ANÁLISIS DE LA SEGURIDAD INFORMÁTICA EN DISPOSITIVOS MÓVILES Y EQUIPOS PERSONALES, Y SU APLICACIÓN EN EL BYOD EN EL ICBF REGIONAL TOLIMA.

DANIEL ALBERTO TRUJILLO CAMPOS
DIEGO ALEXANDER RODRIGUEZ MORA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUÉ TOLIMA
2017

ANÁLISIS DE LA SEGURIDAD INFORMÁTICA EN DISPOSITIVOS MÓVILES Y EQUIPOS PERSONALES, Y SU APLICACIÓN EN EL BYOD EN EL ICBF REGIONAL TOLIMA.

DANIEL ALBERTO TRUJILLO CAMPOS
DIEGO ALEXANDER RODRÍGUEZ MORA

Trabajo de grado (monografía) presentado como requisito para optar al título de Especialista en seguridad informática

Director: JUAN JOSÉ CRUZ GARZÓN
Ingeniero de sistemas
Docente ocasional ECBTI UNAD

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUÉ TOLIMA
2017

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del Jurado

_____
Jurado

_____
Jurado

Ibagué, diciembre 5 de 2017

Dedicatoria

A mi esposa e hijos por ser mi inspiración, gracias por su apoyo y comprensión estoy dando por culminada una etapa más de la vida, esto es por y para ustedes.

Daniel Alberto Trujillo Campos

Dedicatoria

Dedicado a mi familia que siempre me ha apoyado y ha creído en mí, a mi futura esposa Carolina Barreto Núñez quien me ha acompañado en este duro pero fructífero proceso. Cada escaño que subo es gracias a ustedes.

AGRADECIMIENTOS

Al finalizar un trabajo tan importante y arduo como lo es una Especialización, quisiéramos agradecer a la UNAD por la posibilidad que nos ha brindado de recibir una formación académica de alta calidad con la flexibilidad que su esquema de aprendizaje ofrece, gracias a ello realizamos un proceso de formación exitoso que nos permitió seguir con nuestra vida laboral y personal.

Al ICBF un gran agradecimiento por habernos dado la posibilidad de trabajar allí durante nuestro proceso formativo, esto permitió ampliar y aplicar los conocimientos adquiridos en nuestra formación, logrando aplicar este último trabajo en una necesidad real de la institución.

Para nuestro asesor de trabajo el Ingeniero Juan Jose Cruz Garzon, gratitud total por su apoyo, interés y entrega permanente a este trabajo de grado, toda su dedicación y recomendaciones permitieron culminar el mismo a feliz término.

TABLA DE CONTENIDO

Pag.

LISTA DE TABLAS

Pag.

LISTA DE FIGURAS

Pag.

LISTA DE ANEXOS

Pag.

GLOSARIO

ACCESS POINT: “Dispositivo de hardware o software que actúa como un centro de comunicación para los usuarios de dispositivos inalámbricos que desean conectarse a una LAN cableada. Son importantes para proporcionar mayor seguridad inalámbrica y para ampliar el rango físico de servicio a un usuario móvil.”[1]

ANDROID: “sistema operativo para dispositivos móviles basado en núcleo Linux, fue creado por Android Inc., respaldado por el gigante Google, es un sistema pensado para dispositivos táctiles, aunque se distribuye en diferentes modos de presentación”[2], en su versión más actual encontramos Android 8.0 Oreo.

BACKUP: “Copia adicional de los archivos de la computadora que generalmente se guarda en un lugar físicamente separado de los originales. Resulta fundamental para la recuperación cuando se dañan o se pierden los archivos originales.”

BLACKBERRY OS: sistema operativo multitarea para dispositivos móviles desarrollado por BlackBerry, originalmente creado con similitudes al sistema presentado por RIM para computadoras de mano en 1999.

BLUETOOTH: protocolo de comunicación diseñado para dispositivos de bajo consumo que permite la transmisión de voz y datos mediante un enlace de radiofrecuencia en la banda ISM de 2,4GHz.

COBIT: Es un modelo utilizado para valorar los sistemas de información de una entidad.

CONFIDENCIALIDAD: Según [ISO/IEC 13335-1:2004]: se define como: " característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados”.

CONPES: El Consejo Nacional de Política Económica y Social fue creado por la Ley 19 de 1958. Ésta es la máxima autoridad nacional de planeación y se desempeña como organismo asesor del Gobierno en todos los aspectos relacionados con el desarrollo económico y social del país. Para lograrlo, coordina y orienta a los organismos encargados de la dirección económica y social en el Gobierno, a través del

[1] EL SALVADOR. MINISTERIO DE HACIENDA. GLOSARIO SGSI sistema de gestión de seguridad de la información. (2009) [En línea]. San Salvador: Ministerio. Disponible en http://www.mh.gob.sv/portal/page/portal/sgsi/MH_GLOSARIO/Glosario%20para%20Portal.pdf

[2] Tavera Jaramillo, W. y Mahecha Rivera, M. (2016). Identificación de los ataques más realizados en un sitio concurrido por personas que utilizan sus dispositivos móviles y determinación de las vulnerabilidades más comunes en el sistema operativo Android. 115 p. Colombia. Disponible en http://hdl.handle.net/10596/6337

estudio y aprobación de documentos sobre el desarrollo de políticas generales que son presentados en sesión[3].

CONTRASEÑA: Es una palabra o frase secreta, utilizada para acceder a ciertas funciones informáticas.

DELITO INFORMÁTICO: Según OJEDA:

> Está vinculado no sólo a la realización de una conducta delictiva a través de medios o elementos informáticos, o a los comportamientos ilícitos en los que aquellos sean su objeto, sino también a la afectación de la información cómo bien jurídico tutelado, diferente de los intereses jurídicos tradicionales. Toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor, o que, por el contrario, produce un beneficio ilícito a su autor aun cuando no perjudique de forma directa o inmediata a la víctima, y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas.[4]

DLP: (Data Loss Prevention) detecta posibles filtraciones de datos / transmisiones de filtrado de datos y los previene supervisando, detectando y bloqueando datos confidenciales mientras está en uso (acciones de punto final), en movimiento (tráfico de red) y en reposo (almacenamiento de datos).

DMZ: Es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permiten a la red externa.[5]

DOMINIO: Conjunto de objetos con información y políticas de seguridad comunes. En el Microsoft Active Directory es una colección de recursos (cuentas, impresoras, computadoras) que constituyen una frontera de administración y de aplicación de políticas de seguridad.[6]

FIREWALL: Hardware o software que tiene la capacidad para limitar el acceso entre las redes o sistemas conforme a lo estipulado en las políticas de seguridad.[7]

---

[3] COLOMBIA. Departamento de planeación nacional. El Consejo Nacional de Política Económica y Social, CONPES. Ley 19 de 1958. [En Línea]. Bogotá: DPN. Disponible en https://www.dnp.gov.co/CONPES/Paginas/conpes.aspx

[4] OJEDA, Jorge Eliecer, et al. Delitos informáticos y entorno jurídico vigente en Colombia. En: Cuadernos de Contabilidad. 2010. vol. 11, no. 28, p. 41-66. Disponible en http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003&lng=en&tlng=es

[5] El Salvador. MH Glosario SGSI. Óp. Cit., p. 1

[6] Ibíd., p. 1.

[7] Ibíd., p. 1.

HABEAS DATA: Es el derecho que tiene toda persona o institución a solicitar a información que sobre sí mismo se encuentre almacenada en cualquier base de datos y el derecho de ser actualizada o eliminada si así se requiere

HARDWARE: cualquier componente físico tecnológico, que trabaja o interactúa de algún modo con el computador. Incluye elementos internos como el disco duro, CD-ROM, y también hace referencia al cableado, circuitos, gabinete, etc. E incluso a elementos externos como la impresora, el mouse, el teclado, el monitor y demás periféricos.

ICBF: Instituto Colombiano de Bienestar Familiar.

IDS: de sus siglas en inglés (Intrusion Detection System) sistemas de detección de intrusos. Consiste en la de detección de accesos no autorizados a un computador o sistema informático

INFORMACIÓN: Hace referencia a la representación de hechos, que son recopilados para efectuar operaciones comerciales. Utilizada de manera intercambiable con datos, el término incluye, archivos de datos estructurados y no estructurados, archivos de audio o vídeo, mensajes electrónicos o de correo de voz, fax u otro tipo de mensajes, impresos, copias de respaldo o archivadas del original por cualquier medio, etc.

IPS: Sistema de Protección de Intrusiones. Son necesarios para redes que incorporan servidores con aplicaciones críticas y deben ser protegidas con filtrado de antispam en correos entrantes

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

ITIL: un conjunto de libros que ofrecen una guía que constituyen las mejores prácticas en la provisión de servicios TIC en base a los requeridos del cliente

MAGERIT: Es una metodología de análisis y gestión de riesgos.

MDM (Mobile Device Manager): es un tipo de software que permite asegurar, monitorizar y administrar dispositivos móviles sin importar el operador de telefonía o proveedor de servicios. La mayoría de las MDM permiten hacer instalación de aplicaciones, localización y rastreo de equipos, sincronización de archivos, reportes de datos y acceso a dispositivos, todo esto de manera remota. Este tipo de aplicaciones ha tenido una gran aceptación por parte de las empresas y su crecimiento ha sido realmente vertiginoso, esto se ha debido en gran medida a la popularidad que han tenido los Smartphones dentro de las corporaciones.

OPEN SOURCE: El código abierto es un modelo de desarrollo de software basado en la colaboración abierta1. Se enfoca más en los beneficios prácticos (acceso al código fuente) que en cuestiones éticas o de libertad que tanto se destacan en el software libre.

OSI: El modelo de interconexión de sistemas abiertos, más conocido como "modelo OSI", es un modelo de referencia para los protocolos de la red de arquitectura en capas, creado en el año 1980 por la Organización Internacional de Normalización. Se ha publicado desde 1983 por la Unión Internacional de Telecomunicaciones y, desde 1984, la Organización Internacional de Normalización también lo publicó con estándar.

PERFILES DE USUARIO: son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

PERFILES O ROLES: Conjunto de privilegios agrupados bajo un nombre, que permiten realizar una administración más efectiva de los derechos de acceso.[8]

ROUTERS: Facilita conectividad a nivel de red, la función principal es remitir paquetes o interconectar subredes

SEGURIDAD ACTIVA: Se encarga de prevenir, detectar y evitar cualquier incidente en los sistemas informáticos antes de que se produzca (medidas preventivas). Por ejemplo, utilización de contraseñas.

SEGURIDAD FÍSICA: Se asocia a la protección física del sistema ante amenazas como inundaciones, incendios, robos, etc.

SEGURIDAD INFORMÁTICA: La seguridad informática se refiere a las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad.[9]

SEGURIDAD LÓGICA: Mecanismos que protegen la parte lógica de un sistema informático (datos, aplicaciones y sistemas operativos). Uno de los medios más utilizados es la criptografía.

---

[8] Ibíd., p. 1.

[9] P, Aguilera. Seguridad Informática, 3ª Edición., Editorial EDITEX S.A. Madrid España 2010. Disponible en http://www.editex.es/RecuperarFichero.aspx?Id=19810

SEGURIDAD PASIVA: Comprende todas aquellas técnicas o procedimientos necesarios para minimizar las consecuencias de un incidente de seguridad (medidas correctoras). Por ejemplo, las copias de seguridad.

SGSI: Sistema de gestión de la seguridad de la información. Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

SISTEMA DE INFORMACIÓN: es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.

SOFTWARE MALICIOSO: es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

SOFTWARE: es todo programa o aplicación programada para realizar tareas específicas.

Tecnologías de Información (TI): Para Gandini: “se refieren a una rama de la tecnología que se dedica al estudio, aplicación y procesamiento de datos, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, así como el desarrollo y uso del "hardware", "firmware", "software", cualquiera de sus componentes y todos los procedimientos asociados con el procesamiento de datos.”[10]

TIC: tecnologías de la información y las comunicaciones.

VULNERABILIDADES: son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la empresa (amenazas), las cuales se constituyen en fuentes de riesgo.

WIFI: composición inglesa de las palabras “Wireless Fidelity” que indica el mecanismo de conexión de manera inalámbrica de los dispositivos electrónicos.

---

[10] GANDINI, Isabella. Ley de Delitos Informáticos en Colombia, 2010. [En Línea]. disponible en http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia

WINDOWS PHONE: sistema operativo desarrollado por la multinacional Microsoft, fue el sistema que desplazó a Windows Mobile, este sistema integra múltiples servicios predeterminados en su instalación para su fácil manejo, actualmente comanda la marca de Nokia en dispositivos móviles.

Resumen
En la actualidad la movilidad es una tendencia que ha estado incursionando en todos los ámbitos a un nivel exponencial, los computadores, portátiles, el internet inalámbrico, los teléfonos inteligentes, las tabletas y las redes 3G y 4G, presentan constantes avances a diario, y es el entorno organizacional el que más se ha visto influenciando por los dispositivos móviles, dado a la facilidad de trabajo que otorgan.

El Hardware ha sido uno de los obstáculos en las entidades estatales, por limitaciones presupuestales para la compra o alquiler de equipos, sumado a la obsolescencia de los equipos con los que se cuenta, por ello en algunas ocasiones se termina implementando el BYOD (Traiga su propio equipo), lo cual proporciona facilidad de trabajo para las personas que están vinculadas a la entidad, pero agrega múltiples riesgos a la seguridad de la información que se manipula en dichos dispositivos de propiedad de las personas.

Dentro del presente proyecto se busca proponer un estudio metodológico de la seguridad informática en los dispositivos móviles, aplicado al entorno estatal colombiano y en particular al ICBF Regional Tolima en el denominado BYOD, tendencia que supone todo un nuevo reto en la protección de la información corporativa.

Palabras clave: BYOD; Información; Controles; Políticas; Seguridad.

Abstract
Nowadays the mobility is a trend that has been dabbling into all the areas at a considerable level, computers, laptops, internet wireless, smart phones, tablets and 3G and 4G technologies have showed a constant progress. The organizational environment has been remarkably influenced by mobile devices, given by the facility of work that they provide.

Hardware has been one of the obstacles in the entities of the Government, due to budgeting limitations for the purchase or rental of equipment, added to the obsolescence of the equipment that is counted, for that reason sometimes it ends up implementing the BYOD (Bring your own equipment), which provides facility of work for people who are linked to the entity, but adds multiple risks to the security of the information that is handled in those devices owned by individuals.

This project propose a methodological study of computer security on mobile devices, applied to the Colombian Government environment, particularly to the Regional Tolima ICBF in the so-called BYOD, this trend represents a new challenge in corporate information protection.

Keywords: BYOD; Information; Controls; Policies; Security.

INTRODUCCIÓN

La movilidad en informática tal y como se usa hoy en día hace 3 décadas parecía algo de ficción, pero en la era actual esta tendencia incursiono en todos los ámbitos a un nivel exponencial, los computadores, portátiles, el internet inalámbrico, los teléfonos inteligentes, las tabletas y las redes 3G y 4G, presentan constantes avances a diario y algunas de las tecnologías que aún no se terminan de conocer, quedan obsoletas rápidamente, y es el entorno organizacional es el que más se ha visto influenciando por los dispositivos móviles que son un imperante a la hora de trabajar y apoyar la toma de decisiones. En la mayoría de las Empresas de la actualidad, el uso de tecnologías móviles es cotidiano y representa un alto flujo de información interna y hacia el exterior.

El Hardware siempre ha sido un obstáculo en las entidades del estado dado a limitaciones en el presupuesto para la compra o alquiler de equipos, sumado a la obsolescencia de los equipos con los que se cuenta, por ello en algunas ocasiones se termina implementando el BYOD (Traiga su propio equipo), lo cual proporciona facilidad de trabajo para las personas que están vinculadas a la Entidad, pero agrega múltiples riesgos a la seguridad de la información que se manipula en dichos dispositivos de propiedad de las personas.

Dentro del presente proyecto se busca realizar un análisis de la seguridad informática en los equipos personales y dispositivos móviles, aplicado al entorno estatal colombiano y en particular al ICBF Regional Tolima en el denominado BYOD (Traiga su propio equipo) tendencia que supone todo un nuevo reto en la protección de la información corporativa.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

El avance tecnológico y la masificación de dispositivos móviles, genero un cambio cultural mundial en la última década y pasamos de una informática que giraba en torno al computador, a una gran gama de servicios soportados en dispositivos móviles, que no solo son aplicables para el entretenimiento sino también en entornos académicos y empresariales.

Lo anterior género que la dinámica organizacional incluyera los dispositivos móviles como herramientas de trabajo, dado su portabilidad y practicidad de uso, por eso no es extraño encontrar empresas que entregan dispositivos a sus empleados o que, ante la limitante del recurso económico para invertir en los mismos, permita que los empleados lleven sus propios aparatos para ser puestos al servicio de la organización.

Una tendencia mundial apunta al (BYOD), que consiste en una política organizacional que permite, alentar, estimular o imponer, a sus empleados a que utilicen para su trabajo, sus propios dispositivos móviles (portátiles, teléfonos inteligentes, notebooks o tabletas), pudiendo acceder con ellos a recursos privilegiados de la empresa, tales como correo electrónico, suites colaborativas, servidores de archivos, bases de datos, las aplicaciones y a los datos personales de la empresa. Esta tendencia no ha sido ajena a las organizaciones estatales colombianas, y en el caso particular del ICBF Regional Tolima, donde se ha venido experimentando un aumento de esta en los últimos años.

Según lo anterior se plantean varios interrogantes en la aplicación del BYOD en una organización estatal como el Instituto Colombiano de Bienestar Familiar Regional Tolima:

¿La utilización de dispositivos móviles personales en el ICBF Regional Tolima es un deber, o es opcional?, en cualquiera de los dos escenarios ¿está reglamentado?, es decir ¿existen políticas, acuerdos o cláusulas contractuales que limiten el uso de la información institucional?

Algunas de la ventajas de esta práctica radica en que la entidad no gastara fortunas con leasing, compra o alquiler de hardware, pues sus empleados y contratistas aportaran este recurso, que generalmente es de tecnología de punta, aspecto que a veces es un poco más demorado con la tecnología perteneciente a la organización, pero el trasfondo de esta práctica mal aplicada puede acarrear más inconvenientes de seguridad en la información que ventajas de desempeño, por ello es importante a lo largo del presente trabajo analizar las preguntas planteadas con el fin establecer métodos que subsanen los riesgos implícitos en el BYOD.

En algunos estudios se han presentado cifras de quienes creen que se presenta más eficiencia en el empleado que usa su dispositivo en el trabajo y puede usar la tecnología que es de su agrado para desarrollar las actividades cotidianas, incluso Fortinet realizó una encuesta en 15 países donde se pudo comprobar que el 74% de los encuestados adoptan el BYOD como una tendencia y de ellos el 52% considera que usar sus dispositivos en el trabajo es más un `derecho´ que un `privilegio´ y el 48% lo ve como un derecho[11].

No obstante, todas las ventajas anteriormente descritas, no deja de tener un factor importante de riesgo, dado que la seguridad de la información en de dichos dispositivos se torna en un reto para las organizaciones y sus usuarios, pues se debe proteger los dispositivos, las aplicaciones, los datos que viajan por las redes móviles, y los datos almacenados en ellos.

Por ello se hace necesario dar a conocer los riesgos asociados a estos dispositivos con el fin de asumirlos y ofrecer opciones de minimizarlos y que los mismos sean asumidos por las organizaciones.

Todos los pronósticos apuntan a que esta tendencia ira aumentando, según recientes estudios de Ovum sostiene que: "los empleados en mercados de rápido crecimiento ven a BYOD como una forma de avanzar en sus carreras. Así, un 79% piensa que la constante conectividad con aplicaciones de trabajo les permite realizar mejor sus tareas, comparado con un 53,5% en mercados maduros."[12]

Es importante establecer algunos parámetros a la hora de adoptar o no esta tendencia, dado que expertos en el tema consideran un riesgo muy amplio el de promover estas prácticas en la organización, para Fabio Assolini, analista sénior de malware en Kaspersky Lab cree que:

"Aunque no se niegan las tremendas ventajas de que cada empleado "cargue" datos importantes y hasta se sienta impulsado a trabajar desde casa sin pagarle horas extra, medianas y grandes empresas deberían considerar los siguientes riesgos, principalmente en lo que se refiere al tráfico de información importante mediante correo electrónico."[13]

También, Fabio Assolini destaco formas sencillas para atacar una móvil:

---

11 BYOD impone a las empresas el desarrollo urgente de estrategias de seguridad, disponible en http://www.networkworld.es/actualidad/byod-impone-a-las-empresas-el-desarrollo-urgente-de-estrategias-de-seguridad

12 La adopción de BYOD es más acelerada en mercados de rápido crecimiento. [En Línea]. disponible en http://www.la.logicalis.com/noticias-y-eventos/noticias/informe-byod.aspx

13 BYOD ¿el futuro o la ruina de las grandes compañías? [En Línea], disponible en http://www.revistasumma.com/gerencia/41548-byod-el-futuro-o-la-ruina-de-las-grandes-companias.html

Estas son las 4 formas más sencillas en las que un dispositivo móvil puede ser hackeado, haciendo peligrosamente vulnerable la información personal del usuario, y para el tema que estamos considerando, los valiosos datos del lugar donde trabaja:

1. Un e-mail sin doble factor de autenticación es vulnerable, si se pierde o es robado el dispositivo.
2. ¿Una red WiFi sin protección VPN es altamente riesgosa?
3. ¿La filosofía "instale lo que quiera" permite que aplicaciones engañosas (malware) y exploits vulneren la seguridad de nuestra red corporativa?
4. La ausencia de políticas DLP (Data Loss Prevention) por parte del usuario y la compañía.[14]

Cisco por medio del Grupo de soluciones empresariales para Internet (IBSG, Internet Business Solutions Group) expandió su estudio original y genero un interesante documento llamado BYOD:

> una perspectiva global, el cual muestra un estudio con encuestas y cifras sobre el "BYOD y virtualización" con el fin de incluir en el sondeo a personas que toman decisiones de TI en empresas de 1000 o más empleados y en empresas medianas (entre 500 y 999 empleados) en ocho países en tres regiones. Sus resultados mostraron claramente que el crecimiento de BYOD no se limita a los Estados Unidos ni a las grandes empresas, sino que también está incursionando en Pymes abarcando países en vía de desarrollo[15].

1.2 FORMULACIÓN DEL PROBLEMA

¿De qué manera la utilización de dispositivos móviles y equipos personales brindara la adecuada seguridad de la información, mediante la utilización en el BYOD en desarrollo de las actividades del ICBF-Regional Tolima?

[14] Ibíd., p. 1.
[15] BYOD: una perspectiva global. [En Línea]. Disponible en http://www.cisco.com/web/about/ac79/docs/re/byod/BYOD_Horizons-Global_LAS.pdf

2. JUSTIFICACIÓN

Históricamente la seguridad ha sido parte inherente al ser humano en todos los ámbitos de la vida, por lo que el avance en las tecnologías de información planteo un nuevo escenario en el cual deben estar inmersos todos los actores dentro de una organización con el fin de salvaguardar los activos de información.

El contenido del presente trabajo tiene como fin recopilar información existente de la seguridad en dispositivos móviles orientados al BYOD, dado que se convirtió en una tendencia mundial por el avance de las tecnologías y facilidad de acceso a los dispositivos móviles, los cuales están siendo usados al interior de las empresas.

La idea es que el contenido recopilado y estructurado, sirva como consulta y guía para las organizaciones estatales en Colombia particularmente en el ICBF Regional Tolima, que por su estructura organizacional similar aplicaría para el resto de las sedes, que están siendo inmersas en esta tendencia voluntaria e involuntariamente, dado que el BYOD se puede presentar con consentimiento del personal de TI o sin su consentimiento. Se reunirán antecedentes, estado actual del arte, hacia dónde va la tendencia, buenas prácticas para su aplicación y verificación de los riesgos asociados a los dispositivos móviles.

En el escenario del Instituto Colombiano de Bienestar Familiar Regional Tolima, cabe revisar los procedimientos existentes para el uso de los dispositivos móviles y los recursos que están utilizando en la nube desde hace más de 4 años, dado que legalmente existen políticas de confidencialidad e integridad de cierta información institucional, pero que no se evidencian las mismas en la tecnología móvil, lo cual plantea varios riesgos que deben ser identificados y medidos con el fin de poder ser controlados, pues la verificación inicial demuestra desconocimiento de los empleados y contratistas de la responsabilidad que tienen frente a la integridad, disponibilidad y confidencialidad de la información.

El riesgo actual en el ICBF tiende a aumentar, más aún cuando se está implementando redes WIFI en algunas sedes que no contaban con el servicio y algunos contratos están indicando que dentro de la autonomía técnica y administrativa de los contratistas deben aportar su equipo de cómputo para la ejecución de este, lo cual evidencia sin duda una incursión en el BYOD, pero sin la debida planificación.

La importancia del presente proyecto, radica en que la mayoría de las organizaciones no se encuentran preparadas en diversas áreas fundamentales no solo para BYOD sino para todas las demás tendencias o iniciativas móviles, se estima que menos de la mitad de las grandes empresas y un tercio de las medianas tienen una política vigente en relación con el acceso a la red corporativa por parte de los dispositivos móviles de propiedad de los empleados, por lo que la presente monografía puede presentarse como una importante guía que de una visión global del BYOD,

pero a la vez ofrezca buenas prácticas para implementar la misma, donde los riesgos sean conocidos y la organización defina si los asume o no.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar el estado actual de la aplicación del BYOD (Traiga su propio equipo), antecedentes, avances tecnológicos, ventajas y desventajas. con el fin de estudiar la seguridad de la información en los dispositivos móviles y equipos personales en su entorno dentro de la organización estatal Instituto Colombiano de Bienestar Familiar Regional Tolima, con el objeto de establecer la viabilidad o no de sobre el uso de equipos y dispositivos móviles personales. que, a pesar de no ser propiedad de la entidad, si contienen información institucional la cual debe ser clasificada, tratada y protegida.

3.2 OBJETIVOS ESPECÍFICOS

1. Revisar antecedentes y estado actual del BYOD, ventajas, desventajas y casos de éxito.
2. Indagar la seguridad en la información en el manejo actual que se está dando al uso de suites colaborativas y dispositivos móviles en el Instituto Colombiano de Bienestar Familiar Regional Tolima.
3. Generar un análisis sobre el uso de los dispositivos móviles en el Instituto Colombiano de Bienestar Familiar Regional Tolima.
4. Diagnosticar el uso de las herramientas para dispositivos para el desarrollo de las actividades del instituto.
5. Conocer el impacto de la aplicabilidad en el entorno de la seguridad informática del instituto.
6. Conocer la perspectiva de los usuarios y personal de TI, del ICBF Regional Tolima sobre la aplicación del BYOD.
7. Analizar la seguridad informática en la implementación del BYOD en el ICBF Regional Tolima, y realizar recomendaciones sobre su viabilidad.

4. MARCO REFERENCIAL

Dentro del proyecto se analizará el BYOD como nueva tendencia mundial, sus alcances y limitantes para la seguridad informática de la entidad estatal ICBF Regional Tolima, además consultaran antecedentes, bibliografía, normas, metodologías, marcos referenciales, y marcos legales concernientes a la seguridad en dispositivos móviles y personales aplicados al BYOD, con el fin de generar un revisión sobre el estado del arte, las ventajas y las desventajas de aplicarlo y generar unas recomendaciones sobre la aplicabilidad del BYOD en el ICBF Regional Tolima.

A continuación, se relacionan los marcos referenciales, estándares, normas, metodologías concernientes a la seguridad de la información y relacionadas con el BYOD.

4.1 MARCO TEÓRICO

4.1.1 ISO 27000.

Marulanda E. lo describe como: "ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. La seguridad puede ser vista como una medida de robustez de un sistema, respecto a una política de seguridad."[16]

Páez Gonzales nos da una breve descripción de la línea de tiempo para la ISO 27000:

> Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution), es responsable de la publicación de importantes normas como: 1979 Publicación BS 5750 - ahora ISO 9001, 1992 Publicación BS 7750 - ahora ISO 14001, 1996 Publicación BS 8800 - ahora OHSAS 18001.
>
> La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de su información. En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta última norma se renombra como ISO 27002:2005 el 1 de Julio de 2007 manteniendo el contenido, así como el año de publicación formal de la revisión.
>
> A semejanza de otras normas ISO, según (Organization, 2008) la 27000 es realmente una serie de estándares. Los rangos de numeración reservados por ISO van desde

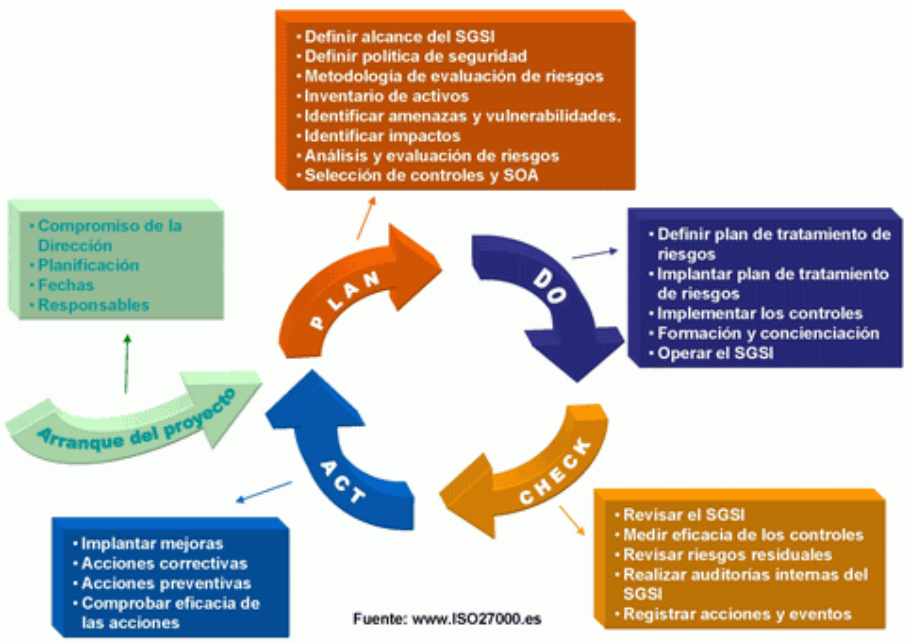
[16] Marulanda Ecehevrry, c. y López Trujillo, m. y Cuesta Iglesias, c. (2009). Modelos de desarrollo para gobierno TI. Scientia Et Technica, [en línea] XV(41), pp.185-190. Disponible en http://www.redalyc.org/articulo.oa?id=84916680032

27000 a 27019 y de 27030, 27044, pasando por 27001, 27002, 27003, 27004, 27005, 27006, 27007, 27011, 27031, 27032, 27033, 27034 y 27799.[17]

Según Echeverria una breve descripción del ISO 27000 y su implementación podría ser:

Básicamente el desarrollo del proceso para la implementación del modelo ISO 27000, se fundamenta en los elementos que aparecen en la figura 1:

Figura 1. Implementación del modelo ISO 27000



Fuente: ISO 27000

Inicialmente se deben tener en cuenta las siguientes fases:

1. Compromiso de la Dirección
2. Planificación, fechas, responsables

Implementación: La cual se puede dar teniendo en cuenta los siguientes elementos: definir plan de tratamiento de riesgos, implantar plan de tratamiento de riesgos, implementar los controles, formación y concienciación, desarrollo del marco normativo necesario, gestionar las operaciones del SGSI y todos los recursos que se le asignen e implantar procedimientos y controles de detección y respuesta a incidentes de seguridad.

Seguimiento: Se dimensiona de la siguiente manera: ejecutar procedimientos y controles de monitorización y revisión, revisar regularmente la eficacia del SGSI, medir la eficacia de los controles y revisar regularmente la evaluación de riesgos así:

[17] Páez González, Daniel David, 2017, propuesta de metodología de evaluación de seguridad informática, aplicada a proveedores de servicios de pequeñas y medianas empresas (Pyme), que accedan a información de personas físicas en el municipio de Toluca, estado de México. ri.uaemex.mx [en línea]. 2017. Disponible en http://ri.uaemex.mx/handle/20.500.11799/67693

1. Realizar regularmente auditorías internas.
2. Revisar regularmente el SGSI por parte de la Dirección
3. Actualizar planes de seguridad
4. Registrar acciones y eventos que puedan tener impacto en la eficacia o el rendimiento del SGSI.

Mejora continua: Como resultado de la implantación de los pasos anteriores se procura el mejoramiento continuo así:

1. Implantar mejoras
2. Acciones correctivas
3. Acciones preventivas
4. Comunicar las acciones y mejoras
5. Asegurarse de que las mejoras alcanzan los objetivos pretendidos. [18]

4.1.2 ISO 27001

Para Betancourt un breve repaso de la ISO 27001 es:

La última versión de esta norma fue publicada a finales del 2013, y corresponde a la principal norma de la serie 27000 debido a que contiene los diferentes requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información en las organizaciones independientes de su tipo, tamaño o naturaleza. Esta norma también incluye los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adoptadas a las necesidades de la organización.

La versión 2013 de la norma ISO 27001, alineo su estructura conforme a los lineamientos definidos en el Anexo SL12 de las directivas ISO/IEC, con el objetivo de mantener la compatibilidad entre las normas ISO de sistemas de gestión que se han ajustado a este anexo. Este enfoque de la estructura de la nueva ISO27001:2013 basado en el Anexo SL, les ayuda a las organizaciones que deseen integrar sus diferentes sistemas de gestión, como el de Calidad, Ambiental, Seguridad de la Información, etc., en un único sistema integrado de gestión, debido a que las normas ISO que se han ajustado al Anexo SL, manejan aspectos comunes como, la misma estructura de alto nivel e idénticos títulos de numerales, textos y términos.

Los dominios de la norma ISO/IEC 27001:2013 corresponde a los diferentes capítulos que establecen los requerimientos que las organizaciones deben cumplir para el establecimiento de un Sistema de Gestión de Seguridad de la Información, los cuales se resumen a continuación:

- INTRODUCCIÓN
- OBJETO Y CAMPO DE APLICACIÓN
- REFERENCIAS NORMATIVAS
- TÉRMINOS Y DEFINICIONES

[18] Ecehevrry, C. E. M., Trujillo, M. L., & Iglesias, C. A. C. (2009). Óp. Cít. P. 189

- CONTEXTO DE LA ORGANIZACIÓN
- LIDERAZGO
- PLANIFICACIÓN
- SOPORTE
- OPERACIÓN
- EVALUACIÓN DE DESEMPEÑO
- MEJORA [19]

4.1.3 ISO 27002

Para Tovar Piraban la ISO 27002:

> Consiste en una guía de buenas prácticas que permiten a las organizaciones mejorar la seguridad de su información. Con este fin, define una serie de objetivos de control y gestión que deberían ser perseguidos por las organizaciones. Éstos se hallan distribuidos en diferentes dominios que abarcan de una forma integral todos los aspectos que han de ser tenidos en cuenta por las organizaciones.
>
> Dominios de la ISO 27002 Estos dominios que estructura la ISO 27002 son:
> - La política de seguridad.
> - Los aspectos organizativos de la seguridad de la información.
> - La gestión de activos.
> - La seguridad ligada a los recursos humanos.
> - La seguridad física y ambiental.
> - La gestión de las comunicaciones y de las operaciones.
> - Los controles de acceso a la información.
> - La adquisición, desarrollo y mantenimiento de los sistemas de información.
> - La gestión de incidentes en la seguridad de la información.
> - La gestión de la continuidad del negocio.
> - Los aspectos de cumplimiento legal y normativo [20]

4.1.4 ISO 31000

Gestión de Riesgos - Principios y Guías - (Suiza, 2009). Esta norma internacional tiene por finalidad apoyar a las entidades de diferentes niveles a administrar los riesgos de forma efectiva. La norma define lineamientos los cuales se deben alcanzar a fin de lograr una efectiva administración de los riesgos. Esta norma internacional plantea que las entidades tomen acciones para desarrollar, implementar y mejorar continuamente bajo un esquema de actuación que sirva de base y que tiene por fin es consolidar las actividades de administración de los riesgos en un marco

---

[19] Betancourt Betancourt, A. (2016). Diseño de un prototipo de software para aplicar análisis GAP a los controles descritos en el anexo a de la norma ISO 27001:2013. [En Linea] Repositorio.utp.edu.co. Disponible en http://repositorio.utp.edu.co/dspace/handle/11059/7728.

[20] Tovar Piraban, C. and Ayala Marín, W. (2017). Implementación red de sincronismo para la expansión de la operación móvil. [En Linea] Repository.usta.edu.co. Disponible en http://repository.usta.edu.co/handle/11634/9104

de gobierno integral incorporando actividades como planes, estrategias, gestión, información, lineamientos entre otros.

Puede ser empleada por diferentes organizaciones del sector gobierno y del entorno privado, organizaciones sin afán de lucro, grupos, personas de cualquier rubro, asociaciones.

Otro aspecto del estándar es su aplicación en todo el proceso de las actividades de una entidad, de la misma forma como una diversa relación de sectores, donde se incorporan aspectos de estrategia, toma de decisiones entre otros. Así mismo, el estándar se puede implementar a diferentes tipologías de riesgos, de diferente naturaleza, cualquiera sea el factor que lo origine. Esta norma brinda los lineamientos, la estructura de trabajo los procedimientos dirigidos a administrar diferentes tipologías de riesgos en una forma coherente, estructurada y evidenciable en diferentes casuísticas.

Principios Fundamentales para la Gestión de Riesgos: El estándar ISO 31000:2009 define los lineamientos y guías de forma general para la administración de riesgos. A efectos de lograr una mejor efectividad, la administración de riesgos dentro de una entidad debe considerar los siguientes lineamientos:

a) Crea valor
b) Integración con las actividades de la entidad
c) Interviene en las decisiones
d) Maneja detalladamente los escenarios inciertos
e) Estructurados, adecuados y sistemáticos
f) Se apoya en la información disponible más adecuada
g) Se ha realizado a medida
h) Considera factores humanos y culturales
i) Se desarrolla de forma inclusiva y transparente
j) Se despliega de forma iterativa, ajustada al cambio y dinámica
k) Permite el proceso de mejora permanente

La norma se apoya en los siguientes factores relevantes a fin de conseguir una eficaz administración de los riesgos:

1. Los fundamentos para la administración de riesgos.
2. El ámbito de acción para la administración de riesgos.
3. El ciclo de administración de riesgos.

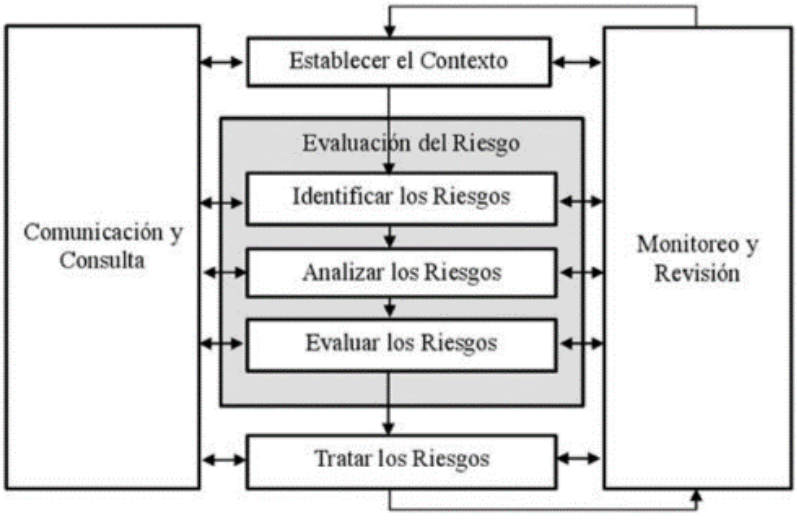
Beneficios de la norma: Los beneficios del estándar para las entidades que lo implementen son los siguientes:

- Incrementar la posibilidad de cumplir las metas
- Impulsar la administración efectiva
- Concientizar sobre la relevancia de gestionar los riesgos de forma integral en la empresa

- Optimizar las actividades de descubrimiento de oportunidades y amenazas
- Lograr los objetivos de cumplimiento respecto a los requerimientos regulatorios y legales en el ámbito nacional e internacional.
- Optimizar la generación de información de orden financiero
- Optimizar el marco de gobierno
- Optimizar el nivel de confianza de las partes interesadas
- Definir un marco de confianza para planificar y tomar decisiones
- Optimizar los mecanismos de control
- Mejorar la gestión de recursos con efectividad para la gestión de riesgos
- Optimizar la consecución de resultados y la efectividad de las operaciones
- •Optimizar los aspectos relacionados a salud, segundad ocupacional, y preservación del medio ambiente.
- Optimizar las medidas de evitar pérdidas y prevención de incidentes
- Reducir las pérdidas
- Incrementar y optimizar la concientización de los colaboradores
- Reforzar los mecanismos de restauración de los procesos organizacionales[21]

Esta norma internacional proporciona los principios y las directrices genéricas sobre la gestión del riesgo, puede utilizarse por cualquier empresa pública, privada o social, asociación, grupo o individuo. Por tanto, no es específica de una industria o sector concreto. En la Figura 2 se muestra su estructura y sus componentes.

Figura 2. Proceso de gestión de riesgos en ENT 5254 e ISO 31000



Fuente: (ISO 31000:2009, 2009)

Algunas de sus características adicionales son:

- Se alinea con los objetivos de negocio.

[21] Rojas Gonzales, E. A. (2017). El sistema de gestión de continuidad de negocios y su relación con los riesgos en las entidades financieras peruanas reguladas por la superintendencia de banca y seguros. [En Línea]. Disponible en http://repositorio.unac.edu.pe/handle/UNAC/2149

- Permite su aplicación a lo largo de la vida de una organización
- Es aplicable a cualquier tipo de riesgo, sin diferenciar su naturaleza, así como si tiene efecto positivo o negativo para la organización.
- Requiere establecer directrices descendentemente desde la parte superior en la estructura organizacional hasta el personal operativo.
- Provee un modelo de proceso detallado. [22]

4.1.5 ITIL V3

El acrónimo ITIL quiere decir: Information Technology Infraestructura Library. En español: biblioteca de libros que tratan de la infraestructura de las tecnologías de la información. Un servicio es un medio de proporcionar valor a los clientes, facilitando los resultados que desean obtener, sin asumir toda La responsabilidad de los costes o riesgos. Un servicio es un compromiso de resultado.

Algunas de las razones que muestran que el mundo de la empresa ha cambiado y, de esta manera, ha modificado el posicionamiento de la informática en la empresa son:

- Los negocios de la empresa cada vez son más dependientes de la informática, en todos los sectores.
- La información se ha convertido en un valor en sí misma.
- El sistema de información es cada vez más complejo.
- Los clientes y usuarios son cada vez más exigentes.
- La competencia cada vez as más feroz para la empresa y también para la informática en la empresa.

Una buena práctica es una práctica que proviene de la puesta en común de muchos retamos de experiencia, que han sido seleccionados, generalizados y estructurados, para permitir su reutilización. Una buena práctica se basa en lo vívido, en al pragmático y no en la teoría.

ITIL no es una norma porque no se trata de un enfoque teórico. Está construido en base a buenas prácticas, a la experiencia vívida y al pragmatismo. Este enfoque no es prescriptivo, es decir no se impone nada, como sucede con una norma. ITIL hay que adaptarlo al enlomo de la empresa.

Los cuatro fundamentos del enfoque ITIL V3 son:

- Las buenas prácticas.
- La gestión de los servicios.
- Los procesos y las funciones.

---

[22] Carazas, V., & Yeffer, J. (2017). Marco de trabajo RISK IT en la gestión de riesgos de tecnología de la información en la Caja Rural de Ahorro y Crédito Los Andes SA-2015. [En línea]. Disponible en http://repositorio.unap.edu.pe/handle/UNAP/5561

- El ciclo de vida de los servicios.

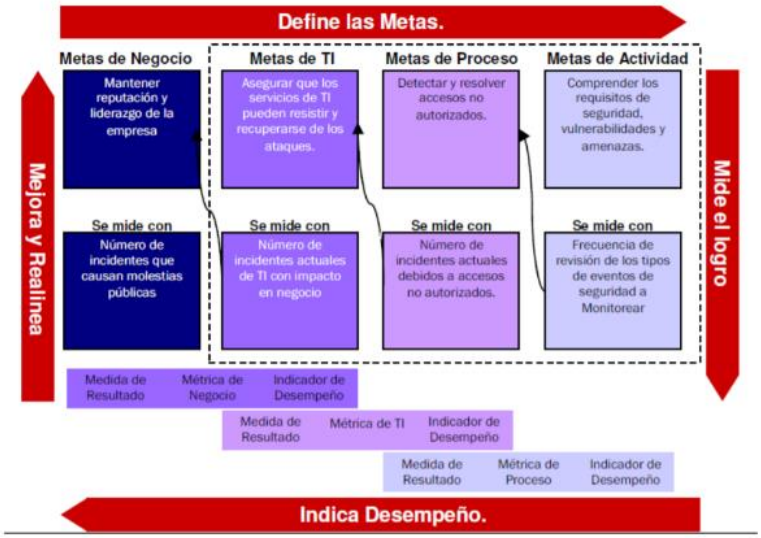
ITIL aporta valor al cliente y usuarios. La informática se abre al negocio. ¿Cómo conseguir estos dos objetivos, si los informáticos no están motivados para hacerlo? En las buenas prácticas ITIL V3 existe información para conseguir motivar a los empleados como, por ejemplo, una mejor definición de los roles y responsabilidades, mayor comunicación de los objetivos que se deben alcanzar, mayor visibilidad de las opciones, las prioridades, etc.[23]

4.1.6 COBIT

Un acercamiento y descripción más resumida de COBIT la encontramos según Estébanes, E. y Cano, J. a continuación:

> Objectives for Information and related Technology (Objetivos de Control para la información y tecnología relacionada) Creado por ISACA Information Systems Audit and Control Association (Asociación de Control y Auditoria de Sistemas de Información) Es un conjunto de herramientas de soporte que permite a la gerencia de las organizaciones el cerrar la brecha entre los requerimientos de control, problemas técnicos y los riesgos del negocio.
>
> Este marco provee buenas prácticas y presenta actividades para el Gobierno de TI que en una estructura manejable y lógica.

Figura 3. CICLO COBIT



Fuente: http://www.ecorfan.org

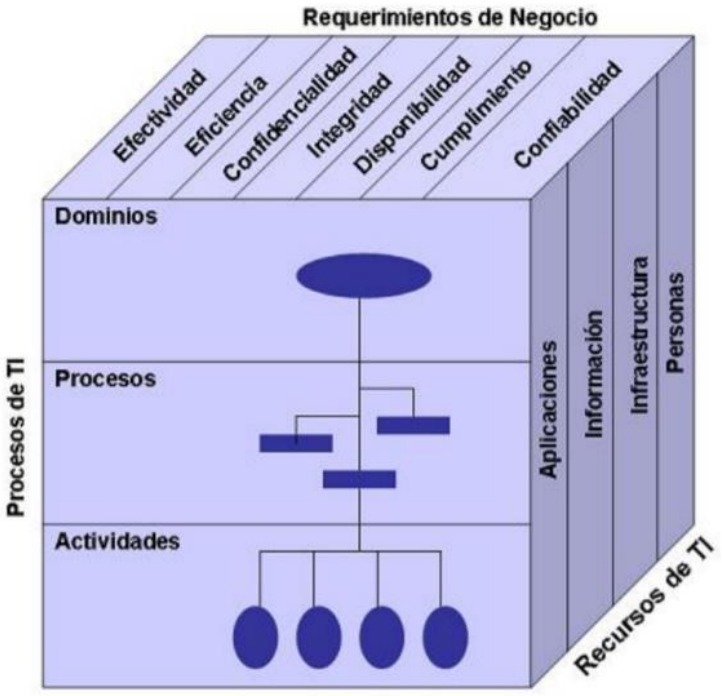
[23] Baud, J. L. (2015). Preparación para la certificación ITIL Foundation V3: ITIL V3-2011: más de 400 preguntas-respuestas (Vol. 3). Ediciones ENI. [En Línea]. Disponible en https://books.google.com.co/books?id=vOEGFt-NoUjcC&lpg=PA25&ots=8uD524OZQR&dq=%22itil%20v3%22&lr=lang_es&hl=es&pg=PA25#v=onepage&q=%22itil%20v3%22&f=false

Versiones COBIT:

- 1ra Edición (1996) incluía la colección y análisis de fuentes internacionales reconocidas
- Versión 2(1998), principal cambio fue la adición de las guías de gestión.
- Versión 3(2003), la versión en línea ya se encontraba disponible en el sitio de ISACA.
- (2003), COBIT fue revisado y mejorado para soportar el incremento del control gerencial, introducir el manejo del desempeño y mayor desarrollo del Gobierno de TI.
- Versión 4 (2005), la cuarta edición fue publicada.
- Versión 4.1(2007), se liberó la versión 4.1 que es la que actualmente se maneja.
- La versión 5, está planeada para ser liberada en el año 2012, esta edición consolidará e integrará los marcos de referencia de COBIT 4.1, Val IT 2.0 y Risk IT.

Los recursos de TI son manejados procesos para alcanzar las metas de TI que responden a los requerimientos del negocio.

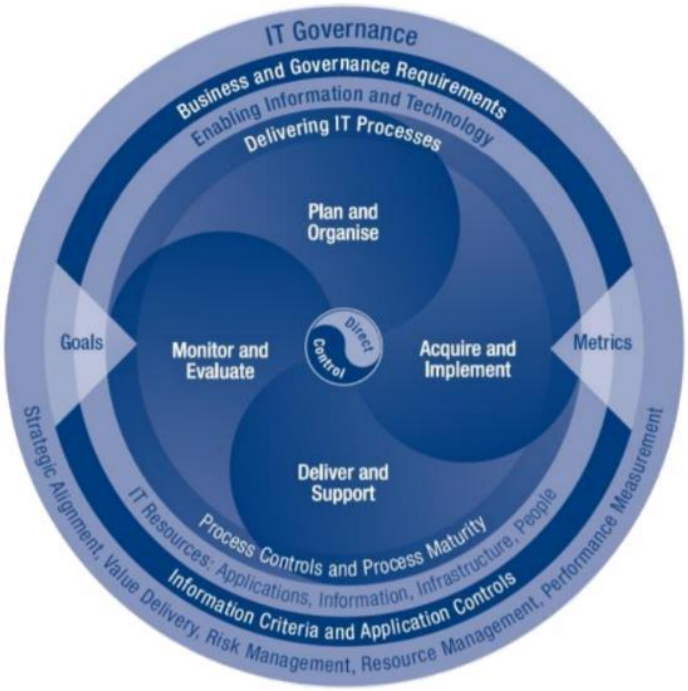
Figura 4. EL CUBO COBIT



Fuente: http://www.ecorfan.org

COBIT 4.1: Está conformado por un conjunto de 34 Objetivos de Control de alto nivel, todos diseñados para cada uno de los Procesos de TI, los cuales están agrupados en cuatro grandes grupos mejor conocidos como dominios, estos se equiparán a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear:

Figura 5. Marco de referencia – COBIT 4.1



Fuente: http://www.ecorfan.org

- Planificación y Organización, proporciona la dirección para la entrega de soluciones y la entrega de servicios.
- Adquisición e Implementación, proporciona las soluciones y las desarrolla para convertirlas en servicios.
- Entrega de servicios, recibir soluciones y hacerlas utilizables para los usuarios finales.
- Soporte y Monitorización, monitorear todos los procesos para el asegurar que se sigue con la dirección establecida

Un concepto clave de COBIT, es la determinación y la mejora sistemática de la madurez del proceso, el cual tiene 6 niveles (0 al 5) para medir el nivel de madurez de los procesos de TI.

0 Inexistente
1 Inicial / adhoc
2 Repetible pero
3 Definido
4 Gestionable y medible
5 Optimizado [24]

[24] Estébanes, E. and Cano, J. (2011). Gobierno de ti a través de Cobit 4.1 y cambios esperados en Cobit 5.0. [En Línea] Dialnet.unirioja.es. Disponible en https://dialnet.unirioja.es/servlet/articulo?codigo=3823460

4.1.7 MAGERIT

Para Gaona Vásquez la metodología MAGERIT la resume en:

MAGERIT es el acrónimo de "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Publicas", creado por el Consejo Superior de Administración Electrónica (CSAE). El uso de esta metodología es de carácter público, pertenece al Ministerio de Administraciones Públicas (MAP) de España.

Se elaboró Magerit porque está dirigido a los medios electrónicos, informáticos y telemáticos, ya que su uso en la actualidad es frecuente, lo cual ha dado lugar al origen de ciertos riesgos que se deben de evitar con medidas preventivas para lograr tener confianza en utilizarlos. "No es posible una aplicación racional de medidas de seguridad sin antes anal izar los riesgos para, así implantar las medidas proporcionadas a estos riesgos, al estado de la tecnología y a los costes (tanto de la ausencia de seguridad como de las salvaguardas). "

La Metodología de Análisis y Gestión de Riesgos de los sistemas de Información de las Administraciones públicas, Magerit, es un método formal para investigar los riesgos que soportan los Sistemas de Información, y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

Historia y Evolución: En la actualidad se encuentra en la versión 3.0, pero el tiempo ha pasado desde la primera publicación de Magerit en 1997, y su segunda publicación en 2005, donde el análisis de riesgos se ha venido consolidando como eje central para la gestión de la seguridad.

Objetivos de Magerit: En el libro I de la publicación de Magerit versión 3 persigue los siguientes objetivos:

Directos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

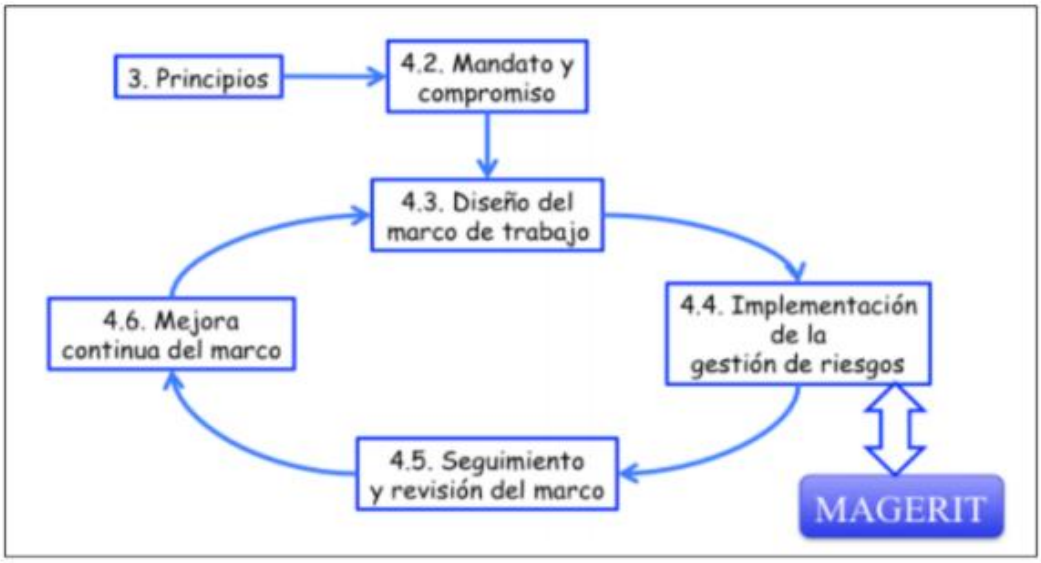
Indirectos:

- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Metodología Magerit versión 3: Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina "Proceso de Gestión de los Riesgos", sección 4.4 ("Implementación de la Gestión de los Riesgos") dentro del "Marco de Gestión de Riesgos". En otras palabras, Magerit implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones

teniendo en cuenta los riesgos derivados de uso de tecnologías de la información.

Figura 6. ISO 31000 - Marco de trabajo para la gestión de riesgos



Fuente: Tomado del Libro 1 de Magerit versión 3

En las "Directrices de la OCDE para la seguridad de sistemas y redes de información-Hacia una cultura de la seguridad", que en su principio 6 dice: 6) Evaluación del riesgo. Los participantes deben llevar a cabo evaluaciones de riesgo.

Existen varias aproximaciones que sirven para analizar los riesgos que pueden sufrir sistemas y las tecnologías de la información y comunicación: guías formales, aproximaciones metódicas y herramientas de soporte. Todas ellas tienen como finalidad el saber cuan seguros o inseguros son los sistemas. Existen muchos elementos que hay que considerar para lograr tener buenos resultados. Es por ello que Magerit está basado sobre una aproximación metódica que no deja lugar a la improvisación, ni dependa de la arbitrariedad del analista. [25]

4.1.8 Osstmm (Open Source Security Testing Methology Manual)

Para Villacrés Machado el estándar OSSTMM lo resume de la siguiente manera:

Representa un estándar de referencia imprescindible, para todo aquel que quiera llevar a cabo un testeo de seguridad en forma ordenada y con calidad profesional. A fin de organizar su contenido, la metodología se encuentra dividida en varias secciones.

[25] Gaona Vásquez, K. (2013). Aplicación de la metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa Pesquera e Industrial Bravito S.A. en la ciudad de Machala. [En Línea] Dspace.ups.edu.ec. Disponible en https://dspace.ups.edu.ec/handle/123456789/5272

Del mismo modo, es posible identificar en ella, una serie de módulos de testeo específicos, a través de los cuales se observan cada una de las dimensiones de seguridad, integradas con las tareas a llevar a cabo en los diferentes puntos de revisión (Seguridad de la Información, Seguridad de los Procesos, Seguridad en las Tecnologías de Internet, Seguridad en las Comunicaciones, Seguridad Inalámbrica y Seguridad Física).

OSSTMM no solo alcanza los ámbitos técnicos y de operación de seguridad tradicionales, sino que, se encarga de normar aspectos tales como: las credenciales del profesional a cargo del test, la forma en la que el test debe ser comercializado, la forma en la que los resultados del mismo deben ser presentados, las normas éticas y legales que deben ser tenidas en cuenta al momento de concretar el test, los tiempos que deberían ser tenidos en cuenta para cada una de las tareas, y por sobre todas las cosas, incorpora el concepto de RAVs (Valores de Evaluación de Riesgo) y con ellos la frecuencia con la cual la prueba debe ser ejecutada a fin de proveer más que una instantánea en el momento de su ejecución.

INTRODUCCIÓN

La OSSTMM comenzó allá por finales del año 2000, y creció rápidamente gracias a la experiencia de miles de personas que contribuyeron al proyecto. Gracias al hecho de ser una metodología libre, los testeadores participan en un gran plan contribuyendo al movimiento open-source, y estandarizando una metodología que todo el mundo pudiera acceder, o a mejorar, por lo que creció enormemente hasta convertirse en uno de los principales referentes en su campo hoy en día.

Originariamente, perteneció al dominio ideahamster.org, que más adelante pasó a ser el actual ISECOM (Institute for Security and Open Methodologies). En 2003, ISECOM estuvo registrada como una organización sin ánimo de lucro en España y en los EEUU. Hasta ahora, la OSSTMM trataba solamente una forma de hacking ético, pero en 2005, pasó a ser una forma de verificar que la seguridad se estaba tratando de forma correcta a nivel operacional, y en 2006, este manual pasó a ser el estándar para aquellos que necesitaran una seguridad más allá del que la legislación y regulaciones ofreciesen.

Un punto importante de la OSSTMM, es el tener en cuenta que el objetivo del manual, es crear un solo método para realizar pruebas de seguridad en profundidad. Es un conjunto de pasos que deben ser realizados una y otra vez, hasta que los resultados esperados se obtengan. No es la idea (ni se encontrará en ninguna otra parte) el recomendar al auditor el utilizar esta metodología como un diagrama de flujos o utilizarla como una serie de pasos con un cierto orden formal, sino simplemente haber completado y revisado todos los pasos que se contemplan, en el tiempo establecido.

Algo en lo que esta metodología hace hincapié, es el hecho de que muchos testeadores de seguridad creen que los tests de seguridad son una “fotografía” del punto actual de seguridad en el sistema. El tener una visión actual y puntual de cómo es el sistema en ese momento. Pero... ¿es esta “fotografía” suficiente? La metodología intenta enriquecerlas con los llamados Risk Assessment Values o Valores de Evaluación de Riesgos (de ahora en adelante RAVs), que proporcionarán información

extra en contextos tales como frecuencias y tiempos al test de seguridad. La “fotografía” se convertirá en un perfil o Profile abordando un rango de variables a lo largo de un periodo de tiempo antes de degradarse por debajo de los niveles de riesgo aceptable.

Por último, otro de los objetivos de la metodología es que pueda evitarse, que el estilo personal, asunciones falsas, o prejuicios de los testeadores intervengan en los resultados del test. El uso de una metodología igual para todo el mundo conseguirá la imparcialidad de los tests, y, por lo tanto, que tengamos una base comparable entre sistemas, pudiendo así comparar unos con otros, y graduarlos. [26]

[26] Villacrés Machado, D. (2011). Propuesta Metodológica para Asegurar Redes Inalámbricas y su Aplicación en la ESPOCH.. [En Línea] Dspace.espoch.edu.ec. Disponible en http://dspace.espoch.edu.ec/handle/123456789/1480?mode=full

4.2 MARCO CONCEPTUAL

4.2.1 BYOD

López Camacho considera algunas pautas para un uso correcto de BYOD:

> La implantación de un programa de BYOD involucra que los empleados utilicen sus propios dispositivos de comunicación móviles, para llevar a cabo trabajo para su empleador, a través de acceso local o remoto a la intranet de la organización. Uno de los objetivos de un programa de BYOD es permitir al empleado ser más productivo y eficiente mediante la selección del dispositivo que mejor se adapte a sus preferencias y necesidades de trabajo, mientras que al mismo tiempo se garantiza la integridad de datos y la protección de fugas de información.
>
> El uso de un dispositivo móvil propiedad de los empleados en el lugar de trabajo se diferencia del uso de un dispositivo móvil corporativo, de dos maneras. La primera es la propiedad: mientras que un dispositivo móvil corporativo es propiedad de la organización que lo emite, un dispositivo BYOD es propiedad del empleado. Esta diferencia en la propiedad resulta en una diferencia en usos entre los dos tipos de dispositivos. Debido a que un dispositivo móvil corporativo es propiedad de la organización, no necesariamente existiría una política que prohíbe o restringe los usos no relacionados con el trabajo.
>
> Por otro lado, debido a que un BYOD es propiedad del empleado y no de la organización en la que él trabaja, se puede suponer, si no se indica explícitamente en la política, que el empleado va a utilizar el dispositivo para uso personal, además de trabajo. La segunda manera gira en torno a que esta situación de BYOD donde se utiliza un dispositivo para fines personales y de trabajo, significa que dos tipos de información fluirán a través del dispositivo, las cuales requerirán una protección adecuada por parte de la organización que emplea a la persona que utiliza un BYOD.
>
> Por un lado, el dispositivo probablemente tendrá acceso a la información personal de los clientes de la organización, es decir, aquellas personas con las que la organización ha interactuado y en el que ha recogido de manera legítima y se usa la información personal. Por otro lado, el dispositivo también podrá contener información personal sobre el empleado a quien pertenece el dispositivo, así como tal vez allegados al empleado, por ejemplo, otras personas importantes, miembros de la familia, amigos, etc. [27]

4.2.2 Protocolos

Para Dordoigne, J. describe los protocolos a partir del modelo OSI de la siguiente

[27] López Camacho, R. and López Obando, R. (2014). Diseño de un Marco de Referencia para regular el uso de BYOD en organizaciones bajo el estándar ISO 27002. [En Línea] Repository.icesi.edu.co. Disponible en https://repository.icesi.edu.co/biblioteca_digital/handle/10906/77346

manera:

> El modelo OSI divide y especifica las funciones propias de la comunicación a través de siete capas lógicas. La materialización de las capas del modelo teórico toma la forma de protocolos. En cada protocolo se aplican diferentes funciones definidas por el modelo. Un protocolo constituye, por tanto, un conjunto de reglas de comunicación. Estas reglas establecen el formato de transmisión de los datos a través de la red.
> El ideal teórico del modelo OSI consiste en implantar un protocolo por capa. En realidad, algunos protocolos operan en varias capas, otros en una capa y algunos solo en una parte de algunas capas, tal como las define el modelo OSI. De hecho, no se debe olvidar que este modelo se creó cuando ya existían muchos otros protocolos, por lo que algunos fabricantes se adaptaron al modelo, mientras que otros siguieron utilizando sus protocolos sin modificarlos.[28]

4.2.3 Protocolos De Seguridad

Para Duchi Paca resume el concepto de protocolos en el ámbito de seguridad informática a:

> Un protocolo de seguridad define las reglas que gobiernan las comunicaciones, diseñadas para que el sistema pueda soportar ataques de carácter malicioso. Protege contra todos los ataques posibles, es generalmente muy costoso por lo cual los protocolos son diseñados bajo ciertas premisas con respecto a los riesgos a los cuales el sistema está expuesto.
> Un protocolo de seguridad también se puede definir como una serie de pasos, que involucran a dos o más entidades principales, diseñadas para realizar una tarea en particular.
> 1. Todas las entidades principales deben conocer los pasos del protocolo de antemano.
> 2. Todas las entidades principales deben estar de acuerdo en seguir y acoplarse al protocolo.
> 3. El protocolo por usar debe ser completo, debe definir qué es lo qué se debe hacer en cualquier circunstancia posible.
> 4. No debe ser posible hacer “más” de lo que el protocolo define.
>
> Un protocolo de seguridad es un conjunto de intercambios en los que intervienen normalmente dos o tres entidades. La entidad iniciadora del protocolo (entidad a), la entidad receptora (entidad b) y una tercera entidad opcional (entidad c) con la misión de autenticación de los intercambios, distribución de claves públicas y/o claves de sesión.[29]

---

[28] Dordoigne, J. (2015). Redes informáticas-Nociones fundamentales (5ª edición):(Protocolos, Arquitecturas, Redes inalámbricas, Virtualización, Seguridad, IP v6...). Ediciones ENI. [En Línea]. Disponible en https://books.google.com.co/books?id=Huwy1L0PEq8C&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

[29] Duchi Paca, E. y Herrera Cárdenas, E. (2015). Desarrollo de una aplicación Web basada en un E-procurement para la Empresa DIGISYSTEM S.A.. [En Línea] Repositorio.espe.edu.ec. Disponible en http://repositorio.espe.edu.ec/handle/21000/10260

4.2.3.1 Dynamic Host Configuration Protocol (DHCP)

Protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.[30]

4.2.3.2 File Transfer Protocol (FTP).

Protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basada en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar o enviar archivos desde el, independientemente del sistema operativo utilizado en cada equipo.[31]

4.2.3.3 Snmp. Por su sigla en inglés (simple network management protocol)

Es un protocolo de la capa de aplicación, su función en facilitar la comunicación y el intercambio de datos administración entre los dispositivos de red. Estos dispositivos generalmente son los routers, switches, servidores, estaciones de trabajo etc. Que soportan este protocolo. El protocolo permite a los administradores de red supervisar el desempeño, buscar y resolver los problemas presentados en cada uno de los dispositivos de la red de datos así como planificar un incremento o crecimiento de la red [32]

4.2.3.4 Protocolo WEP (Wired Equivalent Privacy).

Protocolo para resguardar las redes inalámbricas, por medio de un estándar de encriptación. Se presenta debido a que los canales de comunicación son inseguros y su objetivo principal es garantizar la confidencialidad y evitar que usuarios no autorizados puedan acceder a las redes WLAN, proporcionando autenticidad.

Se destacan las siguientes ventajas:

- Permite utilizar dos métodos de autenticación: Sistema Abierto y Clave Compartida El protocolo WEP es fácil de configurar y cualquier sistema con el

[30] El Salvador. MH Glosario SGSI. Óp. Cit., p. 1

[31] Ibíd., p. 1.

[32] Trujillo Murcia, F. y Celis Perdomo, C. (2017). Proponer un sistema de diagnóstico y monitoreo que permita identificar eventos para resolver problemas de infraestructura de TI, de la red de datos de la empresa Sociedad Clínica Emcosalud. [En línea]. Disponible en http://hdl.handle.net/10596/13386

estándar 802.11 lo soporta.
- Proporciona niveles de seguridad altos.

Dentro de las desventajas se tienen:
- Existe una vulnerabilidad en la captura de paquetes de información por parte de terceros, donde pueden encontrar la contraseña de la red y acceder a ella, las claves de tipo WEP son relativamente fáciles de conseguir por este método.
- No implementa adecuadamente, el enfoque de incrementar el vector de un paquete a otro, en el tamaño de los paquetes de iniciación. Permitiendo que la cantidad de tramas que pasan a través de un punto sea grande, lo que hace que se encuentren dos mensajes con el mismo valor de iniciación
- Las claves de cifrado estáticas son pocas veces cambiadas.
- Existen varias herramientas que pueden permitir romper la clave secreta.

4.2.3.5 Protocolo WPA: WPA (Wi-Fi Protected Access).

Su objetivo es cubrir todas las falencias de seguridad detectadas en el protocolo de seguridad WEP. Trabaja bajo un estándar de MAC, se encuentra orientado a pequeñas oficinas y usuario doméstico. Como indica Guillaume

Dentro de sus principales características se tienen:

- Distribución dinámica de claves
- Incremento de robustez del vector de inicio
- Nuevas técnicas de integridad y autenticación

Tiene las principales ventajas:

- Implementación del Protocolo de Integridad de Clave Temporal (TKIP - Temporal Key Integrity Protocol), permite cambiar las claves dinámicamente a medida que el sistema es utilizado. Evita ataques de recuperación de clave a los que es susceptible WEP.
- Contiene protección contra ataques de "repetición" (replay attacks), cuenta con un contador de tramas.
- Permite trabajar a nivel doméstico y empresarial

Se encuentran las siguientes desventajas:
- No es soportado por muchos dispositivos de red antiguos.
- No todas las tarjetas inalámbricas son compatibles con este estándar.

4.2.3.6 Protocolo WPA2

Diseñado específicamente para cumplir requisitos de entornos empresariales. Es compatible con WPA2

Entre las principales ventajas:

- Utilizado para redes grandes, dado que proporcionan muy buena seguridad.
- Puede trabajar con y sin un servidor de llaves, todas las estaciones de la red usan una llave de tipo PSK (Pre-Shared-Key), en caso contrario se usa habitualmente un servidor IEEE 802.1x.
- Incluye un algoritmo considerado criptográficamente seguro

Su principal vulnerabilidad es el ataque a la clave PSK, ya que toda la información de la red va en formato texto y se transmite cuando un usuario se autentifica. Teniendo en cuenta que la infraestructura de clave pública se compone de un número de elementos necesarios que garantizan la ejecución de operaciones criptográficas, por medio de una tecnología, que proporciona mayor seguridad de la información dentro de una organización.

4.2.3.7 Protocolo EAP (Extensible Authetication Protocol).

Se encarga de la autenticación y autorización, gestionando las contraseñas, capaz de trabajar con tecnología de llave pública. [33]

4.2.4 Seguridad Informática

Los riesgos, en términos de seguridad, se caracterizan por lo general mediante los conceptos de amenaza, vulnerabilidad y controles. La amenaza representa el tipo de acción que tiende a ser dañina, la vulnerabilidad representa el grado de exposición a las amenazas en un caso particular. Finalmente, los controles representan todas las acciones que se implementan para prevenir la amenaza.
Para los controles deben implementarse no sólo son soluciones técnicas, sino también reflejan la capacitación y la toma de conciencia por parte del usuario, además de reglas claramente definidas.

4.2.5 Seguridad De La Información

[33] Cifuentes Rodríguez, J. (2017). Diseño de un modelo de gestión de seguridad en redes de comunicación inalámbricas aplicado a pequeñas empresas del sector privado de la ciudad de Bogotá. Colombia. [En Línea]. Disponible en http://hdl.handle.net/10596/12862

La seguridad de la información es un proceso en el que se da cabida a un creciente número de elementos: aspectos tecnológicos, de gestión-organizacionales, de recursos humanos, de índole económica, de negocios, de tipo legal, de cumplimiento, etc.; abarcando no sólo aspectos informáticos y de telecomunicaciones sino también aspectos físicos, medioambientales, humanos, etc[34].

preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad (ISO/IEC 17799:2005)

4.2.6 Dispositivo Móvil

Dispositivo móvil, también conocido como computadora de bolsillo o computadora de mano, es un tipo de computadora de tamaño pequeño, con capacidades de procesamiento, con conexión a Internet, con memoria, diseñado específicamente para una función, pero que pueden llevar a cabo otras funciones más generales.

4.2.7 Confidencialidad

La información sólo puede ser accedida y utilizada por el personal de la empresa que tiene la autorización para hacerlo. En este sentido se considera que este tipo de información no puede ser revelada a terceros, ni puede ser pública, por lo tanto debe ser protegida y es la que tiende a ser más amenazada por su característica.[35]

la propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no-autorizados (ISO/IEC 13335-1:2004)

4.2.8 Integridad

Se refiere al momento en que la información no ha sido borrada, copiada o modificada, es decir, cuando se conserva tal como fue creada o enviada desde cualquier medio desde su origen hacia su destino.

4.2.9 Disponibilidad

---

[34] BASSAT, Luis. El libro rojo de la publicidad:(ideas que mueven montañas). Debols! llo, 2017. [En Línea]. Disponible en https://books.google.com.co/books?id=_z2GcBD3deYC&lpg=PR14&ots=wsiiAAHVOg&dq=%22Seguridad%20de%20la%20Informaci%C3%B3n%22&lr&hl=es&pg=PR14-IA1#v=onepage&q&f=false

[35] González García, R. A. (2017). Diseño del Sistema de Gestión de Seguridad de la Información (SGSI) para el área de tecnología de la empresa Baker Tilly Colombia Ltda. de la ciudad de Bogotá, bajo la norma ISO 27001: 2013. [En Línea]. Disponible en http://hdl.handle.net/10596/12722

Se refiere a que la información facilitada en cualquier medio digital o software se encuentre disponible para el procesamiento de la información, para el correcto funcionamiento de una organización, así como de sus clientes o personal requerido sin que estos sean interrumpidos.

la propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada (ISO/IEC 13335-1:2004)

4.2.10 Protección

Se puede considerar como protección las medidas que se deben tomar para que en un sistema informático no ocurra lo indeseado y se pueda generar perdida de información.

4.2.11 Riesgo

Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000)

4.2.12 Amenazas

Eventos, hechos o tendencias en el entorno de una Organización que inhiben, limitan o dificultan su desarrollo operativo.

4.2.13 Vulnerabilidad

Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000)

4.2.14 Control

asegurar su conformidad con la estructura de seguridad informática y procedimientos establecidos por la compañía en cuanto el acceso a la información y el monitoreo de los usuarios autorizados.[36]

---

[36] Rodríguez Pinto, A. y Rozo Caballero, R. (2015). Diseño de un plan estratégico para la seguridad de la información tributaria en una entidad pública. [En Línea]. Disponible en http://hdl.handle.net/10596/3613

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo[37].

4.2.15 Dispositivo Móvil

Dispositivo móvil, también conocido como computadora de bolsillo o computadora de mano, es un tipo de computadora de tamaño pequeño, con capacidades de procesamiento, con conexión a Internet, con memoria, diseñado específicamente para una función, pero que pueden llevar a cabo otras funciones más generales.

4.2.16 Equipo Personal

Se refiere al equipo de cómputo de escritorio, portátil, tableta o celular, propiedad de un empleado y no de la empresa.

4.2.17 Acuerdos

Entendidos como los compromisos o cláusulas que se generen con el personal vinculado a una entidad para establecer el alcance y la responsabilidad sobre los activos de información, los mismos pueden contener cláusulas contractuales.

4.2.18 Tecnologías Móviles

Tecnologías de información diseñadas para soportar dispositivos móviles superando la limitante de las tecnologías físicas o fijas.

4.2.19 Backup

Copia de seguridad de algún sistema de información, bases de datos, archivos de usuario o configuración de equipos o dispositivos.

---

[37] Pulido Barreto, A. y Mantilla Rodriguez, J. (2016). Modelo para la implementación del sistema general de seguridad informática y protocolos de seguridad informática en la oficina TIC de la alcaldía municipal de Fusagasugá, basados en la gestión del riesgo informático. [En línea]. Disponible en http://hdl.handle.net/10596/6327

4.3 MARCO LEGAL

4.3.1 Ley 1273 de 2009. (delitos informáticos)

La Ley 1273 del 5 de enero de 2009, reconocida en Colombia como la Ley de Delitos Informáticos, tuvo sus propios antecedentes jurídicos, además de las condiciones de contexto analizadas en el numeral anterior. El primero de ellos se remite veinte años atrás, cuando mediante el Decreto 1360 de 1989 se reglamenta la inscripción del soporte lógico (software) en el Registro Nacional de Derecho de Autor, que sirvió como fundamento normativo para resolver aquellas reclamaciones por violación de tales derechos, propios de los desarrolladores de software. A partir de esa fecha, se comenzó a tener asidero jurídico para proteger la producción intelectual de estos nuevos creadores de aplicativos y soluciones informáticas.[38]

4.3.2 Ley estatutaria 1581 de 2012.

Ley de protección de datos personales. Regulada por (decreto 1377 de 2013). De acuerdo con la Corte Constitucional de Colombia, la efectiva protección de mecanismos que garanticen el habeas data como derecho fundamental y autónomo, requiere del accionar no sólo de los jueces, sino de una institucionalidad administrativa que, además del control y vigilancia de los sujetos de derecho público y privado, tenga la capacidad de fijar política pública y democrática en la materia, en razón de su carácter técnico.

Un avance importante a nivel jurídico se observa con la Ley Estatutaria 1266 de 2008, la cual regula en forma más detallada el derecho fundamental de habeas data que se aplica, en su orden, a bases de datos de carácter financiero, comercial y proveniente de terceros países. Posteriormente, la Ley Estatutaria 1581 de 2012 ha significado un adelanto importante en torno a la protección de cualquier dato personal que sea administrado por entidades públicas y privadas, de acuerdo con los principios generales establecidos en la Constitución. Esta última ley estableció dos categorías de datos que requieren de protección especial y cuyo tratamiento está, en términos generales, prohibido: los llamados datos sensibles que son los que afectan la intimidad de las personas o cuyo uso indebido puede generar discriminación (raza, ideología, orientación política, datos de salud y/o orientación sexual, entre otros) y los datos personales de los niños, niñas y adolescentes. La norma designó la autoridad competente en términos de protección de datos y prohibió la transferencia de datos a países que no tengan un nivel adecuado de protección de estos.

---

[38] Ojeda, Jorge Eliecer, et al. Óp. Cit., p. 1

Es claro que la Carta concibe el Habeas Data como un derecho fundamental autónomo, claramente diferenciado del derecho a la intimidad, al buen nombre y otros derechos fundamentales y como un mecanismo de protección de otros derechos (derechos conexos) frente a la negligencia o los excesos en el manejo de su información en bancos de datos manuales o sistematizados. Igualmente, se concibe como un derecho de doble vía, pues si bien es cierto que los usuarios pueden conocer, actualizar y rectificar las informaciones que de ellos se tiene sobre el cumplimiento de sus obligaciones, también lo es que las instituciones y el resto de la sociedad tienen derecho a conocer la solvencia económica de sus clientes, más aún por tratarse de asuntos de interés general. Es decir, el habeas data supone la facultad de "conocer e incidir sobre el contenido y la difusión personal que se encuentra archivada en bancos de datos y, paralelamente, significa que esa información debe ajustarse a ciertas exigencias mínimas".

Vale la pena resaltar que el derecho de protección de datos implica el poder de disposición y control que faculta a su titular a decidir cuáles de sus datos proporciona a un tercero, así como el saber quién posee esos datos y para qué, pudiendo oponerse a esa posesión o uso. El dato personal se define como toda información concerniente a una persona física identificada o identificable. Pueden ser sensibles (datos ideológicos, características personales, datos de salud, vida sexual, origen) o no sensibles (datos de identificación, datos patrimoniales, datos migratorios).

Ahora bien, en la sociedad contemporánea la protección de algunos derechos humanos se ha visto comprometida frente al uso inadecuado de los avances tecnológicos de la información. Estos derechos se encuentran, directa o indirectamente relacionados, ligados o enlazados con la protección de datos y, por tanto, se consideran derechos conexos: derecho a la información, al buen nombre y a la intimidad. Estos derechos los reconoce la propia Corte Constitucional en su pronunciamiento:

> "La honra y el buen nombre de las personas, (...), constituyen, junto con el derecho a la intimidad los elementos de mayor vulnerabilidad dentro del conjunto de los que afectan a la persona a partir de publicaciones o informaciones erróneas, inexactas o incompletas".

En el contexto colombiano, la jurisprudencia constitucional ha definido el derecho al hábeas data9 como aquel que otorga la facultad al titular de datos personales de exigir de las administradoras de esos datos el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de los datos, así como la limitación en las posibilidades de divulgación, publicación o cesión de los mismos, de conformidad con los principios que regulan el proceso de administración de datos personales que manejen las empresas. Este derecho tiene naturaleza autónoma y notas características que lo diferencian de otras garantías con las que, empero, está en permanente

relación, como los derechos a la intimidad y a la información. [39]

4.3.3 Ley 1712 Del 6 De Marzo Del 2014

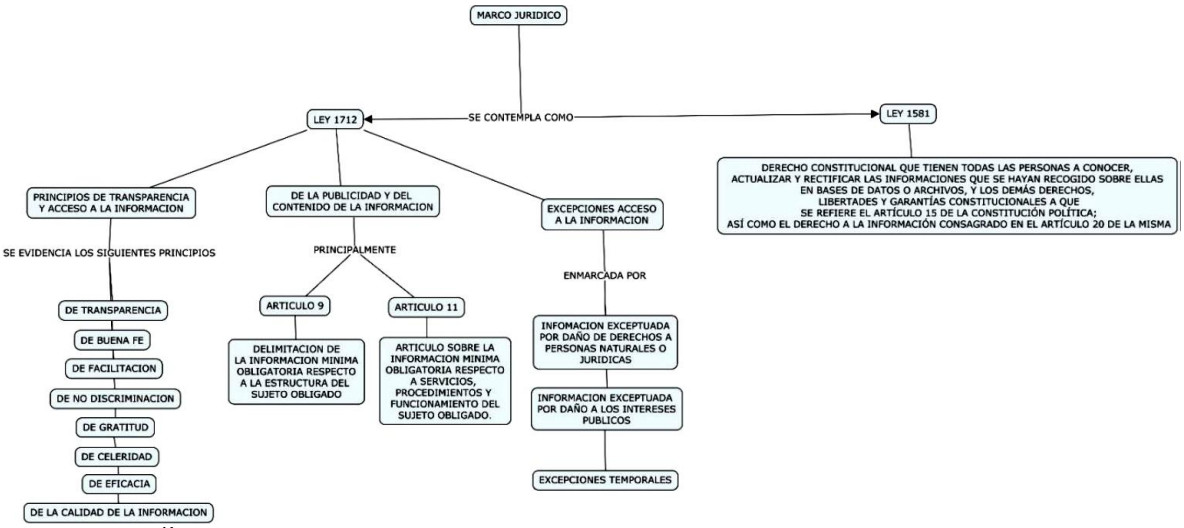
En el año 2014 se promulgo la ley 1712 – “Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, se ratifican los principios de la gestión documental y la necesidad que tienen las entidades del Estado y los nuevos sujetos obligados, de contar con información confiable y oportuna, fortalecer los esquemas de publicación de información, crear y mantener actualizado el registro de activos de información para uso y disposición del público.” (Nación, 2014, pág. 1)

“En ejercicio del derecho fundamental de acceso a la información, toda persona puede conocer sobre la existencia y acceder a la información pública en posesión o bajo control de los sujetos obligados. El acceso a la información solamente podrá ser restringido excepcionalmente. Las excepciones serán limitadas y proporcionales, deberán estar contempladas en la ley o en la Constitución y ser acordes con los principios de una sociedad democrática. El derecho de acceso a la información genera la obligación correlativa de divulgar proactivamente la información pública y responder de buena fe, de manera adecuada, veraz, oportuna y accesible a las solicitudes de acceso, lo que a su vez conlleva la obligación de producir o capturar la información pública. Para cumplir lo anterior los sujetos obligados deberán implementar procedimientos archivísticos que garanticen la disponibilidad en el tiempo de documentos electrónicos auténticos.” (Colombia, 2014, pág. 1) [40]

[39] Cano, L. G. (2012). Protección de datos en Colombia, avances y retos. Revista Lebret, 4(4), 195-214. [En Línea]. Disponible en http://revistas.ustabuca.edu.co/index.php/LEBRET/article/view/336

[40] Castaño Gómez, J. D., & Mesa Ruiz, F. A. (2016). Diseño de una guía para la auditoria de la clasificación de información que vela por el cumplimiento de la ley 1712. [En línea]. Disponible en http://hdl.handle.net/10983/7851

Figura 7. Marco jurídico Ley 1712 y 1581



Fuente: figura 1 [41]

4.3.4 CONPES 3854 Política Nacional De Seguridad Digital

Según Vidal Londoño, el CONPES 3854 establece nuevos lineamentos y hoja de ruta para el país como lo manifiesta a continuación:

> El Gobierno Nacional el día 11 de abril de 2016 a través del Consejo Nacional de Política Económica y Social aprobó la nueva política de Seguridad Digital CONPES 3854 de 2016 que reemplaza al 3701 del 2011, en el cual se establece una política de seguridad y defensa contra posibles ataques digitales a las entidades del Estado, convirtiendo a Colombia en el primer país de Latinoamérica y uno de los primeros en el mundo, en incorporar plenamente las recomendaciones y las mejores prácticas internacionales en gestión de riesgos de seguridad digital emitidas recientemente por la Organización para la Cooperación y el Desarrollo Económicos "OCDE". (CONPES 3854. 2016. Política Nacional de Seguridad Digital. Departamento Nacional de Planeación. República de Colombia. Bogotá).
>
> En esta política se establecen nuevos lineamientos y directrices de seguridad digital y se tienen en cuenta componentes como la educación, la regulación, la cooperación, la investigación, el desarrollo y la innovación.
>
> El CONPES 3854 de 2016 de Seguridad Digital integra los objetivos de defensa del país en relación con la lucha contra el crimen y la delincuencia en Internet, para lo cual se centra en la implementación de cinco frentes de acción específicos, los cuales se mencionan a continuación, así:
>
> - Establecer un marco institucional claro en torno a la seguridad digital, basado

[41] Ibíd., p.14

en la gestión de riesgos.

- Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital.
- Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos.
- Fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos.
- Impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional. [42]

4.3.5 RESOLUCIÓN 9364 DE 2016 ICBF[43]

CAPÍTULO I. DISPOSICIONES GENERALES.

ARTÍCULO 1o. OBJETO. La presente resolución tiene como objeto la actualización de la política general de seguridad de la información del Instituto Colombiano de Bienestar Familiar, así como definir lineamientos frente a su uso y manejo.

ARTÍCULO 2o. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN. El ICBF protege, preserva y administra la integridad, confidencialidad y disponibilidad de la información en el marco de la operación de sus procesos y en cumplimiento de los requisitos legales y reglamentarios, mediante la prevención de incidentes de seguridad de la información a través de gestión de riesgos e implementación de mecanismos de seguridad físicos y lógicos, orientados a la mejora continua en la gestión y el alto desempeño del Sistema de Gestión de Seguridad de la Información, con la finalidad de prestar servicios con calidad y transparencia a la primera infancia, la niñez, la adolescencia y el bienestar de las familias colombianas.

ARTÍCULO 3o. ÁMBITO DE APLICACIÓN. Lo contenido en esta política de Seguridad de la Información, aplica donde el Instituto Colombiano de Bienestar Familiar (ICBF) tenga presencia o desarrolle su acompañamiento a través de la recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, con personal interno o externo, en el desarrollo de la misión institucional y cumplimiento de sus objetivos estratégicos.

ARTÍCULO 4o. OBJETIVOS.

1. Brindar mecanismos de aseguramiento para el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información del ICBF.

[42] Vidal Londoño, J. (2016). Una nueva experiencia en seguridad hacking ético. [En Línea] Repository.unimilitar.edu.co. Disponible en http://repository.unimilitar.edu.co/handle/10654/15838

[43] Colombia. ICBF Resolución 9364 de 2016 – Política Seguridad de la Información. [En Línea] Disponible en http://www.icbf.gov.co/portal/page/portal/Descargas1/Tratamiento%20de%20datos/Resolucion9364-Actualiza-Politica-Seguridad-Informacion.pdf

2. Mitigar los incidentes de Seguridad de la Información en el ICBF.
3. Establecer los lineamientos necesarios para el manejo de la información y los recursos tecnológicos del ICBF.
4. Gestionar los riesgos de seguridad de la información.

CAPÍTULO II.

POLÍTICAS GENERALES DE MANEJO DE INFORMACIÓN.

ARTÍCULO 5o. TRATAMIENTO DE LA INFORMACIÓN. Para el tratamiento de la información de los niños, niñas, adolescentes, familias y comunidades colombianas a las cuales se les presta el acompañamiento en el marco del mandato legal encargado por el Gobierno nacional al ICBF, así como la información de los servidores públicos y colaboradores que participan en el desarrollo de las funciones de dicho mandato, el ICBF cuenta con la "Política de Tratamiento de Datos Personales del Instituto Colombiano de Bienestar Familiar" dando cumplimiento con lo dispuesto en la Ley 1581 de 2012, reglamentada por el Capítulo 25 del Título 2 de la Parte 2 del Libro 2 del Decreto número 1074 de 2015, la Ley 1712 de 2014, reglamentada por el Capítulo 2 del Título 1 de la Parte 1 del Decreto número 1081 de 2015, y las demás normas externas o internas que los modifiquen, adicionen o complementen.

ARTÍCULO 6o. POLÍTICA DE SEGURIDAD DE LOS RECURSOS HUMANOS. El ICBF a través de la Dirección de Gestión Humana debe propender que los servidores públicos entiendan sus responsabilidades frente a la seguridad de la información con el fin de reducir el riesgo de robo, fraude, mal uso de las instalaciones y medios, asegurando la confidencialidad, disponibilidad e integridad de la información.

PARÁGRAFO. La Dirección de Contratación deberá incluir en las minutas de los contratistas cualquiera que sea su modalidad, las cláusulas u obligaciones correspondientes a la seguridad de la información con el fin de reducir el riesgo de robo, fraude, mal uso de las instalaciones y medios, asegurando la confidencialidad, disponibilidad e integridad de la información.

ARTÍCULO 7o. POLÍTICA DE GESTIÓN DE ACTIVOS. El Instituto Colombiano de Bienestar Familiar a través de la Dirección de Información y Tecnología, establecerá y divulgará los lineamientos específicos para la identificación, clasificación y buen uso de los activos de información, con el objetivo de garantizar su protección.

a) Inventario de Activos: Los activos del ICBF deben ser identificados, clasificados y controlados para garantizar su uso adecuado, protección y la recuperación ante desastres. Por tal motivo, se debe llevar el inventario de los activos de información de propiedad del ICBF, discriminado por procesos, regionales y Centros Zonales, de acuerdo a la misma Guía para Desarrollo de Inventario y Clasificación de Activos.

Con el objetivo implantar los controles de seguridad, las dependencias que tienen

la custodia de la información generada en el marco de su función, se encargarán de proteger la información y de mantener y actualizar el inventario de activos de información relacionados con sus servicios (Información, software, hardware y recurso humano);

b) Archivos de Gestión: La Dirección Administrativa a través del grupo de gestión documental y con el acompañamiento del eje de Seguridad de la Información, deben implementar los controles necesarios para que los archivos de gestión cuenten con los mecanismos de seguridad con el fin de proteger y conservar la confidencialidad, integridad y disponibilidad de la información del ICBF;

c) Clasificación de la Información: La clasificación de la información del ICBF está basada de conformidad con la Ley 1712 de 2014 reglamentada por el Capítulo 2 del Título 1 de la Parte 1 del Decreto número 1081 de 2015, la Ley 594 de 2000 (Ley General de Archivos), el Decreto número 1080 de 2015 y lo estipulado en la misma Guía para Desarrollo de Inventario y Clasificación de Activos del ICBF.

ARTÍCULO 8o. RESPONSABILIDADES DE LOS COLABORADORES FRENTE AL USO DE LOS RECURSOS TECNOLÓGICOS. <Artículo modificado por el artículo 1 de la Resolución 3600 de 2017. El nuevo texto es el siguiente:> Todos los colaboradores que hagan uso de los activos de información del ICBF, tienen la responsabilidad de cumplir las políticas establecidas para el uso aceptable de los activos de información, entendiendo que el uso no adecuado de los recursos puede poner en riesgo la continuidad de la misión institucional.

a) Del Uso del Correo Electrónico: El servicio de correo electrónico institucional es una herramienta de apoyo a las funciones y responsabilidades de los funcionarios y contratistas del ICBF, con los siguientes lineamientos:

- El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional. En consecuencia, no puede ser utilizado con fines personales, económicos, comerciales y/o cualquier otro ajeno a los propósitos de la Entidad.

- En cumplimiento de la iniciativa institucional del uso aceptable del papel y la eficiencia administrativa, se debe preferir el uso del correo electrónico al envío de documentos físicos, siempre que la Ley lo permita.

- Los mensajes de correo están respaldados por la Ley 527 de 1999 (por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones), la cual establece la legalidad de los mensajes de datos y las implicaciones legales que conlleva el mal uso de estos.

- Está prohibido el envío de correos masivos (más de 150 destinatarios) a nivel nacional tanto internos como externos, salvo a través de la Dirección General, Subdirección General, Secretaría General, Oficina Asesora de Comunicaciones, Dirección de Planeación y Gestión de Control, Dirección de Gestión Humana y Dirección de Información y Tecnología.

- En las sedes regionales está prohibido el envío de correos masivos (más de 20 destinatarios) tanto internos como externos, salvo a través de los Directores Regionales, así como Coordinadores Regionales y de Centro Zonal.

- Todo mensaje SPAM o Cadena debe ser inmediatamente reportado a la Dirección de Información y Tecnología a través de la Mesa de Servicios como incidente de seguridad de la información según procedimiento establecido. No está permitido el envío y/o reenvío de mensajes en cadena.

- Todo mensaje sospechoso respecto de su remitente o contenido, debe ser inmediatamente reportado a la Dirección de Información y Tecnología a través de la Mesa de Servicios como incidente de seguridad de la información según procedimiento establecido y proceder de acuerdo a las indicaciones de dicha Dirección; lo anterior, debido a que puede ser contentivo de virus, en especial si contiene archivos adjuntos con extensiones .exe, .bat, .prg, .bak, .pif, o tenga explícitas referencias no relacionadas con la misión de la Entidad (como por ejemplo: contenidos eróticos, alusiones a personajes famosos).

- La cuenta de correo institucional no debe ser revelada en páginas o sitios publicitarios, de comercio electrónico, deportivos, agencias matrimoniales, casinos, o cualquier otra ajena a los fines de la Entidad.

- Está expresamente prohibido el uso del correo para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y/o que atenten contra la integridad moral de las personas o instituciones.

- Está expresamente prohibido distribuir información del ICBF, a otras entidades o ciudadanos sin la debida autorización de Director(a) General, Directores Regionales, Subdirector(a) General, Directores Misionales y/o Director(a) de Planeación y Control de Gestión.

- El cifrado de los mensajes de correo electrónico institucional será necesario siempre que la información transmitida esté clasificada como clasificada o reservada en el inventario de activos de información o en el marco de la Ley Colombiana vigente.

- El correo electrónico institucional en sus mensajes debe contener una sentencia de confidencialidad, que será diseñada por la Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos y debe reflejarse en todos los buzones con dominio @icbf.gov.co.

- La divulgación de cifras o datos oficiales de la Entidad sólo podrá ser emitida desde las direcciones de correo electrónico de la Dirección General, Direcciones Regionales, Subdirección General, Oficina Asesora de Comunicaciones y la Dirección de Planeación y Control de Gestión.

- Está expresamente prohibido distribuir información del ICBF a través de correos personales o sitios web diferentes a los autorizados por la Dirección de Información y Tecnología.

- El único servicio de correo electrónico autorizado para el manejo o transmisión de la información institucional en la Entidad es el asignado por la Dirección de Información y Tecnología, y que cuenta con el dominio @icbf.gov.co, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso;

b) Del Uso de Internet: La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos establecerá políticas de navegación basadas en categorías y niveles de usuario por jerarquía y funciones, previa validación del eje de Seguridad de la Información.

De acuerdo al buen uso de los recursos de navegación de la Entidad, se deben tener en cuenta los siguientes lineamientos:

- El uso del servicio de Internet está limitado exclusivamente para propósitos laborales.

- Los servicios a los que un determinado usuario pueda acceder desde internet dependerán del rol o funciones que desempeña en el ICBF y para las cuales esté formal y expresamente autorizado.

- Todo usuario es responsable de informar a la Dirección de Información y Tecnología a través de la Mesa de Servicios, los contenidos o acceso a servicios que no le estén autorizados y/o no correspondan a sus funciones dentro del ICBF.

- Está expresamente prohibido el envío, descarga y/o visualización de páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor y/o que atenten contra la integridad moral de las personas o instituciones.

- Está expresamente prohibido el acceso a páginas web, portales, sitios web y aplicaciones web que no hayan sido autorizadas por el ICBF a través de la política de navegación.

- Está expresamente prohibido el envío y/o descarga de cualquier tipo de software o archivos de fuentes externas, y/o de procedencia desconocida.

- Está expresamente prohibida la propagación de virus o cualquier tipo de código malicioso.

El ICBF se reserva el derecho de monitorear los accesos, y el uso del servicio de internet de todos sus funcionarios o contratistas, además de limitar el acceso a determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro ajeno a los fines de la Entidad;

c) Del Uso de los Recursos Tecnológicos: Los recursos tecnológicos del ICBF son herramientas de apoyo a las labores y responsabilidades de los funcionarios y contratistas. Por ello, su uso está sujeto a las siguientes directrices:

- Los bienes de cómputo se emplearán de manera exclusiva y bajo la completa responsabilidad por el funcionario o contratista al cual han sido asignados, y únicamente para el desempeño de las funciones del cargo o las obligaciones contractuales pactadas. Por tanto, no pueden ser utilizados con fines personales o por terceros no autorizados ante la Dirección de Información y Tecnología mediante solicitud formal por los Directores, Subdirectores, Jefes de Oficina o Coordinadores de Grupos del ICBF a través de la Mesa de Servicios.

- Solo está permitido el uso de software licenciado por la Entidad y/o aquel que sin requerir licencia, sea expresamente autorizado por la Dirección de Información y Tecnología a través de la Subdirección de Recursos tecnológicos. Las aplicaciones generadas o adquiridas por el ICBF en desarrollo de su operación institucional, deben ser reportadas a la Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información, para su administración.

- En caso de que el colaborador deba hacer uso de equipos ajenos al ICBF, estos deberán cumplir con la legalidad del Software instalado, antivirus actualizado y no podrá conectarse directamente a la red del ICBF, sino que deberá hacerlo a través de red de visitante utilizando una VPN suministrada por la Entidad. Estas condiciones deben ser verificadas por los ingenieros de la Subdirección de Recursos Tecnológicos a nivel Central, Regional o Zonal.

- Es responsabilidad de los funcionarios y contratistas mantener copias de seguridad de la información contenida en sus estaciones de trabajo y entregarlas al ICBF en custodia al finalizar la vinculación con la Entidad.

- Los usuarios no deben mantener almacenados en los discos duros de computadores de escritorio, portátiles o discos virtuales de red, archivos de video, música y fotos que no sean de carácter institucional.

- No está permitido fumar, ingerir alimentos o bebidas en el área de trabajo donde se encuentren elementos tecnológicos.

- No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo la disponibilidad de la información por fallas en el suministro eléctrico a los equipos de cómputo.

- Los únicos autorizados para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar y/o reparar sus componentes, son los designados por la Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos para tal labor.

- La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos realizará monitoreo sobre los dispositivos de almacenamientos externos como USB, CD-ROM, Discos Duros externos, entre otros, con el fin de prevenir o detectar fuga de información.

- La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro es la Dirección Administrativa o quien haga sus veces en el nivel regional y zonal, con el fin de llevar el control individual de inventarios. En tal virtud, toda reasignación de equipos deberá ajustarse a los procedimientos y competencias de dicha dependencia.

- La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, debe ser informada de inmediato a la Dirección Administrativa por el funcionario o contratista a quien se le hubiere asignado.

- La pérdida de información debe ser informada con detalle a la Dirección de Información y Tecnología a través de la Mesa de Servicios como incidente de seguridad.

- Todo incidente de seguridad que comprometa la disponibilidad, integridad o confidencialidad de la información debe ser reportado a la mayor brevedad posible a la Mesa de Servicios, siguiendo el procedimiento establecido.

- La Dirección de Información y Tecnologías es la única dependencia autorizada para la administración del software, el cual no debe ser copiado, suministrado a terceros ni utilizado para fines personales.

- Todo acceso a la red de la Entidad mediante elementos o recursos tecnológicos no institucionales deberá ser informado, autorizado y controlado por la Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos.

- Los equipos deben quedar apagados cada vez que el funcionario o contratista no se encuentre en la oficina o durante la noche, esto, con el fin de proteger la seguridad y distribuir bien los recursos de la Entidad, siempre y cuando no vaya a realizar actividades vía remota;

d) Del Uso de los Sistemas o Herramientas de Información: Todos los funcionarios y contratistas del ICBF son responsables de la protección de la información que acceden y/o procesan, así como de evitar su pérdida, alteración, destrucción y uso indebido, para lo cual se dictan los siguientes lineamientos:

- Las credenciales de acceso a la red y a los recursos informáticos (Usuario y Clave) son de carácter estrictamente personal e intransferible; los funcionarios y contratistas no deben revelarlas a terceros ni utilizar claves ajenas.

- Todo funcionario y contratista es responsable del cambio de clave de acceso a los sistemas de información o recursos informáticos periódicamente.

- Todo funcionario y contratista es responsable de los registros y modificaciones de información que se hagan a nombre de su cuenta de usuario.

- En ausencia del funcionario o contratista, el acceso a la estación de trabajo le será bloqueada con una solicitud a la Dirección de Información y Tecnología a través de la Mesa de Servicios, con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, así como a la suplantación de identidad. La Dirección de Gestión Humana debe reportar cualquier tipo de novedad de los funcionarios y el Supervisor del Contrato las novedades de los contratistas.

- Cuando un funcionario o contratista cesa en sus funciones o culmina la ejecución de contrato del ICBF, todos los privilegios sobre los recursos informáticos otorgados le serán suspendidos inmediatamente; la información del empleado y/o contratista serán almacenados en un repositorio de los servidores de la Entidad.

- Cuando un funcionario o contratista cesa en sus funciones o culmina la ejecución de contrato del ICBF, el supervisor o jefe inmediato es el encargado de la custodia de los recursos de información, incluyendo la cesión de derechos de propiedad intelectual de acuerdo a la normativa vigente.

- Todos los funcionarios y contratistas de la Entidad deben respetar lo estipulado en la Ley 23 de 1982 “Sobre derechos de autor”, la Decisión 351 de 1993 de la Comunidad Andina de Naciones, así como cualquier otra que adicione, modifique o reglamente la materia. [44]

4.3.6 Portal Cautivo

Según Proaño Galarza un portal cautivo es:

[44] Colombia. ICBF Resolución 9364 de 2016 – Política Seguridad de la Información. [En Línea] Disponible en http://www.icbf.gov.co/cargues/avance/docs/resolucion_icbf_9364_2016.htm

Un conjunto de herramientas para la administración de la red, las cuales controlan los servicios y protocolos que pueden ser utilizados como, por ejemplo: el ancho de banda asignado por usuario, el tiempo de uso del servicio, control de tráfico que viaja por la red etc. Cuando un usuario intenta establecer conexión para navegar en internet, es redirigido a una página web de autentificación en donde se le solicita credenciales de inicio de sesión; o en su defecto, se le informa las condiciones de uso del servicio inalámbrico, luego de que se haya autentificado podrá hacer uso de la red o del internet.

Existen soluciones de software libre para portales cautivos que permiten su instalación en máquinas con un sistema operativo GNU/LINUX, las cuales funcionan como servidor de autentificación, y los puntos de acceso de red inalámbrica se los instala con una configuración básica; sin embargo, esta configuración puede resultar costosa, debido a que se necesita tener un equipo al que se le pueda instalar un sistema operativo de servidor, conocimientos de dicho sistema operativo y además los puntos de acceso necesarios para dar cobertura inalámbrica. [45]

[45] Proaño Galarza, P. (2009). Diseño e implementación de un portal cautivo utilizando un enrutador inalámbrico de bajo costo y un sistema operativo de código abierto. [En Línea] Repositorio.uisek.edu.ec. Disponible en http://repositorio.uisek.edu.ec/handle/123456789/79

5. CAPITULO I - BRING YOUR OWN DEVICE (BYOD) - TRAE TU PROPIO DISPOSITIVO

Los autores Luna, J. y Martín, J. nos dan un punto de vista acertado del BYOD, según ellos:

> El fenómeno BYOD (Bring Your Own Device), que es la incorporación de los dispositivos personales de los empleados a los sistemas de información corporativos de TI de nuestras organizaciones, ha llegado para quedarse, "no es una moda pasajera" y hay que estar preparados para asumir y controlar todas las amenazas que trae consigo. Al respecto de este nuevo y delicado fenómeno que responde al acrónimo BYOD, hay que evitar que la improvisación lo convierta en BYOD (Bring Your Own Disaster), con resultados inesperados nada deseables y consecuencias irreversibles para nuestras organizaciones y modelos de negocio. [46]

5.1 ORIGEN DEL BYOD.

Si se busca documentación sobre el cómo, cuándo o quien fue el precursor del BYOD, no se encontrará información fidedigna de un inicio de esta tendencia, ya que más que un invento, metodología o diseño de una persona o una compañía, se trató de un movimiento mundial que se fue dando a principios del siglo XXI por el mismo avance de la tecnología, pues cada vez fueron saliendo al mercado equipos con más funciones, más veloces, portables y conectados a la Internet, además que a medida que se fueron masificando su costo fue bajando y se hicieron más accesibles para todos los bolsillos, pasando de ser un lujo a una necesidad por estar comunicado y poder tener herramientas informativas, de ocio, educativas y corporativas siempre a la mano. Es un movimiento similar al de los restaurantes o bares en los años 90, que permitieron que las personas llevaran su propia botella de vino o licor a cambio de una pequeña suma de dinero con el fin de incentivas el consumo de otros productos o mantener su clientela.

Para REYES VÁSQUEZ, "El BYOD es un nuevo fenómeno cultural y tecnológico que permite a los empleados de una organización utilizar sus propios dispositivos móviles personales en las actividades de la empresa donde trabaja conectado a la red corporativa."[47] Esta novedad en las conductas laborales hace que los departamentos de TI presten atención a los riesgos en lo que concierne la seguridad de la información. La piratería industrial se facilita con estos usos y en algunos casos deja en jaque la confidencialidad de las empresas.

---

[46] Luna, J. y Martín, J. (2013). La gestión segura de la información en movilidad ante el fenómeno BYOD: ¿Bring Your Own Device = Bring Your Own Disaster?. [En Línea] Dialnet.unirioja.es. Disponible en https://dialnet.unirioja.es/servlet/articulo?codigo=4391556

[47] Reyes Vásquez, Virgilio Ernesto. "BYOD y la movilidad corporativa". Ing-novación. Revista semestral de ingeniería e innovación de la Facultad de Ingeniería, Universidad Don Bosco. Diciembre de 2012 – Mayo de 2013, Año 3, No. 5. pp. 117-121. ISSN 2221-1136.[En Línea] Disponible en http://www.redicces.org.sv/jspui/bitstream/10972/1985/1/BYOD%20y%20la%20mobilidad.pdf

En términos económicos para las empresas algunos directivos lo consideran muy positivo, pues además de ser equipos de tecnología de punta, se cree que mantiene motivado al empleado y el costo del equipo es asumido por el mismo. Otro factor influyente es que anteriormente una vez finalizado el turno de trabajo, un empleado se desconectaba por completo de temas laborales, con la aplicación del BYOD las empresas cuentan prácticamente con una disponibilidad de 7X24 de sus empleados.

Para Rojas, es importante tener presente que:

> Un error que se presenta de manera frecuente en las organizaciones que tratan de incursionar en la tendencia BYOD es que las políticas de seguridad existentes son bastante cerradas con la finalidad de proteger la red causando inconvenientes cuando los empleados traen sus dispositivos móviles para desarrollar sus labores diarias, incluso el no contar con el conocimiento suficiente y pretender desplegar un sistema BYOD, sin tener en cuenta el antivirus, programas anti-malware que se encuentren instalados en los dispositivos móviles conduce a una gran cantidad de vulnerabilidades ocasionando inconvenientes con las políticas de seguridad existentes, en ocasiones hasta comprometiendo la confidencialidad de la información[48]

Para Luna, J. S., & Martín, J. F. Esta tendencia lleva a los negocios a ver como el:

> BYOD está impulsado por el negocio, “que quiere llevar al mundo de la movilidad sus procesos” para ganar competitividad. Está impulsado por el usuario, “que quiere utilizar sus dispositivos personales de última generación para acceder a los recursos corporativos donde está la información sensible del negocio”; está impulsado por los departamentos Financieros de las organizaciones para reducir “aparentemente” los costes derivados de la adquisición, mantenimiento y renovación por parte de la empresa de estos nuevos activos tecnológicos.[49].

Para Macia, S. un dispositivo personal es un peligro para la empresa porque:

> Un smartphone comprometido, automáticamente pone en riesgo:
>
> - La clave de la/s red/es a la que el dispositivo se conecta
> - El usuario de la cuenta de correo utilizada
> - El usuario de la cuenta de mensajería instantánea utilizada
> - Accesos VPN que puedan haber configurados
> - Información de contactos personales
> - Información de acceso en distintas aplicaciones: Facebook, LinkedIn,
> - Etc

[48] Rojas, D. (2015). "BRING YOUR OWN DEVICE OPORTUNIDADES”, RETOS Y RIESGOS EN LAS ORGANIZACIONES. [En Línea] Revistas.uni.edu.pe. ISSN: 0375-7765 ISSN: 2309-0413 (versión electrónica) Disponible en http://revistas.uni.edu.pe/index.php/tecnia/article/view/17/219

[49] Luna, J. S., & Martín, J. F. Óp. Cít., 104, 65-73.

Distintos problemas de seguridad relacionados con estas tecnologías que han tomado trascendencia pública, los cuales, no sólo podrían estar relacionados con el compromiso de los datos personales de los mismos sino también con ataques dirigidos contra la privacidad o inclusive espionaje[50].

5.2 TENDENCIA BYOD.

Lo intuitivo que son los dispositivos móviles conllevan a que este se utilice en todos los entornos, desde el entretenimiento hasta lo laboral. Esto hace pensar en un ahorro en infraestructura de la corporación, pero también genera un estado de incertidumbre por los riesgos en torno a la seguridad de la información. El usuario promedio actualiza su dispositivo cada 2 años teniendo un mejor componente electrónico.

Debido al crecimiento exponencial que han tenido los dispositivos móviles y la facilidad para la interconectividad con las aplicaciones corporativas basadas en la nube generando un ambiente de trabajo colaborativo ubicuo donde cada empleado trabaja a su ritmo y rompe la barrera del horario laboral llevando sus ocupaciones a espacios que antes no podía, gracias a esta evolución tecnológica tenemos nuevos retos para proteger la información confidencial tanto en lo personal como lo laboral.

Con el uso del BYOD se han creado varias herramientas para salvaguardar los datos sensibles de las empresas teniendo un control de la información y administración de los recursos tecnológicos con que se cuentan. En este orden de ideas el mayor riesgo está en la falta de capacitación al usuario final que es quien pone su dispositivo como ventana al mundo y puede convertirse en una ruta para exponer los bienes intangibles de la compañía.

5.3 CONSIDERACIONES Y TÁCTICAS DE BYOD.

Actualmente las compañías deben realizar un frente al uso correcto del BYOD que sin embargo no es nuevo, se ha incrementado exponencialmente en los últimos años. Desde la aparición de las tabletas rondado el año 2012 a la evolución de los teléfonos inteligentes encontramos que estos elementos cuentan con su propio sistema operativo, nivel de seguridad, aplicaciones que permiten tener acceso a los recursos internos de las empresas. Los administradores de TI tienen unas opciones para enfrentar estas tendencias:

- Establecer políticas de seguridad para el acceso de los dispositivos móviles a la red laboral.

[50] Macia, S. (2014). Seguridad en dispositivos móviles: un enfoque práctico. [En Línea] Sedici.unlp.edu.ar. Disponible en http://sedici.unlp.edu.ar/handle/10915/43678.

- Contratar una solución corporativa para administrar esta conectividad y permitir el estado de confianza en la organización.
- No permitir el uso de BYOD.

Cual sea la tendencia selecciona evidentemente dependerá de la infraestructura corporativa con que se cuenta en el momento y la proyección a futuro que se tenga en la ampliación hacia el uso de soluciones en la nube. Una realidad que crece vertiginosamente en la actualidad con la evolución de la electrónica y las TIC.

Según Vásquez Villacreses, las buenas prácticas de administración de TI para los dispositivos que no son de la compañía deben tener:

> Las consideraciones que se deberán tomar para una correcta administración de dispositivos finales y móviles inician con la implementación de políticas de seguridad y de acceso a la red corporativa claras, las mismas que deben ser redactadas en un documento que se pueda sociabilizar con todos los empleados de tal forma que el personal conozca lo que puede hacer al ocupar sus dispositivos. Al tener un proceso de control de accesos a los sistemas críticos de la empresa la gerencia de TI asegura conocer el perfil del empleado que está solicitando los accesos y así asignarle diferentes niveles y perfiles de acceso para salvaguardar dicha información[51].

5.4 PROPIEDAD INTELECTUAL.

Para regular el BYOD en las empresas se debe tener claro el derecho de propiedad intelectual con el que se maneja la confidencialidad de la información. Creando manifiestos de confidencialidad amparados por las leyes nacionales e internacionales se creará una conciencia hacia el correcto uso de la información privilegiada. Desde las multas pecuniarias hasta la provocación de la libertad tendrán a los usuarios prestos a contribuir con salvaguardar los datos utilizados en sus dispositivos móviles.

De nuevo Vásquez Villacreses nos aporta una clasificación de los delitos que pueden afectar la propiedad intelectual y:

> Según la gravedad de los delitos y en relación al contenido o finalidad y a la infracción a los derechos de propiedad intelectual que realizan se los puede clasificar en:
>
> - Phishing: consiste en él envió de correos electrónicos que simulan ser originales o pertenecer a fuentes confiables ya sean entidades bancarias y cuya finalidad es apropiarse de los datos privados de los usuarios como pueden ser las credenciales de acceso o números de cuentas y tarjetas.

[51] Vásquez Villacreses, L. (2015). Herramientas de seguridad de la información en dispositivos finales y móviles con relación a “BYOD” – caso de estudio de la plataforma IBM Security Endpoint Manager. [En Línea] P. 5., Repositorio.puce.edu.ec. Disponible en http://repositorio.puce.edu.ec/handle/22000/10282

- Tampering: es la modificación sin autorización de datos o código de software para la manipulación del sistema objetivo (victima), con la finalidad de alterar, obtener o borrar información causando la falla general del sistema y en el peor de los casos inhabilitándolo.
- Scanning: es uno de los métodos que lleva mucho tiempo en uso y se encarga de explorar y descubrir puntos de comunicación susceptibles y que son de utilidad para el objetivo en particular. La metodología varía acorde las técnicas, puertos y protocolos soportados.
- Pharming: consiste en enviar al usuario a una página falsa para apropiarse de las credenciales o información crítica o personal, es similar al phishing pero tiene una metodología más avanzada en la que ya no se engaña al usuario mediante correo o links de visita sino que engaña al equipo objetivo para que resuelva las URL correctas hacia direcciones maliciosas o fraudulentas.
- Skimming: es la técnica mediante la cual se trata de obtener las credenciales de las tarjetas de crédito del usuario ya sea mediante el uso de software o hardware durante la transacción facilitando la clonación de tarjetas o el ingreso a la información bancaria para realizar transacciones fraudulentas. (Goncalves, 1997, pág. 25)

Los sujetos que realizan los delitos informáticos son personas que tienen conocimientos avanzados de la informática que buscan lucrar mediante el uso de varias técnicas con finalidad de la sustracción de la información. Es necesario que los empleados de las empresas conozcan los medios por los cuales pueden ser víctimas y salvaguardar la información tanto personal como laboral que poseen[52].

5.5 RIESGO DE LA INFORMACIÓN.

Para Rojas, D. L. M. las características principales de los riesgos asociados al BYOD los fue relacionando en un determinado orden, como se describe:

El riesgo es un factor importante que se debe tener en cuenta a la hora de hablar de un ambiente BYOD, especialmente cuando se considera el depositar los datos de la organización en los dispositivos personales de los empleados.

Bruce Schneier, analiza la percepción que tiene los empleados sobre los riesgos, y concluye que los mismos no se encuentran en la capacidad de realizar una adecuada evaluación de los riesgos a los que se encuentran expuestos, esto debido a la forma como los diferencian.

También indica que los empleados y usuarios reaccionan a los riesgos a medida que se van presentando y no son proactivos en su reconocimiento, dando paso a que las amenazas puedan materializar estos riesgos.

A continuación, se describen los principales riesgos y amenazas a los que se encuentran expuestas las organizaciones que desean implementar BYOD, los cuales

[52] Ibíd., p. 7.

deben ser tratados cuidadosamente en la descripción de la política para que al final sea un éxito y no se vean afectados por incidentes de seguridad ocasionando pérdidas financieras y de imagen corporativa.

Tabla 1. Principales riesgos asociados a BYOD.

RIESGO	DESCRIPCIÓN
Información de Usuario	Nombres de usuarios y contraseñas, información bancaria, certificados instalados, cuentas de correo, pueden verse comprometidas, en caso de pérdida o robo del dispositivo móvil
Información Corporativa confidencial	Datos de carácter confidencial perteneciente a la organización como correos electrónicos, archivos, informes, aplicativos se encuentran en riesgo en caso de un acceso no autorizado sobre el dispositivo sea por descuido, perdía o robo
Teléfono y datos	Puede realizarse la interceptación de llamadas o el sniffing de paquetes, brindando acceso a los datos del dispositivo comprometiendo la información allí almacenada
El mismo dispositivo móvil	La portabilidad que brinda los dispositivos hace que el riesgo de pérdida o robo aumente
Malware.	Un dispositivo infectado con algún software malicioso puede conducir a la fuga de información confidencial, el uso de servicios adicionales como llamadas y envío de mensajes de texto no programados, interrupción parcial o completa del correcto funcionamiento del dispositivo
Spam	Mensajes de correo electrónico no deseados que se reciben de fuentes desconocidas los cuales generan consumo del dispositivo en recursos como ancho de banda y memoria
Phishing	Esto puede llegar a presentar a través de un correo electrónico o un mensaje de texto para engañar al usuario e ingresar a un sitio web falso solicitándole información sensible de la organización
Bluetooth and Wi-Fi	Al conectarse a diferentes redes o compartir archivos el dispositivo puede verse fácilmente infectado lo cual daría paso a la interceptación de datos que viajan desde o hacia los dispositivos móviles

[53]

Fuente: Ibid

5.6 VENTAJAS DEL BYOD.

El BYOD como tendencia mundial creciente supone unas ventajas que las entidades como el ICBF puede explotar, dentro de las principales se encuentra:

- Personal motivado por contar con su propio equipo de cómputo, teléfono inteligente o Tablet, el cual cuenta con disponibilidad de 7 por 24 para cumplir con sus labores así sea de manera remota, además se supone que es un dispositivo de su agrado para trabajar y cuenta con flexibilidad y movilidad.
- En algunas ocasiones estos equipos pueden ser de última tecnología y el costo fue asumido por el empleado.

[53] Rojas, D. L. M. Óp. Cit., p. 6.

- Se cubren necesidades de equipos que la entidad no puede adquirir por temas presupuestales.
- Al ser propio el equipo deberían estar habituados en su funcionamiento lo que se traduciría en eficiencia para la organización.
- No se incluiría en gastos de licenciamiento para esos equipos porque son del trabajador.
- No generarían gastos por concepto de mantenimiento o aseguramiento de los equipos, ya que estos serían asumidos por el trabajador.
- Al ser equipos móviles se podrían conectar al WiFi del ICBF o al internet móvil del trabajador si cuenta con él, lo que generaría mejora de espacio al no tener que contar con un puesto fijo de trabajo que cuente con cableado estructurado.

Como se puede ver la mayoría de las ventajas están relacionadas con disminución de costos y optimización de recursos para la entidad, además de que se cuente con herramientas de trabajo para todos los colaboradores asegurando portabilidad y flexibilidad.

5.7 DESVENTAJAS DEL BYOD.

Al ser una realidad organizacional el BYOD también viene acompañado de algunas desventajas:

- No se puede asegurar que la estación de trabajo sea un equipo confiable.
- La información contenida en los dispositivos personales que pertenezca a la empresa puede no contar con respaldo de seguridad ante perdida de este, daño o salida del empleado de la organización.
- No de compatibilidad de las herramientas institucionales con el hardware o software del dispositivo móvil.
- Falta de control del departamento de TI sobre los equipos personales.
- Un empleado con conocimientos en sistemas que no trabaje en el Departamento de TI, pero pueda usar su equipo sin ningún tipo de restricción y con permisos de administrador sobre su máquina es un riesgo latente para la seguridad de la red interna y la seguridad de la información.
- Equipos con virus o software P2P que saturen la red o envié peticiones no permitidas.

Las desventajas en el BYOD, pasan siempre por el tema de seguridad y en menor cuantía por temas de compatibilidad de las herramientas, lo que también puede generar que empleados terminen atacando la disponibilidad, integridad y confidencialidad de la información de manera intencional o involuntaria.

6. CAPITULO II - INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR REGIONAL TOLIMA

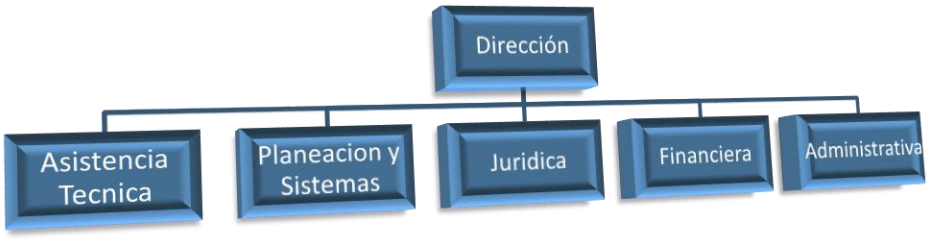
Al consultar el Sitio web del ICBF podemos encontrar esta breve reseña:

> El Instituto Colombiano de Bienestar Familiar ICBF, es la entidad del Gobierno de Colombia que trabaja por el bienestar de los niños, las niñas, los adolescentes y sus familias, es un establecimiento público descentralizado, con personería jurídica, autonomía administrativa y patrimonio propio, creado por la Ley 75 de 1968 y reorganizado conforme a lo dispuesto por la Ley 7 de 1979 y su Decreto Reglamentario No. 2388 de 1979, que mediante Decreto No. 4156 de 2011 fue adscrito al Departamento Administrativo para la Prosperidad Social.
>
> Dentro de su estructura organizacional cuenta con una sede principal denominada Sede de la Dirección general que está ubicada en la ciudad de Bogotá DC, y a su vez tiene sedes Regionales repartidas en los 33 departamentos de Colombia, de estas 33 Regionales dependen 209 centros zonales con el fin de ofrecer los servicios de ICBF en todo el territorio nacional.[54]

Para el caso del presente proyecto, se tomará como Referencia la Regional Tolima, la cual está conformada por la sede principal en la Ciudad de Ibagué (Regional) y de ella dependen 10 CZ (Centros Zonales) Repartidos en 8 municipios considerados principales y distribuidos geográficamente con el fin de lograr cobertura a los servicios brindados para toda la población del departamento (CZ Jordán Ibagué, CZ Galán Ibagué, CZ Ibagué Centro, CZ Lérida, CZ Líbano, CZ Honda, CZ Espinal, CZ Purificación, CZ Chaparral y CZ Melgar).

La sede Regional está dividida en 6 áreas funcionales: Dirección, Asistencia Técnica, Financiera, Planeación y Sistemas, Jurídica y Administrativa, las cuales son las encargadas de realizar el direccionamiento estratégico, el trabajo administrativo, labores de soporte y de apoyo a los Centro Zonales.

Figura 8. Organigrama ICBF.



Fuente: los autores.

[54] Portal ICBF - Instituto Colombiano de Bienestar Familiar ICBF. (2017). El Instituto. [En Línea] Disponible en https://www.icbf.gov.co/instituto

La Regional Tolima en la actualidad cuenta con aproximadamente 430 Colaboradores entre personal de Planta y Contratistas por prestación de servicios, que son los encargados de realizar el trabajo administrativo, misional y de supervisión dentro de la institución. Este recurso humano es el que en la actualidad por algunas condiciones de falta de equipos está generando la posibilidad de usar equipos personales en el ICBF.

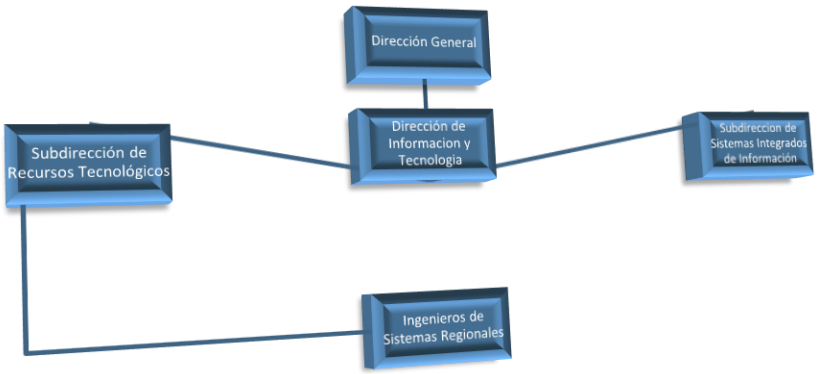
6.1 INFRAESTRUCTURA TECNOLÓGICA DEL ICBF

En la última década el ICBF ha venido implementando un plan estratégico de sistemas que le ha permitido desarrollarse de manera integral en todos los frentes tecnológicos (Hardware, Comunicaciones, Sistemas de Información, almacenamiento, suites colaborativas, servicios de nube, licenciamiento Agreement con Microsoft, Networking, mesa de servicios basado en ITIL y Seguridad de la Información).

Esta apuesta que inicio el ICBF hace algunos años viene dando frutos importantes, lo cual ha generado que en la actualidad sea una de las entidades del estado mejor estructuradas en cuanto a tecnología se refiere, y esté implementando proyectos importantes como la estrategia Gobierno en línea y certificación en ISO 27001 por la implementación del SGSI.

Dentro del modo de operación tecnológico el ICBF cuenta con una DIT (Dirección de información y Tecnología) que está ubicada en la sede Nacional y de ella depende la SRT (Subdirección de Recursos tecnológicos) y la SSI (Subdirección de Sistemas Integrados de Información).

Figura 9. Organigrama Tecnológico ICBF.



Fuente: los autores.

Como se puede apreciar en la figura N°9 la Oficina de Sistemas regional, depende funcionalmente de la SRT, dado que todo el personal técnico en el tema de infraestructura, comunicaciones, seguridad y soporte pertenece a esta subdirección.

6.1.1 Dominio icbf.gov.co

El ICBF cuenta con un dominio corporativo bajo Windows Server que está centralizado y es controlado a nivel nacional, lo que permite tener una RED WAN la cual esta segmentada en diferentes rangos con el fin de dar direccionamiento a las casi 300 sedes que tiene a nivel nacional, eso se logra por medio Canales dedicados contratados con terceros, los cuales son seleccionados anualmente por medio de subastas para prestar el servicio.

6.1.2 Canales de comunicación

Dichos canales permiten la comunicación directa entre sedes de ICBF a nivel nacional y regional, soportando el funcionamiento de los principales servicios tecnológicos que se brindan a los usuarios.

Dentro de estos se encuentran principalmente:

Tabla 2. Servicios TI del ICBF.

SERVICIOS TECNOLÓGICOS DE ICBF	DESCRIPCIÓN
Telefonía IP	Solución de Voz sobre IP para llamadas internas y externas
Office 365 (Correo, ofimática, herramientas colaborativas)	Suite ofimática usada por los Colaboradores ICBF
Sistemas de Información misionales	Sistemas de información que registran la atención de los usuarios de ICBF (Web)
Sistemas de Información de Apoyo Administrativo y Financiero	Sistemas de información para la administración de recurso humano, sistemas de información financieros y contable, sistemas de información de seguimiento.
Internet	Navegación Web de los Colaboradores
File Server	Servidores de archivos descentralizados
Intranet y Portal Web	Información y servicios Web
Seguridad (Proxy, Firewall, Antivirus)	Mecanismos de seguridad
Administración de Equipos y Dispositivos de Red	Servicio de Directorio Activo, monitoreo y administración de equipos
Mesa de Servicios Helpdesk	Mesa de soluciones informáticas.

Fuente: los autores.

Todos estos servicios soportan la labor diaria de los Colaboradores en ICBF y a su vez permiten realizar la atención que se brinda a los niños, adolescentes y familias colombianas.

6.1.3 SGSI En El ICBF

El ICBF en la actualidad está implementando un SGSI, proceso que ha sido considerado exitoso y arroja resultados positivos al estar certificado en ISO 27001 en el proceso de gestión tecnológica. Este proceso ha generado importantes avances en la identificación de activos de información, análisis de riesgos, plan de continuidad y recuperación, cultura de seguridad en los colaboradores de ICBF, planes de sensibilización, entre otros. Por lo que lograr implementar el BYOD de manera óptima le dará robustez a su SGSI, y cerrará muchas más brechas de seguridad.

6.1.4 Problemática Equipos De Cómputo ICBF

La Regional Tolima cuenta en la actualidad con un parque computacional propio cercano a 390 equipos. Año tras año realiza compras de equipos nuevos de última tecnología con el fin de proveer equipos al personal que no cuenta con este recurso, y a su vez la idea es ir reemplazando los equipos obsoletos, que en la actualidad son casi el 80 %. Esta situación está generando un inconveniente, dado que por temas presupuestales y la política de austeridad del gasto de las entidades públicas, cada año se adquieren menos equipos; por ejemplo, para el año 2014 se adquirieron 54 equipos, en 2015 38, en 2016 34 y se espera que a finales del 2017 se adquieran 14.

Lo anterior muestra una reducción drástica de compras de equipos año tras año, lo que genera cada vez más colaboradores sin equipo proporcionado por la entidad, sumado al nivel de obsolescencia y con un aumento de personal año tras año del 2% está generando que algunos colaboradores opten por traer su propio equipo de cómputo portátil para poder realizar las labores asignadas en el instituto.

El escenario descrito directamente está introduciendo al ICBF Regional Tolima al BYOD, pues ante ausencia de herramientas tecnológicas institucionales los colaboradores se ven prácticamente obligados a llevar sus equipos con el fin de poder cumplir con sus obligaciones contractuales. Pero el tema no para allí, pues dado el auge de los dispositivos móviles (Smartphones y Tabletas) también es muy frecuente que los colaboradores usen sus equipos móviles para realizar labores relacionadas con el trabajo, principalmente correo electrónico y algunos aplicativos por medio de dichos dispositivos.

6.1.5 Riesgos asociados al BYOD en el ICBF Regional Tolima

Con el fin de establecer los riesgos asociados al BYOD en el ICBF Regional Tolima se realiza un análisis de riesgos exclusivamente para el uso de dispositivos móviles dentro de la red ICBF, lo anterior para poder verificar los controles existentes y los que se pueden implementar con el fin de disminuir los riesgos y darles el tratamiento adecuado. La identificación y el tratamiento del riesgo se realizó alineado con las normas ISO 31000 de 2009 y los posibles controles según los anexos de la ISO 27001 de 2013.

Los riesgos identificados fueron:

R1: Perdida de información institucional; debido al uso de dispositivos móviles personales en las funciones afectando Confidencialidad, Integridad, Disponibilidad del proceso.

R2: Ataque informático o afectación por virus por acceso a la red cableada o WiFi no autorizado; debido a Equipos personales en la red corporativa, puntos de red desatendidos. Afectando Confidencialidad, Integridad, Disponibilidad y Continuidad del proceso.

R3: Divulgación de información Confidencial, clasificada o reservada para el instituto; debido a Perdida o mal manejo de dispositivo personal en funciones de ICBF afectando Confidencialidad e Integridad del proceso.

R4: Saturación de la Red WAN y LAN por programas como P2P, Proxy, servicios de streaming o gestores de descarga; debido a Equipos personales con herramientas instaladas y no permitidas en ICBF afectando Disponibilidad y Continuidad del proceso.

R5: Dispositivos desactualizados, rooteados o con software ilegal, debido a Equipos móviles como teléfonos inteligentes desactualizados o rooteados o portátiles con sistema operativo sin licenciar con activaciones piratas. afectando Integridad y Disponibilidad del proceso.

De los riesgos identificados, se determinó una prioridad o importancia por su gravedad de la siguiente manera.

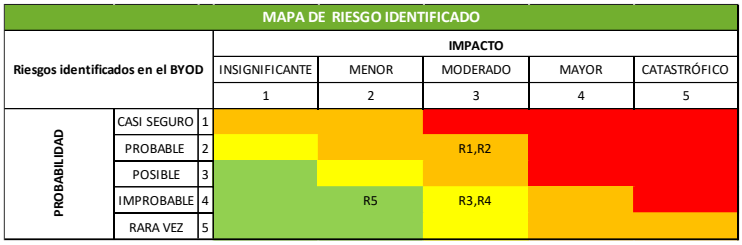
Tabla 3. Prioridad de los Riesgos.

RIESGO	PRIORIDAD
R2	1
R1	2
R3	3
R4	4
R5	5

Fuente: los autores.

Donde 1 es el más crítico. Según la matriz de identificación del riesgo (Ver Figura 11) se obtuvo el siguiente mapa del riesgo (Ver Figura 10):

Figura 10. Mapa de calor, según matriz del riesgo en el ICBF.



Fuente: los autores.

Figura 11. Matriz del riesgo RG en el ICBF.

ID	PROCESO (DUEÑO DEL RIESGO)	CONTEXTO INTERNO	CONTEXTO EXTERNO	PRIORIDAD	TIPO DE ACTIVO AFECTADO	2.2 Análisis del riesgo						2.3 Evaluación del riesgo			OPCIONES TRATAMIENTO	CONTROLES ANEXO A ISO 27001:2013
						RIESGO: AFECTACIÓN A LA ORGANIZACIÓN + CAUSA ESPECIFICA + AFECTACIÓN	TIPO DE RIESGO	AMENAZAS	CONSECUENCIAS NEGATIVAS	CONSECUENCIAS POSITIVAS	REGIONALES O PROCESOS AFECTADOS	DESCRIPCIÓN DE LOS CONTROLES ACTUALES	PROBABILIDAD	IMPACTO	NIVEL		
R1	Gestión de la Tecnología e Información	- FINANCIEROS: Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada. - TECNOLOGÍA: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información. - COMUNICACIÓN INTERNA: Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.	- ECONÓMICOS: Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia. - COMUNICACIÓN EXTERNA: Mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad.	2	- Información Digital	Perdida de informacion institucional, debido al uso de dispositivos moviles personales en las funciones afectando Confidencialidad, Integridad , Disponibilidad del proceso.	Riesgos de Tecnologia	Carencia de recursos tecnológicos	- Pérdidas Financieras - Pérdida de Credibilidad - Incumplimientos legales - Sanciones	- No hay consecuencias positivas identificadas.	- TOLIMA	CONTROL: Copias de seguridad y entrega de informacion al finalizar vinculacion RESPONSABLE: Coordinadores Áreas FRECUENCIA: Anual TIPO DE CONTROL: Preventivo NATURALEZA DEL CONTROL: Manual CONTROL DOCUMENTADO: SÍ CALIFICACIÓN DEL CONTROL: ADECUADO	MODERADO	MODERADO - Afectación Imagen del proceso o área a Nivel de la Entidad. - Sanciones a nivel de Oficina Jurídica o Control Interno. - Llamados de atención a nivel Organizacional.	ALTA IMPORTANTE	Reducir el Riesgo	A.5.1. Orientación de la Dirección para la Gestión de la Seguridad de la Información. - A.5.1.1. Políticas para la Seguridad de la Información. - A.5.1.2. Revisión de las Políticas para seguridad de la información.
R2	Gestión de la Tecnología e Información	- FINANCIEROS: Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada. - TECNOLOGÍA: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.	- ECONÓMICOS: Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia. - TECNOLÓGICOS: Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.	1	- Información Digital - Hardware - Software	Ataque informato o afectacion por virus por acceso a la red cableada o WiFi no autorizado , debido a Equipos personales en la red corporativa, puntos de red desatendidos. afectando Confidencialidad, Integridad , Disponibilidad y Continuidad del proceso.	Riesgos de Tecnologia	- Estructura Obsoleta y/o Inadecuada Carencia de recursos tecnológicos - Ataque Informático	- Pérdidas Financieras - Pérdida de Credibilidad - Incumplimientos legales - Daños a la insfraestructura Física - Sanciones - Interrupción de la Operación o del Servicio - Daños a la insfraestructura Tecnológica	- No hay consecuencias positivas identificadas.	- TOLIMA	CONTROL: Restringir permisos de administrador RESPONSABLE: Subdirectores de Área FRECUENCIA: Diaria TIPO DE CONTROL: Preventivo NATURALEZA DEL CONTROL: Automático CONTROL DOCUMENTADO: SÍ CALIFICACIÓN DEL CONTROL: ADECUADO CONTROL: Manejo de Contraseñas para las redes WiFI RESPONSABLE: Subdirectores de Área FRECUENCIA: Diaria TIPO DE CONTROL: Preventivo NATURALEZA DEL CONTROL: Automático CONTROL DOCUMENTADO: SÍ CALIFICACIÓN DEL CONTROL: ADECUADO	MODERADO	MODERADO - Afectación Imagen del proceso o área a Nivel de la Entidad. - Sanciones a nivel de Oficina Jurídica o Control Interno. - Llamados de atención a nivel Organizacional.	ALTA IMPORTANTE	Reducir el Riesgo	A.5.1. Orientación de la Dirección para la Gestión de la Seguridad de la Información. - A.5.1.1. Políticas para la Seguridad de la Información. - A.5.1.2. Revisión de las Políticas para seguridad de la información. A.13.1. Gestión de la Seguridad de las Redes. - A.13.1.1. Controles de redes. - A.13.1.2. Seguridad de los servicios de red. - A.13.1.3. Separación en las redes. A.13.2. Transferencia de información. - A.13.2.2. Acuerdos sobre transferencia de información. - A.13.2.4. Acuerdos de confidencialidad o de no divulgación.
R3	Gestión de la Tecnología e Información	- FINANCIEROS: Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada. - TECNOLOGÍA: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información. - ESTRATÉGICOS: Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo. - COMUNICACIÓN INTERNA: Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.	- POLÍTICOS: Cambios de gobierno, legislación, políticas públicas, regulación. - TECNOLÓGICOS: Avances en tecnología, acceso a sistemas de información externos, gobierno en línea. - COMUNICACIÓN EXTERNA: Mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad.	3	- Información Digital	Divulgacion de informacion Confidencial, clasificada o reservada para el instituto, debido a Perdida o mal manejo de dispositivo personal en funciones de ICBF afectando Confidencialidad e Integridad del proceso.	Riesgos de Tecnologia	- - Falta de actividades de sensibilización - Falta de claridad en la asignación de roles y responsabilidades - Sabotajes Internos y Externos - Personal mal intencionado	- Pérdidas Financieras - Pérdida de Credibilidad - Incumplimientos legales - Sanciones	- No hay consecuencias positivas identificadas.	- TOLIMA	CONTROL: Verificacion de equipos portatiles personales RESPONSABLE: Profesional Especializado FRECUENCIA: Cuando ocurra TIPO DE CONTROL: Preventivo NATURALEZA DEL CONTROL: Manual CONTROL DOCUMENTADO: SÍ CALIFICACIÓN DEL CONTROL: ADECUADO	IMPROBABLE	LIGERAMENTE DAÑIÑO - Pérdidas Económicas menores a 500 SMLV. - Afectación Imagen grupo a nivel área o proceso. - Sanciones a nivel grupo. - Llamados de atención a nivel grupo.	MODERADO	Reducir el Riesgo	A.7.1. Antes de asumir el empleo. - A.7.1.2. Términos y condiciones del empleo. A.7.2. Durante la ejecución del empleo. - A.7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información.
R4	Gestión de la Tecnología e Información	- TECNOLOGÍA: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información. - COMUNICACIÓN INTERNA: Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.	- TECNOLÓGICOS: Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.	4	- Servicio - Hardware	Saturacion de la Red WAN y LAN por programas como P2P, Proxy, servicios de streaming o gestores de descarga., debido a Equipos personaes con herramientas instaladas y no permitidas en ICBF afectando Disponibilidad y Continuidad del proceso.	Riesgos de Continuidad	- Desconocimiento del proceso, actividad o procedimiento - Negligencia de los funcionarios, colaboradores y/o contratistas - Inadecuado soporte tecnológico	- Interrupción de la Operación o del Servicio - Daños a la insfraestructura Tecnológica	- No hay consecuencias positivas identificadas.	- TOLIMA	CONTROL: Verificacion del equipo al realizar la primera conexion a la red de ICBF RESPONSABLE: Profesional Especializado FRECUENCIA: Cuando ocurra TIPO DE CONTROL: Detectivo NATURALEZA DEL CONTROL: Manual CONTROL DOCUMENTADO: SÍ CALIFICACIÓN DEL CONTROL: SUSCEPTIBLE A MEJORAR	IMPROBABLE	LIGERAMENTE DAÑIÑO - Pérdidas Económicas menores a 500 SMLV. - Afectación Imagen grupo a nivel área o proceso. - Daños insignificantes de la infraestructura de la entidad.	MODERADO	Asumir o Aceptar el Riesgo	A.5.1. Orientación de la Dirección para la Gestión de la Seguridad de la Información. - A.5.1.2. Revisión de las Políticas para seguridad de la información. A.9.1. Requisitos del Negocio para Control de Acceso. - A.9.1.2. Acceso a redes y a servicios en red. A.16.1. Gestión de incidentes y mejoras en la seguridad de la información. - A.16.1.3. Reporte de debilidades de seguridad de la información. - A.16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información.
R5	Gestión de la Tecnología e Información	- TECNOLOGÍA: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información. - COMUNICACIÓN INTERNA: Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.	- TECNOLÓGICOS: Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.	5	- Información Digital - Servicio	Dispositivos desactualizados, rooteados o con software ilegal, debido a Equipos moviles como telefonos inteligentes desactualizados o roteados o portatiles con sistema operativo sin licenciar con activaciones piratas. afectando Integridad y Disponibilidad del proceso.	Riesgos de Tecnologia	Inadecuada asignación de recursos tecnológicos - Desconocimiento del proceso, actividad o procedimiento - Negligencia de los funcionarios, colaboradores y/o contratistas - Fallas en la plataforma tecnológica	- Interrupción de la Operación o del Servicio - Daños a la insfraestructura Tecnológica		- TOLIMA	CONTROL: Verificacion de equipo portatil al primer ingreso a la red institucional RESPONSABLE: Profesional Especializado FRECUENCIA: Cuando ocurra TIPO DE CONTROL: Preventivo NATURALEZA DEL CONTROL: Manual CONTROL DOCUMENTADO: SÍ CALIFICACIÓN DEL CONTROL: ADECUADO	RARO	MENOR - Pérdidas Económicas entre 501 a 1000 SMLV. - Afectación Imagen grupo o área a nivel del Macro proceso - Daños pequeños de la infraestructura de la entidad	MENOR	Reducir el Riesgo	A.5.1. Orientación de la Dirección para la Gestión de la Seguridad de la Información. - A.5.1.2. Revisión de las Políticas para seguridad de la información. A.13.1. Gestión de la Seguridad de las Redes. - A.13.1.2. Seguridad de los servicios de red. - A.13.1.3. Separación en las redes.

Fuente: los autores. (Adaptada de https://www.icbf.gov.co/el-instituto/sistema-integrado-de-gestion/formato-matriz-riesgos-sgsi-v3)

6.2 ASPECTOS DEL BYOD EN EL ICBF

El ICBF en la actualidad se encuentra implementando un SGSI (Sistema de Seguridad en la Información), en el cual su sede principal denominada Sede de la Dirección General, ya se encuentra certificada por el ICONTEC en la Norma ISO 27001 2013 para el proceso de Gestión Tecnología. Obtenido este logro la siguiente apuesta es sostener la certificación y hacerla extensiva a las 33 Regionales, mediante procesos de maduración y sensibilización al personal de todas las Regionales.

Dentro de la política actual de seguridad Resolución 9364 de septiembre del año 2016, se hace alusión al tema de los equipos personales sobre el uso de la red de ICBF en los mismos, en su ARTICULO OCTAVO Numeral C.

Todo Acceso a la red de la entidad mediante elementos o recursos tecnológicos no institucionales deberá ser informado, autorizado y controlado por la dirección de información y tecnología DIT a través de la subdirección de recursos tecnológicos SRT.

Dado lo anterior se puede decir que para alguien poder usar su equipo portátil o Tablet en la Red interna de ICBF, solo se debe dirigir por uno de los canales autorizados (Teléfono, Correo o módulo de autogestión) a la mesa de soluciones informáticas y solicitar un caso para revisión y conexión de su equipo a la red interna.

Una vez solicitado el personal de TI deberá revisar dos cosas en el equipo:

- Que el sistema operativo este licenciado.
- Que cuente con un antivirus activado y actualizado.

Estos dos requisitos, a pesar de ser importantes dejan algunos vacíos en sí mismos, pues al verificar el equipo, como se puede saber si en verdad es un sistema operativo licenciado y no fue activado con algún activador pirata, que como es sabido a pesar de funcionar, la mayoría de los activadores traen código malicioso en su interior generando un riesgo mayor para la organización.

Si se cumple con los 2 requisitos mencionados el equipo se puede unir a la red de ICBF y se obtiene navegación y acceso a los aplicativos requeridos desde la máquina.

Y a partir de este momento la responsabilidad de la información que se tenga en el equipo será responsabilidad del usuario únicamente.

6.3 APLICACIÓN DE ENCUESTAS

Se aplica encuestas a los colaboradores del ICBF para evaluar según su tipo de usuario como perciben la incorporación del BYOD en sus labores diarias. Para ello se dividen dos grupos, uno de usuarios generales y otro de responsables de las áreas de TI.

6.3.1 Encuesta Profesionales de TI ICBF a Nivel Nacional

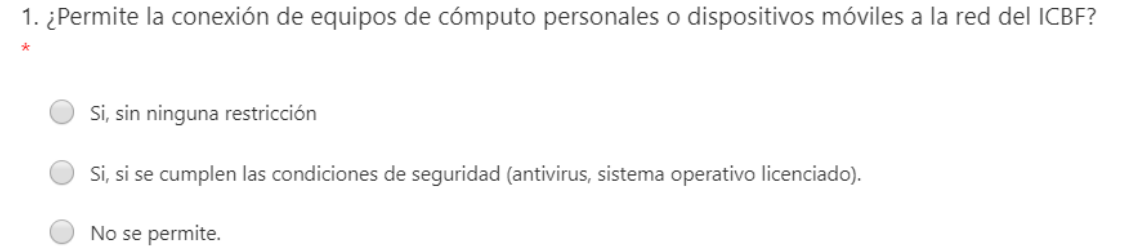
A pesar de existir la claridad en la Política de Seguridad, el tema del BYOD aún no está muy claro para el personal de TI (Tecnologías de Información) ni para los colaboradores de ICBF, que son quienes están usando sus equipos en actividades laborales y contractuales, algunos por necesidad y otros por gusto propio. Por ello con el fin de obtener una percepción de ambos (Profesionales de TI y Usuarios) se elaboró una encuesta para cada uno de los actores con el fin de obtener un acercamiento a la realidad del BYOD en el ICBF Regional Tolima.

Como se mencionó dentro de la estructura organizacional del ICBF, el mismo cuenta con 33 Regionales y en cada una de ellas existe personal liderando el proceso de Gestión Tecnológica. Para el presente año 77 profesionales en TI distribuidos en todo el país, realizan todas las actividades de soporte en la regionales, además de encargarse de la administración e implementación del SGSI.

Por ello y con el fin de obtener algunos datos sobre el BYOD en el ICBF, se solicitó a una muestra del 20% de los Ingenieros Regionales (15) el diligenciamiento de una encuesta que permitiera obtener datos importantes sobre el criterio de cada uno en sus Regionales.

La encuesta conto con 4 preguntas y se realizó en línea tomando las primeras 15 respuestas.

Figura 12. Participación pregunta 1 Profesionales TI ICBF

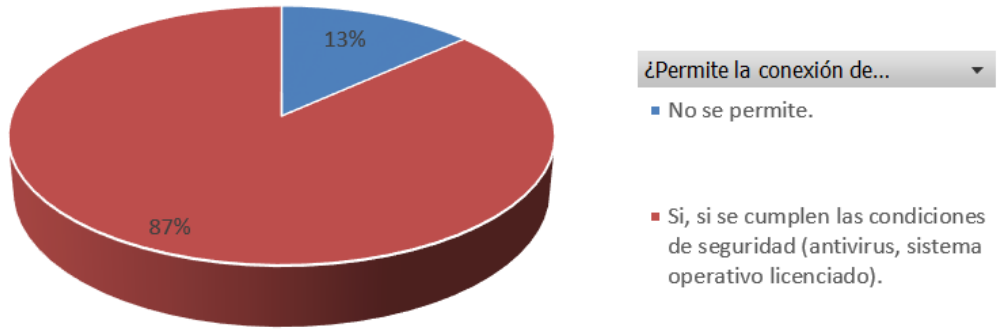


¿Permite la conexión de equipos de cómputo personales o dispositivos móviles a la red del ICBF?	Total
No se permite.	2
Si, si se cumplen las condiciones de seguridad (antivirus, sistema operativo licenciado).	13
Total general	**15**

Fuente: los autores.

Este resultado evidencio que el 87% de Ingenieros está permitiendo el uso de equipos personales en ICBF bajo algunas condiciones y que el 13 % no lo permite. Lo importante de este análisis, es que una tercera opción era la de “Si lo permite sin ninguna restricción” y esta respuesta se quedó con el 0% de las respuestas. Estos resultados muestran una conciencia importante por parte del personal de TI en la necesidad de aplicar controles y políticas sobre el uso de equipos personales dentro de la red del ICBF en cada una de sus regionales.

Figura 13. Grafico pregunta 1 para profesionales de TI.



Fuente: los autores.

Figura 14. Participación pregunta 2 Profesionales TI ICBF

2. ¿Cuál cree que sea el mayor riesgo de conectar equipos personales a la red del ICBF? *

- Acceso no autorizado a la información o modificación de la misma
- Ataques informáticos contra la infraestructura del ICBF
- Riesgo por virus o software instalado en la máquina que sature la red.
- Posible pérdida o divulgación de información institucional en caso de pérdida del dispositivo.

¿Cuál cree que sea el mayor riesgo de conectar equipos personales a la red del ICBF?	Total
Acceso no autorizado a la información o modificación de la misma	3
Ataques informáticos contra la infraestructura del ICBF	1
Posible pérdida o divulgación de información institucional en caso de pérdida del dispositivo.	4
Riesgo por virus o software instalado en la máquina que sature la red.	7
Total general	**15**

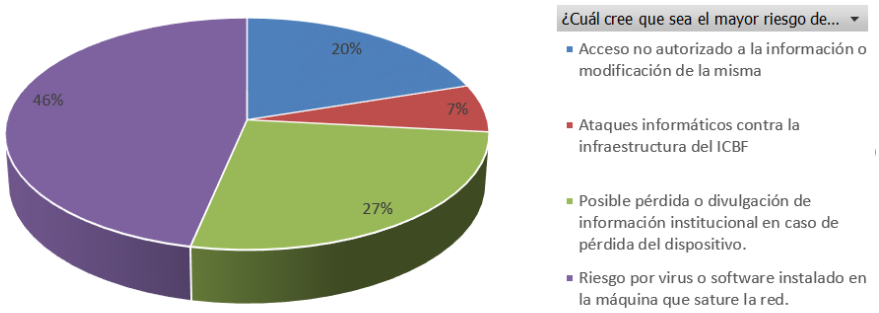
Fuente: los autores.

Para esta pregunta se evidencio que la principal preocupación del personal de TI en el uso de equipos personales dentro de la red de ICBF es con un 46% el riesgo por virus que tengan los equipos o algún software de pueda introducir tráfico de red no deseado como P2P o escáneres de red. La segunda preocupación con un 27% tiene que ver con la pérdida o divulgación de la información institucional que contengan los dispositivos en caso de pérdida de este. Con un 20% la tercera preocupación es

un acceso abusivo a la información de ICBF y por último con un 7% algún ataque informático contra infraestructura del ICBF.

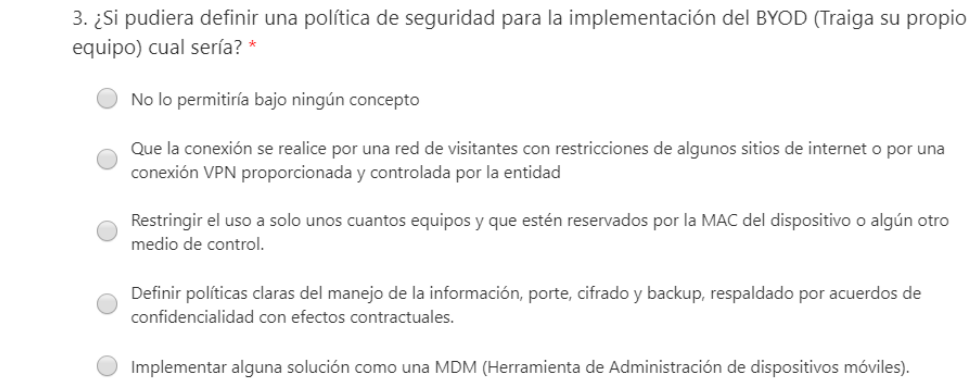
Estos resultados son contundentes al mostrar una preocupación alta por parte de los profesionales de TI en algunas vulnerabilidades que pueden ser explotadas por parte de un usuario desprevenido o un posible atacante interno y atentar contra la seguridad informática de la entidad.

Figura 15. Grafico pregunta 2 para profesionales de TI



Fuente: los autores.

Figura 16. Participación pregunta 3 Profesionales TI ICBF



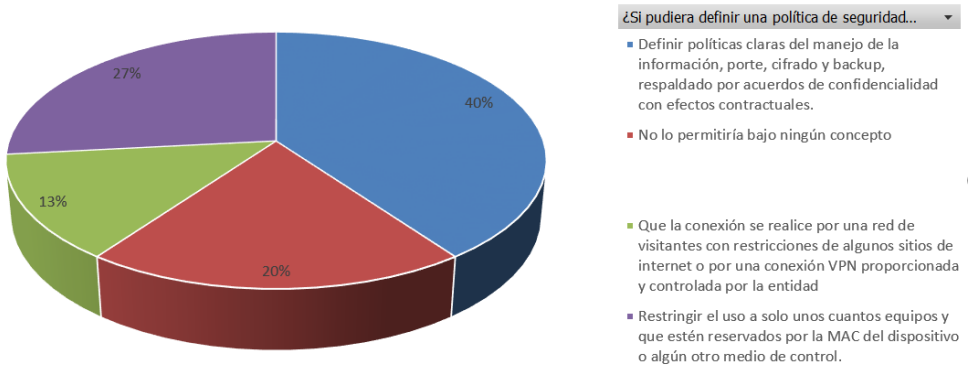
¿Si pudiera definir una política de seguridad para la implementación del BYOD (Traiga su propio equipo) cual sería?	Total
Definir políticas claras del manejo de la información, porte, cifrado y backup, respaldado por acuerdos de confidencialidad con efectos contractuales.	6
No lo permitiría bajo ningún concepto	3
Que la conexión se realice por una red de visitantes con restricciones de algunos sitios de internet o por una conexión VPN proporcionada y controlada	2
Restringir el uso a solo unos cuantos equipos y que estén reservados por la MAC del dispositivo o algún otro medio de control.	4
Total general	**15**

Fuente: los autores.

Para esta pregunta se observa que la alternativa más aceptada para implementar el BYOD en el ICBF con un 40% es la de definir políticas claras del manejo de la información, que incluyan porte cifrado y backup de la información, soportado con acuerdos de confidencialidad con efectos contractuales.

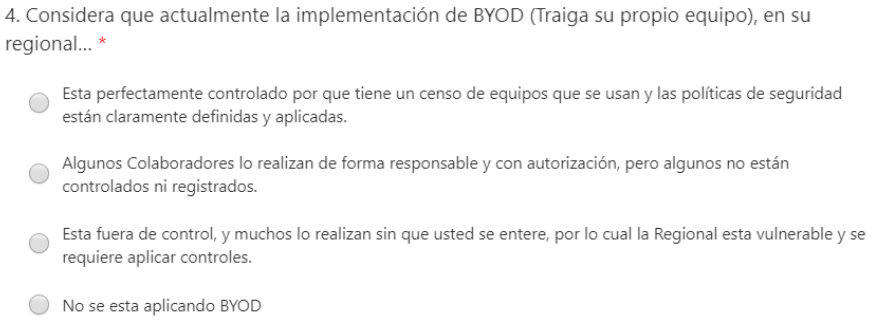
La segunda opción con el 27% de los encuestados es limitar el uso de dispositivos personales solo a unos pocos y que estén controlados por algún método como la reserva de la dirección MAC. En la tercera opción con el 20% de las respuestas se inclina por no permitir bajo ningún concepto el uso de dispositivos personales, lo que supone la premisa de restringir todo es mejor por seguridad y por último el 13% se inclina por medidas de seguridad tecnológicas fuertes como el uso de un portal cautivo, redes de visitantes o uso de VPN para permitir el ingreso de equipos personales a la red institucional.

Figura 17. Grafico pregunta 3 para profesionales de TI.



Fuente: los autores.

Figura 18. Participación pregunta 4 Profesionales TI ICBF



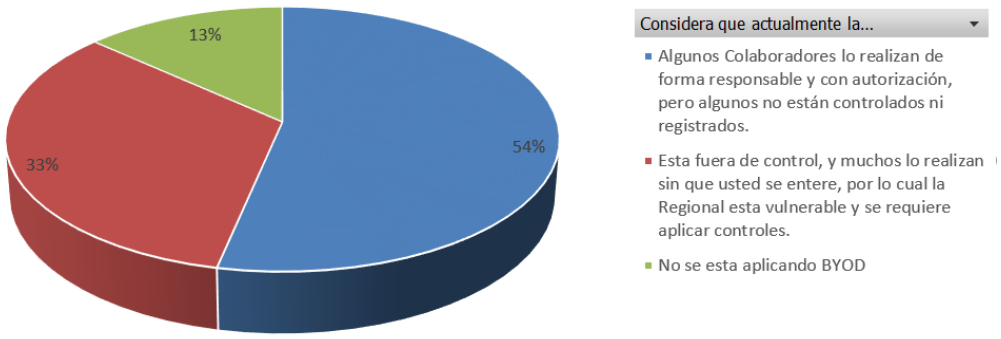
Considera que actualmente la implementación de BYOD (Traiga su propio equipo), en su regional...	Total
Algunos Colaboradores lo realizan de forma responsable y con autorización, pero algunos no están controlados ni registrados.	8
Esta fuera de control, y muchos lo realizan sin que usted se entere, por lo cual la Regional esta vulnerable y se requiere aplicar controles.	5
No se esta aplicando BYOD	2
Total general	**15**

Fuente: los autores.

Respecto a la aplicación del BYOD actualmente en el ICBF el Personal de TI considera con un 54% que la mayoría de los colaboradores que usan sus equipos personales lo están haciendo de forma responsable y siempre consultando al área de sistemas, sin embargo, algunos no están registrados ni controlados.

Por el contrario, el 33% opina que es un tema que esta fuera de control y se requiere tomar medidas de manera urgente, lo cual es un indicador importante, pues a pesar de no ser la mayoría si es una muestra importante que está indicando que el riesgo actual está latente. Por último, el 13% no está implementando el BYOD en su regional según datos de la encuesta.

Figura 19. Grafico pregunta 4 para profesionales de TI.



Fuente: los autores.

Queda claro que a pesar de no estar regulado aun el BYOD en el ICBF el personal de TI entiende la nueva tendencia y está dispuesto a tomar acciones que permitan el uso responsable de equipos personales para las labores institucionales salvaguardando la información e infraestructura, generando que esta tendencia sea un apoyo para la eficiencia de los objetivos institucionales y no una dificultad de seguridad.

La encuesta Online se encuentra en:
https://forms.office.com/Pages/ResponsePage.aspx?id=86WSPXq8eU-qMXl5IP3eJvz-sb_kqTe9Dr2WP4cRU_wtUMEhBUVROSkk4N0wwQVA0NEV-KMjVXUVM5MC4u

6.3.2 Encuesta Colaboradores ICBF Regional Tolima

La segunda encuesta que se realizó con el fin de obtener información importante sobre la aplicación del BYOD en el ICBF Regional Tolima, la población objeto fueron los trabajadores de la institución, tomando una muestra del 7% de la totalidad del personal. La idea de esta es obtener datos importantes que permitieran dar un indicio del uso de equipos personales en actividades laborales.

La encuesta se realizó en línea a 30 colaboradores y conto con 30 respuestas.

Figura 20. Participación pregunta 1 Colaboradores ICBF

1. Cuando va a usar su dispositivo personal en el ICBF ud: *
cualquier dispositivo, así sea solo para Correo Electrónico.

- Lo realiza cuando lo requiere con una conexión física o una clave de WiFi que conoce?
- Consulta Al área de Tecnología si es viable?
- Nunca los conecta a la Red Interna de ICBF
- No usa Dispositivos personales para el trabajo

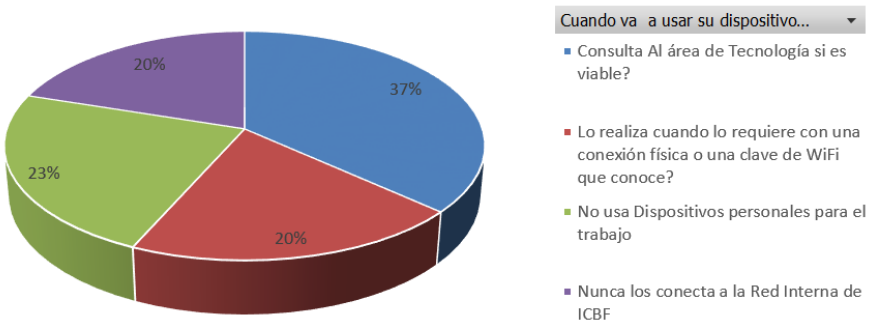
Cuando va a usar su dispositivo personal en el ICBF ud:	Total
Consulta Al área de Tecnología si es viable?	11
Lo realiza cuando lo requiere con una conexión física o una clave de WiFi que conoce?	6
No usa Dispositivos personales para el trabajo	7
Nunca los conecta a la Red Interna de ICBF	6
Total general	**30**

Fuente: los autores.

Sobre el uso de equipos personales en el ICBF, se puede evidenciar en la encuesta que el 37% de las personas que usan equipos personales en su trabajo consultan al personal de TI antes de usarlos, lo cual indica un buen grado de aceptación de la política de seguridad del ICBF resolución 9364 articulo 8 numeral c que se mencionó anteriormente. También se encontró que el 23% manifiesta no usar dispositivos personales en el trabajo y el 20% dice nunca conectarlos a la red del ICBF, lo cual representa el 43% de la encuesta de da un parte de tranquilidad al área de TI.

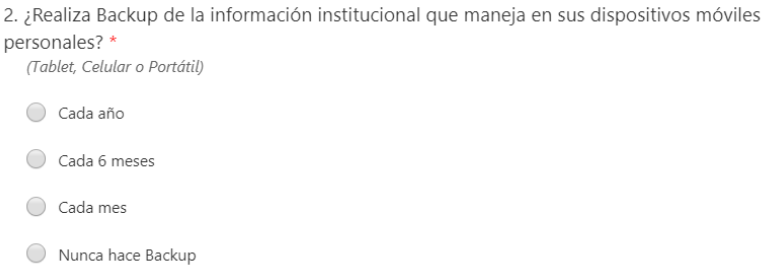
La parte que podría preocupar de esta pregunta es el 20% que asegura que conecta los equipos personales directamente a la red cableada del ICBF cuando lo requiere o que usa una contraseña de Wifi que conoce, este porcentaje es el que representa una vulnerabilidad para el ICBF dado que no está controlado por la entidad.

Figura 21. Grafico pregunta 1 Colaboradores ICBF.



Fuente: los autores.

Figura 22. Participación pregunta 2 Colaboradores ICBF



¿Realiza Backup de la información institucional que maneja en sus dispositivos móviles personales?	Total
Cada 6 meses	4
Cada año	13
Cada mes	3
Nunca hace Backup	10
Total general	**30**

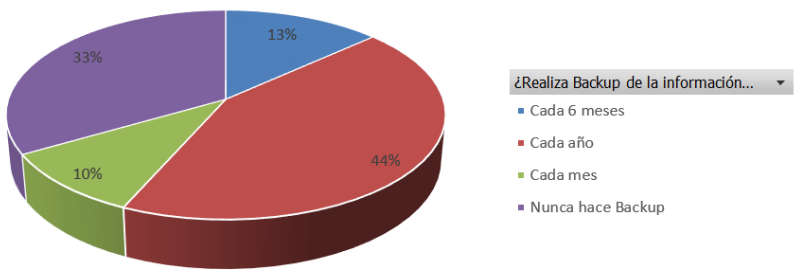
Fuente: los autores.

En la segunda pregunta, se hace referencia al tema del Backup o copia de seguridad, pues en la encuesta realizada al personal de TI fue uno de los temas de más preocupación y la política de seguridad resolución 9364 aclara tajantemente que la copia de seguridad es responsabilidad de cada uno de los colaboradores.

En este ítem se pudo observar que el 67% de las personas encuestadas realiza copia de seguridad, solo varia la periodicidad 44% cada año, 13% cada 6 meses y 10% cada mes. El inconveniente estaría con ese 13% que manifiesta nunca realizar copia de seguridad, pues al ocurrir algún incidente con su dispositivo personal tal como perdida o daño existiría un alto riesgo de pérdida o filtración de información institucional.

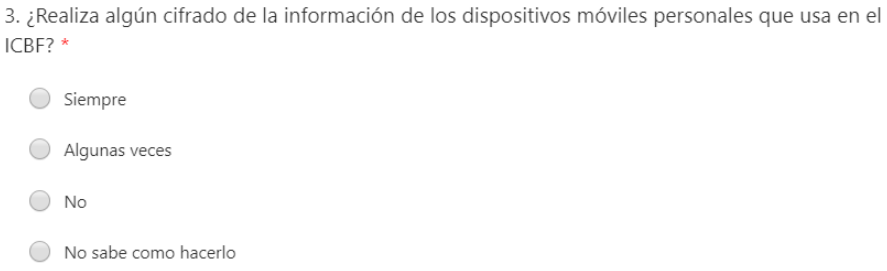
Cabe resaltar que dentro de las opciones que cuentan los colaboradores para sus copias de seguridad están servicios de nube debidamente licenciadas y respaldadas como OneDrive de Office 365 y servidores de archivos propios de ICBF NAS (Network Access Server), por lo que queda evidenciado que se cuenta con los medios para cumplir con la resolución 9364 a cabalidad en su numeral Octavo C.

Figura 23. Grafico pregunta 2 Colaboradores ICBF.



Fuente: los autores.

Figura 24. Participación pregunta 3 Colaboradores ICBF

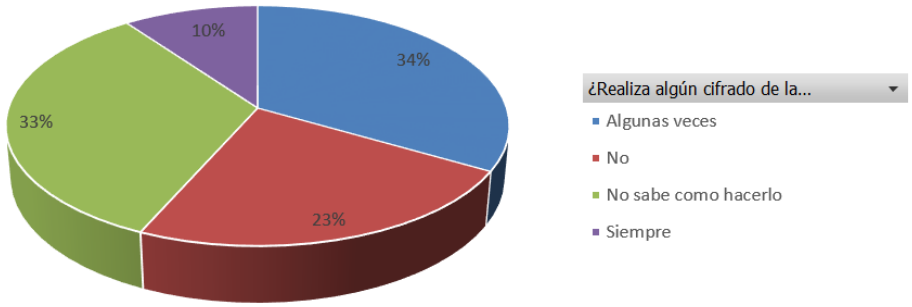


¿Realiza algún cifrado de la información de los dispositivos móviles personales que usa en el ICBF?	Total
Algunas veces	10
No	7
No sabe como hacerlo	10
Siempre	3
Total general	**30**

Fuente: los autores.

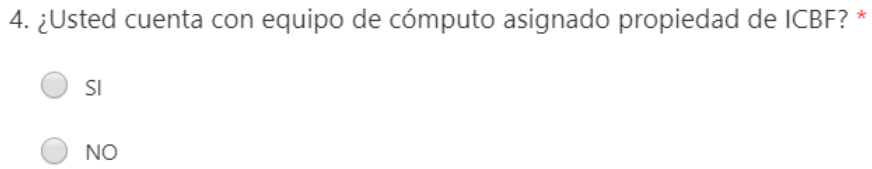
La tercera pregunta de la encuesta hace referencia si las personas que usan equipos personales o memorias USB, realizan algún cifrado de la información, lo anterior dado que como estrategia de seguridad en el ICBF se promueve el uso de la herramienta BitLocker para cifrar la información de medios extraíbles con el fin de evitar fuga de información en caso de pérdida del dispositivo, lo cual arrojo una situación desfavorable en este Ítem de seguridad, pues solo el 10% de los encuestados realiza el cifrado siempre, el 34% algunas veces, el 33% dice no saber cómo se hace a pesar de las constantes capacitaciones y envíos de manuales que se han realizado de la herramienta BitLocker y el 23% simplemente no lo realiza, por lo que queda demostrado que se debe trabajar más en el uso de dicha herramienta y aplicar adicionalmente controles con dispositivos como celulares donde se tenga configurado el correo institucional para que cuente con clave o patrón de seguridad, o si es un equipo personal para que el mismo cuente con una clave de inicio al no poder estar en el dominio icbf.gov.co

Figura 25. Grafico pregunta 3 Colaboradores ICBF.



Fuente: los autores.

Figura 26. Participación pregunta 4 Colaboradores ICBF

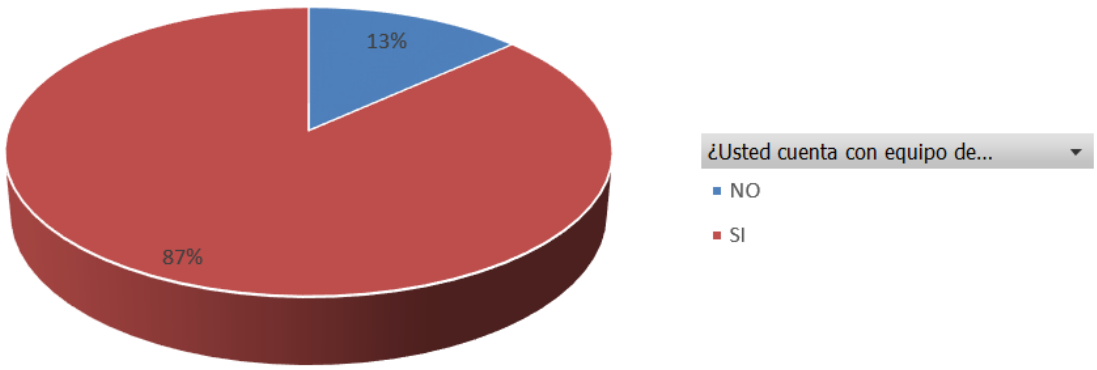


¿Usted cuenta con equipo de cómputo asignado propiedad de ICBF?	Total
NO	4
SI	26
Total general	**30**

Fuente: los autores.

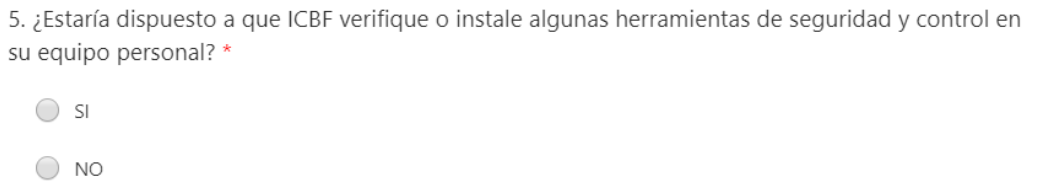
La cuarta pregunta simplemente revela la cantidad de los trabajadores encuestados que no cuentan con la herramienta de trabajo (computador) proporcionado por la entidad que es del 13% frente a un 87% que, si cuenta con ella, ese 13% es el que en ocasiones se ve en la necesidad de llevar su equipo de cómputo personal al ICBF, para poder realizar su trabajo.

Figura 27. Grafico pregunta 4 Colaboradores ICBF.



Fuente: los autores.

Figura 28. Participación pregunta 5 Colaboradores ICBF

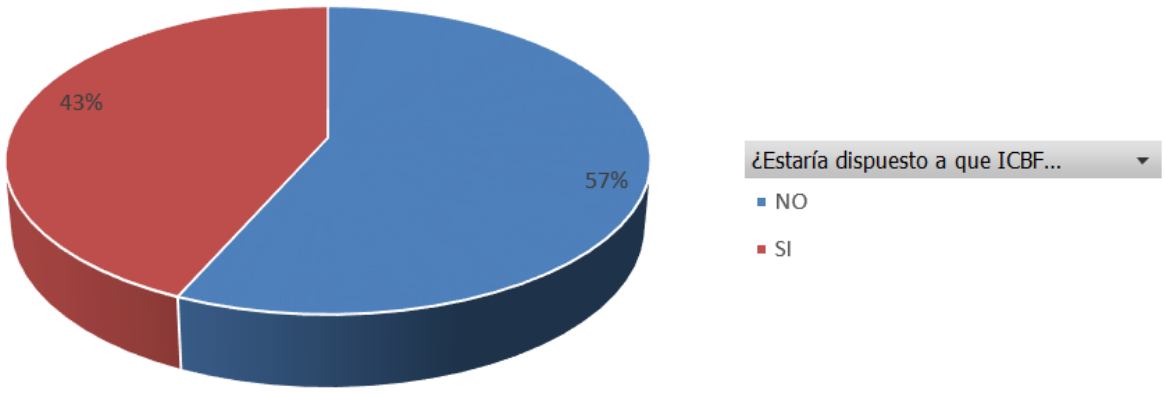


¿Estaría dispuesto a que ICBF instale algunas herramientas de seguridad y control en su equipo persona	Total
NO	17
SI	13
Total general	**30**

Fuente: los autores.

La última pregunta hace referencia a si los trabajadores de ICBF Regional Tolima, estarían dispuestos a que la entidad por medio de una herramienta como un MDM (Mobile Device Management) o cualquier otro tipo de monitoreo realice validaciones sobre el uso de sus equipos personales, donde el 57% está en desacuerdo y el 43% está de acuerdo, resultado que supone una resistencia de más de la mitad de los trabajadores para que sus equipos personales puedan ser monitoreados.

Figura 29. Grafico pregunta 5 Colaboradores ICBF.



Fuente: los autores.

7. CAPITULO III - RECOMENDACIONES PARA APLICAR BYOD EN EL ICBF REGIONAL TOLIMA

A pesar de todos los cuestionamientos que se realizan al BYOD por temas de seguridad, esta tendencia continuará creciendo en el mundo, pues es inherente al avance de la tecnología y la movilidad, por lo que es una oportunidad de mejorar la gestión de los procesos de ICBF soportados en TI.

Es por ello que el BYOD en el ICBF, debe verse como una oportunidad para mejorar la gestión que realiza la entidad, no solo en la Regional Tolima si no en todo el país, pues cada regional tiene en términos generales la misma situación a nivel de falta de equipos para todos sus colaboradores, incluso algunas actividades de la parte de supervisión o misional de la entidad son más practicas usando dispositivos móviles.

¿Entonces qué se debe hacer en el ICBF para poder implementar el BYOD?, a continuación, se describen algunas recomendaciones para la implementación del BYOD.

7.1 POLÍTICA DE SEGURIDAD

Dada la situación actual de la entidad, lo primero que se debe hacer es revisar la política de seguridad (Resolución 9364 de 2016), ya que a pesar de estar muy bien estructurada y abarca todos los de temas del SGSI y el uso de los recursos tecnológicos, aun no regula el uso de dispositivos móviles en el ICBF, por lo que un buen comienzo es definir responsabilidades por parte de los colaboradores de ICBF con los dispositivos móviles que usa en el trabajo, acompañadas de acuerdos de confidencialidad que ya existen pero carecen de sanciones pecuniaria o administrativas lo cual dejaría reglas claras para el manejo de la información institucional.

Dentro de los proyectos integrales de ICBF el SGSI debe ir alineado a una Arquitectura empresarial por lineamiento de MINTIC, lo cual es una gran oportunidad de alinear política de SGSI, BYOD y objetivos del Negocio.

7.2 PLAN DE SENSIBILIZACIÓN

Dentro del plan de trabajo anual del Personal de TI del ICBF existen indicadores que miden el estado de las sensibilizaciones en SGSI a los colaboradores, lo cual se ha convertido en una fortaleza de la entidad, generando una conciencia sobre todos los temas de seguridad de la información.

Estas sensibilizaciones se deben focalizar y hacer que lleguen a todas las personas, pues generalmente a las capacitaciones terminan asistiendo las mismas personas de siempre y algunos nunca asisten por falta de tiempo o falta de empatía hacia temas tecnológicos, por lo que un nuevo plan debe incluir cantidad de horas por funcionario que garanticen su asistencia, sea personal o virtual y ser requisito para calificación de desempeño o continuidad del contrato según la vinculación de cada uno.

Algunas estrategias como el acompañamiento de MINTIC y el material de apoyo brindado en gobierno digital o arquitectura empresarial, pueden ser fundamentales a la hora de involucrar a todas las personas de la entidad en el uso de un BYOD responsable.

7.3 DEFINIR MEDIDAS DE SEGURIDAD PARA LOS DISPOSITIVOS MÓVILES

Cada colaborador que use su equipo personal en cualquier actividad institucional debe cumplir con algunos mínimos requisitos de seguridad, algunos elementos pueden ser básicos y no implicarían grandes costos ni desarrollos; por ejemplo, en el caso de los colaboradores que usan con su cuenta de correo y chat institucional en el celular, deberían por lo menos tener un patrón de seguridad o clave para poder acceder a su dispositivo o si es un portátil personal que no está en dominio debería tener una cuenta local con una clave alfanumérica de más de 8 caracteres, estas simples medidas darían una grado más de seguridad en caso de pérdida, descuido o robo del equipo.

Pero si lo que se pretende es tener una solución robusta que permita la administración de los dispositivos móviles usados en la entidad, se debería pensar en la implementación de una MDM (Mobile Device Manager), para lo cual existen muchas opciones en el mercado y algunas de ellas son open source y solo se debería incurrir en los costos de implementación, además son modulares y se pueden usar independiente mente de la plataforma (IOS, Android, BlackBerry o Windows).

Estas soluciones cuentan con control de aplicaciones permitiendo desplegar las instalaciones de forma centralizada y controlando aquellas que son necesarias, además se puede restringir instalaciones y manipulación por parte del usuario.

Otra de las bondades de esos sistemas es poder administrar perfiles por dispositivo para realizar configuración de perfiles de correo, calendario, contactos, accesos de VPN, lo que podría ser útil a la hora de retirar fácilmente los privilegios en casos de pérdida o robo. Adicionalmente se tendría la opción de protección de los datos mediante cifrado del dispositivo o un borrado seguro en caso de requerirse.

Una alternativa importante para aplicar en ICBF y más teniendo en cuenta que ya tiene algunas soluciones de este fabricante (FORTINET), sería evaluar su:

Estrategia integral de seguridad BYOD de Fortinet, que está diseñada para proteger a las organizaciones mediante la autenticación de dispositivos, el control del comportamiento de los usuarios en la red y la restricción de los derechos de acceso a datos se construye alrededor de una combinación de seis capacidades diferenciadoras clave:

- Una amplia gama de opciones de despliegue de alto desempeño que soportan la conectividad LAN y WAN y se centran en torno a la familia de appliances FortiGate.
- La falta de licenciamiento "por usuario" o "por asiento" significa que los clientes pueden agregar nuevos dispositivos a su red sin incurrir en cargos adicionales de licencia. Esta característica es crítica ya que el número de dispositivos conectados a la red pueden duplicarse o incluso triplicarse debido a que los usuarios traen sus teléfonos inteligentes y tabletas para trabajar.
- Una consola de administración consolidada y centralizada
- Controladores inalámbricos integrados en todos los appliances FortiGate para una mejor visibilidad y control de aplicaciones y de usuarios, detección de puntos de acceso no autorizados, acceso para invitados y administración del ancho de banda.
- Capacidad Wi-Fi incorporada para asegurar las implementaciones de redes LAN en ciertos modelos FortiGate, con lo cual se reduce la necesidad de un punto de acceso inalámbrico separado
- Clientes VPN móviles y soft-tokens interoperables para autenticación de doble factor
- Independientemente de la alternativa o fabricante de la solución, un MDM se postula como una gran ayuda para disminuir brechas de seguridad en la implementación del BYOD.[55]

Estas soluciones permiten que se realice un monitoreo y tener estadísticas sobre los dispositivos móviles lo cual es un gran alivio para la seguridad y el personal de TI, pero se debe tener en cuenta hasta donde se podría llagar ya que al ser los equipos de los trabajadores se debe llegar a consensos, ya que como se pudo ver en la encuesta realizada el 57% de los trabajadores de ICBF no estaría dispuesto a que se realizara algún tipo de monitoreo en su equipo.

7.4 PROCEDIMIENTO PARA CONECTAR EQUIPO A LA RED DE ICBF

Como se mencionó anteriormente, para poder usar equipos personales en el ICBF basta con verificar una lista de chequeo donde solo se mira si el equipo cuenta con sistema operativo licenciado y un antivirus actualizado, pero en realidad no se verifica si esta activación es legal o se realizó por medio de un activador pirata.

[55] Securitic.com.mx. (2012). SecuriTIC. [En Línea] Disponible en http://securitic.com.mx/noticias/210-fortinet-amplia-y-mejora-su-solucion-de-seguridad-de-redes-para-byod

Para poder dar solución a esta vulnerabilidad se podría optar por usar algún programa como Volume Activation Management Tool, que es una herramienta gratuita de Microsoft que permite convalidar si las licencias de un equipo son genuinas, esto permitiría para el caso de los portátiles personales, validar que realmente es software licenciado.

7.5 SEGURIDAD EN REDES

Dentro del marco referencial, se mencionaron algunos protocolos y métodos de seguridad que se podrían implementar para las redes en el BYOD, estos protocolos son fundamentales para poder contar con una seguridad soportada en capa 3, 4 y 5 del modelo OSI, por lo que se hace necesario implementar portal cautivo para asegurarse de no tener conexiones anónimas dentro de la red ICBF, pues cualquier persona podría ingresar con un cable de red a un punto fijo, además se podría contemplar la asignación de conexiones VPN para los colaboradores que usen su equipo portátil personal y de esta manera ingresar a los servicios de red de forma segura.

8. CRONOGRAMA

Tabla 4. Cronograma de actividades.

ACTIVIDAD	MES 1	MES 2	MES 3	MES 4	MES 5	MES 6
Estudio del caso: se analizará el estado actual del arte y los diferentes conceptos que existen sobre BYOD Y su uso en general.						
Ajustes a la Propuesta solicitada por el Director de Trabajo						
Se realizará verificaciones del uso de tecnologías móviles en el ICBF Regional Tolima con el fin de encontrar hallazgos en las prácticas realizadas, verificar casos reales, entrevistas y encuestas al personal de TIC y Usuarios.						
Análisis de resultados						
Según el caso de estudio realizar recomendaciones para la aplicación del BYOD en la organización.						
Análisis y desarrollo: se estudia cada esquema de trabajo ofrecido por las diferentes fuentes de información y se estructura a manera de pre informe.						
Verificación de correcciones y observaciones.						
Documento definitivo después de las revisiones necesarias que se hagan para llegar a un informe escrito de acuerdo con el objeto propuesto al inicio.						
Sustentación del trabajo ante el director y el jurado.						

9. CONCLUSIONES

1. El BYOD seguirá incursionando en el mundo laboral, la globalización de los sistemas con la masificación de la internet lleva a tener mucha atención a este fenómeno que hace generar mayor inversión en seguridad y estrategias para prevenir la pérdida del activo más importante en un sistema de información SI como lo son sus datos.

2. En el ICBF Regional Tolima se viene trabajando bastante en algo que debe ser lo primordial en un entorno empresarial y es la sensibilización a su recurso humano con el fin generar un valor agregado en apropiación de las TI y su correcto uso para beneficio de la entidad estatal que presta un servicio esencial a la comunidad y debe por ley salvaguardar la custodia de la historia familiar de los niños, niñas y adolescentes NNA del país.

3. Cada vez en más probable que un funcionario tenga un nuevo dispositivo móvil con mejores prestaciones que los asignados en las compañías. Esto hace que también se combinen otras en un sentido más amplio BYOT (bring your own technology-traiga su propia tecnología) esto indica no solo usar el componente móvil sino también la conectividad personal a la internet con el avance que vemos como por ejemplo las redes 4G con anchos de bandas superiores a muchas entidades.

4. Cualquier entidad que quiera implementar el BYOD, cuenta con marcos de referencia y metodologías suficientes para poderlo aplicar a su contexto, además la normatividad colombiana cuenta con grandes avances en temas relacionados con delitos informáticos, datos abiertos, protección de datos personales y regulación por parte de MINTIC.

5. Los profesionales de TI de ICBF son conscientes del riesgo que representa el uso de equipos personales sin los respectivos controles, pero también tienen claro que es una tendencia mundial y que bien aplicada con las medidas necesarias de seguridad se puede ver reflejado en mayor productividad por facilidad de acceso a la tecnología.

6. Los Colaboradores de ICBF están usando sus dispositivos personales en sus labores por lo que el BYOD, ya no es una alternativa sino una realidad.

7. A pesar de tener una política de seguridad informática, el ICBF no ha profundizado en el tema del BOYD y como contrarrestar un posible ataque informático por esta causa. Existen muchas soluciones por software que pueden subsanar esta deficiencia, pero también queda entre dicho que tan efectivas son a largo plazo ya que con la incorporación de servicios en la nube ya el empleado puede acceder desde cualquier parte del mundo a todo su contenido almacenado en la

nube creando un gran agujero de seguridad en el caso de que no esté capacitado para el adecuado uso de estas nuevas tecnologías que están invadiendo todos los escenarios laborales y académicos del mundo.

8. El ICBF tiene un alto grado de madurez en la implementación de su SGSI, por lo que una apuesta en un futuro cercano es reglamentar y hacer los ajustes necesarios a nivel administrativo, tecnológico, contractual y de sensibilización para poder implementar el BYOD de forma segura.

9. Con este trabajo de monografía damos el primer paso para empezar a determinar el mejor camino que el ICBF debe implementar en su política de seguridad de la información en aras de salvaguardar la información de los NNA y las familias colombianas.

REFERENCIAS BIBLIOGRÁFICAS

BASSAT, Luis. El libro rojo de la publicidad:(ideas que mueven montañas). Debols! llo, 2017. {En línea}. {20 octubre de 2017}. Disponible en https://books.google.com.co/books?id=_z2GcBD3deYC&lpg=PR14&ots=wsiiAAHVOg&dq=%22Seguridad%20de%20la%20Informaci%C3%B3n%22&lr&hl=es&pg=PR14-IA1#v=onepage&q&f=false

Baud, J. L. (2015). Preparación para la certificación ITIL Foundation V3: ITIL V3-2011: más de 400 preguntas-respuestas (Vol. 3). Ediciones ENI. {En línea}. {06 octubre de 2017}. Disponible en https://books.google.com.co/books?id=vOEGFtNoUjcC&lpg=PA25&ots=8uD524OZQR&dq=%22itil%20v3%22&lr=lang_es&hl=es&pg=PA25#v=onepage&q=%22itil%20v3%22&f=false

Betancourt, A. (2016). Diseño de un prototipo de software para aplicar análisis GAP a los controles descritos en el anexo a de la norma ISO 27001:2013. {En línea}. {29 septiembre de 2017}. P. 36 Disponible en http://repositorio.utp.edu.co/dspace/handle/11059/7728.

BYOD ¿el futuro o la ruina de las grandes compañías? {En línea}. {01 septiembre de 2017}, disponible en http://www.revistasumma.com/gerencia/41548-byod-el-futuro-o-la-ruina-de-las-grandes-companias.html

BYOD impone a las empresas el desarrollo urgente de estrategias de seguridad, {En línea}. {01 septiembre de 2017} disponible en http://www.networkworld.es/actualidad/byod-impone-a-las-empresas-el-desarrollo-urgente-de-estrategias-de-seguridad

BYOD: una perspectiva global. {En línea}. {08 septiembre de 2017}. Disponible en http://www.cisco.com/web/about/ac79/docs/re/byod/BYOD_Horizons-Global_LAS.pdf

Cano, L. G. (2012). Protección de datos en Colombia, avances y retos. Revista Lebret, 4(4), 195-214. {En línea}. {27 octubre de 2017}. Disponible en http://revistas.ustabuca.edu.co/index.php/LEBRET/article/view/336

Carazas, V., & Yeffer, J. (2017). Marco de trabajo RISK IT en la gestión de riesgos de tecnología de la información en la Caja Rural de Ahorro y Crédito Los Andes SA-2015. {En línea}. {29 septiembre de 2017}. Disponible en http://repositorio.unap.edu.pe/handle/UNAP/5561

Castaño Gómez, J. D., & Mesa Ruiz, F. A. (2016). Diseño de una guía para la auditoria de la clasificación de información que vela por el cumplimiento de la ley 1712. {En línea}. {27 octubre de 2017}. Disponible en http://hdl.handle.net/10983/7851

Cifuentes Rodríguez, J. (2017). Diseño de un modelo de gestión de seguridad en redes de comunicación inalámbricas aplicado a pequeñas empresas del sector privado de la ciudad de Bogotá. Colombia. {En línea}. {20 octubre de 2017}. Disponible en http://hdl.handle.net/10596/12862

COLOMBIA. Departamento de planeación nacional. El Consejo Nacional de Política Económica y Social, CONPES. Ley 19 de 1958. {En línea}. {11 agosto de 2017} Bogotá: DPN. Disponible en https://www.dnp.gov.co/CONPES/Paginas/conpes.aspx

Colombia. ICBF Resolución 9364 de 2016 – Política Seguridad de la Información. {En línea}. {27 octubre de 2017}. Disponible en http://www.icbf.gov.co/portal/page/portal/Descargas1/Tratamiento%20de%20datos/Resolucion9364-Actualiza-Politica-Seguridad-Informacion.pdf

Colombia. ICBF Resolución 9364 de 2016 – Política Seguridad de la Información. {En línea}. {27 octubre de 2017}. Disponible en http://www.icbf.gov.co/cargues/avance/docs/resolucion_icbf_9364_2016.htm

Dordoigne, J. (2015). Redes informáticas-Nociones fundamentales (5ª edición):(Protocolos, Arquitecturas, Redes inalámbricas, Virtualización, Seguridad, IP v6...). Ediciones ENI. {En línea}. {13 octubre de 2017}. Disponible en https://books.google.com.co/books?id=Huwy1L0PEq8C&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Duchi Paca, E. y Herrera Cárdenas, E. (2015). Desarrollo de una aplicación Web basada en un E-procurement para la Empresa DIGISYSTEM S.A.. {En línea}. {13 octubre de 2017}. Disponible en http://repositorio.espe.edu.ec/handle/21000/10260

EL SALVADOR. MINISTERIO DE HACIENDA. GLOSARIO SGSI sistema de gestión de seguridad de la información. (2009) {En línea}. {04 agosto de 2017}. San Salvador: Ministerio. Disponible en http://www.mh.gob.sv/portal/page/portal/sgsi/MH_GLOSARIO/Glosario%20para%20Portal.pdf

Estébanes, E. and Cano, J. (2011). Gobierno de ti a través de Cobit 4.1 y cambios esperados en Cobit 5.0. P. 26 {En línea}. {06 octubre de 2017}. Disponible en https://dialnet.unirioja.es/servlet/articulo?codigo=3823460

GANDINI, Isabella. Ley de Delitos Informáticos en Colombia, 2010. {En línea}. {25 agosto de 2017} disponible en http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia

Gaona Vásquez, K. (2013). Aplicación de la metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa Pesquera e Industrial Bravito S.A. en la ciudad de Machala. P. 154 {En línea}. {06 octubre de 2017}. Disponible en https://dspace.ups.edu.ec/handle/123456789/5272

González García, R. A. (2017). Diseño del Sistema de Gestión de Seguridad de la Información (SGSI) para el área de tecnología de la empresa Baker Tilly Colombia Ltda. de la ciudad de Bogotá, bajo la norma ISO 27001: 2013. {En línea}. {20 octubre de 2017}. Disponible en http://hdl.handle.net/10596/12722

La adopción de BYOD es más acelerada en mercados de rápido crecimiento. {En línea}. {01 septiembre de 2017} disponible en http://www.la.logicalis.com/noticias-y-eventos/noticias/informe-byod.aspx

López Camacho, R. and López Obando, R. (2014). Diseño de un Marco de Referencia para regular el uso de BYOD en organizaciones bajo el estándar ISO 27002. P. 134 {En línea}. {13 octubre de 2017}. Disponible en https://repository.icesi.edu.co/biblioteca_digital/handle/10906/77346

Luna, J. y Martín, J. (2013). La gestión segura de la información en movilidad ante el fenómeno BYOD: ¿Bring Your Own Device = Bring Your Own Disaster? {En línea}. {03 noviembre de 2017}. Disponible en https://dialnet.unirioja.es/servlet/articulo?codigo=4391556

Macia, S. (2014). Seguridad en dispositivos móviles: un enfoque práctico. {En línea}. {03 noviembre de 2017}. Disponible en http://sedici.unlp.edu.ar/handle/10915/43678

Marulanda Ecehevrry, c. y López Trujillo, m. y Cuesta Iglesias, c. (2009). Modelos de desarrollo para gobierno TI. Scientia Et Technica, XV(41), pp.185-190. {En línea}. {15 septiembre de 2017}. Disponible en http://www.redalyc.org/articulo.oa?id=84916680032

OJEDA, Jorge Eliecer, et al. Delitos informáticos y entorno jurídico vigente en Colombia. En: Cuadernos de Contabilidad. 2010. vol. 11, no. 28, p. 41-66. {En línea}. {18 agosto de 2017}. Disponible en-http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003&lng=en&tlng=es

P, Aguilera. Seguridad Informática, 3ª Edición., Editorial EDITEX S.A. Madrid España 2010. {En línea}. {25 agosto de 2017} Disponible en http://www.editex.es/RecuperarFichero.aspx?Id=19810

Páez González, Daniel David, 2017, Propuesta de metodología de evaluación de seguridad informática, aplicada a proveedores de servicios de pequeñas y medianas empresas (Pyme), que accedan a información de personas físicas en el municipio de Toluca, estado de México. Ri.uaemex.mx {En línea}. {22 septiembre de 2017}. Disponible en http://ri.uaemex.mx/handle/20.500.11799/67693

Portal ICBF - Instituto Colombiano de Bienestar Familiar ICBF. (2017). El Instituto. {En línea}. {10 noviembre de 2017}. Disponible en https://www.icbf.gov.co/instituto

Proaño Galarza, P. (2009). Diseño e implementación de un portal cautivo utilizando un enrutador inalámbrico de bajo costo y un sistema operativo de código abierto. {En línea}. {27 octubre de 2017}. Disponible en http://repositorio.uisek.edu.ec/handle/123456789/79

Pulido Barreto, A. y Mantilla Rodriguez, J. (2016). Modelo para la implementación del sistema general de seguridad informática y protocolos de seguridad informática en la oficina TIC de la alcaldía municipal de Fusagasugá, basados en la gestión del riesgo informático. {En línea}. {27 octubre de 2017}. Disponible en http://hdl.handle.net/10596/6327

Reyes Vásquez, Virgilio Ernesto. “BYOD y la movilidad corporativa”. Ing-novación. Revista semestral de ingeniería e innovación de la Facultad de Ingeniería, Universidad Don Bosco. Diciembre de 2012 – Mayo de 2013, Año 3, No. 5. pp. 117-121. ISSN 2221-1136. {En línea}. {03 noviembre de 2017}. Disponible en http://www.redicces.org.sv/jspui/bitstream/10972/1985/1/BYOD%20y%20la%20mobilidad.pdf

Rodríguez Pinto, A. y Rozo Caballero, R. (2015). Diseño de un plan estratégico para la seguridad de la información tributaria en una entidad pública. {En línea}. {27 octubre de 2017}. Disponible en http://hdl.handle.net/10596/3613

Rojas Gonzales, E. A. (2017). El sistema de gestión de continuidad de negocios y su relación con los riesgos en las entidades financieras peruanas reguladas por la superintendencia de banca y seguros. {En línea}. {29 septiembre de 2017}. Disponible en http://repositorio.unac.edu.pe/handle/UNAC/2149

Rojas, D. (2015). "BRING YOUR OWN DEVICE OPORTUNIDADES”, RETOS Y RIESGOS EN LAS ORGANIZACIONES. {En línea}. {03 noviembre de 2017}. Revistas.uni.edu.pe. ISSN: 0375-7765 ISSN: 2309-0413 (versión electrónica) Disponible en http://revistas.uni.edu.pe/index.php/tecnia/article/view/17/219

Securitic.com.mx. (2012). SecuriTIC. {En línea}. {17 noviembre de 2017}. Disponible en http://securitic.com.mx/noticias/210-fortinet-amplia-y-mejora-su-solucion-de-seguridad-de-redes-para-byod

Tavera Jaramillo, W. y Mahecha Rivera, M. (2016). Identificación de los ataques más realizados en un sitio concurrido por personas que utilizan sus dispositivos móviles y determinación de las vulnerabilidades más comunes en el sistema operativo Android. 115 p. Colombia. Disponible en http://hdl.handle.net/10596/6337

Tovar Piraban, C. and Ayala Marín, W. (2017). Implementación red de sincronismo para la expansión de la operación móvil. P. 47 {En línea}. {11 agosto de 2017}. Disponible en http://repository.usta.edu.co/handle/11634/9104

Trujillo Murcia, F. y Celis Perdomo, C. (2017). Proponer un sistema de diagnóstico y monitoreo que permita identificar eventos para resolver problemas de infraestructura de TI, de la red de datos de la empresa Sociedad Clínica Emcosalud. {En línea}. {20 octubre de 2017}. Disponible en http://hdl.handle.net/10596/13386

Vásquez Villacreses, L. (2015). Herramientas de seguridad de la información en dispositivos finales y móviles con relación a “BYOD” – caso de estudio de la plataforma IBM Security Endpoint Manager. {En línea}. {10 noviembre de 2017}. P. 5., Repositorio.puce.edu.ec. Disponible en http://repositorio.puce.edu.ec/handle/22000/10282

Vidal Londoño, J. (2016). Una nueva experiencia en seguridad hacking ético. {En línea}. {27 octubre de 2017}. Repository.unimilitar.edu.co. Disponible en http://repository.unimilitar.edu.co/handle/10654/15838

Villacrés Machado, D. (2011). Propuesta Metodológica para Asegurar Redes Inalámbricas y su Aplicación en la ESPOCH. P. 202 {En línea}. {13 octubre de 2017}. Disponible en http://dspace.espoch.edu.ec/handle/123456789/1480?mode=full

LISTA DE ANEXOS

ANEXO A – DOCUMENTO CONPES 3854

Documento
CONPES

3854

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL
REPÚBLICA DE COLOMBIA
DEPARTAMENTO NACIONAL DE PLANEACIÓN

POLÍTICA NACIONAL DE SEGURIDAD DIGITAL

Ministerio de Tecnologías de la Información y las Comunicaciones
Ministerio de Defensa Nacional
Dirección Nacional de Inteligencia
Departamento Nacional de Planeación

Versión aprobada

Bogotá, D.C., 11 de abril de 2016

ANEXO B - RESOLUCIÓN ICBF 9364 2016

Inicio Artículo

RESOLUCIÓN 9364 DE 2016

(septiembre 13)

Diario Oficial No. 50.000 de 18 de septiembre de 2016

INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR

CECILIA DE LA FUENTE DE LLERAS

DIRECCIÓN GENERAL

Por la cual se actualiza la Política de Seguridad de la Información, se definen lineamientos frente su uso y manejo y se deroga una resolución

Resumen de Notas de Vigencia

NOTAS DE VIGENCIA:

- Modificada por la Resolución 3600 de 2017, 'por la cual se modifica la Resolución número 9364 de 2016, "por la cual se actualiza la Política de Seguridad de la Información, se definen lineamientos frente su uso y manejo y se deroga una resolución"', publicada en el Diario Oficial No. 50.242 de 23 de mayo de 2017.

LA DIRECTORA GENERAL DEL INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR CECILIA DE LA FUENTE DE LLERAS,

en uso de sus facultades legales y estatutarias señaladas en las Leyes 7ª de 1979, 87 de 1993, el artículo 78 de la Ley 489 de 1998 y el artículo 2.2.9.1.2.3 del Decreto número 1078 de 2015, y

CONSIDERANDO:

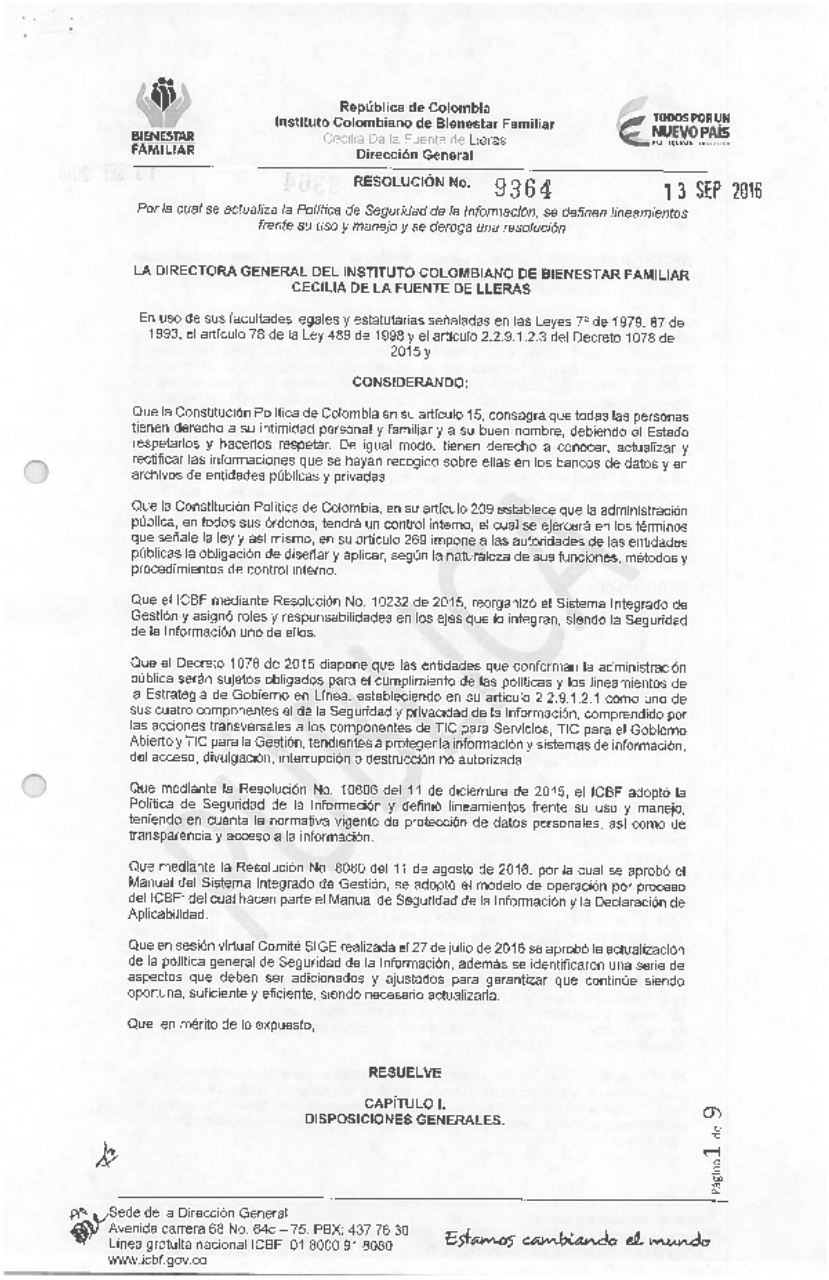
Que la Constitución Política de Colombia en su artículo 15, consagra que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, debiendo el Estado respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas;

Que la Constitución Política de Colombia, en su artículo 209 establece que la administración pública, en todos sus órdenes, tendrá un control interno, el cual se ejercerá en los términos que señale la ley y así mismo, en su artículo 269 impone a las autoridades de las entidades públicas la obligación de diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno;

Que el ICBF mediante Resolución número 10232 de 2015, reorganizó el Sistema Integrado de Gestión y asignó roles y responsabilidades en los ejes que lo integran, siendo la Seguridad de la Información uno de ellos;

Que el Decreto número 1078 de 2015 dispone que las entidades que conforman la administración pública serán sujetos obligados para el cumplimiento de las políticas y los

ANEXO C - RESOLUCIÓN 9364 POLÍTICA-SEGURIDAD-INFORMACIÓN



BIENESTAR FAMILIAR

República de Colombia
Instituto Colombiano de Bienestar Familiar
Cecilia De la Fuente de Lleras
Dirección General

TODOS POR UN NUEVO PAÍS

RESOLUCIÓN No. 9364 **13 SEP 2016**

Por la cual se actualiza la Política de Seguridad de la Información, se definen lineamientos frente su uso y manejo y se deroga una resolución

LA DIRECTORA GENERAL DEL INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR CECILIA DE LA FUENTE DE LLERAS

En uso de sus facultades legales y estatutarias señaladas en las Leyes 7ª de 1979, 87 de 1993, el artículo 78 de la Ley 489 de 1998 y el artículo 2.2.9.1.2.3 del Decreto 1078 de 2015 y

CONSIDERANDO:

Que la Constitución Política de Colombia en su artículo 15, consagra que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, debiendo el Estado respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas

Que la Constitución Política de Colombia, en su artículo 209 establece que la administración pública, en todos sus órdenes, tendrá un control interno, el cual se ejercerá en los términos que señale la ley y así mismo, en su artículo 269 impone a las autoridades de las entidades públicas la obligación de diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno.

Que el ICBF mediante Resolución No. 10232 de 2015, reorganizó el Sistema Integrado de Gestión y asignó roles y responsabilidades en los ejes que lo integran, siendo la Seguridad de la Información uno de ellos.

Que el Decreto 1078 de 2015 dispone que las entidades que conforman la administración pública serán sujetos obligados para el cumplimiento de las políticas y los lineamientos de la Estrategia de Gobierno en Línea, estableciendo en su artículo 2.2.9.1.2.1 como uno de sus cuatro componentes el de la Seguridad y privacidad de la información, comprendido por las acciones transversales a los componentes de TIC para Servicios, TIC para el Gobierno Abierto y TIC para la Gestión, tendientes a proteger la información y sistemas de información, del acceso, divulgación, interrupción o destrucción no autorizada

Que mediante la Resolución No. 10806 del 11 de diciembre de 2015, el ICBF adoptó la Política de Seguridad de la Información y definió lineamientos frente su uso y manejo, teniendo en cuenta la normativa vigente de protección de datos personales, así como de transparencia y acceso a la información.

Que mediante la Resolución No. 8080 del 11 de agosto de 2016, por la cual se aprobó el Manual del Sistema Integrado de Gestión, se adoptó el modelo de operación por proceso del ICBF del cual hacen parte el Manual de Seguridad de la Información y la Declaración de Aplicabilidad.

Que en sesión virtual Comité SIGE realizada el 27 de julio de 2016 se aprobó la actualización de la política general de Seguridad de la Información, además se identificaron una serie de aspectos que deben ser adicionados y ajustados para garantizar que continúe siendo oportuna, suficiente y eficiente, siendo necesario actualizarla.

Que en mérito de lo expuesto,

RESUELVE

CAPÍTULO I.
DISPOSICIONES GENERALES.

Sede de la Dirección General
Avenida carrera 68 No. 64c – 75. PBX: 437 76 30
Línea gratuita nacional ICBF 01 8000 91 8080
www.icbf.gov.co

ANEXO D - LEY 1581 2012

LEY ESTATUTARIA 1581 DE 2012

(octubre 17)

Diario Oficial No. 48.587 de 18 de octubre de 2012

CONGRESO DE LA REPÚBLICA

Por la cual se dictan disposiciones generales para la protección de datos personales.

Jurisprudencia Vigencia

EL CONGRESO DE COLOMBIA

DECRETA:

TÍTULO I.

OBJETO, ÁMBITO DE APLICACIÓN Y DEFINICIONES.

ARTÍCULO 1o. OBJETO. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Jurisprudencia Vigencia
Concordancias

ARTÍCULO 2o. ÁMBITO DE APLICACIÓN. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.

El régimen de protección de datos personales que se establece en la presente ley no será de aplicación:

a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.

Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley;

b) A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo;

c) A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia;

ANEXO E - LEY 1273 DE 2009

LEY No. 1273 5 ENE 2009

"POR MEDIO DE LA CUAL SE MODIFICA EL CÓDIGO PENAL, SE CREA UN NUEVO BIEN JURÍDICO TUTELADO – DENOMINADO "DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS"- Y SE PRESERVAN INTEGRALMENTE LOS SISTEMAS QUE UTILICEN LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, ENTRE OTRAS DISPOSICIONES".

EL CONGRESO DE COLOMBIA

DECRETA:

ARTÍCULO 1° Adiciónase el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor:

CAPÍTULO PRIMERO
De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

ARTÍCULO 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

ARTÍCULO 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

ARTÍCULO 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

ARTÍCULO 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

ARTÍCULO 269E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

ARTÍCULO 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compile, intercepte, divulgue, modifique o emplee códigos

ANEXO F - DELITOS INFORMÁTICOS Y ENTORNO JURÍDICO VIGENTE EN COLOMBIA

Delitos informáticos y entorno jurídico vigente en Colombia*

Jorge Eliécer Ojeda-Pérez

Economista, Universidad La Gran Colombia, Bogotá, Colombia. Ingeniero de sistemas, Universidad Antonio Nariño, Bogotá, Colombia. Especialista en sistemas de información, Universidad de los Andes, Bogotá, Colombia. Magíster en ingeniería industrial, Universidad de los Andes, Bogotá, Colombia. Profesor de medio tiempo, Universidad Santo Tomás de Aquino, USTA, Bogotá, Colombia. Investigador principal del grupo de investigación en Seguridad Informática y Delitos Informáticos de la especialización en Auditoría de Sistemas, Universidad Santo Tomás de Aquino, USTA.

Correo electrónico: jojeda10@gmail.com

Fernando Rincón-Rodríguez

Abogado, Universidad Libre de Colombia, Bogotá, Colombia. Director Especialización en Auditoría y Administración de la Información Tributaria, Universidad Santo Tomás de Aquino, USTA, Bogotá, Colombia. Consultor jurídico del grupo de investigación en Seguridad Informática y Delitos Informáticos de la especialización en Auditoría de Sistemas de Universidad Santo Tomás de Aquino, USTA.

Correo electrónico: fernandorincon@usantotomas.edu.co

Miguel Eugenio Arias-Flórez

Ingeniero de telecomunicaciones, Universidad Santo Tomás de Aquino, USTA, Bogotá, Colombia. Ingeniero superior de telecomunicación, Ministerio de Educación, Madrid, España. Especialista en gerencia de proyectos de telecomunicaciones, Universidad Santo Tomás de Aquino, USTA, Bogotá, Colombia. Máster en administración de negocios, MBA, Escuela Europea de Negocios, Salamanca, España. Profesor de tiempo completo, Universidad Santo Tomás de Aquino, USTA, Bogotá, Colombia. Coinvestigador del grupo de investigación en Seguridad Informática y Delitos Informáticos de la especialización en Auditoría de Sistemas de la Universidad Santo Tomás de Aquino, USTA.

Correo electrónico: miguelarias@usantotomas.edu.co.

Libardo Alberto Daza-Martínez

Economista, Pontificia Universidad Javeriana. Magíster en ciencias económicas, Universidad Santo Tomás de Aquino, USTA. Especialista en pedagogía para el desarrollo del aprendizaje autónomo de la Universidad Nacional Abierta y a Distancia, UNAD. Director de las especializaciones: Auditoría de Sistemas y Gerencia de Negocios Internacionales. Líder del grupo de investigación en Seguridad Informática y Delitos Informáticos de la especialización en Auditoría de Sistemas de la Universidad Santo Tomás de Aquino, USTA.

Correo electrónico: libardodaza@usantotomas.edu.co.

* El presente artículo es producto del trabajo de investigación desarrollado por el grupo de investigación Seguridad y Delitos Informáticos, SEGUDELIN, de la especialización en Auditoría de Sistemas de la Universidad Santo Tomás de Aquino, USTA. El artículo fue preparado de marzo a mayo de 2010.