Guía para proteger y usar de forma segura su móvil en la empresa

Plan de proyecto

INSTITUTO NACIONAL DE CIBERSEGURIDAD

INDICE

1 Plan de proyecto

Cada vez son más los dispositivos móviles que los trabajadores de una empresa usan a nivel particular. Esto, sumado a la capacidad tecnológica actual que permite conexiones desde prácticamente cualquier lugar y a la creciente demanda de los trabajadores de poder acceder a los datos, correo y demás desde cualquier ubicación, hace que cada vez más los dispositivos personales de los trabajadores se usen para fines empresariales. Esto se conoce como "Bring your own device" (BYOD). A nivel de dispositivos hoy en día casi todos los trabajadores disponen de móviles con tecnologías de conexiones a internet (3G, 4G, WIFI…) o de compartición de datos (bluetoth…). Además, cada usuario dispone de un tipo de dispositivo diferente, con diferente hardware, software y distintas aplicaciones instaladas (algunas de ellas incluso maliciosas).

Este nuevo concepto en el uso de los dispositivos de los propios trabajadores abre un nuevo campo en cuanto a la capacidad del trabajador para realizar tareas laborales desde sus dispositivos móviles. Esto implica beneficios y desventajas/peligros que hay que valorar y controlar.

Esta guía recopilará recomendaciones para garantizar una utilización segura del móvil: como proteger la información que contiene, como actuar en caso de pérdida o robo, como realizar conexiones seguras…

1.1 Justificación del proyecto

Conforme aumentan las capacidades tecnológicas de los dispositivos móviles también aumenta su uso en el puesto de trabajo. Los números y las estadísticas son claras en este sentido. Según estadísticas de diferentes empresas (Gartner, Ovum, IBM, Vertic, Flurry, Magic Software, Motorola and Harris Pol), recogidas en un estudio[1] a inicios de 2013:

- Había un bilión de smartphones en el mundo.
- El 81% de americanos usaba su dispositivo móvil para el trabajo.
- El aumento del número de usuarios de smartphones anual a nivel mundial es del 42%.
- En 2012 se vendieron 821 millones de smartphones y tabletas en todo el mundo.
- El incremento de la productividad laboral por el uso de las aplicaciones en móviles es del 45%.

[1] http://www.ribbit.net/frogtalk/id/143/byod-stats-what-business-leaders-need-to-know-right-now

Otro estudio[2] que recoge datos de diferentes empresas de inicios de 2012 decía qué:

- El 74% de empresas permitía algún tipo de uso de BYOD.

Esto hace que el BYOD (bring your own device) esté en aumento y que cada vez más se utilicen dispositivos personales para el día a día en el trabajo. Esto reporta ventajas y desventajas. Como principal beneficio está el citado incremento de la productividad laboral. Dentro de las desventajas se encuentra la seguridad de estos dispositivos. Los problemas de seguridad y las posibles fugas de información de estos dispositivos pueden acarrear graves consecuencias para la empresa donde trabajan los propietarios de estos dispositivos. Así lo demuestra el estudio anterior llevado a cabo con varias compañías, que reporta diferentes estadísticas que ponen en peligro los datos que contienen o a los que acceden esos dispositivos móviles:

- El 46% de usuarios prestan sus dispositivos a otras personas.
- El 35% guardan su password del correo del trabajo en el móvil.
- El 37% no tienen activas las opciones de bloqueo.
- El 66% de trabajadores dice que su empresa no tiene implementados políticas de BYOD.
- El 80% de la actividad a través del BYOD no está siendo administrada.
- El incremento de malware detectado en el último año (2012) fue del 155%.
- El segundo estudio también revela datos críticos para la seguridad de las empresas:
- En 2012 menos del 10% de las empresas eran plenamente conscientes de los dispositivos que accedían a su red.
- El 55% de los trabajadores revelaron haber enviado correos o ficheros de empresa a sus cuentas personales usadas en el móvil.
- El 48% dicen conectarse a redes wi-fi inseguras.

Así pues, podemos afirmar que esta nueva forma de relación trabajador-empresa implica riesgos para la información y futuro de la empresa y que sea de especial interés el estudio de las debilidades del uso de los dispositivos móviles personales como sistema emergente en el mundo profesional. Debemos centrar la atención en la fuga de datos empresariales que pueden deberse a:

- Robo de móviles. Cada vez que un móvil es robado los datos que contiene y aquellos datos accesibles desde aplicaciones instaladas en el móvil pueden ser robadas y usadas con fines desconocidos.

[2] http://www.forbes.com/sites/markfidelman/2012/05/02/the-latest-infographics-mobile-business-statistics-for-2012/

- Instalación de aplicaciones infectadas con capacidad para robar datos. En un estudio reciente realizado por Alcatel-Lucent (http://www.digitalnewsasia.com/sites/default/files/files_upload/MKT2014087076EN_Kindsight_H1_2014_Malware_Report.pdf) publicado el 9 de septiembre de 2014 muestra que las amenazas a dispositivos móviles y equipos de escritorio aumentaron considerablemente durante el primer semestre de 2014. En el informe se asegura que los casos de malware en dispositivos móviles se vieron incrementados en un 17% durante ese primer semestre de 2014
- Análisis de envío y recepción de datos a través de conexiones inseguras (WIFI de un bar, bluetooth mal configurado...). Cada vez más proliferan los puntos de acceso gratuitos para bien del usuario, pero un uso inseguro de estos puntos de acceso puede permitir a otras personas asociadas al mismo punto analizar nuestro tráfico de red y obtener datos relevantes.
- Préstamo del móvil a otra persona.
- Ataques de ingeniería social. A través de estos ataques un atacante podría intentar instalar algún tipo de malware en el dispositivo móvil o bien intentar obtener datos de forma directa (simulando un pago al banco, intentado sacar más respuestas de las debidas a través del envío de correos....).

Es por este conjunto de hechos que es de especial interés la elaboración de una guía para proteger y usar los móviles de forma segura.

1.2 Objetivos

El objetivo principal es la elaboración de una guía para proteger y usar de forma segura los móviles en la empresa. Como la perspectiva del uso de los dispositivos móviles y la protección de los datos de la empresa debe acometerse desde el lado del empresario/departamento IT así como de los empleados se desarrollarán dos guías diferenciadas atendiendo a este criterio marcando dos subobjetivos a cumplir:

- Ofrecer a la empresa y al trabajador información de como proteger sus datos cuando estos son accedidos desde dispositivos móviles.
- Ofrecer a la empresa y al trabajador recomendaciones del uso y protección de dispositivos móviles.

1.3 Descripción general del proyecto

Para la elaboración de la guía podemos diferenciar las siguientes fases de estudio:

- Estudio de los problemas del uso del móvil en la empresa: Análisis de los diferentes problemas que pueden surgir a la hora de usar los dispositivos móviles en la empresa. Listado de tipos de ataques, métodos de obtención de datos que puede usar un atacante…
- Estudio de los métodos para evitar/reducir la problemática: Búsqueda de métodos para reducir la problemática.
- Estudio de las tecnologías aplicables: Búsqueda de las tecnologías aplicables para llevar a cabo la aplicación de los métodos estudiados en el apartado anterior.
- Elaboración de una relación de aplicaciones que faciliten la aplicación de los métodos para evitar/reducir la problemática: Búsqueda de las mejores aplicaciones que puedan ser de ayuda a la hora de buscar soluciones para aplicar las tecnologías adecuadas para la protección de los datos y los dispositivos móviles.

Una vez realizados los apartados anteriores podremos elaborar las guías.

1.4 Riesgos preliminares

- Tiempo limitado. Dificultad en el cumplimiento de los plazos al tener que alternar este proyecto con mi situación laboral actual. Esto plantea que los plazos para realizar el proyecto puedan ser difíciles de alcanzar.
- Falta de información. Dificultad para encontrar información relacionada con la temática a tratar. Es posible que no se haya tratado este tema con anterioridad. Esto puede implicar un retraso en la primera fase del proyecto definida anteriormente.
- Falta de metodologías o aplicaciones. Dificultad para encontrar metodologías o aplicaciones destinadas a móviles. Esto podría darse el caso si aún no se ha tratado la temática como es debido dentro de la elaboración de programas de protección para los móviles.

En las siguientes tablas se tomarán los siguientes valores para cuantificar los riesgos y las medidas para poder paliarlos:

- Muy Alto: 5
- Alto: 4
- Medio: 3
- Bajo: 2
- Muy Bajo: 1

Tabla 1. Tabla de riesgos

Identificador	Riesgo	Probabilidad	Impacto	TOTAL
Tiempo limitado	Dada la carga de trabajo de otros proyectos/trabajo, plantea la posibilidad de no lograr todos los objetivos	Media (3)	Medio/alto (5)	15
Falta de información	Dificultará la obtención y listado de los problemas que podemos encontrar así como de las tecnologías que usan los dispositivos móviles	Alto (1)	Alto (4)	4

Falta de aplicaciones o metodologías	Dificultará la obtención de información en cuanto a recursos (apliaciones o metodologías) para proteger los dispositivos móviles y los datos que manejan	Alta (3)	Alto (4)	12

Sobre estos tres riesgos detectados, se van a tomar una serie de contramedidas para su mitigación:

Tabla 2. Tabla de acciones para la mitigación de riesgos

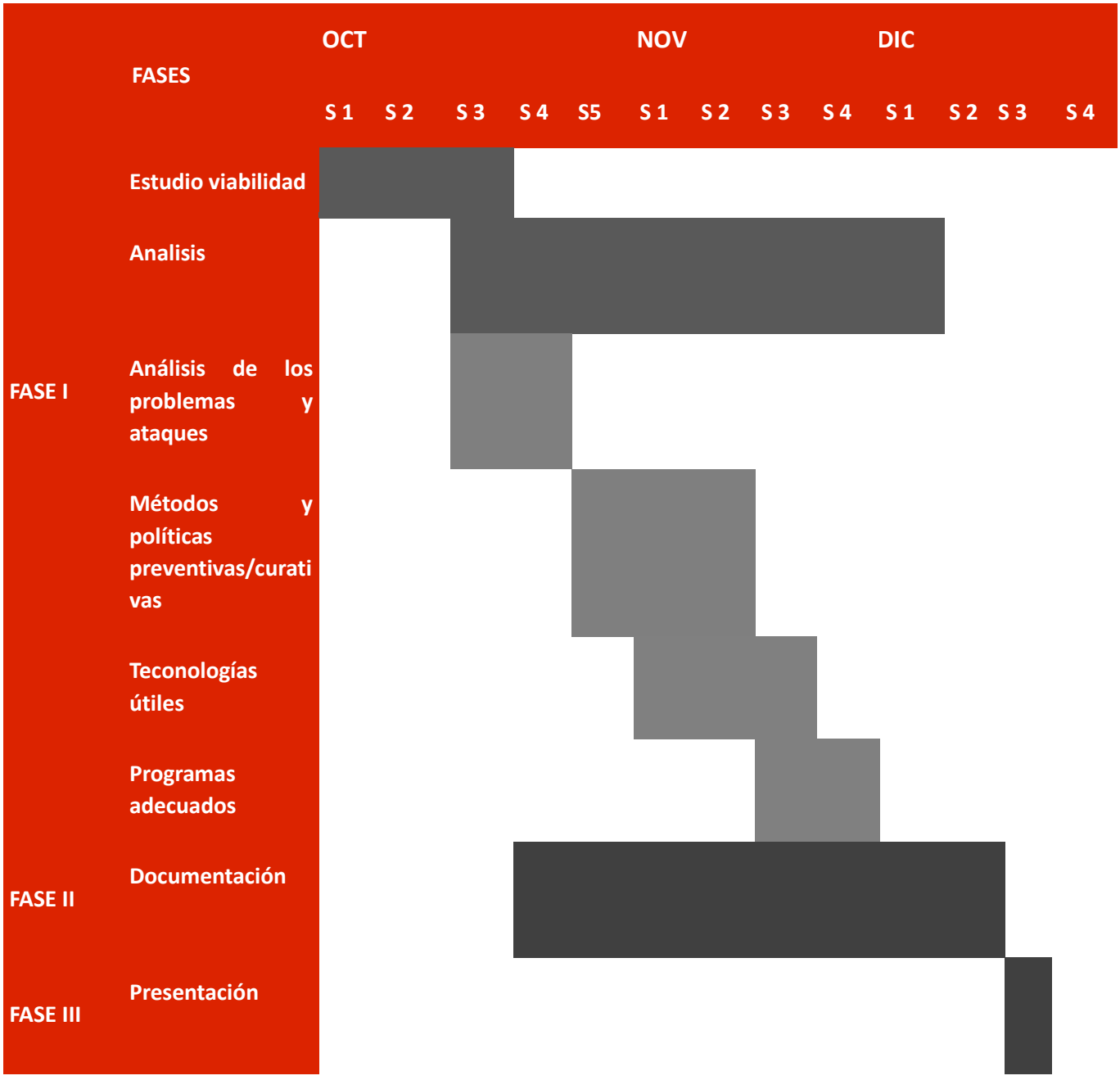
Identificador	Acciones de mitigación	Probabilidad	Impacto	TOTAL (residual)
Tiempo limitado	Trabajo rápido. Ser concisos.	Media (3)	Medio/alto (5)	15
Falta de información	Obtención de información por internet. Contactar con instituciones/departamentos que hayan podido tratar el tema pero que no hayan publicado sus trabajos.	Alto (1)	Alto (4)	4
Falta de aplicaciones o metodologías	Obtención de información por internet. Contactar con instituciones/departamentos que hayan podido tratar el tema pero que no hayan publicado sus trabajos.	Alta (3)	Alto (4)	12

1.5 Planificación

El proyecto tiene como fecha de cierre 18 de diciembre de 2014. Las fases a realizar durante el proyecto son las siguientes:

- FASE I: Estudio de viabilidad y análisis: Ejecución del plan de proyecto y obtención de datos e información. Del 29 de septiembre al 5 de diciembre. El apartado análisis de esta FASE I se puede separar en varias subtareas:
    1. Análisis de los problemas y ataques: Del 13 al 24 de octubre.
    2. Métodos y políticas preventivas/curativas: Del 27 de octubre al 14 de noviembre.
    3. Tecnologías útiles: Del 3 al 21 de noviembre.
    4. Programas adecuados: Del 17 al 28 de noviembre.
- FASE II: Documentación. Del 20 de octubre al 12 de diciembre.
- FASE III: Presentación del análisis. Del 15 al 18 de diciembre.

A continuación se muestra una tabla donde de forma gráfica se pueden ver las fases del proyecto. Te tomará como fecha de entrega la tercera semana de diciembre, ya que se cuenta que haya posibles retrasos y dificultades y por tanto se espera llegar la fecha de cierre con el suficiente tiempo de antelación:



1.6 Criterios de aprobación

Para considerar el proyecto como válido, se deberá de hacer entrega:

- El presente documento del proyecto completado a su finalización.
- La guía para proteger y usar su móvil de forma segura su móvil en la empresa.

- La guía para proteger y usar de forma segura los datos de empresa accedidos desde móviles.

1.7 Organigrama y responsabilidades

Jefe de Proyecto
Narcís Altirriba Claramunt
Consultor de Seguridad
Narcís Altirriba Claramunt

Cliente
Jorge Chinea