LA SEGURIDAD DE LA INFORMACIÓN EN DISPOSITIVOS MÓVILES PERSONALES DE USO PROFESIONAL

Leal Cubaque, Edicson Daniel
danielleal.col@gmail.com
Universidad Piloto de Colombia

Resumen—El propósito del presente artículo, es identificar algunos de los principales riesgos de seguridad a los que se puede ver expuesta una empresa al no contemplar riesgos inherentes asociados a dispositivos de uso personal en entornos de trabajo y mencionar algunas medidas de seguridad como configuraciones seguras (hardening) y herramientas que ayudaran a mitigar estos riesgos, fortaleciendo la línea base de seguridad que se maneje en el entorno de trabajo actual.

Abstract— the purpose of this article is to identify some of the main security risks to which a company can be exposed when not contemplating inherent risks associated with devices for personal use in work environments. Additionally, mention some security measures such as secure configurations (hardening) and tools that will help mitigate these risks, strengthening the baseline of security that is managed in the current work environment.

Índice de Términos— Dispositivos móviles, seguridad de la información, BYOD, protección de datos.

I. INTRODUCCIÓN

La llegada de los Smartphone ha tenido un impacto importante en la vida de las personas, desde el desarrollo de actividades en su vida cotidiana hasta transportar enormes cantidades de datos de forma sencilla y rápida, generando una tendencia en el mundo, llamada "Bring Your Own Device" (BYOD). Que en español significa "Traer dispositivos personales" y con esto se hace referencia no solo a computadoras, sino a Smartphone, memorias USB, tabletas, incluyéndolos en el día a día y dando oportunidad al teletrabajo. [1] Es aquí donde las empresas deben estar preparadas para estas nuevas metodologías y más teniendo en cuenta que el empleador no puede hacer mayores exigencias a estos dispositivos por temas de privacidad y datos personales.

Sin profundizar mucho en las empresas que han adoptado esta forma de trabajo, podemos ver casos cotidianos donde los empleados acceden al correo corporativo desde un lugar diferente a la oficina mediante celulares, tabletas, etc. El equipo de ventas también maneja información sensible para la empresa al acceder a historiales de clientes o al realizar consultas de productos, servicios y ni hablar de la nueva necesidad de acceder a un servidor corporativo desde un lugar diferente a la organización. Esto último se convirtió en algo indispensable para seguir compitiendo en un mercado digital donde la accesibilidad desde cualquier lugar es decisiva.

Este constante crecimiento de uso de dispositivos móviles personales en las empresas acarrea riesgos de seguridad como son:

- Perdida de información
- Uso de conexiones no seguras
- Robo de dispositivos móviles
- Ingeniería social
- Falta de control sobre aplicaciones que utiliza el usuario

Para respaldar lo anterior es necesario mencionar que según el sitio web Android para desarrolladores, cerca de un 50% de los Smartphone utilizan versiones iguales o inferiores a Android 6.0 lo que muestra una vulnerabilidad latente en el entorno.

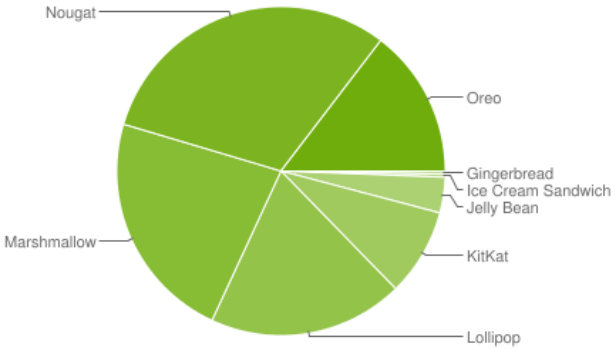

Fig. 1. Versiones de plataforma Android. Obtenida de https://developer.android.com/about/dashboards/

Ante estos riesgos se debe establecer en las empresas, políticas y mecanismos que permitan la gestión de dispositivos móviles de forma segura, adoptando procesos de hardening y haciendo que se cumplan una serie de requisitos que vayan de la mano con las políticas de seguridad de la empresa. Sin

embargo, no podemos dejar de lado el usuario final, el cual debe ser involucrado con los temas de seguridad concientizándolo del correcto uso de los dispositivos, las amenazas y riesgos a los que está expuesta la compañía por un uso inadecuado de dispositivos e información.

II. RIESGOS Y AMENAZAS DE SEGURIDAD

A continuación, daremos una visión general de los principales riesgos a los que está expuesto un dispositivo móvil, destacando los que son de uso personal:

Actualmente los smartphone son unos de los objetivos preferidos por los delincuentes, a pesar de los esfuerzos realizados por el ministerio de las Tic con la inclusión de la Política Nacional de Seguridad y Convivencia Ciudadana, sigue siendo un tema pendiente por controlar, si a lo anterior agregamos que una empresa maneja información sensible un incidente puede representar un valor más alto que el del mismo aparato. Adicionalmente los descuidos de los usuarios al dejar una memoria conectada, o usar dispositivos en lugares públicos sin algunas precauciones, acarrea gastos incalculables al tratarse de información sensible que se almacena en dichos dispositivos.

A. Conexiones no seguras

Empleados con dispositivos móviles verán la necesidad de conectarse a redes externas a la laboral o a la ofrecida por el operador que haya definido la empresa, con el fin de ahorrar datos, mejorar la velocidad o cobertura, en las cuales se realiza intercambio de información sensible de la empresa. Adicionalmente algunos protocolos tienen vulnerabilidades o algoritmos de cifrado débiles por ejemplo, bluetooth o NFC.

B. Robo de credenciales

Los usuarios no son conscientes de los potenciales riesgos que se pueden presentar por abandonar el equipo sin bloquear, usar la misma clave para todas las aplicaciones, guardar contraseñas en la billetera, compartir la clave a familiares para alguna consulta o jugar en los smartphone, puede llegar a generar que personas no autorizadas accedan a información sensible.

C. Ubicación GPS

La instalación de aplicaciones desconocidas puede utilizar este tipo de servicios para acceder a ubicaciones y de esta manera realizar ingeniería social, permitiendo que la competencia intente aprovechar este tipo de datos para descubrir clientes o actividades que generen un peligro para el negocio.

Sin embargo, son más los usos positivos que pueden generar este tipo de servicio al momento de querer realizar seguimientos a despachos de pedidos, seguimiento a vendedores, pero necesariamente debe acompañarse de hardening y políticas de seguridad para los empleados, todo esto sin dejar de lado que podemos hablar de dispositivos personales en los cuales se manejan actividades e información de carácter personal.

D. Usuarios

Son el punto fundamental de la seguridad, ya que por más medidas que se tengan en una empresa, si el usuario no está correctamente informado y capacitado sobre los distintos riesgos que se pueden presentar y cómo manejarlos, se pueden materializar los riesgos y traer consecuencias como perdidas de reputación, económicas, propiedad intelectual, clientes y otro tipo de costos inmersos.

Los usuarios están potencialmente expuestos a ataques de ingeniería social, la cual consiste en manipulación psicológica, es decir, hacer que las personas hagan lo que uno quiere que hagan [2]. Por ejemplo, realizar fraudes haciéndose pasar como trabajador de un banco y solicitar que digiten la clave en el teléfono celular, spoofing que consiste en suplantación de identidades, como lo puede ser páginas web, correo electrónico falseando el origen para que la víctima piense que es de origen de confianza [3].

Cuando un usuario es consciente de este tipo de amenazas y sus consecuencias, podrá aportar a la política de seguridad de la empresa, aprenderá a manejar los distintos incidentes que se presenten, evitará efectos indeseados sobre la información y los dispositivos, se creará un compromiso entre la empresa y el empleado con la seguridad y la información, concientizando sobre el correcto uso de dispositivos no solo móviles sino de cualquier activo de la empresa.

E. Falta de control de la gestión de dispositivos.

Los empleados no son expertos en el manejo de tecnología, y mucho menos en la configuración de aplicaciones, lo cual puede generar que se realice una mala manipulación de configuraciones, se instalen aplicaciones inseguras o modificadas. Las principales detecciones de app modificadas se han encontrado en México y Colombia, las cuales corresponden a una variante en particular llamada Android/Autoins.C. [4] Y podrían traer como consecuencia secuestro de información, e impactos económicos de gran magnitud para la empresa.

III. COMO REDUCIMOS LOS RIESGOS

Para llevar a cabo esta tarea vamos a basarnos en la ISO 27001 y como primera medida se debe identificar los dispositivos críticos que tiene la organización, esto se puede hacer de acuerdo con la clasificación de información que se tenga y al grado de vulnerabilidad, esto con el fin de identificar que controles son necesarios para reducir el riesgo.

Vulnerabilidad es una debilidad que puede afectar un activo o un control de proceso, una vulnerabilidad es la falta de un antivirus. Esto crea una amenaza que es el ataque de un virus que puede deteriorar o destruir la información almacenada en ordenadores, o el software destinado al tratamiento de la información. [5]

Se debe definir que metodología se usará para el análisis y gestión del riesgo, la cual se aplicará en los activos (dispositivos críticos) que la organización defina, asociando vulnerabilidades y amenazas para encontrar el impacto que puede llegar a tener de acuerdo al riesgo existente. Impacto hace referencia a la cantidad de daño que puede causar una amenaza que explota una vulnerabilidad [6]

Dentro de las muchas metodologías que se pueden utilizar para el manejo de riesgos, existe la metodología MAGERIT la cual fue elaborada por el Consejo Superior de Administración Electrónica de España, reuniendo en un documento técnicas y ejemplos de cómo realizar análisis de riesgos [7]. La ventaja de esta metodología es que permite priorizar los riesgos más críticos y adicionalmente está alineada con la norma ISO, lo que siempre será un aporte a la mejora de los sistemas de gestión. Esta metodología está compuesta por un conjunto de guías y un panel de herramientas de apoyo, con sus respectivas guías de uso.

1. Guía de aproximación la cual está orientada a identificar los posibles riesgos, estableciendo un punto de arranque sobre las medidas que se deben tomar a la hora de disponer y ejecutar.
2. Guía de procedimientos y técnicas son suficientes para hacer el análisis y gestión del riesgo en cualquier sistema de información.
3. Guía de responsables del dominio se integra a la guía de procedimientos.
4. Guía para desarrolladores de aplicaciones facilita la inserción de medidas de seguridad adecuadas en proyectos.

Otra opción de metodología es el estándar COBIT el cual es muy conocido ya que fue creado por ISACA 5 para TI y el Gobierno de TI. Definiendo entradas y salidas, objetivos, actividades, medidas de rendimiento y modelo de madurez básico. Está basado en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos agrupados para entregar la información pertinente y confiable que requiere una organización para alcanzar sus objetivos.

Cobit 5 une sus 5 principios permitiendo que las organizaciones construyan un marco efectivo de gobierno y administración basado en los 7 habilitadores.

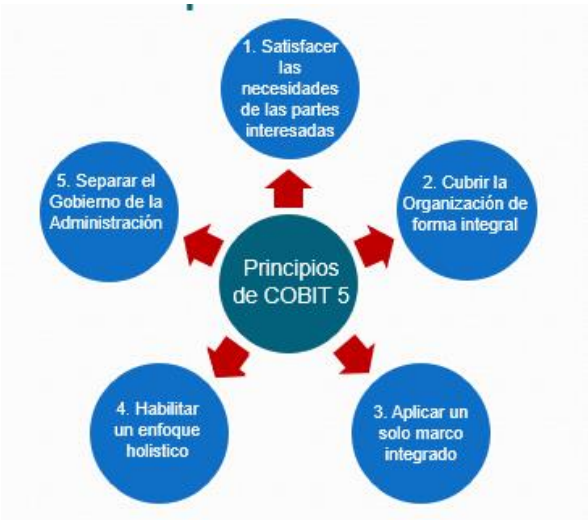

Fig. 2. Principios de cobit 5. Obtenida de https://chauditoriaucaldas1700813714.wordpress.com/2013/12/21/principios-de-cobit-5/

A. Hardening

Debemos asegurar tanto los dispositivos móviles para uso profesional como los datos de la empresa, realizando *hardening* de configuración a cada uno de los elementos donde se almacena o transporta la información, sin dejar de lado que estamos trabajando con equipos personales y no podemos restringir todo. El endurecimiento de configuraciones (Hardening), servirá para minimizar algunos riesgos como acceso no autorizado, perdida de dispositivos, y algunos otros riesgos.

- Contraseñas complejas, acompañado de autenticaciones de múltiple factor y aplicaciones que ayuden a administrarlas.
- Programas de seguridad como filtros, antivirus, antispam según la necesidad y capacidad del dispositivo. No olvidemos que estamos tratando con equipos BYOD los cuales no necesariamente tendrán una configuración de rendimiento óptima.
- Cifrado de datos o del dispositivo teniendo en cuenta que se trabaja con dispositivos de uso personal y que se debe hacer por mutuo acuerdo, dándole a conocer al usuario las ventajas y desventajas de hacer uso de estas medidas de seguridad y acompañándolas de cláusulas donde especifique el mutuo acuerdo.
- Gestionar contraseñas mediante sistemas que garanticen la dificultad de las mismas
- Gestionar las actualizaciones de software en dispositivos, incluyendo los móviles y respaldándolo con una política de actualización y cláusula de mutuo acuerdo con el usuario que presta el dispositivo móvil de uso personal.
- El GPS permitirá localizar dispositivos para su ubicación y seguimiento de manera constante.
- El bloqueo y borrado remoto permitirá eliminar

datos sensibles del dispositivo en caso de robo o de cierta cantidad de intentos fallidos de ingreso.
- Supervisión y seguimiento de las aplicaciones en ejecución sin embargo estas opciones son más completas desde el uso de herramientas como MDM mencionado anteriormente.

Se deben incorporar herramientas que ayuden a gestionar dispositivos móviles MDM (Mobile Device Manageement), MAM (Mobile Application Management), EMM (Enterprise Mobility Management)

- MDM (Mobile Device Manageement), proporciona supervisión de las terminales permitiendo bloquear, controlar y hacer cumplir las políticas de dispositivos. [8]
- MAM (Mobile Application Management) permite controlar los usuarios que acceden a las apps desde los dispositivos autorizados logrando un servicio de valor añadido. [8]
- EMM (Enterprise Mobility Management), es una combinación de gestión de dispositivos móviles (MDM), gestión de aplicaciones móviles (MAM) y gestión de la información móvil (MIM) cubriendo el control de políticas de los dispositivos, la gestión de red y los servicios.

Al tratar dispositivos personales para uso empresarial, se debe prestar mayor atención para asegurar un éxito en la implementación y conseguir una participación activa de los usuarios en la protección de dispositivos e información.

Se debe revisar que servicios realmente se van a utilizar y deshabilitar aquellos que están activos de fabrica con el fin de disminuir las posibles entradas de elementos no deseados, por ejemplo, si no se van a usar servicios DHCP, DNS es recomendable no activar este tipo de servicios en los router, o switch sino en dispositivos que ofrezcan mayor seguridad y robustez. Por lo tanto, se debe deshabilitar estas funcionalidades a través de sus archivos de configuración, como apoyo los fabricantes y algunas empresas dedicadas a temas de seguridad realizan diferentes recomendaciones, sin embargo, es importante mencionar que cada infraestructura tiene una necesidad diferente por lo tanto se debe revisar y ajustar de acuerdo al tipo de industria y negocia, a la necesidad y los recursos disponibles por parte de la empresa.

B. Acuerdos de uso de aplicaciones.

Este puede ser uno de los puntos más difíciles de lograr ya que se debe estar de acuerdo con el usuario que preste el dispositivo personal, sin embargo si se contemplan las aplicaciones cotidianas acompañadas de algunas herramientas que brinde la empresa, se puede lograr un trabajo mancomunado entre empleado y empleador que busque proteger tanto información personal como empresarial, generando un ambiente de seguridad para ambas partes y una reducción de costos en la que se vería un beneficio mutuo.

Sin embargo, se deben tener políticas sobre las aplicaciones permitidas y sugeridas para instalar, teniendo presente que los accesos de algunas apps deben ser gestionados con cautela y de forma preventiva. Este punto debería ir acompañado de una constante orientación al empleado de que apps son sugeridas, las configuraciones sugeridas y/o obligatorias dependiendo el tipo de información y el dispositivo, sitios oficiales de descargas, etc.

C. Cloud.

Teniendo en cuenta que la tendencia de almacenamiento en la nube durante los últimos años ha ido incrementando y dejando de lado el caso de uso que mejor aplica (pública, privada e hibrida) o las capas sobre las que trabaja (infraestructura plataforma y software). [9] Se debe tener cuidado con manera que los empleados está accediendo especialmente con los dispositivos personales, ya que puede ser más seguro tenerlos en la nube y solicitar un acceso adicional que tenerlos guardados en el dispositivo localmente.

Adicionalmente debemos usar el cifrado de comunicación, las condiciones de uso, acuerdos de niveles de servicio con las respectivas penalidades, mantenimiento, procedimientos en casos de incidentes de seguridad, restricciones del proveedor, procedimientos de backup, etc.

D. Backup.

Desde el 31 de marzo de 2011 se celebra el Word Backup Day; día de la copia de seguridad, fecha usada para concienciar la importancia de realizar un respaldo de la información [10]. Pero no basta únicamente con realizar un backup una vez, este debe realizarse de forma periódica y verificar que dicha copia funcione, ya que de nada sirve que hacer una copia de datos desactualizados o que al momento de usarla no funcione. Y a pesar de que no sea una medida que nos protege de ataques, si se realiza de forma correcta se garantizara que se recuperaran los datos de forma rápida.

A pesar de que esta medida es muy común en la empresa, también es muy común realizar copias de seguridad de dispositivos móviles personales de uso corporativo. Es por esto que debemos tener presentes algunas medidas para realizar respaldo teniendo en cuenta las ya mencionadas a lo largo del artículo.

- Realizar los respaldos en un dispositivo distinto, como por ejemplo en la nube. Se sugiere que estos sitios puedan ser gestionados por la misma empresa con el fin de tener control y gestión de la información empresarial sensible.
- Automatizar dichas copias de forma periódica (tener presente la red que se usa).

- Tener procedimientos para realizar y probar copias de seguridad a nivel web y local.
- Capacitar usuarios de manera tal que realizar y restaurar sus copias de seguridad, teniendo control sobre dichas copias y la razón por la cual se están restaurando.

E. Protección de conexiones.

Antes de mencionar algunos mecanismos que aseguren confidencialidad de datos en las comunicaciones, es indispensable sensibilizar al usuario con el fin de que actúen de manera preventiva y cautelosa en redes públicas ya que se encuentran desprotegidas y el empleado es quien puede marcar diferencia al momento de intentar un incidente de seguridad.

La utilización de canales cifrados seguros como las VPN, permitirá crear un túnel a través de internet dando una capa de seguridad adicional para acceder a servicios de la empresa [11].

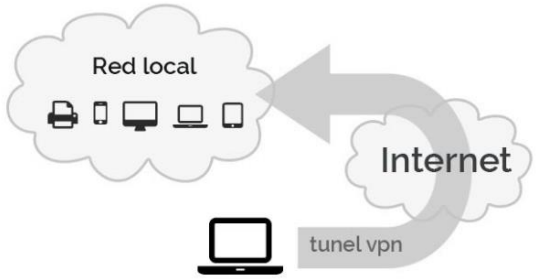

Fig. 3. Conexión a través de VPN. Obtenida de https://www.xataka.com/seguridad/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene

El uso de sitios web seguros con protocolo SSL y certificados permitirán crean un ambiente seguro para los empleados y así proteger los datos. Sin embargo, también se debe hacer uso de mecanismos que comprueben los niveles de seguridad en el equipo remoto que desea conectarse a la red corporativa. Este sistema de comprobación o chequeo de los equipos remotos debe ser percibido como una ayuda a la seguridad ya que se puede estar tratando con dispositivos móviles personales de uso profesional y no como una imposición de la empresa.

Con el protocolo IPSec que nos ofreces la VPN se puede asegurar el flujo de paquetes, garantizar una autenticación mutua, establecer parámetros criptográficos y adicionalmente ayudará al cumplimiento de la Ley de Protección de Datos (LOPD) de España, el negocio será menos vulnerable a ataques, la empresa no se expone a sanciones ni a perdida de reputación.

De igual manera el desactivar la conexión automática a redes permitirá que el usuario sepa en qué momento está conectado su dispositivo, sin embargo, se debe intentar priorizar el uso de redes 3G o 4G.

Las redes de nueva generación (NGN) están orientadas a servicios independientes y ofrecen elementos nuevos y protocolos más eficientes, además la redundancia en configuración, la cual no todas las empresas pueden darse el lujo de poseer, pero cada día se hace más necesario con el fin de garantizar respaldos en caso de fallas de seguridad.

F. Políticas.

Se debe tener presente que las políticas de seguridad están clasificadas en 3 clases. [6]

- **De consejo**: aquí se definen consecuencias a las posibles violaciones, discute las conductas y acciones que son aceptables.
- **De regulación:** Son mandatarias y se deben cumplir de acuerdo a la legislación aplicable para la organización.
- **De información**: informan acerca de objetivos empresariales, misión, visión, etc.

Como se ha mencionado a lo largo del artículo, es necesario que las medidas técnicas de protección de dispositivos móviles estén acompañadas de una regulación corporativa formal como lo son las políticas de uso y de seguridad.

La política debe estar alineada con la misión de la organización y dirigida a roles y no a personas individualmente. Especificando que debe hacer y no quien lo debe hacer.

La política de uso de dispositivos móviles personales debe establecer permisos y restricciones en cuanto al su uso como herramienta de trabajo. De igual manera existen algunos dispositivos que deberían ser incluidos como lo son los smartwatchs y otros que se conectan a los teléfonos. Algunos aspectos mínimos a desarrollar en la política son

- Tipos de dispositivos no autorizados.
- incluir dispositivos BYOD a los requisitos de seguridad y política general de seguridad
- Parámetros de seguridad para dispositivos móviles personales.
- Actualizaciones de aplicaciones y sistema operativo.
- Estar acorde con la ley de protección de datos personales y demás legislación del país.
- Tipo de información a sincronizar en la nube.
- Revisión a las políticas de seguridad de dispositivos móviles personales.
- Incentivar el uso de dispositivos móviles personales con el fin de obtener un beneficio de empleado y empleador.
- Buscar el compromiso de todos los niveles jerárquicos de la empresa.
- Considerar todas las partes involucradas.
- Documentos para firmar el mutuo acuerdo de uso

de dispositivos móviles personales.

G. Registro y seguimiento

El anexo A de la norma ISO 27001:2013 en su literal A.12.4 menciona que se deben registrar eventos y generar evidencia y para esto es necesario tener presentes algunos elementos como son:

- Elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades de usuario.
- Proteger instalaciones e información de registro contra alteración y acceso no autorizado.
- Las actividades del administrador y operador de sistema se deben registrar y revisar con regularidad.
- Los relojes de todos los sistemas deben estar sincronizados con una única fuente de referencia de tiempo.

Estos elementos permitirán tener una gestión avanzada y brindaran una guía de qué tipo de configuraciones adicionales son necesarias para mantener segura nuestra información y el tipo de usuarios que manejan los acceden a los recursos de la organización.

IV. CONCLUSIONES

El uso de dispositivos móviles personales está inmerso en la mayoría de las empresas y se deben crear controles para minimizar los riesgos que representan.

Muchos de los controles mencionados sirven para gestionar dispositivos móviles y de escritorio, lo que representa una inversión única y ahorro en compra de aparatos.

La revisión de seguridad a dispositivos móviles personales crea conciencia tanto al empleado como empleador ya que se maneja información sensible para ambas partes.

La capacitación de usuarios es un punto clave que se debe contemplar a lo largo de cualquier implementación de seguridad.

La competitividad comercial genera la necesidad de acceder a datos remotamente exigiendo a las empresas crear políticas y controles de seguridad enfocados en dispositivos BYOD

Las metodologías de riesgo facilitan la administración de los riesgos ya que aportan un marco de trabajo ya definido

V. REFERENCIAS

[1] H. Balanta, «Colombia Digital,» 6 febrero 2017. [En línea]. Available: https://colombiadigital.net. [Último acceso: 02 10 2018].

[2] welivesecurity, «welivesecurity.com,» eset, 06 enero 2016. [En línea]. Available: www.welivesecurity.com. [Último acceso: 04 10 2018].

[3] a. moreno tablado, «Hacking etico,» [En línea]. Available: www.hackin-etico.com. [Último acceso: 04 10 2018].

[4] D. Giusto Bilic, «Welivesecurity,» eset, 02 marzo 2018. [En línea]. Available: www.welivesecurity.com. [Último acceso: 03 10 2018].

[5] ISOTools, «isotootls.org,» 18 06 2017. [En línea]. Available: www.isotools.org. [Último acceso: 23 11 2018].

[6] J. M. STEWART, «Certified Information Systems Security Professional Guide,» tittel, Canada, 2011.

[7] C. Gutierrez Amaya, «welivesecurity,» eset, 14 05 2013. [En línea]. Available: www.welivesecurity.com. [Último acceso: 2018 11 23].

[8] tuyú technology, «gestion de dispositivos móviles,» gdm, 16 12 2016. [En línea]. Available: www.gestiondispositivosmoviles.com. [Último acceso: 03 10 2018].

[9] A. Iglesias Fraga, «ticbeat,» 01 enero 2018. [En línea]. Available: www.ticbeat.com. [Último acceso: 01 noviembre 2018].

[10] S. Bortnik, «welivesecurity,» 31 03 2011. [En línea]. Available: www.welivesecurity.com. [Último acceso: 08 11 2018].

[11] R. IVAN, «xataka,» 20 08 2018. [En línea]. Available: www.xataka.com. [Último acceso: 10 11 2018].

Autor
Edicson Daniel Leal Cubaque
Ing. de sistemas
Est. Especialización en Seguridad Informática
Universidad Piloto de Colombia
Auditor interno en ISO 27001