Deloitte.

Nuevas amenazas a las tecnologías móviles

Android APK

Jong Park

2 de Diciembre de 2015

Contenido

Deloitte.

Revisión a las aplicaciones móviles

- Introducción
- Aplicaciones móviles
  - ✓ Importancia
  - ✓ Amenazas
  - ✓ Propuesta
- Caso Real
- Conclusiones

Revisión a las aplicaciones Móviles

Introducción

- Con base en la importancia que han adquirido las tecnologías móviles en las diferentes organizaciones y la interacción cada vez mayor de los usuarios finales con las organizaciones a través de las aplicaciones e interfaces móviles, el equipo de Cyber Security de Deloitte México realiza revisiones de seguridad extensivas que permiten la identificación oportuna del nivel de riesgo al que la información puede estar expuesta.

Aplicaciones Móviles
Importancias y amenazas

Aplicaciones Móviles

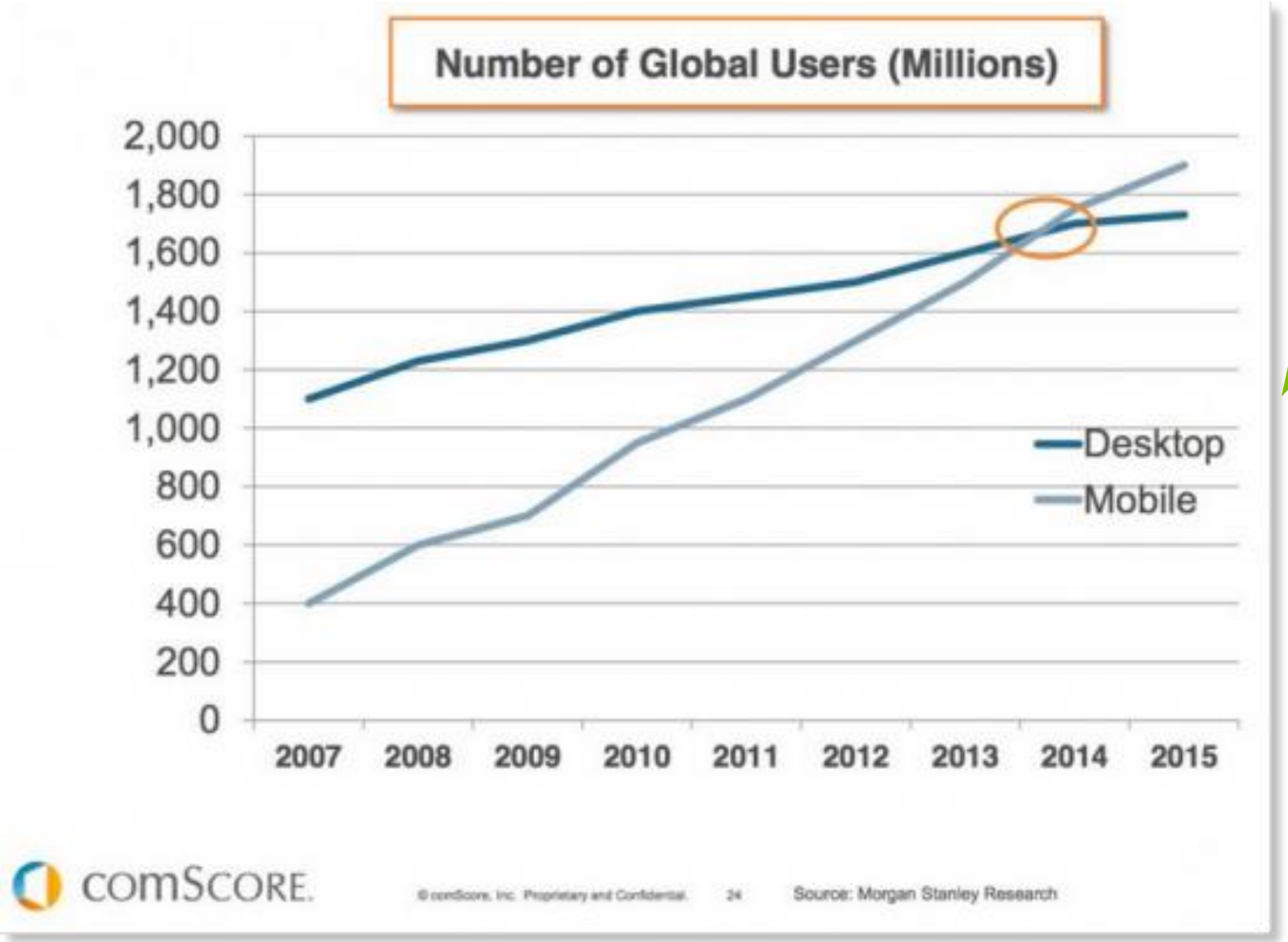
Importancia

- Las aplicaciones móviles son la innovación y el crecimiento de ingreso ya que proporcionan una interacción entre los negocios y sus clientes.

- Las aplicaciones móviles son esenciales para la transformación digital de los negocios ofreciendo un servicio más personalizado a cada uno de sus clientes.

Aplicaciones Móviles

Importancia



El número de usuarios de los dispositivos móviles ha rebasado el número de usuarios de computadoras de escritorio.

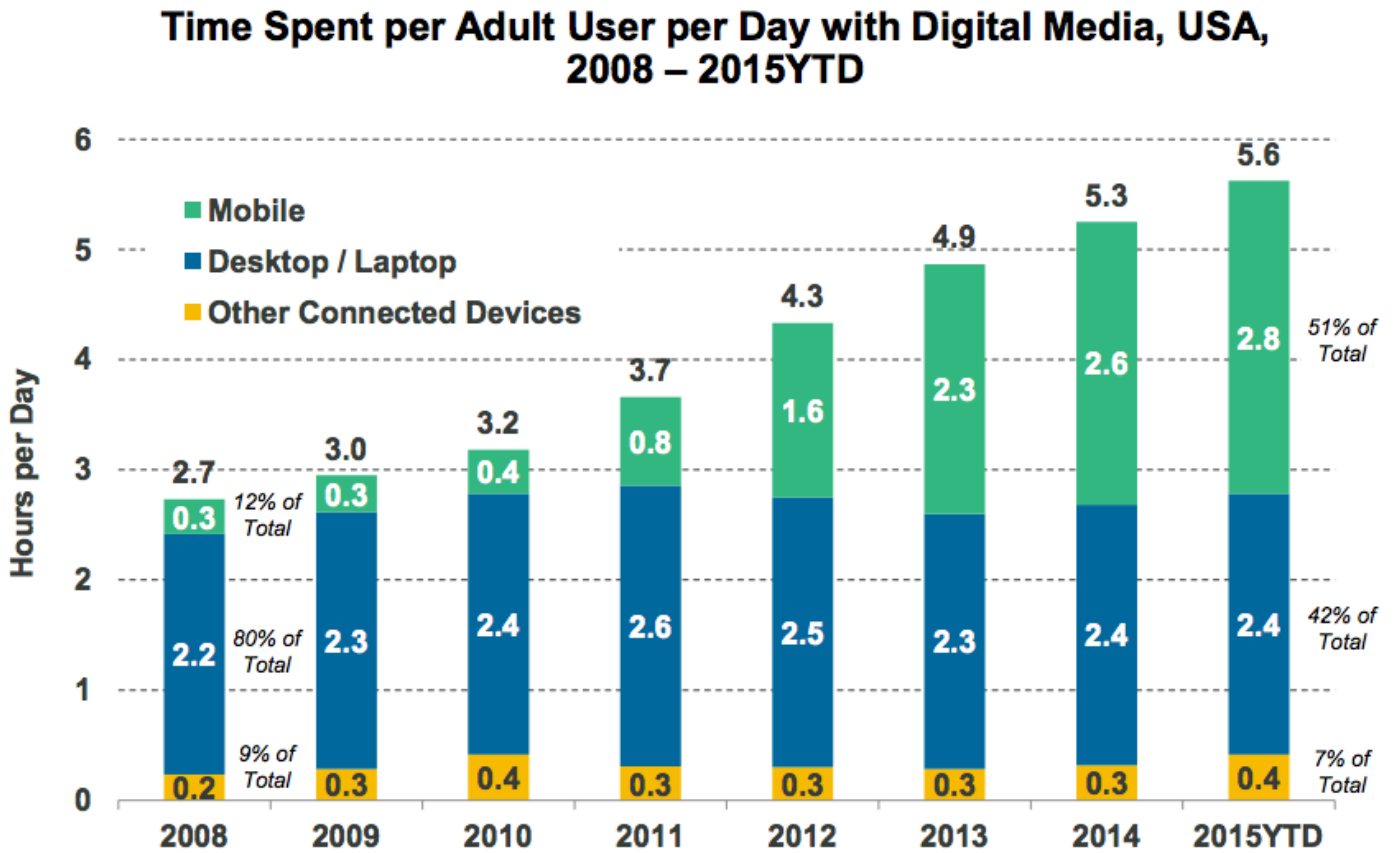
Aplicaciones Móviles

Importancia

Deloitte.

Los usuarios usan más los dispositivos móviles para consultar el contenido digital.

Internet *Usage* (Engagement) Growth Solid
+11% Y/Y = Mobile @ 3 Hours / Day per User vs. <1 Five Years Ago, USA



@KPCB Source: eMarketer 9/14 (2008-2010), eMarketer 4/15 (2011-2015). Note: Other connected devices include OTT and game consoles. Mobile includes smart[ablet. Usage includes both home and work. Ages 18+; time spent with each medium includes all time spent with that medium, regardless of multitasking.

14

Aplicaciones Móviles

Amenazas

- Las aplicaciones móviles están expuestas a diversas vulnerabilidades que podrían comprometer la confidencialidad, integridad o disponibilidad de la información de las organizaciones y usuarios finales.

- El área de desarrollo de aplicaciones móviles es un espacio nuevo, por lo que las empresas todavía no cuentan con expertos para probar problemas de seguridad y privacidad

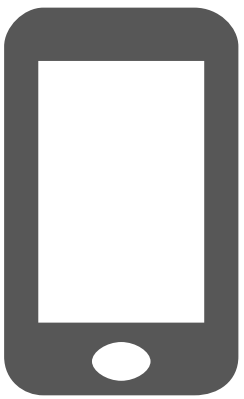
Aplicaciones Móviles

Amenazas

Deloitte.

Eslabón más débil de la seguridad de las empresas son los dispositivos móviles seguido por las redes sociales (Cyber Edge Group)

El 75% de las aplicaciones móviles no cumplen con los requerimientos básicos de seguridad (Gartner)



1 de cada 5 usuarios de Android han experimentado una amenaza móvil en 2014 (Kaspersky Lab)

Kaspersky Lab detectó 1,363,549 ataques únicos durante 2014. En comparación con 335,000 ataques únicos durante el 2013 hubo un incremento de 407%

Aplicaciones Móviles

Propuesta

- Realizar pruebas de seguridad basadas en mejores prácticas y metodologías enfocadas en tecnologías móviles con el fin de analizar:
  - ✓ Código
  - ✓ Diseño
  - ✓ Empaquetamiento
  - ✓ Cifrado
  - ✓ Instalación
  - ✓ Ejecución en diferentes condiciones en las que podría estar sujeto la aplicación.

Caso Real

Aplicación Móvil en Android

Caso Real

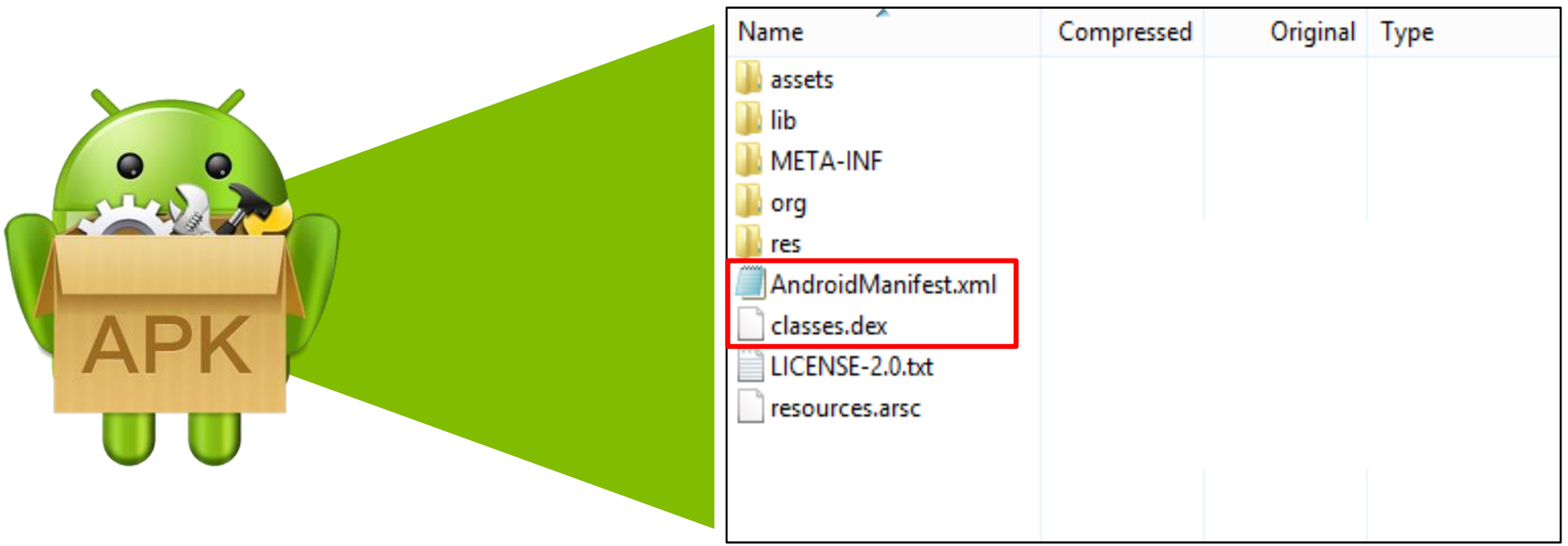
Introducción

- Como parte de los servicios ofrecidos por Deloitte, el equipo realizó una revisión sobre una aplicación móvil para los clientes de esta organización..
- Esta aplicación recibe información altamente confidencial de los usuarios para funcionar

Caso Real

Aplicación

- Como parte de set de pruebas generado para la revisión de esta aplicación, se validaron los controles (OWASP TOP 10)* mediante el análisis a través de ingeniería inversa a la aplicación. Esta fue descompilada y pudimos observar diversos recursos de la aplicación.



*Para más información consultar https://www.owasp.org/

Figura 1. Estructura de APK en Android

Caso Real

Ingeniería inversa

JAVA

Lenguaje de Alto Nivel

Fácil de Leer y Escribir

SMALI

Lenguaje de Bajo Nivel

Se puede re-empaquetar como APK

Caso Real

Análisis de código

- Para la validación se decidió realizar una prueba de inserción de código a la aplicación. De esta forma un atacante puede modificar el flujo lógico de la aplicación para lograr su objetivo.

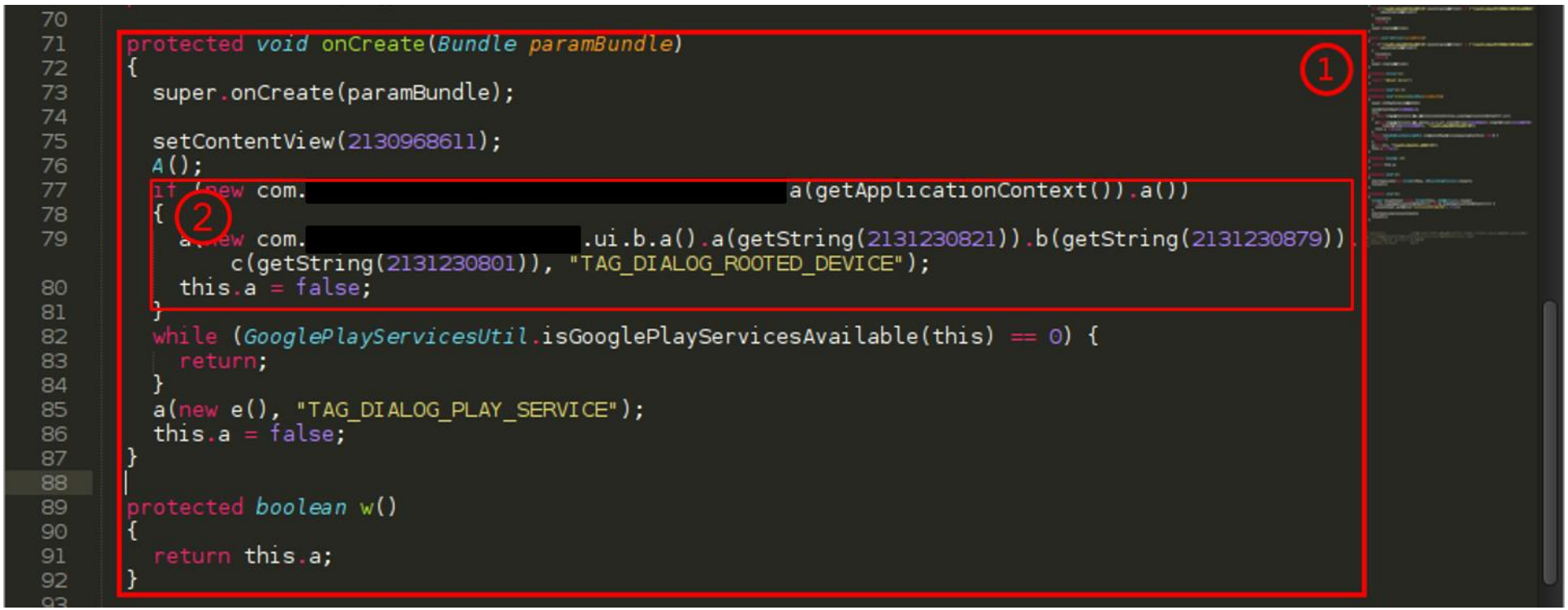


Figure 3. Main Activity – Decompilado a un lenguaje que es human readable

Caso Real

Modificación de código

- La inserción de código se realiza en un lenguaje de bajo nivel y se vuelve a empaquetar como la aplicación original.

```
.method protected onCreate(Landroid/os/Bundle;)V
    .locals 3
    .param p1, "savedInstanceState"    # Landroid/os/Bundle;

    .prologue
    const/4 v2, 0x0

    invoke-super {p0, p1}, Lcom/[redacted]/ui/activity/BaseActivity;->onCreate(
    Landroid/os/Bundle;)V

    const v0, 0x7f040023

    invoke-virtual {p0, v0}, Lcom/[redacted]/ui/activity/SplashActivity;->
    setContentView(I)V

    invoke-direct {p0}, Lcom/[redacted]/ui/activity/SplashActivity;->A()V

    new-instance v0, Lcom/[redacted]mobileclientutilities/a;

    invoke-virtual {p0}, Lcom/[redacted]/ui/activity/SplashActivity;->
    getApplicationContext()Landroid/content/Context;

    move-result-object v1

    invoke-direct {v0, v1}, Lcom/[redacted]mobileclientutilities/a;-><init>(Landroid/content
    /Context;)V

    invoke-virtual {v0}, Lcom/[redacted]/mobileclientutilities/a;->a()Z

    move-result v0
```

Figure 4. Main Activity – Decompilado a un lenguaje bajo nivel

Caso Real

Riesgo

- Debido a esta vulnerabilidad se encontró que la aplicación está expuesta a:
  - Robo de información confidencial de clientes
  - Ataques de phising causando daño reputacional a la organización

Conclusiones

Punto de vista de seguridad

Conclusiones

Punto de vista de seguridad

- Las tecnologías y desarrollos móviles están creciendo día a día y ofrecen a usuarios y organizaciones una gran cantidad de ventajas para la realización de sus actividades de forma cómoda y ágil.
- Sin embargo, éstas aplicaciones contienen información confidencial y de negocio que puede ser comprometida si no se cuenta con desarrollos robustos y alineados a prácticas de seguridad que permitan disminuir los riesgos de forma considerable

Deloitte.