NUEVAS FORMA DE TRABAJO USANDO MdM

TRABAJO DE GRADO: Resumen Ejecutivo

JAVIER ENRIQUE GUATAME JAMAICA

1512010894

Asesor(es)
GIOVANNY ANDRES PIEDRAHITA SOLORZANO

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2016

1. Resumen Ejecutivo

El presente proyecto tiene como objetivo presentar como es posible apoyar el acceso de colaboradores de una organización a la infraestructura de la misma de forma segura, cumpliendo con las definiciones de seguridad que estén vigentes en la organización.

Para ello, no es ajeno que si se trata de mantener la seguridad de información en sistemas tecnológicos es necesario usar sistemas tecnológicos; para preservar la información; llevándonos a definir que para este caso es necesaria la implementación de una solución para la Administración de Dispositivos Móviles – MdM, que le permita a una organización gestionar los dispositivos móviles corporativos y personales de aquellos colaboradores que requieran acceder a los datos de la organización; preservando la información de los clientes, proveedores, colaboradores etc.

El uso del MdM permitirá la administración de los dispositivos móviles manteniendo un inventario actualizado de los dispositivos que se encuentren registrados con información de usuarios, marca, numero de celular, sistema operativo, aplicaciones instaladas, espacio de almacenamiento entre otros; de esta forma es que el MdM puede consultar el nivel de confianza de los dispositivos de acuerdo a las políticas de seguridad configuradas en el mismo para permitir el acceso a la información de la organización.

Lo que se pretende mostrar a las organizaciones es que existen formas de permitir el acceso a los datos de la organización de forma segura, facilitando que mejoren u optimicen sus procesos; sobre todo si se requiere mantener la información actualizada y disponible para su consulta fuera de las oficinas para permitir que los colaboradores puedan aprovechar oportunidades de negocio.

1.1. Metodología

Se define la siguiente metodología para asegurar el acceso y transmisión de información, que es requerida por el área comercial para cumplir con sus procesos de afiliación, actualización de datos y consulta que requeriré para su trabajo diario fuera de las instalaciones de la organización utilizando la aplicación móvil desarrollada para tal propósito.

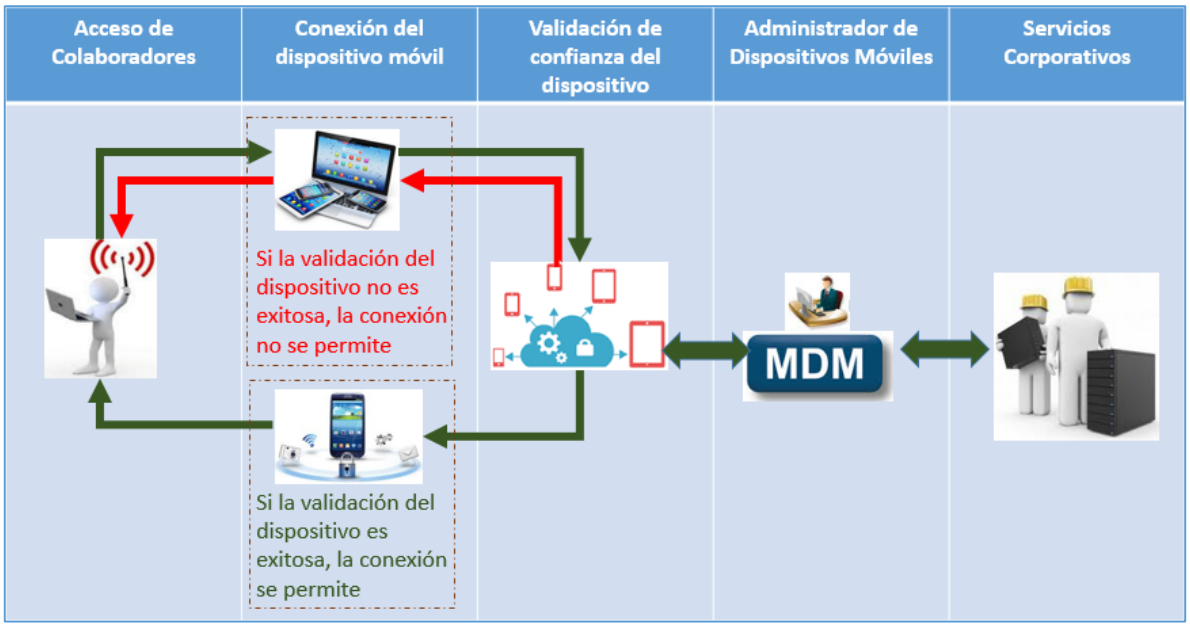
A continuación se documenta el resultado de las actividades realizadas sobre cada una de las etapas de la metodología:

1. Identificar y entender el problema: Se establece que se requiere solucionar el uso y acceso seguro de la aplicación corporativa creada para el área comercial; la cual permitirá que los comerciales fuera de las instalaciones de la organización puedan acceder a los datos de afiliados usando el dispositivo móvil asignado
2. Identificar los riesgos de seguridad de la información: Como riesgo principal se establece que si hay acceso a los datos corporativos es posible que se materialice la fuga de información, además de accesos no autorizados, daño a la integridad de la información, robo de información.
3. Plantear la solución: De acuerdo al problema y a los riesgos identificados, se define que es necesario brindar una solución que permita gestionar los dispositivo móviles de forma segura y la transmisión de la organización debe cumplir con ciframiento y acceso seguro; por lo que se recomienda implementar un Administrador de Dispositivos Móviles – MdM.
4. Definir la metodología de implementación: Se realiza el análisis y alistamiento de los requisitos de implementación de acuerdo a la arquitectura necesaria para el correcto funcionamiento de la herramienta. Por lo que es necesario definir un plan de trabajo.
5. Implementar la herramienta seleccionada: Instalación de la herramienta y configuración de la misma, con el fin de que cumpla con los requisitos de la organización.
6. Monitoreo: Actividad que deberá ser realizada por el administrador de la herramienta o por el área que realice las actividades de monitoreo, para validar su funcionamiento y aplicación de las políticas definidas.

Como parte de la metodología, se ha contemplado la implementación de la herramienta y no solo su selección; a continuación se describe la metodología de

implementación de la herramienta; la cual es sencilla y más aún su administración; como primera medida la organización debe realizar un análisis de las aplicaciones e información corporativa a la cual los colaboradores tendrán acceso usando sus dispositivos móviles, luego se realiza el enrolamiento de dispositivos y usuarios asignando el perfil correspondiente para que hagan uso de la información corporativa.

El administrador del MdM, realizará la configuración respectiva de los niveles de confianza que debe cumplir los dispositivos móviles para que se apliquen las políticas de seguridad definidas; pues de esta forma es que se restringe el acceso a los datos y/o aplicaciones cuando el dispositivo no cumple con las condiciones de seguridad requeridos.



1.2. Resultados

Los resultados luego de la implementación de la herramienta, a nivel de seguridad son:

- Preservar la información de la organización para su acceso externo
- Mantener las políticas de seguridad de la organización en ambientes externos
- Reducir la posibilidad de fuga de información
- Evitar el acceso de personas no autorizadas a los sistemas de la organización
- Oportunidad de negocios por la disponibilidad de información por parte de los colaboradores
- Mejorar los procesos del área comercial cuando se encuentran fuera de las instalaciones de la organización, de acuerdo a lo definición por I+P (Innovación y productividad)

Los resultados funcionales de la herramienta son:

- Ubicación de los dispositivos móviles por GPS
- Borrado de información del dispositivos móvil remotamente en caso de robo
- Instalación de aplicaciones de forma remota
- Bloqueo de funciones
- Control de navegación
- Acceso al correo corporativo

1.3. Alcance

El presente proyecto tiene como alcance, dar a conocer como mediante un MdM se puede apoyar los niveles de seguridad de una organización cuando esta requiere que sus colaboradores accedan a aplicaciones y/o información usando dispositivos móviles para mitigar riesgos como:

- Fuga de información
- Accesos no autorizados
- Robo de información
- Suplantación de identidad
- Escaneos no autorizados a la red

Por lo cual también se abordara documentación sobre las bondades de un MdM en un entorno corporativo, describiendo su funcionamiento y parte de las configuraciones que en este se pueda realizar para mantener la seguridad de la información cuando se accede a esta desde dispositivos móviles.

Este no pretende, describir tal cual el funcionamiento ni implementación detallada de un MdM puesto que existen diferentes fabricantes y sus características tanto de funcionamiento como de implementación varían.