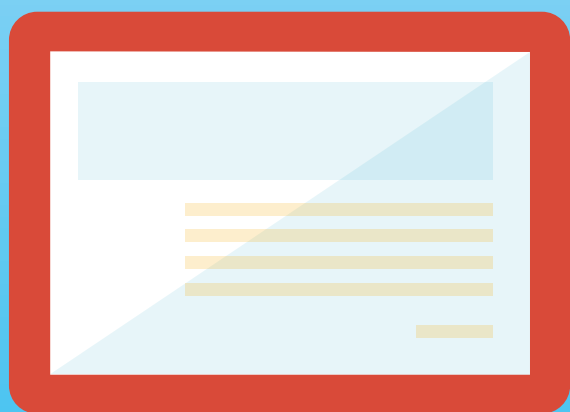


Una solución completa de movilidad segura

para Smartphones y Tabletas



Uhuru® Mobile - Una solución completa






LAS PRINCIPALES CARACTERÍSTICAS DE UHURU MOBILE SON LAS SIGUIENTES:

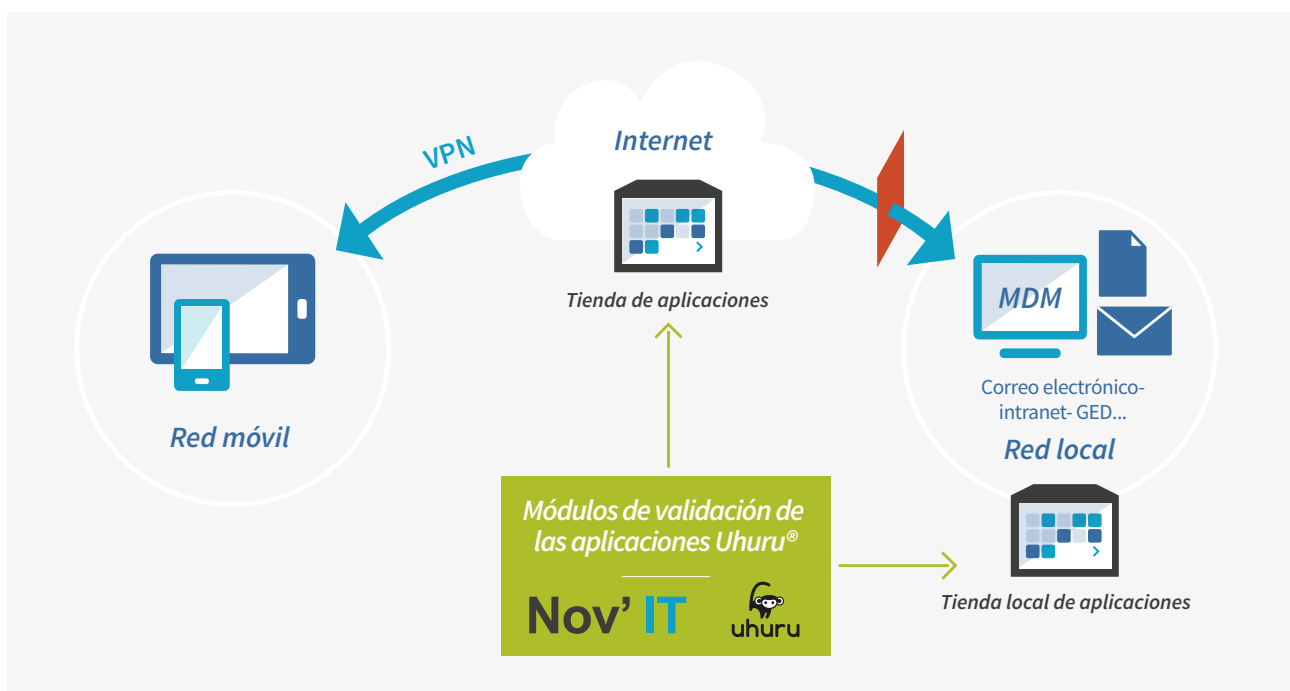
- SOLUCIONES DE SEGURIDAD PARA DISPOSITIVOS MÓVILES:** cifrado de datos, cifrado de voz (VoIP), cifrado de SMS, protección contra malware y exploits
- FACILIDAD DE USO :** los dispositivos móviles con sistemas Android de fácil uso
- GESTIÓN CENTRALIZADA :** mediante una consola Web (MDM)
- CONTROL DE LAS APLICACIONES :** proceso de validación y certificación

Uhuru® mobile es un producto elaborado en el marco de un proyecto denominado “DAVFI” patrocinado parcialmente por el Fondo nacional para la sociedad digital (FSN) administrado por la entidad financiera estatal Caja de Depósitos y Consignación.

Uhuru® mobile funciona en teléfonos móviles de última generación basados en Android® tales como Nexus®, Samsung®, Sony®...

UHURU® MOBILE ES UNA SOLUCIÓN COMPLETA QUE INCLUYE:

-  Un sistema operativo seguro para Smartphones, Tabletas y PCs basadas en Android
-  Módulos para la detección de malware utilizando análisis dinámico y de comportamiento
-  Una tienda de aplicaciones certificadas listas para la instalación en los dispositivos
-  Varias herramientas de validación para la integración de aplicaciones a la tienda
-  Una consola centralizada para la gestión de la flota de dispositivos móviles



Para los smartphones y tabletas

LA PROTECCIÓN DE LOS DISPOSITIVOS MÓVILES SE REALIZA EN TODOS LOS NIVELES DEL SISTEMA:

- | **A NIVEL DE KERNEL:** protección contra la ejecución de códigos desconocidos o maliciosos. Protección contra ataques físicos
- | **A NIVEL DEL SISTEMA:** control de Integridad del Sistema al momento de arranque. Protección dinámica de los recursos críticos. Protección dinámica contra los hooks (llamadas al Sistema)
- | **A NIVEL DE DATOS:** cifrado de datos del usuario. Protección de los recursos de autenticación del usuario (certificados)
- | **A NIVEL DE LAS APLICACIONES:** control de las aplicaciones al momento de arranque del sistema operativo, bloqueo de los privilegios de administrador.
- | **A NIVEL DE LAS COMUNICACIONES:** cifrado de SMS y de VoIP de punto a punto (usando un servidor de señalización)
- | **A NIVEL DE UN SISTEMA DE ENGAÑO:** sistema destinado a engañar a aquellas aplicaciones que emplean GPS sin verdadera legitimidad (enviando coordenadas falsas)

Los equipos son compatibles con todos los operadores móviles

Tienda de aplicaciones

Cada organización (compañías, administración pública etc.) tiene su propia tienda de aplicaciones.

Se analiza y se garantiza la seguridad de cada aplicación antes de integrarla a la tienda de aplicaciones.

Los administradores pueden instalar aplicaciones mediante la consola de administración centralizada. Los usuarios pueden instalar por si mismos las aplicaciones disponibles directamente desde sus terminales.

Todas las aplicaciones que están disponibles se ajustan a la política de seguridad de la organización y al perfil de cada usuario.

Cada usuario tiene un acceso a sus propias aplicaciones dependiendo de las funciones o puesto que desempeña en la organización.

La tienda se encuentra dentro de la organización o puede ser gestionada por Nov'IT (bajo el modelo SaaS)

Las organizaciones tienen un acceso al catálogo vigente y pueden solicitar la inclusión de una nueva aplicación. Una vez probada por Nov'it, se incorpora a la tienda si la misma no contiene ningún tipo de código malicioso

Nov'IT puede analizar, certificar, y publicar una aplicación en una hora

Ningún dato perteneciente al usuario es enviado o almacenado en Nov'IT.

Gestión de dispositivos móviles

Las herramientas de gestión que se encargan de los dispositivos móviles forman parte de la oferta completa de Uhuru® Mobile. La gestión centralizada incluye las siguientes funcionalidades:

- **INSTALACIÓN/ELIMINACIÓN DE APLICACIONES** por usuario o grupo de usuarios
- **INTERCONEXIÓN CON LOS DIRECTORIOS** de empresas e instituciones (LDAP, Active Directory)
- **CONFIGURACIÓN DE LAS CUENTAS DE USUARIO** (correo electrónico, VPN, acceso a directorios)
- **ACCESO MEDIANTE LA CONSOLA WEB**

Proceso de validación de las aplicaciones

Se realiza el **análisis de las aplicaciones** antes del proceso de implementación en equipos. Eso permite disponer de una alta capacidad de cálculo y de una amplia gama de herramientas de validación.

Antes de publicar las aplicaciones a usuarios o administradores por medio de las herramientas de gestión centralizada, Nov'IT realiza un proceso de **validación del comportamiento de las aplicaciones**.

SE LLEVAN A CABO PRUEBAS A PARTIR DE:

- ⊗ Un motor de detección de malware
- ✓ Un motor de análisis estático y dinámico
- 📅 Análisis específicos para detectar vulnerabilidades de seguridad

HASTA LA FECHA, NOV'IT HA VALIDADO MÁS DE 400 APLICACIONES TALES COMO:



CLIENTE DE CORREO ELECTRÓNICO*



NAVEGADOR FIREFOX



LECTOR RSS



REPRODUCTOR DE VIDEO



LECTOR OFFICE/PDF

Ciertas aplicaciones emplean tecnologías de geolocalización sin verdadera legitimidad. En vez de excluirlas, Nov'it prefirió integrar un sistema cuyo objetivo es enviar coordenadas de localización falsas para evitar que los usuarios sean rastreados sin su conocimiento y consentimiento. El administrador tiene la capacidad de deshabilitar esta función. Los usuarios reciben una notificación por medio de una alerta.

**Compatibles con IMAP, IMAP sobre SSL, POP3 y Exchange 2003/2007 (con WebDAV)*