



UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EFFECTOS DEL USO DE CELULAR EN TÉRMINOS DE SEGURIDAD
INFORMÁTICA EN MILLENNIALS AL TRATAR SUS DATOS
PERSONALES.

ROMAN CABRERA ROLENDY DEL ROCIO
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2020



UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES
CARRERA DE CONTABILIDAD Y AUDITORÍA

EFFECTOS DEL USO DE CELULAR EN TÉRMINOS DE SEGURIDAD
INFORMÁTICA EN MILLENNIALS AL TRATAR SUS DATOS
PERSONALES.

ROMAN CABRERA ROLENDY DEL ROCIO
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2020



UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES
CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

EFFECTOS DEL USO DE CELULAR EN TÉRMINOS DE SEGURIDAD INFORMÁTICA
EN MILLENNIALS AL TRATAR SUS DATOS PERSONALES.

ROMAN CABRERA ROLENDY DEL ROCIO
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

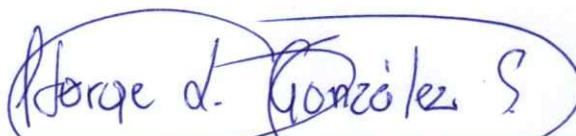
GONZALEZ SANCHEZ JORGE LUIS

MACHALA, 21 DE FEBRERO DE 2020

MACHALA
21 de febrero de 2020

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado EFECTOS DEL USO DE CELULAR EN TÉRMINOS DE SEGURIDAD INFORMÁTICA EN MILLENNIALS AL TRATAR SUS DATOS PERSONALES., hacemos constar que luego de haber revisado el manuscrito del precitado trabajo, consideramos que reúne las condiciones académicas para continuar con la fase de evaluación correspondiente.



GONZALEZ SANCHEZ JORGE LUIS

0703333898

TUTOR - ESPECIALISTA 1



PARRA OCHOA EUDORO BENITO

0701063406

ESPECIALISTA 2



OCHOA CAICEDO HECKLER ROTHWELL

0702681917

ESPECIALISTA 3

Fecha de impresión: viernes 21 de febrero de 2020 - 14:43

EFECTOS DEL USO DE CELULAR EN TÉRMINOS DE SEGURIDAD INFORMÁTICA EN MILLENNIALS AL TRATAR SUS DATOS PERSONALES

por Rolendy Del Rocío Román Cabrera

Fecha de entrega: 09-feb-2020 11:03p.m. (UTC-0500)

Identificador de la entrega: 1254445558

Nombre del archivo: ROLENDY_DEL_ROCIO_ROMAN_CABRERA.pdf (71.01K)

Total de palabras: 1835

Total de caracteres: 10534

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

La que suscribe, ROMAN CABRERA ROLENDY DEL ROCIO, en calidad de autora del siguiente trabajo escrito titulado EFECTOS DEL USO DE CELULAR EN TÉRMINOS DE SEGURIDAD INFORMÁTICA EN MILLENNIALS AL TRATAR SUS DATOS PERSONALES., otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

La autora declara que el contenido que se publicará es de carácter académico y se enmarca en las disposiciones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

La autora como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 21 de febrero de 2020



ROMAN CABRERA ROLENDY DEL ROCIO
0704762327

RESUMEN

La sociedad moderna caracterizada por la interacción *online*, donde las redes sociales, video juegos, video llamadas y actividades multimedia han desplazado a las tareas cotidianas, gracia al soporte de las tecnologías de comunicación e información.

La auditoría informática es una disciplina que busca proteger la información e integridad de datos, mediante controles o medidas aplicables tanto al entorno personal como profesional.

Los millennials son jóvenes cuyas prácticas informáticas conllevan riesgos, que no han sido abordados desde la perspectiva de la seguridad personal, se conjuga criterios de auditoria para proponer medidas y analizar los efectos adversos en función de su percepción de riesgo, se aplica la metodología deductiva e inductiva dirimiendo criterios por medio de una revisión bibliográfica.

En los resultados se postulan los hallazgos derivados de las ventajas, desventajas, técnicas de seguridad y medidas para minimizar los riesgos/amenazas que conlleva utilizar un Smartphone, además se expresa inferencias sobre la cultura digital de la era contemporánea que, a pesar de sus facilidades, también expresa contrariedades.

Palabras clave: Millenials, Smartphone, riesgos, seguridad informática, auditoria.

ABSTRACT

The modern society characterized by online interaction, where social networks, video games, video calls and multimedia activities have displaced everyday tasks, thanks to the support of communication and information technologies.

Computer auditing is a discipline that seeks to protect information and data integrity, through controls or measures applicable to both personal and professional environments. Millennials are young people who have computer practices that carry risks, which have not been approached from the perspective of personal security, audit criteria are combined to propose measures and analysis of adverse effects based on their perception of risk, the deductive and inductive methodology solving criteria through a literature review.

The results postulate the findings derived from the advantages, disadvantages, security techniques and measures to minimize the risks / risks involved in using a smartphone, in addition to expressing inferences about the digital culture of the contemporary era that despite its facilities, also expresses setbacks.

Keywords: Millenials, Smartphone, risks, computer security, audit.

ÍNDICE DE CONTENIDOS

RESUMEN	- 3 -
ABSTRACT.....	- 3 -
ÍNDICE DE CONTENIDOS	- 4 -
ÍNDICE DE ILUSTRACIONES	- 5 -
ÍNDICE DE CUADROS	- 5 -
1. INTRODUCCIÓN.....	- 6 -
2. DESARROLLO	- 7 -
2.1 Marco teórico:	- 7 -
2.1.1 Contabilidad y auditoría.....	- 7 -
2.1.2 Auditoria Informàtica.	- 7 -
2.1.3 Seguridad de la informaciòn.	- 7 -
2.1.4 Millennials.	- 7 -
2.1.5 Vulnerabilidades en Smartphone.	- 7 -
2.1.6 Amenazas más comunes en celulares.	- 8 -
2.1.7 Controles para proteger datos personales.	- 8 -
2.2 Caso Práctico:.....	- 8 -
2.2.1 Redes Sociales.	- 8 -
2.2.2 Ventajas y desventajas del celular.	- 9 -
2.2.3 Medidas de seguridad alternativas.	- 10 -
2.2.4 Efectos en la seguridad de los millennials.	- 10 -
3. CONCLUSIONES:.....	- 11 -
4. REFERENCIAS BIBLIOGRÁFICAS	- 12 -

ÍNDICE DE ILUSTRACIONES

Ilustración 1. Redes sociales más utilizadas por menores mediante Smartphone - 9 -

ÍNDICE DE CUADROS

Cuadro 1. Ventajas y desventajas del celular - 9 -

1. INTRODUCCIÓN

Las tecnologías avanzan de manera vertiginosa cambiando la concepción del mundo que nos rodea, hoy por hoy no existe ninguna organización, entidad o individuo ajeno a las cualidades que prestan los dispositivos informáticos; ya sea el uso del ordenador, Smartphone o cualquier medio digital para ejercer sus funciones.

Sin lugar a duda, la sociedad evoluciona a la vez que retroalimenta al hombre en su proceso de adaptación, tanto que inclusive se habla de una ciber cultura donde las tecnologías de la comunicación e información imperan como eje al realizar trabajos, encomiendas, entretenimiento o cualquier función social; además que para los jóvenes los celulares son su ventana al *mundo* haciendo amigos e interactuando a niveles tan subjetivos que prácticamente son inseparables de sus actividades cotidianas.

Las bondades de los sistemas cloud computing en conjunto con sus potencialidades, tienen su contra parte en términos de inseguridad, puesto que también son un medio para vulnerar sus datos personales, suplantar identidades o inclusive ser instrumento de ataques a terceros al efectuar fines mal intencionados.

Los millennials son el termino común para referirse a las generaciones nacidas a partir del año 1990 hasta el 2000, actualmente su rango de edad es de los 20 a los 30 años caracterizándose por su transformación cultural, romper esquemas e interactuar simbióticamente con las redes sociales; sin embargo, han desplazado a conductas tradicionales y tienen a desfasarse de las tendencias normadas por sus predecesores.

El presente trabajo incursiona en la temática de la auditoría informática, buscando determinar cuáles son las incidencias en términos de seguridad informática en el uso del Smartphone en millennials respecto a sus datos personales, este caso práctico identifica las vulnerabilidades y propone controles para mitigar los efectos adversos del uso desconcientizado de su celular.

La metodología utilizada es deductiva e inductiva al inferir las falencias de seguridad, posibles ataques, medidas de prevención o conductas que pueden adoptarse; la investigación bibliográfica y análisis comparativo son las técnicas seleccionadas al recopilar datos e información relevantes.

En las conclusiones se evidencia el cumplimiento de la propuesta, en contraste con lo delineado en el caso práctico, también se dan a conocer las opiniones del autor en expresar su dominio de la temática como implemento de su desarrollo profesional.

2. DESARROLLO

En esta sección se sintetizan los criterios esenciales del trabajo, enuncia la terminología adecuada en función de fuentes científicas; además se relata la resolución del caso en forma secuencial junto a las apreciaciones del autor desde la óptica de la auditoría Informática.

2.1 Marco teórico:

Se enlistan los conceptos más importantes, necesarios al definir el desarrollo del proyecto; siendo conceptualizados de acuerdo con su relación con la carrera de contabilidad y auditoría.

2.1.1 Contabilidad y auditoría.

Es una rama de la ingeniería que utiliza criterios matemáticos, para satisfacer las necesidades de contar con información contable de calidad, dar confiabilidad a los balances a la vez que verifica el cumplimiento de las disposiciones técnicas pertinentes (Cevallos Bravo & Latorre Aizaga, 2016).

2.1.2 Auditoría Informática.

Auditar es dar una revisión clara, de carácter holístico sobre el grado de eficiencia de los sistemas, explicado por un profesional debidamente calificado (Biler-Reyes, 2017); en el caso de la informática es analizar los sistemas y recursos tecnológicos para identificar vulnerabilidades y responder oportunamente ante ellas.

2.1.3 Seguridad de la información.

Es mantener al mínimo los riesgos informáticos y garantizar la operatividad del sistema en forma continua, a un costo accesible para la empresa (Quiroz-Zambrano & Macías-Valencia, 2017); en pocas palabras es un proceso permanente donde se aplica e implementa una serie de conductas preventivas y predictivas.

2.1.4 Millennials.

Son una de las generaciones mejor catalogadas, se caracterizan por ser pro activos, valorar el trabajo independiente, informatizar las labores junto a su vida personal en equilibrio, además de interactuar permanentemente con las redes sociales (Zavala-Villalón & Frías Castro, 2018).

2.1.5 Vulnerabilidades en Smartphone.

Los celulares han evolucionado como una herramienta tecnológica adaptable y versátil, siendo de uso múltiple en educación, trabajo, comunicación e inclusive interacción social; sin embargo, mientras más sofisticado sea, es más vulnerable.

De acuerdo con Mejía (2019), dichas vulnerabilidades son:

- Aplicaciones con riesgos estáticos
- Aplicaciones que solicitan permisos en forma dinámica
- Desactualizaciones de sistema operativo
- VPN (Red privada virtual de operadoras)
- Red de Wireless Fidelity

2.1.6 Amenazas más comunes en celulares.

En seguridad, se define como amenaza a todo factor tanto externo como interno que facilita un ataque, o que permite explotar una debilidad. Según Martínez, De la N, Cruz y Álvarez (2018) las más comunes en los teléfonos móviles son:

- Phishing (enmascarar sitios web), vishing (engañar para revelar datos sensibles), smishing (engañar via SMS para llamar a un tercero y darle información personal)
- Vulnerar cuentas de redes sociales
- Espionaje de llamadas, SMS, registros
- Rastreo GPS
- Obtener datos sensibles asociados a sus cuentas monetarias

2.1.7 Controles para proteger datos personales.

Son variados, deben considerarse situaciones como avería, robo o extravió del equipo; ante ellos tales medidas son aplicables:

- Borrado de datos remoto
- Autenticación en dos pasos, con correo electrónico y sms en redes sociales
- Tener aplicaciones de seguridad para codificar o respaldar datos
- Evitar vincular cuentas bancarias o sensibles en forma directa
- Patrones de bloqueo complejo y activar borrado al tercer intento fallido

2.2 Caso Práctico:

El objetivo es determinar cuáles son los efectos tanto favorables como adversos que causa el celular, en términos de seguridad informático en lo referente a datos personales.

2.2.1 Redes Sociales.

La educación mediática sobre el correcto uso de las TCI's como transmitir información, comunicación instantánea, reconocimiento de usuarios y acceso a internet, evidentemente requieren datos personales que, por descuido, desconocimiento o simplemente falta de cultura traen riesgos a su integridad física e imagen digital.

Según Pacheco, Lozano y Gonzàlez (2018), algunos riesgos son:

- Acoso sexual en especial a mujeres
- Problemas legales o conflictos por calumnias o comentarios mal intencionados
- Sexting, grooming o engaños para fines malintencionados

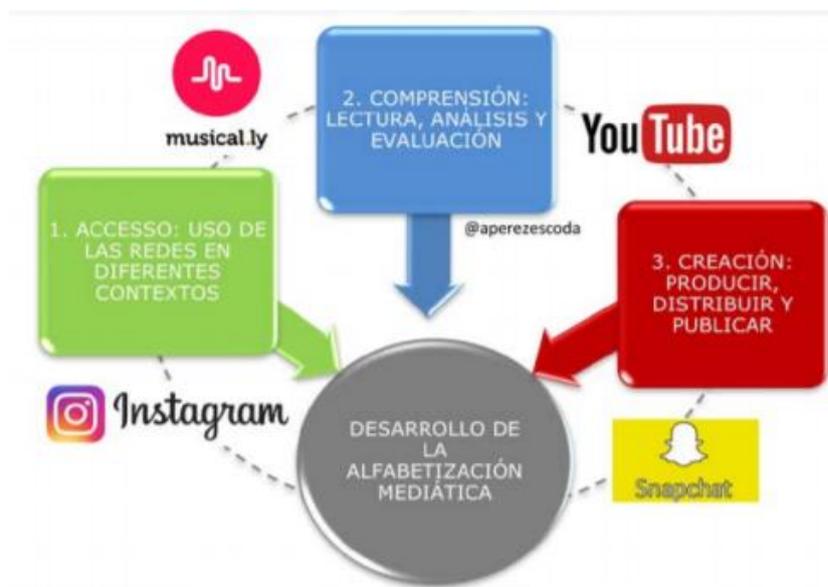


Ilustración 1. Redes sociales más utilizadas por menores mediante Smartphone

Fuente: (Pérez Escoda, 2018)

2.2.2 Ventajas y desventajas del celular.

Se abordan todas las inferencias y percepciones del riesgo, desde una perspectiva múltiple en ámbitos sociales, educativos, laborales, puesto que se trata sobre la seguridad personal que engloba a todo tanto formal como informalidad en la gestión de datos.

VENTAJAS	DESVENTAJAS
Acceso a información e internet	Fácil identificación en redes sociales o seguimiento a la persona
Variedad en canales de información	Permite varios medios para acosar o intimidar
Retroalimentación y flexibilidad de aprendizaje	Poner datos en sitios web deja vulnerable a robos, virus, hackers
Conocer su posición y estado en todo momento	Pérdida de datos e información en caso de robo/daño irreparable
Fácil acceso a servicios de seguridad, respaldo, reconocimiento, entre otros	Suplantar identidad, cuentas bancarias, injurias o cualquier acto vía digital
Evita gastos excesivos en comunicarse frente a otros medios	Falta de cultura y buenas prácticas en seguridad informática

Cuadro 1. Ventajas y desventajas del celular

Fuente: (Gómez Collado, Contreras Orozco, & Gutiérrez Linares, 2016)

Una de las anomalías que traen los Smartphone es el desarrollo del aislamiento familia, social físico y aptitudes negativas para su entorno; por ende, los padres junto a educadores deben ejercer autoridad al indicar las adversidades e incentivar una utilización paralela y responsable del celular.

2.2.3 Medidas de seguridad alternativas.

Aunque no existe un manual, ni guía en alguna institución o normativa legal; si existen medidas a considerar como las siguientes:

- *Borrado remoto de datos:* Uno de los servicios de *google* es mediante la cuenta *gamil* asociada, se puede restaurar el teléfono a estado de fábrica anulando cualquier intento de un mal uso.
- *Bloqueo mediante código IMEI:* Se puede bloquear totalmente al teléfono, mediante la operadora para evitar su uso por terceros.
- *Acceso en dos pasos:* Para evitar vulnerar redes sociales se puede solicitar código por sms, reconocimiento facial, código al correo o alguna barrera que impida el libre acceso.
- *Encriptar datos:* Usar algoritmos como EL (Rivest, Shamir y Adleman (RSA) por medio de configuración a servidores facilita encriptar datos vía inalámbrica en dispositivos móviles (Solís, Pinto, & Solis, 2017); esto evita ataques tanto externos como internos bien podría ser usado en la universidades.
- *Cultura de seguridad:* Adoptar buenas prácticas como cerrar sesión correctamente, respaldar datos, dejar de dar mi ubicación y no publicar que hace ni donde, son factores que delegan vulnerabilidad a los jóvenes (Arellano Martínez, 2017).

2.2.4 Efectos en la seguridad de los millennials.

La seguridad informática está directamente relacionada con la cultura, seguridad física e integridad; puesto que al publicar información sensible en tiempo real como què hacen, donde y con quién son susceptibles a robos e incluso al exhibir sus datos personales pueden suplantar identidad, acosarlos o ser víctimas de un delito.

Nuevamente se expresa que el mayor factor de riesgo, es la *conducta humana* gracias a que no puede medirse ni cuantificarse, ellos mismos generan una situación vulnerable que facilita a las amenazas dañarlos; otro aspecto es la falta de cultura en seguridad tanto de casa como instituciones educativas.

Un efecto positivo es la capacidad de dinamizar la educación, trabajo, acceso a oportunidades y sociedades; pero a su vez como contra parte se tiene acosos, contenido inapropiado, polémicas por comentarios e imagen en redes sociales, exposición a peligro por dar sus datos, entre otros efectos no contemplados al hablar de las potencialidades de las TIC`s en investigaciones académicas.

Las medidas mencionadas pueden reducir la vulnerabilidad, pero no evitar el robo o alguna situación fortuita, que amerite cuestiones fuera del alcance del presente estudio.

3. CONCLUSIONES:

Los millennials por desconocimiento, falta de cultura e ignorancia presentan una percepción de riesgo casi nula, poniéndose ellos mismos en riesgo al dar sus datos personales, publicar sus actividades y decir en todo momento su ubicación; esta información puede ser usada para fines malintencionados por terceros.

Las medidas citadas son prácticas contrarrestando los efectos negativos como el aislamiento social, exponer datos sensibles, ataques externos y describir cómo actuar en caso de perder el celular; un punto destacable es que las bondades tecnológicas opacan sus riesgos y las instituciones académicas no realizan estudios que reduzcan las vulnerabilidades, ni se socializa medidas para que los padres eduquen correctamente sobre el uso adecuado del Smartphone.

La auditoría informática también es aplicable al ámbito personal, porque la sociedad del conocimiento es inseparable de las TIC`s; haciendo imperiosa la necesidad de ejercer una cultura para limitar los riesgos inherentes e integrar controles que garantice la accesibilidad, disponibilidad y confiabilidad de los datos tanto personales como profesionales.

Pese a existir efectos positivos como la accesibilidad al conocimiento, dinamizar el aprendizaje e igualdad de oportunidades; las contrariedades derivadas son de carácter psicológico como el aislamiento social e irrespeto, que sumado al elevado contenido de la web son peligrosos para jóvenes sin criterio propio, por lo tanto; se aconseja concatenar estudios clínicos afines al discretizar las variables cognitivas que han mutado por culpa del celular, gestionando una percepción del riesgo casi nula sin medir realmente las consecuencias.

4. REFERENCIAS BIBLIOGRÁFICAS

- Arellano Martínez, I. (2017). La cultura sobre seguridad informática en las redes sociales: el caso de los estudiantes de la Preparatoria de San Diego Cuentla, México. *Revista Iberoamericana de las Ciencias Sociales y Humanísticas; Vol 6, No 11*, 1-11.
- Biler-Reyes, S. A. (2017). Auditoria. Elementos esenciales. *Dominio de las Ciencias, Vol. 3, N°. Extra 1*, 138-151.
- Cevallos Bravo, M. V., & Latorre Aizaga, F. L. (2016). El papel del auditor contable. *Revista Publicando, Vol. 3, N°. 9*, 373-386.
- Gómez Collado, M. E., Contreras Orozco, L., & Gutiérrez Linares, D. (2016). El impacto de las tecnologías de la información y la comunicación en estudiantes de ciencias sociales: un estudio comparativo de dos universidades públicas. *Innovación educativa (México, DF), Vol 16, No 71*, 61-80.
- Martínez Santander, C. J., de la N. Cruz Gavilanes, Y., Cruz Gavilanes, T., & Álvarez Lozano, M. I. (2018). Seguridad por capas frenar ataques de Smishing. *Dominio de las Ciencias,, Vol. 4, N°. 1*, 115-130.
- Mejía, J. (2019). Detectando aplicaciones maliciosas en Smartphone con sistema Android a través del uso de una aplicación. *RISTI - Revista Ibérica de Sistemas e Tecnologías de Informação, No 19*, 82-93.
- Pacheco Amigo, B. M., Lozano Gutiérrez, J. L., & González Ríos, N. (2018). Diagnóstico de utilización de Redes sociales: factor de riesgo para el adolescente. *RIDE. Revista Iberoamericana para la Investigación y el Desarrollo Educativo, Vol 8, No 16*, 1-20.
- Pérez Escoda, A. (2018). Uso de smartphones y redes sociales en alumnos/as de Educación Primaria. *Prisma Social: revista de investigación social, N°. 20*, 76-91.
- Quiroz-Zambrano, S. M., & Macías-Valencia, D. G. (2017). Seguridad en informática: consideraciones. *Dominio de las Ciencias, Vol. 3, núm. 4*, 137-156.
- Solís, F., Pinto, D., & Solis, S. (2017). Seguridad de la información en el intercambio de datos entre dispositivos móviles con sistema Android utilizando el método de encriptación RSA. *Enfoque UTE vol.8 supl.1*, 160 - 171.
- Zavala-Villalón, G., & Frías Castro, P. (2018). Discurso millennial y desafíos en la gestión de recursos humanos en Chile. *Psicoperspectivas, Vol 17, No 3*, 1-12.