta 8



Fuente: Elaboración propia

Gráfico 9 Pregunta 9



Fuente: Elaboración propia

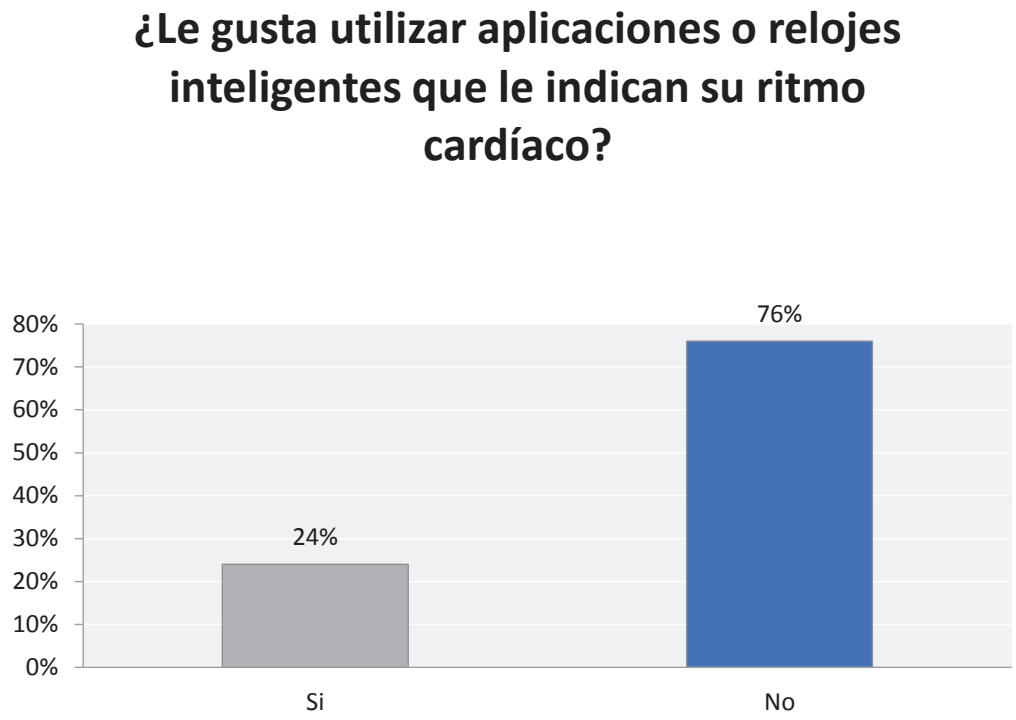
Gráfico 10 Pregunta 10

Fuente: Elaboración propia

Gráfico 11 Pregunta 11

Fuente: Elaboración propia

Gráfico 12 Pregunta 12



Fuente: Elaboración propia

Preguntas y formato para la encuesta

La presente encuesta se realiza con el fin de obtener datos por parte de los usuarios de la red, con el fin de analizar los comportamientos que los encuestados presentan utilizando distintas herramientas tecnológicas a su alcance.

1. Como usuario de cualquier red social: ¿Utiliza usted la red social para proveer datos personales, compartir fotografías o interactuar con sus familiares?
   a. Sí
   b. No

2. ¿Sabía usted que las redes sociales reciben al menos un millón de ciberataques diarios?
   a. Sí
   b. No

Si su respuesta es No pasar a la pregunta número 4

3. ¿Por qué razón los usuarios o clientes de las redes sociales deberían preocuparse de los ciberataques?
   a. No debería preocuparme, el problema es de la red social.
   b. No entiendo qué es un ciberataque
   c. Mis datos podrían ser robados, para luego hacerme una extorsión con el fin de robarme dinero.
   d. Otra razón _____

4. ¿Utiliza usted las plataformas bancarias electrónicas para hacer consultas o transacciones?
   a. Sí
   b. No
5. ¿Por qué razón utiliza usted la plataforma bancaria electrónica? O ¿Por qué razón no utiliza usted la plataforma bancaria electrónica?

   _____
6. La mensajería instantánea es un medio gratuito en la mayoría de los casos, y rápido que utilizamos para contactarnos entre las personas, ¿Ha creado usted o es parte de un grupo en el trabajo utilizando la plataforma de la mensajería instantánea?
   a. Sí
   b. No
7. ¿Comparte usted información del trabajo por medio del grupo creado en la mensajería instantánea?
   a. Sí
   b. No

8. ¿Por qué razón se comparten datos por medio de la mensajería instantánea? o ¿Por qué razón no se comparten datos por medio de la mensajería instantánea?

   _____

9. ¿Le gusta hacer compras en línea ya sea de productos o servicios? Por ejemplo en Amazon o Netflix.
   a. Sí
   b. No

   Si su respuesta es No pasar a la pregunta 12
10. ¿Provee usted datos personales y números de sus tarjetas de crédito o débito al hacer sus compras?
    a. Sí
    b. No
11. ¿Conoce bien las políticas de seguridad de las plataformas tecnológicas por medio de las cuales usted comparte voluntariamente datos personales y números de tarjetas?
    a. Sí
    b. No
12. ¿Le gusta utilizar aplicaciones o relojes inteligentes que le indican su ritmo cardíaco?
    a. Sí
    b. No

Bibliografía

Beckett, Hellen (2016). Industria 4.0 no sin seguridad.

Recuperado de http://businessvalueexchange.com/es/2016/05/26/industria-4-0-no-sin-ciberseguridad/

Consejo de la Unión Europea (2016). Medidas para garantizar un nivel común,

De Seguridad de las redes y sistemas de información de la Unión.

Dekker Dimitra, Liveri (2015). Cloud Security Guide for SME's.

European Union Agency for Network and Information Security.

Gómez, Hilda (2015). La Ciberamenaza que tendremos que enfrentar en 2016,

Según Intel Security. Recuperado de http://www.pcworld.es/seguridad/las-ciberamenazas-que-tendremos-que-enfrentar-en-2016-segun-intel-security

Herrero Alcántara, Toñi (2016). La Seguridad, un reto para el despegue de IoT

Recuperado de http://www.ciospain.es/industria-y-utilities/la-seguridad-un-reto-para-el-despegue-de-iot

Hernández, R.; Fernández, C. y Batista, P. (2010). Metodología de la investigación.

(5 Ed.),México, D. F.: McGraw-Hill Interamericana

Lewis, James A (2016). Fomento de confianza cibernética y, diplomacia en América Latina,

y el Caribe. Centro de Estudios Estratégicos e Internacionales.

Fernández, Víctor (2016). Cómo optimizar la inversión en seguridad

Consolidando los riesgos. Recuperado de http://businessvalueexchange.com/es/2016/06/06/como-optimizar-la-inversion-en-seguridad-consolidando-los-riesgos/

Fernández, Víctor (2016) Atacar las Amenazas, la mejor manera de prevenir ataques

En la empresa. Recuperado de http://businessvalueexchange.com/es/2016/06/10/atacar-las-amenazas-la-mejor-manera-de-prevenir-ataques-en-la-empresa/

Rossen, Naydenov, (2015). Big Data Security Good Practices and Recommendation,

on the Security of Big Data Systems. European Union Agency for Network and Information Security.

Van Den Gregory (2015). Gestión de Riesgos de Ciberseguridad y el Pirateo a Sony.

Recuperado de https://www.bt.es/innovacion/gestion-de-riesgos-de-ciberseguridad-y-el-ataque-a-sony#.V5KV-O_rvIU