FACULTAD DE POSTGRADO

TESIS DE POSTGRADO

PROPUESTA DE UN MARCO DE REFERENCIA PARA EL CONTROL DE BYOD EN LAS INSTITUCIONES GUBERNAMENTALES DEL SECTOR FINANCIERO DE HONDURAS

SUSTENTADO POR:

ALVIN ONAM RUBIO AVILA

EDWIN JOEL BULNES VASQUEZ

PREVIA INVESTIDURA AL TÍTULO DE MÁSTER EN GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

TEGUCIGALPA, F.M, HONDURAS, C.A.

OCTUBRE, 2017

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA

UNITEC

FACULTAD DE POSTGRADO

AUTORIDADES UNIVERSITARIAS

RECTOR

MARLON ANTONIO BREVE REYES

SECRETARIO GENERAL

ROGER MARTÍNEZ MIRALDA

DECANO DE LA FACULTAD DE POSTGRADO

JOSÉ ARNOLDO SERMEÑO LIMA

PROPUESTA DE UN MARCO DE REFERENCIA PARA EL CONTROL DE BYOD EN LAS INSTITUCIONES GUBERNAMENTALES DEL SECTOR FINANCIERO DE HONDURAS

TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO DE

MÁSTER EN

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

ASESOR

CARLOS ROBERTO ARIAS

JORGE RAÚL MARADIAGA CHIRINOS

FACULTAD DE POSTGRADO

PROPUESTA DE UN MARCO DE REFERENCIA PARA EL CONTROL DE BYOD EN LAS INSTITUCIONES GUBERNAMENTALES DEL SECTOR FINANCIERO DE HONDURAS

AUTORES:

Alvin Onam Rubio Avila y Edwin Joel Bulnes Vasquez

Resumen

El propósito del proyecto se basó en una propuesta de un marco de referencia para el control de BYOD en las instituciones gubernamentales del sector financiero de Honduras. La finalidad de este proyecto es que el marco de referencia propuesto sea implementado de acuerdo al análisis de riesgo individual de cada institución o proceso de negocio especifico, lo que ayudara a mitigar el riesgo de fuga de información confidencial. Para poder proponer el marco de referencia se realizó una investigación exploratoria, encuestas a empleados y entrevistas a expertos, así mismo se consultaron artículos científicos, y analizaron estándares internacionales para este tipo de marco. Los resultados mostraron que es necesario utilizar un marco de referencia para el control de BYOD, esto debido a que la mayoría de empleados que almacenan información confidencial en sus dispositivos móviles, no tienen los controles necesarios para proteger la información o mitigar los riesgos a los que se exponen. Se recomienda realizar un análisis de factibilidad para determinar si los usuarios deben utilizar los dispositivos móviles para temas laborales, y si esto es factible, aplicar los controles del marco propuesto en esta tesis.

Palabras clave: BYOD, Ciencias de la Computación, Control, Seguridad, Tecnologías de la Información

GRADUATE SCHOOL

PROPOSAL FOR A REFERENCE FRAMEWORK FOR THE CONTROL OF BYOD IN THE GOVERNMENTAL INSTITUTIONS OF THE FINANCIAL SECTOR OF HONDURAS

AUTHORS:

Alvin Onam Rubio Avila and Edwin Joel Bulnes Vasquez

Abstract

The purpose of the project was based on a proposal of a reference frame for the control of BYOD in the governmental institutions of the financial sector of Honduras. The purpose of this project is that the frame of reference has been implemented according to the individual risk analysis of each institution or specific business process, which helps to mitigate the risk of leakage of confidential information. In order to propose the frame of reference, an exploratory research, employee surveys and interviews with experts was carried out. Scientific articles and international standards were also consulted for this type of framework. The results that it is necessary to use a frame of reference for the control of BYOD, this is due to the large number of employees who store confidential information on their mobile devices, do not have the necessary controls to protect the information or mitigate the risks to which It is recommended to carry out a feasibility analysis to determine if users should use mobile devices for labor issues, and if this is feasible, apply the controls of the framework proposed in this thesis.

Keywords: BYOD, Computer Science, Control, Security, Information Technology

DEDICATORIA

Dedico esta tesis a Dios, por estar conmigo, darme salud, inteligencia y sabiduría para poder alcanzar esta meta y las metas anteriores.

A mi esposa Karen por animarme en los momentos difíciles, a mis hijas Teresa de 3 años y Esther de 1 año por su compresión cuando les decía que “iba a pintar”. A mi padre Rigoberto por comprender mis ausencias y por sus palabras de aliento, igual a mis hermanos, cuñadas, sobrinos y sobrinas, y es mi mayor deseo, ser para estos últimos un ejemplo de esfuerzo y dedicación. A mi madre que está en el cielo, que siempre fue una mujer esforzada y valiente.

Alvin Onam Rubio Avila

Dedico está tesis a Dios todopoderoso, sin Él no tendría el poder, voluntad y la fuerza que me permitieron poder concluir está maestría y de la cual estoy completamente seguro que fue gracias a su infinita bendición.

A mi esposa Alma Rosa Pinel, quien fue la principal impulsora de que este servidor pudiera seguir estudiando y quien ha estado a mi lado en todo momento recibiendo su apoyo, gracias mi amor por tu amor incondicional, a mi hija, Alina Sofía Bulnes, quiero que sepas que este trabajo y está maestría está dedicada especialmente a ti mi amor, tu eres nuestra más grande bendición y mientras Dios lo permita siempre lucharé para que tú y tu madre tengan lo indispensable.

Edwin Joel Bulnes Vasquez

AGRADECIMIENTO

Al personal docente de UNITEC por la transferencia de conocimiento realizada, así mismo, sus experiencias. Por el tiempo ordinario y extraordinario dedicado a ampliar nuestro conocimiento a lo largo de estos dos años que traen un gran aporte a nuestro desarrollo profesional.

A los empleados de las instituciones del sector financiero hondureño, a los expertos entrevistados, el Master en Seguridad de la Información, Ing. Edy Milla, al Experto en Seguridad Informática y Master el Ing. Ivan Flores, al Profesional de Seguridad de Sistemas de Información y Certificado (CISSP) el Lic. Carlos Arteaga, quienes nos brindaron su experiencia y amplio recorrido académico y profesional en estos temas.

Agradecemos al Dr. Carlos Arias y Dr. Jorge Maradiaga, por su experiencia y asesoría en el desarrollo de este documento, así mismo al Dr. Marco Antonio López al cuál le estamos muy agradecidos por los conocimientos, consejos y orientación brindada para poder llevar con éxito los estudios realizados en la presente tesis.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE GRAFICOS

ÍNDICE DE TABLAS

CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

Este capítulo brindará al lector un panorama específico de los temas relacionados con los riesgos que tienen la información institucional al ser almacenada en los dispositivos móviles como Smartphones y Tablets personales que utilizan los empleados.

1.1 Introducción

Una gran parte de la información privada de personas y empresas es robada desde los dispositivos móviles de usuarios que cuentan con una capacitación mínima o casi nula en temas de seguridad de la información, así mismo un gran porcentaje de las empresas no cuentan con las herramientas, políticas y controles mínimos necesarios para proteger la información institucional que es almacenada en los dispositivos móviles personales de sus empleados.

Los dispositivos móviles como Smartphone y Tablet han incrementado las oportunidades de las empresas en lograr que sus empleados sean más productivos, sin necesidad de estar sentados frente a una computadora de escritorio o esperar a que regresen a la oficina de una reunión para atender un correo. Los empleados pueden recibir correos, estar monitoreando la evolución de un proceso, almacenar documentos en sus dispositivos móviles personales para participar en una reunión o hacer una presentación. Pero todo esto se hace en muchas empresas sin los controles que permitan proteger la información sensible de la institución.

Por lo antes mencionado se realizará una investigación de las herramientas, políticas y controles aplicados por las instituciones gubernamentales del sector financiero de Honduras (IGSFH) y proponer un marco de referencia que controle la tendencia de traer tu propio dispositivo móvil (BYOD por sus siglas en inglés) en estas instituciones.

1.2 Antecedentes del Problema

La tendencia de BYOD es ahora una necesidad para las nuevas generaciones, las empresas demandan ser más productivas en un mundo que cambia a un ritmo acelerado, es por ello que es necesario permitir el BYOD y que estos se conecten a servicios como el correo electrónico y otros servicios internos de la institución para que puedan estar informados o tomar decisiones en

menor tiempo y desde casi cualquier ubicación geográfica, pero las instituciones no tienen control de la información confidencial de la institución que se está almacenando en estos dispositivos móviles personales, los cuales tienen un alto índice de pérdida, extravío o robo.

1.3 Definición del Problema

Los problemas a los que se enfrentan las empresas son por temas de seguridad de la información, debido a que la información es almacenada en estos dispositivos móviles, ya que estos no tienen un control estricto de las redes a las que se conectan, tampoco de las aplicaciones que descargan. También son dispositivos que se pueden perder fácilmente o pueden ser robados. Harris (2012) expresa "Los riesgos de perder información confidencial se vuelve un factor a considerar para aplicar controles, siendo que uno de cada cinco empleados británicos, es decir el 21% admite que guarda información crítica de trabajo en dispositivos de medios extraíbles como unidades flash. Esta cifra aumenta hasta el 27% para los mayores de entre 25 y 34 años."

1.4 Pregunta de Investigación

¿Cuál es el marco de referencia que el gobierno hondureño está implementando para el control de BYOD, utilizados para el intercambio de información sensible de la institución o conectarse a las IGSFH?

1.5 Objetivos

A continuación, se mencionan los objetivos generales y específicos que se cumplirán con el desarrollo de este trabajo de investigación.

1.5.1 Objetivo General

Proponer el marco de referencia para el control de dispositivos móviles personales conectados a los servicios informáticos propios de la institución, realizando una investigación de los controles existentes en las IGSFH, para proteger la información sensible institucional que es almacenada en dichos dispositivos.

1.5.2 Objetivo Específicos

- Realizar entrevistas con expertos de seguridad de la información para conocer de primera mano los controles que se deberían estar aplicando en las instituciones gubernamentales.
- Determinar si los empleados de las instituciones gubernamentales están conscientes de los riesgos relacionados con el mal manejo de la información institucional sensible en los dispositivos móviles personales.
- Reportar las mejores prácticas para aplicar los controles de seguridad de la información en dispositivos móviles personales.
- Elaborar un marco de referencia para el control de dispositivos móviles personales.

1.6 Justificación

Las empresas necesitan resguardar su información, es por ello que aplican controles rigurosos a lo interno de las instituciones, y es un reto el poder resguardar la información que sale de las fronteras de la empresa, y que los empleados estén conscientes del riesgo que conlleva almacenar información en sus dispositivos sin los controles de seguridad requeridos. Es importante para las empresas aplicar una correcta política de acuerdo a los estándares actuales y mejores prácticas.

CAPÍTULO II. MARCO TEÓRICO

Este capítulo brindará al lector información actualizada y relevante acerca del uso de dispositivos móviles personales en las empresas, y la información respecto a los estándares y normativas que se deben considerar al permitir el uso de dichos dispositivos.

2.1 ¿En qué Consiste BYOD?

El acrónimo de BYOD (Bring Your Own Device) es una clara referencia a otro muy conocido en el mundo anglosajón, BYOB (Bring Your Own Beer), término utilizado en el ámbito social, solicitando que cada invitado a determinada fiesta debe llevar su propia bebida. El término empezó a ser conocido desde el año 2003, pero su auge comenzó en el año 2011 (Leavitt, 2013). Año en que el mercado de dispositivos como teléfonos inteligentes, tabletas digitales y otros dispositivos personales comenzó a repuntar. Desde entonces ha ido en aumento la presión para

habilitar y brindar soporte al uso de todos estos dispositivos en el ámbito laboral, convirtiendo la necesidad de adoptar BYOD en más que una simple opción.

Evidentemente, en los últimos años los usuarios corporativos han trasladado el uso computacional de la empresa a un ambiente externo, es decir, que el acceso a la información corporativa se realiza desde los hogares, aeropuertos, conferencias, etc. Convirtiéndose en trabajadores móviles que necesitan acceder remotamente a los activos de la organización utilizando sus propios dispositivos como parte de la tendencia de BYOD. Por otra parte, cada vez hay más proyectos donde las diferentes compañías y contratistas tienen que trabajar de forma colaborativa, en la mayoría de los casos a distancias geográficas considerables e incluso en husos horarios totalmente diferentes. Debido a este cambio los ambientes computacionales no están completamente controlados por los administradores de TI (Tecnologías de la Información) y es por eso que se necesita adoptar nuevos marcos de referencia que permitan asegurar la información de la organización que fluye a través de estas tendencias. Erróneamente y quizás por el uso del término por parte de fabricantes de soluciones de seguridad inalámbrica, se asocia BYOD a contar con mecanismos de control de accesos o utilizar algoritmos de encripción más fuertes para la autenticación de los usuarios, sin embargo, la ideología de BYOD como se observará más adelante va mucho más allá de eso.

2.2 ¿Cómo Surge BYOD?

La historia de la computación moderna desde su nacimiento en la década de los años 60's, brinda suficiente información para visualizar las transiciones que esta ha sufrido a través del tiempo, siendo esta evolución directamente proporcional a las necesidades que van surgiendo en el usuario final. Si se visualiza una perspectiva, esta evolución comienza con el progreso de los servidores mainframe a las computadoras personales, y avanza con el desarrollo de la era de la información al posicionarse nuevas tecnologías de intercomunicación en la década de los 90's con el surgimiento del internet (Olalere, Abdullah, Mahmod & Abdullah, 2015).

Hoy en día es un hecho conocido el observar que la computación móvil ha suplantado la computación basada en internet debido a un nuevo concepto traído a la industria de la computación, conocido como "La nube", concepto que a la vez ha sido un catalizador en la

proliferación de aplicaciones livianas accesibles y el perfeccionamiento de dispositivos móviles (teléfonos inteligentes, tabletas, computadoras portátiles, etc.), sumado a esto el hecho que el usuario ha logrado la experiencia de poder realizar las tareas que antes ejecutaba desde una estación de trabajo ahora desde la palma de su mano.

Es debido a lo mencionado en el párrafo anterior que muchas empresas optan porque su personal traiga sus dispositivos móviles personales a su lugar de trabajo, esta portabilidad ha logrado también que surja una nueva metodología de trabajo, "a cualquier hora y cualquier lugar" (Disterer & Kleiner, 2013, p. 45). En resumen, la gente ha optado por traer sus dispositivos móviles y conectarse a la red corporativa de sus empresas realizando su trabajo, pero a la vez teniendo la posibilidad de poder conectarse a los recursos ofrecidos por el internet, entre estas, plataformas de redes sociales y contenido multimedia, tales como Facebook y YouTube solo para indicar algunos en particular.

Otro factor relevante relacionado con el crecimiento exponencial en el uso de dispositivos móviles, ha sido el aspecto generacional, de acuerdo a Seppanen & Gualtieri (2012) investigadoras de la fundación de cámara de comercio de Estados Unidos, una generación en particular siempre muestra rasgos generalizados y únicos que terminan por influir en la cultura y crean un impacto duradero en el curso de la misma.

Para comprender la relevancia de este concepto en el tema de BYOD, es útil definir las generaciones que actualmente se encuentran activas trabajando, generando dinero e interactuando con la tecnología, de acuerdo al Pew Research Center (2010), los segmentos generacionales actuales se muestran en la tabla 1.

Tabla 1. Segmentos generacionales

Generación	Nacimiento	Edad actual	Concepto
Baby Boomers	1946–1964	53-71 años	Generación en proceso de retiro laboral o con jubilación establecida.
Generación X	1965–1979	38-52 años	Generación con niños pequeños y con una carrera ya establecida.
Millennials	1980–1999	18-37 años	Generación con carrera inicial o un poco establecida.
Generación Z	2000–	Menores de 17 años	La generación más joven, típicamente aun recibiendo algún

Generación	Nacimiento	Edad actual	Concepto
			tipo de educación o por salir de ella.

Fuente: (Center, 2010b)

La casa de estudios de mercado Nielsen Company (2016) afirma y de acuerdo a grafico 1 que hasta el tercer trimestre del año 2016 en los Estados Unidos la generación Millennials encabezaba como la generación con mayor consumo de dispositivos móviles, seguida por la generación X.

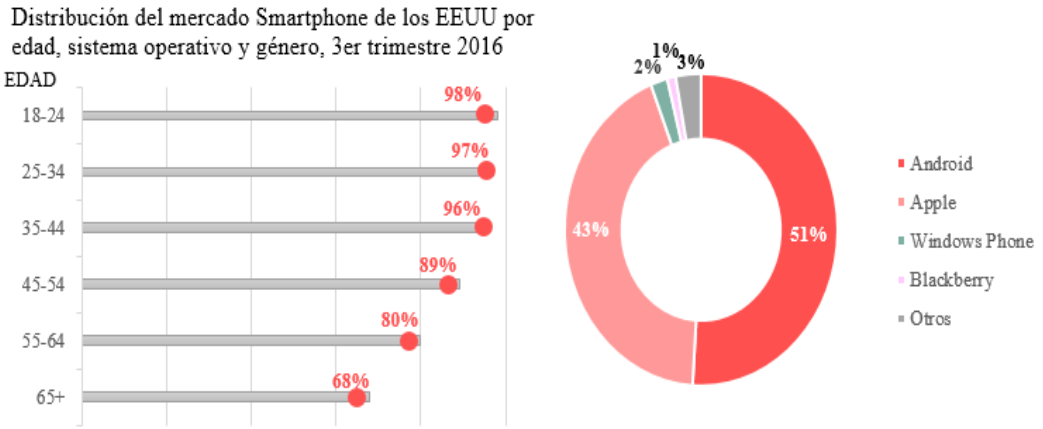

Grafico 1: Distribución del mercado Smartphone de los EEUU por edad, sistema operativo y género, 3er trimestre 2016

Fuente: (Nielsen Company, 2016)

2.3 El Fenómeno BYOD a Nivel Internacional

Como se mencionaba en párrafos anteriores, la tendencia del uso de dispositivos móviles no es propia del mercado estadounidense, sino que se ha convertido en un fenómeno global. CISCO es una de las empresas líderes en materia de telecomunicaciones y redes, realizó un estudio en ocho (8) países de tres (3) diferentes regiones (Latinoamérica, Asia y Europa) como expansión del estudio previo llamado "BYOD and Virtualization: Top 10 Insights", realizado en Estados Unidos y otros diecisiete (17) países con economías mixtas tanto emergentes como países desarrollados. En este nuevo estudio Cisco IBSG (2012) reveló que el 75% de usuarios de economías emergentes como Malasia, Singapur, Brasil, India y el 40% de usuarios de países desarrollados como Estados Unidos, Inglaterra, Suiza, Japón, Italia utilizaban sus propios

dispositivos móviles para propósitos laborales, conteniendo información de la empresa para la cual laboraban. El estudio de predictibilidad de Gartner en el año 2014 predijo que para el año 2018, más del 50% de usuarios usarán una tableta digital o teléfono inteligente para todas sus actividades en línea, y el 40% de las empresas establecerán la conexión inalámbrica como la conexión predeterminada por sus muchos beneficios y la conexión tradicional de cables como el modelo por excepción, mostrando que BYOD se ha convertido en algo común en las economías emergentes y economías desarrolladas (Gartner, 2014a).

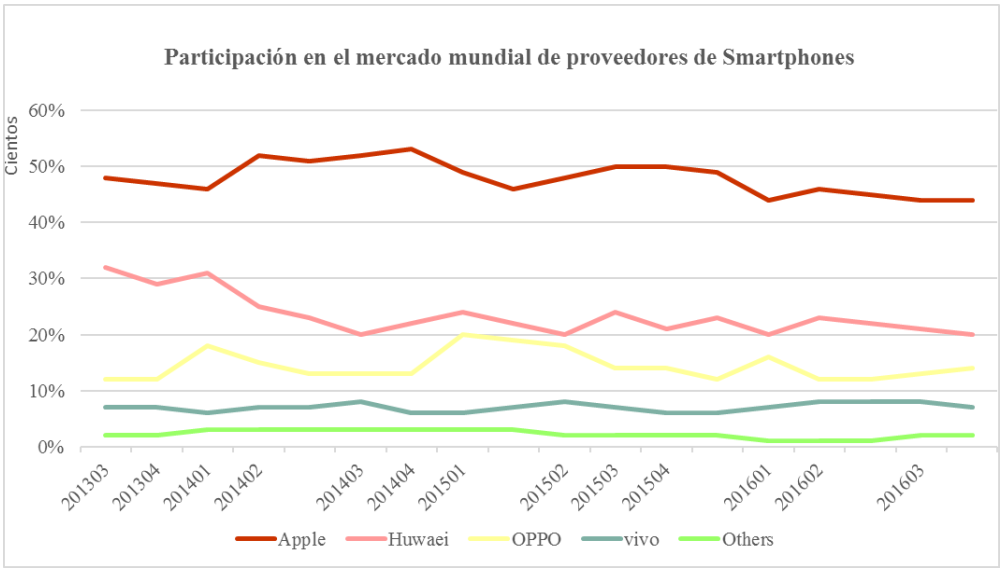

Grafico 2: Participación en el mercado mundial de proveedores de Smartphone

Fuente: (IDC, 2016a)

De acuerdo al último estudio de IDC (2016) presentado en grafico 2, para el cuarto trimestre del 2016 en el mercado de teléfonos inteligentes se habían vendido 363.2 millones de unidades a nivel mundial, siendo China el mercado que mostraba un patrón de mayor madurez. Android dominaba el mercado con una representación de 86.8% y el fabricante Samsung continuaba como líder global.

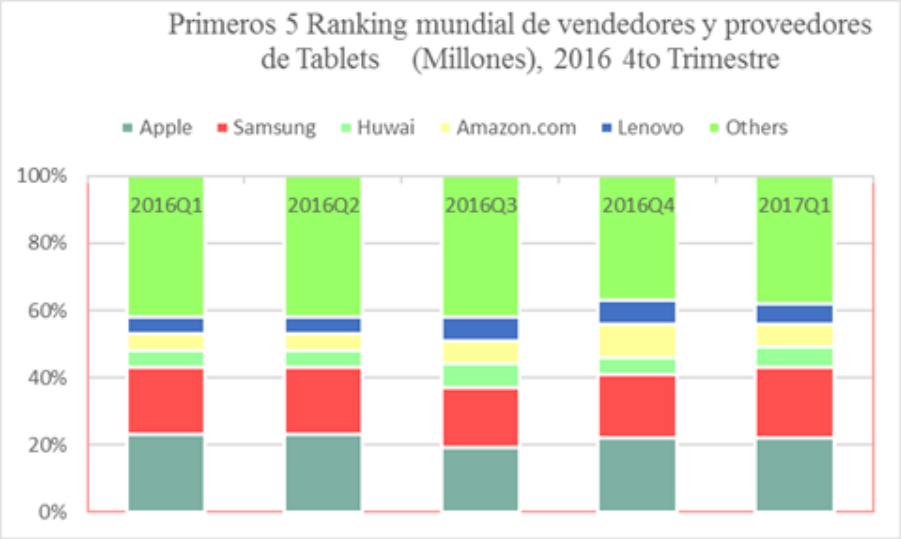

Grafico 3: Primeros 5 Ranking mundial de vendedores y proveedores de Tablets

Fuente: (IDC, 2016c)

En el mercado de las Tablets es todo lo contrario, de acuerdo al estudio de IDC para el cuarto trimestre del 2016 de acuerdo a grafico 3 se viene dando una tendencia negativa, siendo este trimestre el noveno en el cual las ventas de Tablets han decaído. Los fabricantes lograron durante este periodo vender 52.9 millones de unidades representando un decrecimiento de 20.1% comparado con el mismo cuarto en el año 2015, a pesar de esto, el estudio demuestra que Android continúa liderando como el sistema operativo más utilizado, pero Apple sigue liderando el mercado de fabricantes con un segmento del 20.4 % (IDC, 2016d).

La evolución de estos dispositivos ha sido una respuesta a la demanda de información que el usuario requiere para el desempeño de las diferentes actividades o tareas que realiza utilizando tecnología móvil, el fabricante de seguridad Kaspersky durante el año 2016 identificó que la tendencia de los usuarios en el uso de su dispositivo móvil era principalmente actividades que incluían el uso de correo electrónico para personas de generación X y aplicaciones de contenido social para personas que se encuentran dentro de la generación Millennials, también estaban dentro de sus actividades el uso de aplicaciones de banca y compras en línea.

Este estudio reveló también, que los usuarios utilizan los dispositivos móviles para cada aspecto de su vida, incluyendo el guardar dentro de estos información de carácter sensitivo, por

ejemplo, 9 de cada 10 usuarios almacenan dentro de los dispositivos datos privados sin que estos se encuentren cifrados o protegidos por una solución de seguridad, y en la mayoría de casos sin la autorización correspondiente para poder efectuar tal acción, la tabla 2 muestra que tipo de contenido es almacenado dentro de los dispositivos.

Tabla 2. Los consumidores de datos almacenan en diferentes dispositivos

Detalles	**Porcentajes**		
Fotos/videos/música/libros electrónicos	70%	62%	67%
Mensajes de correo electrónico personales	56%	51%	50%
Direcciones/Contactos telefónicos	50%	28%	55%
Archivos para uso personal	46%	44%	26%
Contraseñas para cuentas de correo electrónico personales	36%	31%	28%
Contraseñas para cuentas personales en línea (Ejemplo: Redes sociales, foros, etc.)	34%	29%	27%
Mensajes/Conversaciones enviadas a través de mensajes de aplicaciones como Whatsapp	34%	14%	42%
Archivos para uso laboral	32%	31%	18%
Mensajes de correo electrónico para uso laboral	29%	25%	26%
Detalles de cuentas de juegos	25%	20%	22%
Detalles bancarios	24%	21%	17%
Información sensitiva/Información personal que no quiero que otras personas vean	22%	18%	16%
Otras credenciales de pago	21%	18%	13%
Contraseñas para cuentas de correo electrónico del trabajo	19%	16%	15%
Contraseñas para VPN del trabajo/Acceso a intranet	11%	9%	9%
Alguna información financiera	44%	39%	35%
Alguna contraseña	57%	53%	49%
Alguna información privada	87%	83%	88%
	Cualquier dispositivo	Computadora	Dispositivo móvil

Fuente: (Kaspersky, 2016a)

Otro hecho a destacar dentro de este esquema, son las estadísticas que muestran lo vulnerable que son los dispositivos móviles a la hora de ser víctimas de ataques cibernéticos y delitos como el robo o pérdida física de los aparatos, quedando la información sensitiva bajo peligro de ser expuesta ante terceros, el estudio de Kaspersky en la tabla 3 muestra precisamente que los principales ataques cibernéticos tienen como propósito conseguir este tipo información (Kaspersky, 2016b).

Tabla 3. Detalles solicitados por los ciberdelincuentes

Detalles	Total	16 a 24	25 a 34	35 a 44	45 a 54	55 en adelante
Información de pago	**34%**	29%	36%	35%	30%	43%
Acceso de banca en línea	**32%**	22%	30%	40%	39%	36%
Información personal privada como dirección y fecha de nacimiento	**30%**	34%	27%	29%	34%	27%
Acceso a correo electrónico	**27%**	28%	28%	34%	22%	18%
Acceso a redes sociales	**24%**	24%	27%	30%	18%	9%
Acceso a sitios de compras	**17%**	17%	22%	19%	12%	9%
Acceso a mensajería instantánea y comunicación	**15%**	15%	18%	21%	12%	2%
Algún otro tipo de información privada/información sensible	**15%**	16%	15%	12%	11%	19%
Acceso a cuentas de juego	**14%**	15%	18%	15%	8%	2%

Fuente: (Kaspersky, 2016a)

Según un estudio realizado por la casa consultora Kensington y documentado por la revista especializada en tecnología ChannelPro Network (2012) el extravío o robo físico de los aparatos móviles resulta en pérdidas de datos o información que resulta mucho más costosa que el valor del aparato en sí, la perdida de datos va desde información confidencial hasta incluso propiedad intelectual, según este estudio la pérdida de un dispositivo incluye, el tiempo de inactividad, soporte y mantenimiento con un excedente de hasta 49,000.00 US$. Otros datos interesantes son:

- Una portátil es robada cada 53 segundos.
- 70 millones de teléfonos inteligentes son perdidos cada año, recuperándose únicamente el 7%.
- El 80% de los costos involucrados en la pérdida de computadoras o dispositivos portátiles corresponden a información sensitiva de las compañías que ha sido robada.
- 52% de los dispositivos son robados de la oficina o lugar de trabajo y un 24% de lugares de conferencias.

2.4 Madurez de BYOD a Nivel Internacional

De la misma forma como la amenaza ante la pérdida de información confidencial almacenada en dispositivos móviles ha evolucionado, lo ha hecho también los diferentes mecanismos para asegurar dicha información. El avance en el diseño de los dispositivos móviles y sumado a esto el progreso en el desarrollo de los diferentes sistemas operativos, interfaces y

ambientes colaborativos ha hecho surgir un nuevo reto en el campo de las tecnologías de la información, poder retomar el control sobre el acceso a la información confidencial.

De acuerdo al estudio anual realizado por la consultora Gartner a través del consultor David A. Willis (2014) hasta el 2013 todavía muchos Gerentes de Seguridad de la Información no entendían los beneficios de adoptar políticas para BYOD, y aparentemente había mucha mayor aceptación en los Estados Unidos que en Europa sobre esta metodología, los principales motivos por los cuáles la transición hacia políticas BYOD no fluía con mayor rapidez eran los siguientes:

1. **Resistencia Personal**: Los empleados tienden a pensar que, al someter sus dispositivos a políticas empresariales, estas pudieran invadir su espacio familiar o personal.
2. **Costos**: La empresa tiene costos que asumir para poder brindar la conectividad segura a los dispositivos de sus empleados, entre estos, licenciamiento, soporte, configuración y mantenimiento. En muchas ocasiones la alta dirección no ve como estos costos pueden convertirse en algo productivo para la compañía.
3. **Seguridad**: Es evidente que todo dato consultado por un dispositivo ajeno a la organización resulta en pérdida de control por parte de la empresa ante dicha información, es necesario adoptar también un nivel de confianza sobre el empleado.

Los datos del estudio de Gartner sobre la adopción de BYOD son los mostrados en la tabla 4.

Tabla 4. Adopción de BYOD

	U.S	U.K	Canada	Brazil	Russia	India	China
Computadora de escritorio	47%	38%	47%	56%	10%	55%	54%
Computadora portatil	41%	32%	41%	57%	7%	68%	56%
Celular estándar	33%	29%	27%	50%	36%	84%	78%
Smartphone	55%	38%	47%	71%	5%	85%	76%

Fuente: (Gartner, 2014b)

2.5 BYOD 1.0

Al inicio del marco teórico se explicaba que la adopción de BYOD iba más allá de reforzar los algoritmos de autenticación de la red inalámbrica de una empresa, en el año 2009 BYOD consistía básicamente de dos componentes principales, un Administrador de dispositivos móviles (MDM por sus siglas en inglés) y un dispositivo de administración de Redes Privadas Virtuales (VPN por sus siglas en inglés):

1. El MDM se encarga de poder administrar y asegurar los dispositivos que se conectan a la red, incluyendo una pequeña protección para los datos que se almacenan en el dispositivo.
2. El segundo componente, crea un túnel que encripta la comunicación del dispositivo con la red corporativa, proveyendo una capa de seguridad al tráfico que fluye desde el dispositivo hacia la red corporativa.

Esta idea contiene altos niveles de seguridad, sin embargo, se enuncian algunos inconvenientes de la misma:

1. Se requiere un sacrificio tanto del empleador como del empleado; el primero pierde control sobre información sensitiva y el segundo pierde privacidad de sus datos personales, y se expone al riesgo de que estos sean eliminados.
2. Aunque existe la posibilidad de tener acceso remoto seguro a la red corporativa, no se tiene forma de controlar la información almacenada en el dispositivo, es por ello que una vez saliendo de la organización, los datos quedan a juicio del empleado.
3. No se contaba con un modelo de protección para los dispositivos contra Malware, Virus u otros contenidos perjudiciales para el dispositivo y perjudiciales para la organización.
4. No existía forma de poder manejar los dispositivos que habían sido perdidos o robados, teniendo como resultado la perdida de la información almacenada en dichos dispositivos.

Para poder mitigar algunas de las carencias de esta versión inicial de BYOD, muchos de los fabricantes de soluciones de seguridad perimetral optaron una arquitectura de acceso seguro como se muestra en la figura 1, agregando a sus equipos algún tipo de solución que permitiera tanto el monitoreo de dispositivos conectados a la red corporativa como políticas que de alguna manera protegieran contra amenazas latentes como malware o ransomware, permitiendo además controlar el uso de aplicaciones restringidas dentro del ámbito corporativo.

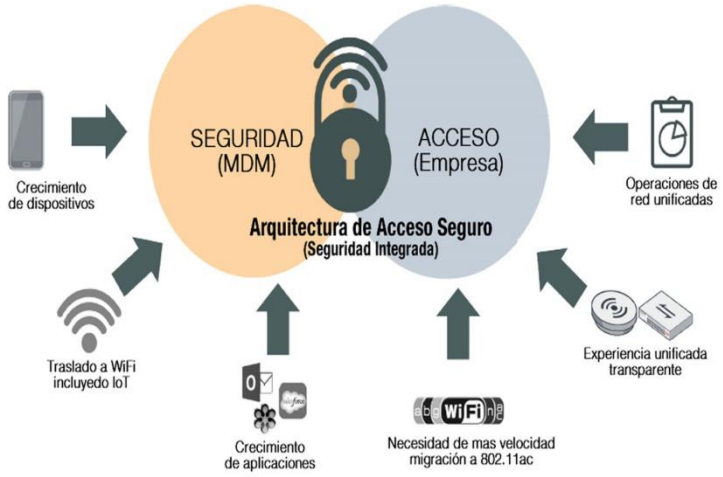

Figura 1: Solución segura de acceso

Fuente: (FORTINET INC., 2017)

En resumen, BYOD 1.0 es el primer intento de la industria para poder solventar problemas relacionados con dispositivos móviles personales y el manejo de la información corporativa, ciertamente el enfoque a nivel de dispositivo tiene sus inconvenientes, pero es precisamente el poder fortalecer el esquema lo que ha hecho evolucionar hacia BYOD 2.0 agregando un nuevo marco de referencias que envuelve las aplicaciones corporativas dentro de una capa adicional de seguridad.

2.6 BYOD 2.0

Un informe de la firma consultora Forrester dirigida por el analista Thomas Brownlee (2013) mostraba los avances de BYOD durante el año 2016, estos avances muestran un resurgimiento de BYOD ya no como una necesidad impuesta por parte de gobierno TI

(Tecnologías de la Información), sino más bien como una solicitud o requerimiento por parte del usuario final, sin embargo a pesar de esa exigencia por parte del usuario, los diferentes Jefes de TI (CIO por sus siglas en inglés) han logrado ver que aún hay detalles que faltan por afinar para que BYOD se convierta en algo ideal, entre ellos los siguientes factores:

- BYOD todavía no es escalable; hay demasiados procesos ineficientes y que se ejecutan de forma manual.
- Las políticas de BYOD requieren una mejor automatización para hacerlas más eficientes.
- No hay una adecuada visualización de los costos que involucra ejecutar un proyecto BYOD en la organización.
- A pesar de los avances no existe todavía una visualización adecuada del comportamiento del usuario final.

Desde el año 2013 hasta la fecha, muchos de estos factores mencionados anteriormente han ido sido despejados por los principales actores en el funcionamiento de BYOD 2.0, de manera que una solución completa de BYOD consiste en que cumpla con los siguientes requisitos sumados a los vistos en BYOD 1.0:

1. Que cuente con políticas que abarquen cada aspecto del uso de las herramientas corporativas sin que estas afecten los datos personales o privados de los usuarios.
2. Las soluciones BYOD deben ser multiplataforma y con una administración centralizada.
3. Los dispositivos que se conecten a la red corporativa deberán ingresar a un ambiente aislado usado como medida de seguridad, bloqueando el acceso a características no deseables, aplicaciones y juegos.
4. Las soluciones deben incorporar un rastreo en tiempo real y reportes que muestre la información de cada dispositivo y el comportamiento del mismo
5. Las soluciones deben contar con la capacidad de poder bloquear el acceso a información corporativa o acceso aplicaciones de la empresa si los dispositivos han sido robados o han sido extraviados.

6. La solución BYOD no debe estar ahora limitada a los dispositivos que son agregados a la red corporativa, sino más bien debe abarcar a aquellos dispositivos que son llevados fuera de la organización y que se conectan externamente a los recursos informáticos de la organización.

2.7 Evolución de BYOD en Honduras

Para conocer en detalle cual ha sido la evolución del BYOD en Honduras es necesario primero conocer el mercado de dispositivos móviles en América Latina especialmente en los llamados mercados emergentes, de acuerdo al estudio realizado por (GSMA, 2016) se espera que hacia el año 2020, el crecimiento de suscriptores de dispositivos móviles alcance los 100 millones de suscriptores, convirtiéndose Latinoamérica en una de las regiones con mayor crecimiento en el mundo, por ejemplo, para el mercado de Smartphones se prevé que para el año 2020 la región cuente con alrededor de 260 millones de conexiones de Smartphones más que los existentes a finales del año 2015.

Algo muy importante a considerar es que la tecnología móvil ha contribuido al mejoramiento de la productividad y eficiencia de los empleados y empresas, por lo menos de tres (3) maneras diferentes:

1. Por una parte, los servicios básicos de voz y texto impulsan un ambiente más colaborativo haciendo que la comunicación sea más efectiva agilizando la productividad.
2. El avance de tecnologías 3G y 4G hace más eficiente el acceso a la información con beneficios en sectores como, por ejemplo, la agricultura, salud, educación y finanzas.
3. A pesar que Centroamérica se ve rezagada en comparación con el resto de Latinoamérica en el uso de servicios móviles, se espera que durante los próximos cuatro años generen beneficios en la reducción de costos y un incremento en la eficiencia de áreas como fabricación, logística y ventas.

De acuerdo al estudio realizado por GSMA Intelligence en Latinoamérica el uso de tecnología móvil provocó un ingreso de alrededor de 250,000 millones de dólares de valor agregado, equivalente al 5% del PIB (Producto Interno Bruto) de la región. En el caso de

Honduras contaba hasta el año 2016 con 5.3 millones de suscriptores de telefonía, de los cuales 3.1 millones corresponden a Smartphones con la capacidad de conectarse a banda ancha e internet (CONATEL, 2017).

Algunas razones por las cuáles el aumento de dispositivos móviles y la inclusión de tecnologías como 3G y 4G se han visto frenados en territorio hondureño han sido las siguientes:

1. El cargo a la que se ven sometidos los proveedores de servicio por llamadas internacionales entrantes.
2. Aporte de tasa de seguridad a los servicios móviles recauda por la ATIC.
3. Aporte al FITT (Fondo de Inversiones de Telecomunicación y Tecnologías de la información) recaudado por CONATEL.

El incremento del uso de los dispositivos móviles también ha sido el catalizador de muchos proyectos de gran utilidad a la sociedad hondureña, por ejemplo, los operadores móviles en conjunto con CONATEL (Comisión Nacional de Telecomunicaciones) y el Ministerio de Educación están implementando el uso de una plataforma de Contenidos Educativos Digitales con difusión en el sistema público de educación del país, potenciando la inclusión social y robusteciendo el sistema educativo con un contenido virtual estructurado y apegado al plan de estudios del país.

A la par del crecimiento del segmento de redes tecnológicas y del sector de dispositivos móviles inteligentes ha ido el desarrollo de servicios que han aportado inclusión digital a la ciudadanía hondureña, uno de las aplicaciones pioneras al respecto ha sido la desarrollada por la empresa Millicom, desde 2013 ha lanzado al mercado hondureño una aplicación financiera llamada Tigo Money, la cual ofrece diversos servicios que van desde el pago de sueldos, asistencia financiera proveniente de organizaciones no gubernamentales hasta el desarrollo de la economía del país mediante diversos servicios financieros como créditos, remesas o pólizas de seguro, esto ha brindado a los beneficiarios una poderosa primera experiencia e interacción con la tecnología.

Lo mismo puede decirse de las diversas aplicaciones para dispositivos móviles que han surgido durante los recientes años en el mercado local, que han fomentado en el ciudadano promedio la capacidad de poder interactuar con la tecnología, de manera que un hondureño común puede hoy en día desplazarse por los diferentes servicios que necesita para poder realizar sus actividades diarias, desde leer un periódico nacional, poder efectuar tareas financieras, actividades de tributación u otros trámites gubernamentales hasta poder interactuar con diversas herramientas relacionadas con el lugar en el cuál labora.

Es precisamente esta habituación en el ciudadano promedio lo que ha hecho necesario cuestionar, si se cuenta en el país con una metodología para poder proteger las diversas actividades que realiza cada habitante que hace uso de un dispositivo móvil en los diferentes servicios prestados, y además, si las instituciones financieras gubernamentales han fomentado una política que vaya de acuerdo a las mejores prácticas de seguridad de la información en el contenido que ven sus empleados en los diferentes dispositivos móviles.

2.8 BYOD y Estándares de Seguridad

El activo más valioso de toda empresa es la información, es por ello que las empresas aplican controles rigurosos para evitar que esta sea robada. Pero cuando las empresas se enfrentan a la necesidad de adaptarse a un entorno tecnológico que permite conectar dispositivos móviles como teléfonos inteligentes y tabletas a sus redes internas y desde internet, se vuelve un riesgo potencial para la perdida de información.

El nuevo entorno de transferencia de información considera que los estándares de seguridad deben aplicarse no solo a los dispositivos propios de la institución, sino también a aquellos dispositivos móviles personales de los empleados y que utilizan para estar conectados a los servicios informáticos de la institución.

Los estándares de seguridad son genéricos y cada empresa los adopta de acuerdo a su necesidad, y para controlar los dispositivos móviles personales deben de existir una política institucional, que esté aprobada por el directorio o junta directiva de la institución, Entre los estándares de seguridad para BYOD se consideran elementos del ISO27000, ITIL, COBIT y

componentes de estándares de referencias y cumplimiento como, por ejemplo, PCI-DSS, SOX o COSO. Para poder determinar dentro que estándares o plataformas de control son las adecuadas para poder proteger la información accedida por los dispositivos móviles, es necesario que se determine lo que se entiende por un dispositivo móvil encajado dentro de la terminología de BYOD.

¿Qué es un Dispositivo Móvil?

Para propósito de este estudio determinamos que, dispositivos móviles son todos aquellos aparatos tales como:

- Smartphones o teléfonos inteligentes
- Laptops o computadoras portátiles
- Tablets o tabletas digitales
- Asistentes Digitales Portables (PDA)
- Dispositivos portables dotados de almacenamiento y con un puerto USB (Universal Serial Bus), como, por ejemplo, reproductores MP3, tarjetas módems con capacidad de conexión de WIFI, Bluetooth, EDGE/GPRS/3G
- Cámaras digitales
- Dispositivos con capacidad de identificación de radio frecuencia, para almacenamiento de datos y administración e identificación de activos.

En pocas palabras son todos aquellos dispositivos que pueden brindar al usuario la oportunidad de acceder a la información y recursos de la empresa sin necesidad de estar conectado a la red de la empresa o permanecer dentro de los ámbitos físicos de la misma.

Es precisamente esta portabilidad la que puede convertir a los dispositivos móviles en una amenaza y un riesgo a la postura de seguridad de la empresa, en la mayoría de casos el riesgo de seguridad es causado por las vulnerabilidades que un dispositivo puede presentar y ser susceptible ante ataques maliciosos, por otra parte, es importante recordar que mucha de la información almacenada sin el debido control y sin estar cifrada puede ser interceptada fácilmente, y además de la fuga de información los dispositivos móviles sin control pueden ser un motivo de propagación de malware (del inglés “malicious software) a la red corporativa.

Los riesgos de utilizar dispositivos móviles para utilizar herramientas corporativas son abundantes, y en la mayoría de los casos poder gestionar el control de la información manipulada por los mismos requerirá del uso de capas adicionales de protección y acceder al uso de herramientas de encripción de terceros. A continuación, la tabla 5 presenta vulnerabilidades conocidas, amenazas asociadas y los riesgos que necesitan ser entendidos a la hora de lidiar con dispositivos móviles en una empresa.

Tabla 5. Vulnerabilidades, amenazas y riesgos conocidos en dispositivos móviles

Vulnerabilidad	Amenaza	Riesgo
Es más inseguro enviar información por redes inalámbricas que hacerlo por una red cableada.	Un intruso puede causar daño a la información de la empresa.	La intercepción de información puede resultar en brechas de datos sensitivos, dañar la reputación de la empresa o enfrentarla a acciones legales.
La movilidad ofrece a los usuarios la oportunidad de alejarse de los límites de la empresa y dejar atrás muchos controles de seguridad.	Los dispositivos móviles que cruzan los límites y el perímetro de la red, pueden transportar y propagar malware en la red.	La propagación de malware, puede resultar en pérdida o fuga de información y corrupción de los datos, haciendo imposible el acceso a ellos.
La tecnología Bluetooth es muy conveniente para que los usuarios puedan tener conversaciones con manos libres, sin embargo, si se deja encendida puede ser fácilmente detectable.	Un atacante puede descubrir un dispositivo y lanzar un ataque.	Corrupción del dispositivo, pérdida de datos, interceptación de llamadas, posible exposición de información sensible.
Información sin cifrar es almacenada en el dispositivo.	En el evento que alguien externo intercepte la data en tránsito o que robe el dispositivo, o que el empleado pierda el dispositivo, los datos pueden ser leídos y usados sin dificultad.	Exposición de datos sensitivos puede resultar en daño a los clientes, empleados y la empresa.
La pérdida de datos puede afectar la productividad del empleado o resultar en costos considerables a la empresa.	Los dispositivos móviles pueden ser fácilmente robados o perdidos por su portabilidad. La información almacenada en esos dispositivos no siempre es recuperable.	Los trabajadores dependientes de la información en el móvil, no podrán trabajar si este fuera robado o extraviado.
El dispositivo no tiene requerimientos de autenticación aplicados.	Si el dispositivo es extraviado o robado, un extraño puede acceder al dispositivo y a toda la información.	La intercepción de información puede resultar en brechas de datos sensitivos, dañar la reputación de la empresa o enfrentarla a acciones legales.
La empresa no administra el dispositivo.	Si no existe una estrategia para dispositivos móviles, los empleados pueden optar por traer sus propios dispositivos no garantizados. Y aunque no accedan a la red corporativa, pueden interactuar con correo	Fuga de datos, propagación de malware puede ocurrir en caso de pérdida o robo del dispositivo.

Vulnerabilidad	Amenaza	Riesgo
	electrónico o almacenar documentos confidenciales.	
El dispositivo permite la instalación de aplicaciones de terceros no firmadas digitalmente.	Las aplicaciones pueden transportar malware, virus o troyanos y pueden convertir el dispositivo en una puerta hacia intrusos que deseen ingresar a la red corporativa.	Propagación de malware, fuga de datos o intrusión a la red corporativa.

Fuente: (ISACA, 2010a)

En las secciones anteriores de este capítulo se mostraba como los dispositivos móviles se han convertido en un activo muy valioso en las operaciones de las empresas, es muy importante además de conocer los diferentes riesgos, saber cómo manejarlos, evitarlos y en la medida de lo posible, mitigarlos. Algo a tomar en consideración es que debido al constante desarrollo y evolución de los dispositivos móviles es necesario crear estrategias que ayuden a asegurar que los riesgos son contabilizados y administrados de la forma apropiada independientemente de la versión, modelo y tipo de dispositivo.

Por otro lado es importante que el Jefe de Seguridad de la Información (CISO por sus siglas en inglés) de cada institución se encargue de establecer la seguridad de dispositivos móviles como parte de la cultura organizacional de la empresa, además será necesario establecer un plan estratégico que no solamente se encargue de crear valor para la institución sino que además se encargue de mitigar los riesgos que pongan en peligro el activo más valioso con el que cuentan una institución, en este caso, la información de cómo opera el negocio, los diferentes procesos del mismo y la información procesada.

Como menciona la Asociación de Auditoría y Control de Sistemas de Información en su informe de seguridad de dispositivos móviles, una estrategia empresarial siempre deberá contener una política que contenga un ciclo de vida completo de soporte, conformado por controles de seguridad que incluyan autenticación de doble factor, cifrado de datos, integridad de las aplicaciones, y un servicio que permita la trazabilidad completa de los dispositivos móviles en el uso de las aplicaciones de la empresa y lo más importante es que no estará sujeta a los límites

físicos de la empresa, sino con la capacidad de monitorear y proteger la información y uso de las aplicaciones aun fuera del ámbito de la empresa (ISACA, 2010b) .

Esta política de seguridad deberá contener los siguientes elementos:

- Deberá ser una política aplicable a una variedad de dispositivos, independientemente de su tipo, versión y sistema operativo.
- El control de dispositivos deberá ser administrado centralmente por el personal designado por la empresa.
- La política de seguridad debe ser simple y fácil de implementar y brindar soporte.
- Debe ser flexible para los usuarios administradores, usuarios finales y dispositivos.
- Enfocada en la protección de la información en caso de robo o extravío de los dispositivos móviles.
- Auditable en todas sus partes.
- Deberá contener un protocolo de pruebas que incluya verificación o recuperación de datos en caso de desastre.

Es importante tener en cuenta que el poder desplegar el uso de dispositivos móviles dentro de cualquier organización no puede ser tomado como un asunto explícitamente técnico, recordemos que una brecha de seguridad puede afectar el desempeño de las labores del empleado, el flujo de información organizacional y los procesos del negocio, una manera de visualizar las estrategias ante los riesgos puede ser la presentada en la tabla 6:

Tabla 6. Riesgos y estrategias en el uso de dispositivos móviles

Riesgo	Estrategias
Un dispositivo extraviado o robado	Implementar una consola de administración central para el control remoto de dispositivos, poder dar seguimiento de ubicación, borrado de datos, cambio de contraseña o autenticación, asegurándose que la información en los dispositivos móviles esté cifrada y sea inutilizable en caso de pérdida o robo.
Proveer soporte para varios dispositivos	Recurrir a gestores de dispositivos móviles administrados de forma centralizada y multiplataforma.
Controlar el flujo de datos en múltiples dispositivos	Asegurar los sistemas que son accedidos con autorización, control de privilegios y mecanismos de

	encripción.
Evitar que los datos se sincronicen en dispositivos móviles de una manera no autorizada	Monitorear y restringir las transferencias de datos en cualquier tipo de dispositivo desde una consola centralizada.
Mantenerse al día con el uso de los últimos modelos de dispositivos	Crear conciencia de los usuarios sobre los activos de información, los riesgos y el valor para la empresa.
Promover la responsabilidad y transparencia con el uso de dispositivos móviles.	Dar seguimiento a la forma en que se utilizan dispositivos, y proporcionar retroalimentación regular a la gestión.
Demostración del cumplimiento normativo	Implementar una consola de administración central para gestionar todas las etapas de la gestión de activos, desde la instalación hasta su retiro

Fuente: (ISACA, 2010a)

2.9 Comparativas entre Normativas

En el desarrollo del marco teórico se ha podido observar lo importante que es que una organización cuente con políticas de seguridad para dispositivos móviles, sin embargo, un reto importante a considerar por la mayoría de las organizaciones es saber cuál normativa aplicar, como se explicaba al inicio BYOD contiene elementos de estándares como, por ejemplo, ISO27000, ITIL, COBIT y componentes de estándares de cumplimiento como, por ejemplo, PCI-DSS, SOX o COSO. En esta sección se considerará brevemente las diferencias entre las normativas existentes más populares y se brindará un marco de referencia a seguir por parte de las IGSFH para implementar BYOD en base al estándar de seguridad ISO 27002. Basándose en el estudio realizado por los investigadores Ali, Soomro, & Brohi en artículo científico sobre mapeo de los diferentes estándares de tecnología en el año 2013 las similitudes y diferencias de los principales marcos son las brindadas a continuación.

2.10 Estándar de Seguridad ISO 27000

2.10.1 Utilidad

Usados en conjunto ISO 27001 e ISO 27002 permiten desarrollar un plan para implementar un sistema de gestión de seguridad de la información con el fin de adoptar controles de seguridad en la organización.

2.10.2 Propósito de Uso

Ayuda a cualquier organización a seleccionar las medidas de seguridad apropiadas, utilizando para ello catorce (14) dominios de controles de seguridad que proporcionan más orientación sobre como una organización puede implementar la normativa.

2.10.3 Fortalezas de ISO 27000

La fortaleza de ISO 27000 es que las organizaciones pueden optar por implementar solo las estrategias de seguridad necesarias para su organización y con la flexibilidad de poder adaptarlas si los procesos cambian con el tiempo o si se necesita una mayor cobertura de seguridad.

2.10.4 Debilidades de ISO 27000

La debilidad de ISO 27000 radica en el hecho que maneja una visión muy amplia de los estándares de seguridad y no brinda requisitos concretos que ofrezcan a la organización una mayor orientación sobre la implementación de las estructuras de seguridad para cumplimiento del estándar, lo que puede obligar a la organización a un mayor esfuerzo para una comprensión profunda de los pasos que deben tomar para proteger su información vulnerable y someterse a obtener una amplia habilidad técnica con el fin de seguir las directrices establecidas.

2.10.5 Acreditación o Certificación

No existe una certificación ISO 27000 directa, una organización utiliza el marco ISO 27002 para definir e implementar las estrategias que conducirán a la infraestructura de la seguridad de la información para poder optar a la certificación ISO 27001. ISO 27000 es un marco que se utiliza en todo el mundo desarrollado originalmente por la British Standards Institution.

2.10.6 En que Ocasiones Utilizar ISO 27000

El marco ISO 27000 debe elegirse cuando una organización está buscando una arquitectura de seguridad de la información que proporcione medidas genéricas de seguridad, también cuando se necesite la orientación para certificarse con el estándar de cumplimiento de ISO 27001, lo que

puede conducir a una garantía mayor de seguridad para la organización o un cumplimiento necesario con las leyes que la organización está operando.

2.11 Marco de Referencia COBIT

2.11.1 Utilidad de COBIT

El marco COBIT proporciona orientación para poder alinear los procesos de TI a los objetivos y necesidades del negocio. Esto se hace abordando las tareas de TI con una base amplia utilizando para ello objetivos específicos de control.

2.11.2 Propósito de Uso de COBIT

El marco COBIT está formado por más de cincuenta fuentes de buenas prácticas de múltiples organizaciones de estándares internacionales, que se especializan en tratar de vincular la gobernanza de TI con la gobernanza empresarial, estas se utilizan con el objetivo de automatizar los servicios de TI tanto como sea posible, sin la pérdida de la gobernanza en todo el entorno empresarial. Para la implementación de COBIT se utiliza el llamado círculo de procesos COBIT (PDCA), un ciclo que incluye criterios de información, planificación y organización, adquisición e implementación, entrega y soporte, monitoreo.

Con este modelo las empresas pueden dividir sus prácticas en subsecciones de la meta general y utilizar la escala de calificación COBIT la cuál al final puede brindar un panorama que ofrezca un plan de acción claro.

2.11.3 Fortalezas de COBIT

La principal fortaleza del marco COBIT es su fuerte vinculación entre los objetivos de negocio en conjunto con el marco de TI de la organización. Por otro lado, COBIT también tiene un gran enfoque hacia los objetivos de una organización y las acciones para poder alcanzarlos, lo que incluye operaciones de negocios diarios, fusiones y seguridad de la información. Con esto, COBIT crea un entorno de gestión de la información persistente que asegura soluciones de TI alineadas a los negocios y afianza que los objetivos de una organización estén a la vanguardia de todos los empleados.

2.11.4 Debilidades de COBIT

Una de las debilidades más evidentes del marco es la falta de enfoque en cómo lograr los objetivos necesarios para el cumplimiento de COBIT en la organización. Además, dicho marco puede ser difícil de implementar debido a la necesidad de que todos los interesados participen en la creación y gestión del mismo. Algo a tomar en cuenta es que preferiblemente este marco debe ser implementado mientras la organización es bastante pequeña o se necesitará reservar un tiempo significativo para identificar y crear todos los pasos necesarios para realizar plenamente el marco COBIT.

2.11.5 Acreditación o Certificación

Con el fin de convertirse en una empresa acreditada como COBIT es necesario que dentro de la organización existan empleados que hayan asistido a un curso certificado COBIT. No existe certificación o estándar de cumplimiento, sin embargo, COBIT es un marco normativo y legislativo, mundialmente reconocido y producido por ISACA.

2.11.6 Cuando Utilizar COBIT

El marco COBIT debe ser elegido cuando una organización necesita entender y alinear los objetivos de negocio y TI para crear un plan de seguridad eficaz que impregne todos los aspectos de una organización. COBIT tendrá una presencia persistente que reducirá los gastos generales a largo plazo, pero una empresa puede tener dificultades para implementar este marco sin revisar sus prácticas de información.

2.12 Marco de Referencia NIST

2.12.1 Utilidad de NIST

NIST se utiliza para proporcionar documentación que describe un nivel mínimo de requisitos para la seguridad de la información para las agencias federales del gobierno de los Estados Unidos. El propósito es establecer recomendaciones para la implementación de los requisitos establecidos en la Ley Federal de Administración de la Seguridad de la Información

(FISMA por sus siglas en inglés) de 2002. El marco del NIST debe usarse junto con un programa de seguridad de la información en profundidad.

2.12.2 Propósito de Uso

El marco del NIST fue creado como una base de controles en el entorno de seguridad de la información federal cubriendo tres (3) niveles principales: Técnico, Gerencial y Operacional. Estos controles aseguran que se siga el ciclo de seguridad de información requerido para los servicios de información federales. El ciclo de vida consiste en iniciación, adquisición, desarrollo, implementación, evaluación, operación, mantenimiento y disposición.

2.12.3 Fortalezas de NIST

La principal fortaleza de NIST es el catálogo de documentación adquirido, el cual puede utilizarse para implementar un sólido entorno de seguridad dentro de una organización, ya que el NIST ha sido desarrollado para que las agencias gubernamentales estadounidenses aseguren la confidencialidad. NIST proporciona un nivel mínimo de requisitos que debe implementarse para un sistema de información seguro con el fin de crear la base necesaria para que una organización pueda mantener y garantizar la seguridad.

2.12.4 Debilidades de NIST

Una de las debilidades del marco del NIST es su falta de enfoque en cualquier aspecto de seguridad financiero, lo que puede hacer que no se tome en cuenta cuando se necesite buscar información de mejores prácticas de seguridad en una organización. Además, para evitar consumo innecesario de tiempo importante saber exactamente qué buscar, debido a la gran cantidad de información con que cuenta el catálogo del NIST.

2.12.5 Acreditación o Certificación

NIST únicamente ofrece pautas para cumplir con los sistemas de información federales y los requisitos, tales como FISMA. El cumplimiento de las directrices del NIST es obligatorio para las instituciones gubernamentales de los Estados Unidos, en otras palabras, NIST no cuenta con una certificación que pueda ser adquirida.

2.12.6 Cuando Utilizar NIST

El marco del NIST puede ser elegido cuando es necesaria una gestión mucho más profunda de los controles de seguridad de una organización. También es obligatorio utilizar NIST cuando una organización necesita cumplir con los requisitos del FISMA. A pesar de eso NIST puede ser utilizado por organizaciones grandes o pequeñas para ayudar a lograr una base segura para su información y debe ser utilizado en conjunto con un plan de seguridad.

2.13 Marco de Referencia ITIL

2.13.1 Utilidad de ITIL

El marco proporciona directrices sobre las mejores prácticas en el campo de la gestión de servicios de TI, reduce la dependencia de los servicios de proveedores centrándose en los procesos internos de tecnología de la información. Este marco se utiliza para mitigar los riesgos de los servicios de información que aún no han alcanzado un ciclo de vida maduro, centrándose en las necesidades de la base de clientes

2.13.2 Propósito de Uso

El propósito de ITIL está basado en el ciclo de vida del servicio, que consta de los procesos de estrategia del servicio, diseño del servicio, transición del servicio, operación del servicio y mejora continua del servicio, hay información oficial sobre cada componente del ciclo de vida del servicio que ha sido documentada con el fin de desarrollar un ambiente de gestión de servicios eficaz y eficiente para la prestación de servicios empresariales.

2.13.3 Fortalezas de ITIL

La fortaleza del marco ITIL es su repetitividad de los métodos de servicio desarrollados por el gobierno británico, centrándose en las tareas básicas orientadas hacia el futuro que se alinean con las necesidades del cliente. ITIL crea un lenguaje claro de comunicación para todas las partes involucradas con la utilización de los recursos de TI e intenta alinear las necesidades de esos recursos con los requisitos del negocio

2.13.4 Debilidades de ITIL

Puede haber una falta de enfoque organizacional en general y la metodología sólo puede utilizarse como parte de la adquisición de una certificación de calidad. A pesar de su uso a nivel mundial el marco ITIL no es reconocido como un estándar y carece de una comprensión en profundidad de los costos asociados con factores relevantes como las necesidades del cliente y su interacción con el negocio.

2.13.5 Acreditación o Certificación de ITIL

El marco ITIL fue creado por el gobierno británico para gestionar eficazmente los recursos de TI. Este marco no es un estándar. En cambio, una organización si puede utilizar la información proporcionada en la documentación de ITIL para desarrollar e implementar un plan para lograr la certificación ISO / IEC 20000.

2.13.6 Cuando Utilizar ITIL

El marco de ITIL debe ser elegido cuando la calidad del servicio necesita ser mejorada en los servicios de gestión de TI de una organización. Este marco le da a una empresa una metodología que ayudan a que administrar las tareas cotidianas, especialmente cuando el objetivo es lograr la satisfacción del cliente o usuario final.

De acuerdo al informe del 2014 del National Institute of Standards and Technology, llamado Marco para la Mejora de la Ciberseguridad de las Infraestructuras Críticas, un marco núcleo de seguridad está basado cinco funciones concurrentes y continuas que consisten en las acciones de identificar, proteger, detectar, responder y recuperar. Cada función contiene las áreas a proteger y las acciones a realizar de una manera categorizada, si se realiza un mapeo entre este marco y los diferentes estándares de seguridad estudiados y orientados al tema de BYOD se obtiene lo presentado en la tabla 7:

Tabla 7. Marco núcleo de ciberseguridad

Función	Categoría	Subcategoría	Referencias
Identificar	Gestión de Activos (ID.AM): Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar objetivos de negocio se identifican y gestionan de acuerdo con su importancia relativa para los objetivos de negocio y la estrategia de riesgo de la organización.	ID.AM-1: Los dispositivos físicos y sistemas dentro de la organización son inventariados.	• CCS CSC 1 • COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Las plataformas de software y aplicaciones propiedad de la organización son inventariadas.	• CCS CSC 2 • COBIT 5 BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: Las comunicaciones y flujos de datos organizacionales son monitoreados.	• CCS CSC 1 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4 • ISO/IEC 27001:2013 A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
Proteger	Control de Acceso (PR.AC): El acceso a los activos e instalaciones asociadas está limitado a usuarios, procesos o dispositivos autorizados, ya las actividades y transacciones autorizadas.	PR.AC-3: Los accesos remotos deben ser administrados.	• COBIT 5 APO13.01, DSS01.04, DSS05.03 • ISA 62443-2-1:2009 4.3.3.6.6 • ISA 62443-3-3:2013 SR 1.13, SR 2.6 • ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1 • NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20
		PR.AC-5: Se debe proteger la integridad de la red, incorporando segregación donde sea apropiado.	• ISA 62443-2-1:2009 4.3.3.4 • ISA 62443-3-3:2013 SR 3.1, SR 3.8 • ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, SC-7

Función	Categoría	Subcategoría	Referencias
	Seguridad de Datos (PR.DS): La información y los registros (datos) se manejan de acuerdo con la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	PR.DS-1: Los datos almacenados deben ser protegidos.	• CCS CSC 17 • COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06 • ISA 62443-3-3:2013 SR 3.4, SR 4.1 • ISO/IEC 27001:2013 A.8.2.3 • NIST SP 800-53 Rev. 4 SC-28
		PR.DS-2: Los datos en tránsito deben ser protegidos.	• CCS CSC 17 • COBIT 5 APO01.06, DSS06.06 • ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 • ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 • NIST SP 800-53 Rev. 4 SC-8
		PR.DS-3: Los activos se gestionan formalmente durante la remoción, las transferencias y la disposición.	• COBIT 5 BAI09.03 • ISA 62443-2-1:2009 4. 4.3.3.3.9, 4.3.4.4.1 • ISA 62443-3-3:2013 SR 4.2 • ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 • NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16
		PR.DS-5: Protección contra fuga de información debe ser implementada.	• CCS CSC 17 • COBIT 5 APO01.06 • ISA 62443-3-3:2013 SR 5.2 • ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 • NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4

Función	Categoría	Subcategoría	Referencias
	Procesos y Procedimientos de Protección de la Información (PR.IP): Se mantienen y utilizan políticas de seguridad (que abordan el propósito, el alcance, las funciones, las responsabilidades, el compromiso de la administración y la coordinación entre las entidades organizacionales), procesos y procedimientos para administrar la protección de los sistemas y activos de información.	PR.IP-11: La ciberseguridad está incluida en las prácticas de recursos humanos (por ejemplo, despidos y selección de personal).	• COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 • ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 • ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4 • NIST SP 800-53 Rev. 4 PS Family
	Tecnología de Protección (PR.PT): Las soluciones de seguridad técnica se gestionan para garantizar la seguridad y la resistencia de los sistemas y activos, de acuerdo con las políticas, procedimientos y acuerdos relacionados.	PR.PT-2: Los medios extraíbles están protegidos y su uso está restringido según la política.	• COBIT 5 DSS05.02, APO13.01 • ISA 62443-3-3:2013 SR 2.3 • ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 • NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7
		PR.PT-4: Las comunicaciones y redes de datos están protegidas.	• CCS CSC 7 • COBIT 5 DSS05.02, APO13.01 • ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 • ISO/IEC 27001:2013 A.13.1.1, A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7
Detectar	Monitoreo Continuo de Seguridad (DE.CM): El sistema de información y los activos son monitoreados a intervalos discretos para identificar eventos de ciberseguridad y verificar la efectividad de las medidas de	DE.CM-4: Código malicioso es detectado.	• CCS CSC 5 • COBIT 5 DSS05.01 • ISA 62443-2-1:2009 4.3.4.3.8 • ISA 62443-3-3:2013 SR 3.2 • ISO/IEC 27001:2013 A.12.2.1 • NIST SP 800-53 Rev. 4 SI-3

Función	Categoría	Subcategoría	Referencias
	protección.	DE.CM-5: Código móvil sin autorización es detectado.	• ISA 62443-3-3:2013 SR 2.4 • ISO/IEC 27001:2013 A.12.5.1 • NIST SP 800-53 Rev. 4 SC-18, SI-4. SC-44
		DE.CM-6: Se supervisa la actividad del proveedor de servicios externos para detectar posibles eventos de ciberseguridad.	• COBIT 5 APO07.06 • ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 • NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-8: Escaneos de vulnerabilidad son realizados.	• COBIT 5 BAI03.10 • ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 • ISO/IEC 27001:2013 A.12.6.1 • NIST SP 800-53 Rev. 4 RA-5
Responder	Planificación de Respuesta (RS.RP): Los procesos y procedimientos de respuesta se ejecutan y mantienen para asegurar la respuesta oportuna a eventos de ciberseguridad detectados.	RS.RP-1: El plan de respuesta es ejecutado durante o después de un evento.	• COBIT 5 BAI01.10 • CCS CSC 18 • ISA 62443-2-1:2009 4.3.4.5.1 • ISO/IEC 27001:2013 A.16.1.5 • NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
	Comunicaciones (RS.CO): Las actividades de respuesta se coordinan con las partes interesadas internas y externas, según proceda, para incluir el apoyo externo de los organismos encargados de hacer cumplir la ley.	RS.CO-2: Los eventos se reportan de acuerdo con los criterios establecidos.	• ISA 62443-2-1:2009 4.3.4.5.5 • ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 • NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8
		RS.CO-3: La información se comparte con los planes de respuesta.	• ISA 62443-2-1:2009 4.3.4.5.2 • ISO/IEC 27001:2013 A.16.1.2 • NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
	Análisis (RS.AN): El análisis se realiza para asegurar una respuesta adecuada y apoyar las actividades de recuperación.	RS.AN-1: Se investigan las notificaciones de los sistemas de detección.	• COBIT 5 DSS02.07 • ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • ISA 62443-3-3:2013 SR 6.1 • ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 • NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4

Función	Categoría	Subcategoría	Referencias
		RS.AN-3: Análisis forense es realizado.	• ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 • ISO/IEC 27001:2013 A.16.1.7 • NIST SP 800-53 Rev. 4 AU-7, IR-4
	Mitigación (RS.MI): Se realizan actividades para prevenir la expansión de un evento, mitigar sus efectos y erradicar el incidente.	RS.MI-1: Los incidentes son contenidos.	• ISA 62443-2-1:2009 4.3.4.5.6 • ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 • ISO/IEC 27001:2013 A.16.1.5 • NIST SP 800-53 Rev. 4 IR-4
		RS.MI-2: Los Incidentes son mitigados.	• ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 • ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 • NIST SP 800-53 Rev. 4 IR-4
		RS.MI-3: Las vulnerabilidades recientemente identificadas se mitigan o documentan como riesgos aceptados	• ISO/IEC 27001:2013 A.12.6.1 • NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5
	Mejoras (RS.IM): Las actividades de respuesta organizacional se mejoran incorporando las lecciones aprendidas de las actividades actuales y anteriores de detección / respuesta.	RS.IM-1: Los planes de respuesta incorporan las lecciones aprendidas.	• COBIT 5 BAI01.13 • ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 • ISO/IEC 27001:2013 A.16.1.6 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
Recuperar	Planificación de la Recuperación (RC.RP): Los procesos y procedimientos de recuperación se ejecutan y se mantienen para asegurar la restauración oportuna de sistemas o activos afectados por eventos de ciberseguridad.	RC.RP-1: El plan de recuperación se ejecuta durante o después de un evento.	• CCS CSC 8 • COBIT 5 DSS02.05, DSS03.04 • ISO/IEC 27001:2013 A.16.1.5 • NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8

Fuente: (National Institute of Standards and Technology, 2014b)

CAPÍTULO III. METODOLOGÍA

El objetivo de este capítulo es presentar la forma en que se llevará a cabo este trabajo de investigación, así mismo las razones por las cuales se escogieron los métodos de investigación seleccionados para contestar la pregunta de investigación.

3.1 Selección de las IGSFH

Las empresas privadas internacionales y nacionales, así mismo las gubernamentales son bastante celosas con la información que pueden proveer a este tipo de estudio. Y siendo que ambos maestrantes, quienes estuvimos desarrollando este estudio tenemos una relación laboral y profesional con el gobierno de Honduras, nos facilitó la obtención de la información requerida para este estudio.

Algunas instituciones gubernamentales, secretarías y comisiones hondureñas carecen de controles para la seguridad de la información almacenada en dispositivos móviles, lo que genera un riesgo a la información confidencial de cada institución. Se supone, por el conocimiento que se tiene de Honduras, que no todas las instituciones, secretarías y comisiones gubernamentales autónomas y semiautónomas están conscientes del riesgo que implican el BYOD, así mismo, que las instituciones que deberían estar más preocupadas con este tema son las instituciones de gobierno que tienen responsabilidad financiera/económica nacional e internacional (ver figuras 2 y 3), las cuales se mencionan a continuación: (López, 2014)

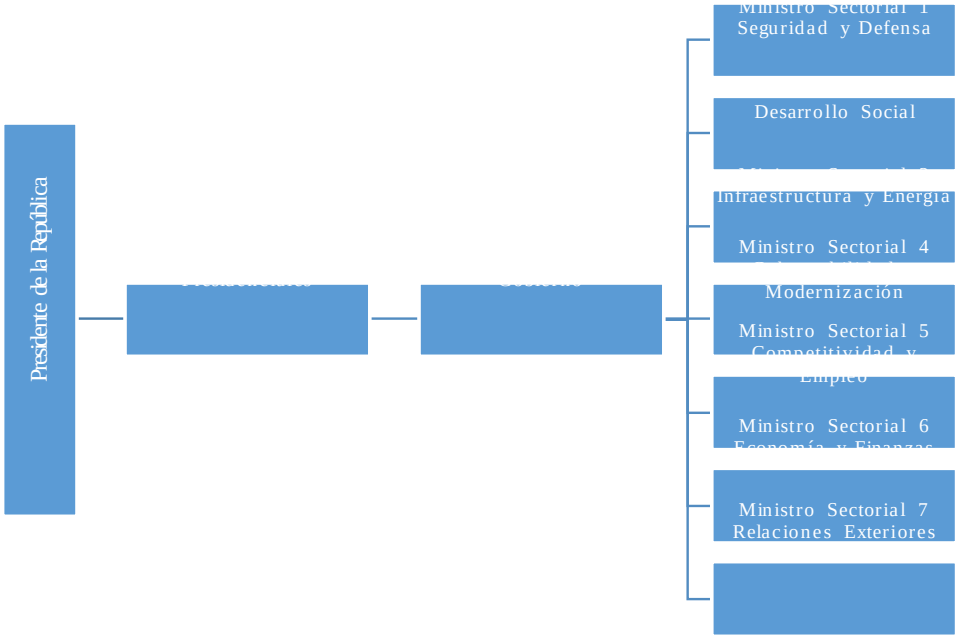

Figura 2: Estructura del gobiernos de Honduras bajo el mandato del Presidente Juan Orlando Hernández

Fuente: (Lopez, 2014)

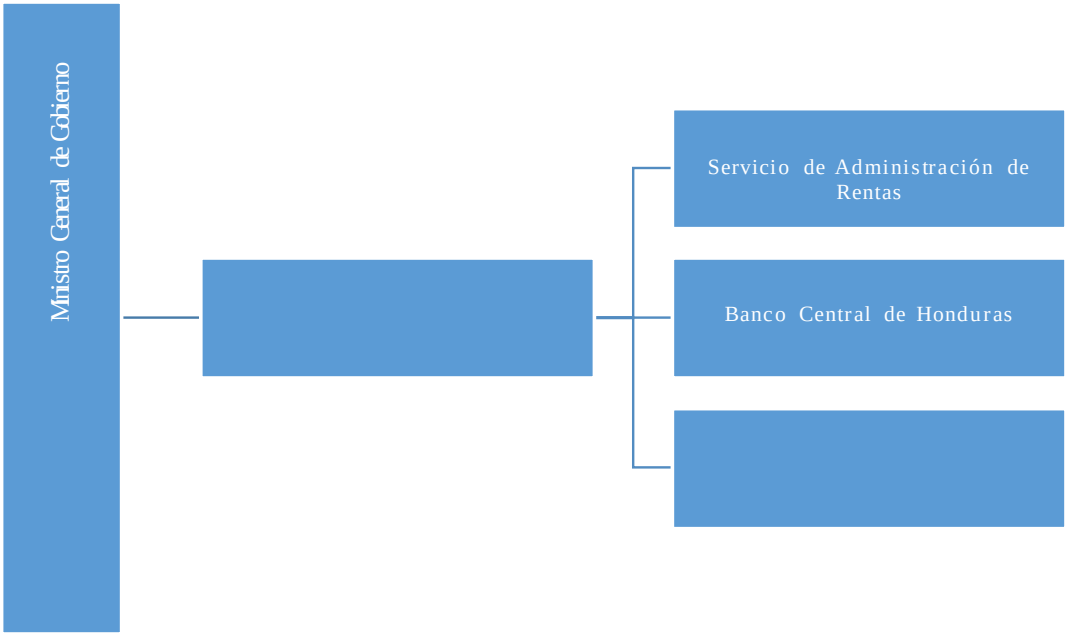

Figura 3: Estructura del gobiernos de Honduras bajo el mandato del Presidente Juan Orlando Hernández

Fuente: (Lopez, 2014)

- Banco Central de Honduras (BCH)
- Secretaria de Finanzas (SEFIN)
- Servicio de Administración de Retas (SAR)

3.2 Investigación

Como primera actividad fue recopilar la información de lo relacionado con la seguridad de la información y los beneficios del BYOD, entrevistas con expertos, leer libros relacionados con el tema de seguridad de la información y normativas , revistas con información actualizada sobre el fenómeno de BYOD, artículos científicos y de revistas profesionales; y la información recopilada nos permitió visualizar las diferentes áreas que aborda este tema de investigación tanto lo legal, políticas, recurso humano, tecnología, inversión, productividad, imagen institucional, entre otros. Siendo necesario el enfoque a las áreas específicas como lo son las políticas internas de una institución, recurso humano y tecnológico para el presente trabajo de investigación.

3.3 Investigación Exploratoria

El fenómeno de BYOD está impactando en el manejo de la información confidencial, sin embargo, debido a que en Honduras el tema de seguridad de la información todavía no tiene la madurez de otros países, es necesario realizar un estudio exploratorio para conocer por medio de un método científico el conocimiento y comportamiento de los empleados de las IGSFH en estos dos temas.

De los métodos científicos utilizados para realizar estudios científicos, se seleccionó el estudio exploratorio debido a que este aplica a temas de investigación poco estudiados.

> Los estudios exploratorios se realizan cuando el objetivo es examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o no se han abordado antes. Es decir, cuando la revisión de la literatura revelo que tan sólo hay guías no investigadas e ideas vagamente relacionadas con el problema de estudio, o bien si deseamos indagar sobre temas y áreas desde nuevas perspectivas.(Hernandez Sanpieri, Fernandez-Collado, & Baptista Lucio, 2006, p. 100)

3.4 Entrevistas con Expertos

Las entrevistas con profesionales nacionales que tengan una trayectoria reconocida en temas de seguridad de la información o seguridad informática permitirán conocer desde una perspectiva a nivel experto de los temas que involucran el BYOD y las amenazas que estos dispositivos representan cuando no son gestionados y controlados correctamente. Las reuniones con dichos profesionales serán previas a lanzar una encuesta con los empleados de las instituciones, con el objetivo de mejorar la encuesta que se realizará a los empleados de las IGSFH.

Es importante indicar que el desarrollo de un trabajo de investigación de este tipo requiere el apoyo de varias fuentes de información, siendo una de estas fuentes una persona experta en temas de seguridad de la información o seguridad informática. Y como nos lo señala el Diccionario de la RAE, una persona experta es aquella experimentada, especializada o con grandes conocimientos en una materia. El tener la opinión de un profesional experto genera un alto valor este trabajo de tesis que está en desarrollo, siendo este trabajo enfocado a la realidad internacional y más enfocada a la realidad nacional de las IGSFH.

Los expertos a seleccionar son personas con una trayectoria profesional y académica en la seguridad de la información y preferiblemente, personas con estudios y trabajos realizados en países más evolucionados en este tema. Los requisitos del experto antes expuestos se deben a que la seguridad de la información e informática tiene un desarrollo mayor en otros países y en Honduras no se ha tenido un desarrollo significativo.

3.5 Investigación Cuantitativa

El objetivo de este trabajo de tesis es poder brindar un marco de referencia para el control de uso de BYOD a los usuarios de las IGSFH, es necesario conocer cuál es el comportamiento que en este momento un usuario promedio tiene en el uso de los dispositivos móviles, su interacción con los recursos e información de la institución donde labora y con esa información poder desarrollar una matriz de los riesgos más significativos al utilizar BYOD. Para lo antes indicado se aplicará una encuesta como parte de metodología de investigación a una muestra de la población de las IGSFH.

3.6 Población

La población de las IGSFH asciende a aproximadamente 2,524 personas, las cuales utilizan actualmente los recursos de cada institución y que son usuarios potenciales en el uso de BYOD, este dato fue obtenido del portal de la IAIP (Instituto de Acceso a la Información Pública), el cual contiene la estructura orgánica de cada institución gubernamental, incluida la cantidad de funcionarios que trabajan en cada una de las IGSFH objeto de este estudio.

3.7 Muestra

La muestra es una parte de la población que puede ser utilizada como referencia para saber lo que piensa toda la población, para poder determinar la muestra de la población se debe seguir un proceso de cinco pasos los cuales se muestran en la figura 4. Cabe recalcar que para obtener una muestra que simbolice lo que la población quiere es de suma importancia seguir al pie el proceso que se verá a continuación.

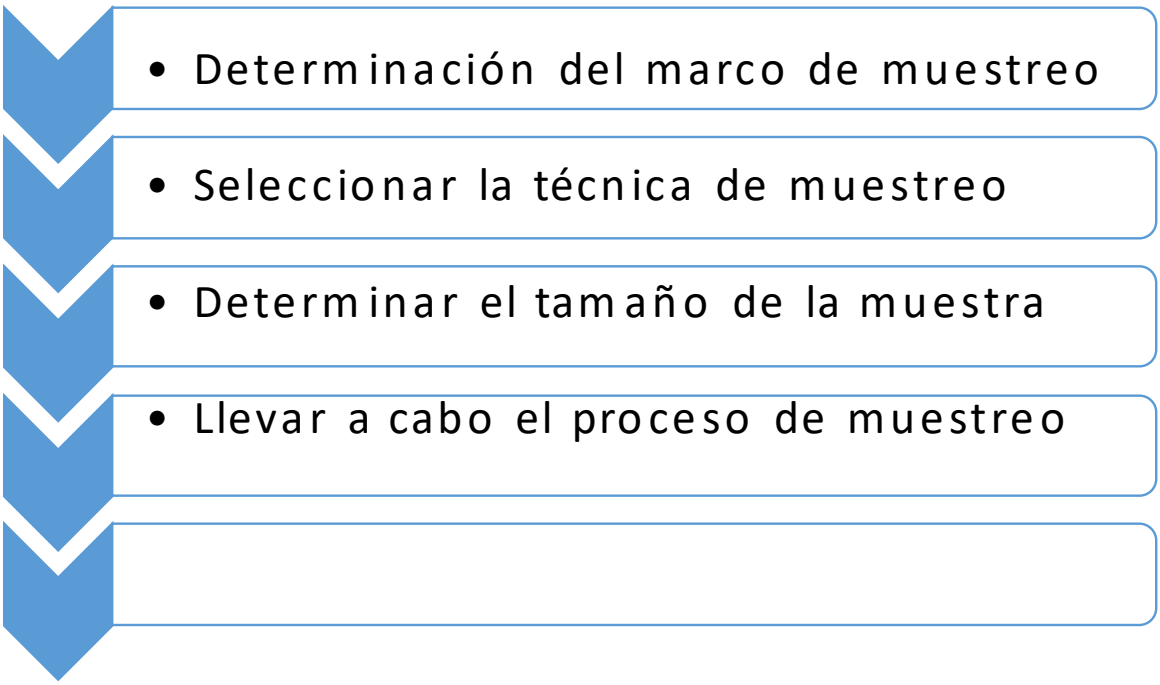

Figura 4: Selección de muestra

Fuente: (Malhotra Page, 2013)

Para determinar la muestra que se utilizará en la institución se hará uso de la ecuación estadística para proporciones poblacionales (1) la cual se presenta a continuación:

$$n = \frac{Z^2 p(1-p)}{e^2}$$

(1)

Dónde:

n = tamaño de la muestra.

Z = nivel de confianza.

p = proporción real de la población.

e= porcentaje de error de la muestra

Basados en la fórmula anterior donde n=0.36 resultado obtenido del muestreo de las primeras 30 encuestas realizadas de la prueba piloto, un nivel de confianza de Z=91% y un margen de error de e=9% el tamaño de la muestra sería de ochenta y dos (82) encuestas.

3.8 Instrumentos Utilizados

Para poder llevar a cabo este trabajo de tesis se deberá de hacer uso de herramientas que ayuden a establecer los lineamientos que ayuden a determinar el comportamiento de los usuarios de las IGSFH en el uso de BYOD.

3.9 Matriz de Variables

La tabla 8 corresponde a la matriz de variables que muestra cómo se va estructurar la encuesta a la población e las IGSFH en el tema relacionado con BYOD:

Tabla 8. Variables

Variable	Concepto	Operacional	Dimensiones	Indicadores	Unidad de Medida	Escala	Valor Final
Extravío	Pérdida del dispositivo móvil con riesgo a que la información de la institución sea expuesta a terceros no autorizados	Riesgo de exposición de la información confidencial de la institución.	N/A	N/A	Nominal dicotomi-co	Nomi-nal	-Si -No
Robo	Pérdida del dispositivo móvil con alto riesgo a que la información de la institución sea expuesta a terceros no autoriza-dos	Riesgo de exposición de la información confidencial de la institución.	N/A	N/A	Nominal dicotomi-co	Nomi-nal	-Si -No
Red inalámbrica Pública	Nivel de Exposición a red inalámbrica publica	Riesgo de exposición a los siguientes ataques, robo de Información, vectores de ataque, robo de Credenciales.	N/A	N/A	Rango de frecuen-cia	Ordinal	-Nunca (1) -Casi nunca (2) -A veces (3) -Casi siempre (4) -Siempre (5)

Variable	Concepto	Operacional	Dimensiones	Indicadores	Unidad de Medida	Escala	Valor Final
Red inalámbrica corporativa -va	Acceso a recursos informáticos de la institución desde la red inalámbrica corporativa.	Riesgo de exposición a los siguientes ataques: Robo de Información de los sistemas informáticos, puntos de ataque hacia los sistemas informáticos corporativos, robo de credenciales, denegación de servicios, infección de virus, troyanos, y malware.	N/A	N/A	Rango de frecuencia	Ordinal	-Nunca (1) -Casi nunca (2) -A veces (3) -Casi siempre (4) -Siempre (5)
Correo Electrónico	Aplicación de correo electrónico de la institución instalado en el dispositivo móvil.	El rango de conexión y otras variables puede ocasionar que el servidor de correo sea susceptible a ataques de SPAM, Robo de Información, Infección de Virus, Pivote de ataques a otros sistemas.	Duración de la contraseña.	Caducidad de la contraseña	Intervalos de tiempo	Ordinal	-Cada 30 días (5) -Cada 60 días (4) -Cada 90 (3) -Más de 90 días (2) -Nunca(1)
			Frecuencia de Conexión al Correo.	Regularidad de conexión	Rango de frecuencia	Ordinal	-Nunca (1) -Casi nunca(2) -A veces (3) -Casi siempre (4) -Siempre (5)
			Descarga de Archivos Adjuntos	Regularidad de descarga de adjuntos	Rango de frecuencia	Ordinal	-Nunca (1) -Casi nunca (2) -A veces (3) -Casi siempre (4) -Siempre (5)

Variable	Concepto	Operacional	Dimensiones	Indicadores	Unidad de Medida	Escala	Valor Final
Seguridad de la Informaci-ón	Mide el nivel de seguridad de la información de las instituciones analizando algunos controles básicos que deben estar ejecutándose.	Riesgo de que la información confidencial de la institución sea fácilmente vulnerada debido a que no existen controles o no se están ejecutando de la forma adecuada.	Capacitaciones sobre seguridad de la información.	N/A	Nominal dicotómi-co	Nomi-nal	-Si -No
			Uso de acuerdos de confidencialidad.	N/A	Nominal dicotómi-co	Nomi-nal	-Si -No
			Registro de dispositivos móviles.	N/A	Nominal dicotómic o	Nomi-nal	-Si -No
			Clasificación de la información.	N/A	Nominal dicotómic o	Nomi-nal	-Si -No

Fuente: (Elaboración propia)

3.10 Fiabilidad de la Encuesta

Uno de los métodos recomendados para comprobar la fiabilidad de pruebas o encuestas es el de consistencia interna, dentro de este método se encuentra el coeficiente de Alfa de Cronbach el cual es uno de los más utilizados por investigadores, de acuerdo a Huh, Delorme & Reid (2006), "el valor de fiabilidad en investigación exploratoria debe ser igual o mayor a 0.6 y en estudios confirmatorios debe estar entre 0.7 y 0.8.", la investigación que se realizará en el presente trabajo es investigación exploratoria, los resultados de la prueba realizada en la herramienta estadística SPSS arrojan el resultado expuesto en la tabla 9.

Tabla 9. Estadísticas de fiabilidad

Estadísticas de fiabilidad	
Alfa de Cronbach	Alfa de Cronbach basada en los elementos tipificados
,649	,658

Fuente: (Elaboración propia)

CAPÍTULO IV. ANALISIS Y RESULTADOS

4.1 Análisis de Situación Seguridad de la Información en IGSFH

Con el propósito de tener conocimiento sobre donde sentar las bases del marco de referencia para el control de dispositivos móviles personales conectados a los servicios informáticos propios de cada institución, ha sido necesario realizar una investigación exploratoria que nos permita tener en cuenta la situación actual del país, para esto ha sido necesario recurrir a la institución gubernamental que se encarga de realizar regulaciones sobre las telecomunicaciones en Honduras.

4.2 Reseña de CONATEL

CONATEL Es un organismo estatal desconcentrado que ejecuta, mediante la regulación y coordinación, la política de Telecomunicaciones en la República de Honduras. CONATEL fue fundada el 5 de diciembre de 1995, mediante Decreto 185/95. Entre sus principales funciones se encuentran:

1. Formular las políticas de telecomunicaciones del país integradas en la ley marco de telecomunicaciones, siendo además ente de investigación, combate y sanción de infracciones.
2. Emite las regulaciones y normas técnicas requeridas para la prestación de servicios de telecomunicaciones.
3. Emite regulaciones con respecto a las tarifas que podrían cobrar los operadores de servicios de telecomunicaciones.
4. Clasifica los servicios de telecomunicaciones, otorgando autorizaciones, permisos, registros, y licencias, para prestación de servicios de telecomunicaciones y de ser el caso, los renueva, modifica, declara su caducidad o los revoca de acuerdo con el correspondiente reglamento.
5. Aprueba normas sobre la homologación de equipos y aparatos de telecomunicaciones.

De acuerdo al último organigrama emitido por la institución en febrero del 2016, la institución está conformada por una directiva general y estructurada en siete grandes direcciones,

siendo las más representativas para el objeto del estudio de este documento por su aspecto técnico, la Dirección de Gestión del Espectro Radioeléctrico y la Dirección de Gestión de Servicios de Telecomunicaciones. En el caso de la Dirección de Gestión de Servicios de Telecomunicaciones está conformada por dos departamentos, uno dedicado a la regulación de servicios y proyectos de telecomunicaciones y el otro a la supervisión de la calidad de servicio brindada por las diversas empresas que prestan servicios de telecomunicación en Honduras (ver organigrama en la URL: http://portalunico.iaip.gob.hn/).

Todos los años CONATEL publica un informe con los principales indicadores estadísticos del sector de telecomunicaciones de HONDURAS, el cual tiene como fin mostrar el desempeño o comportamiento del sector de telecomunicaciones durante un periodo especifico, este informe presenta detalles desde el tráfico de las redes telefónicas hasta indicadores de las redes del servicio de Internet y la conectividad de banda ancha. Este informe recopila la información obtenida por parte de todos los prestadores de servicio como obligación establecida en el Marco legal vigente del Sector de Telecomunicaciones.

4.2.1 Situación Actual en Protección del Ciudadano

Durante la entrevista realizada a la Dirección de Gestión de Telecomunicaciones confirmando si existía actualmente algún marco orientado a la protección del ciudadano hondureño contra ciberataques se pudo notar el esfuerzo y avance que CONATEL ha tenido en los últimos años convirtiéndose en un aliado del usuario final que utiliza el servicio brindado por las diversas compañías de telecomunicaciones, siendo los principales logros de este departamento los siguientes:

a. Ley de llamadas caídas, tiene como objetivo medir la calidad de servicio de los diferentes operadores de servicio, permitiendo retornar al usuario los minutos de llamadas en que el usuario ha sufrido pérdida involuntaria del servicio prestado.
b. Decreto de Listas Blancas, tiene como objetivo poder evitar la adulteración de las características que identifican un dispositivo como único (IMEI, Frecuencia, etc.), típica en mercado negro para reventa de dispositivos extraviados o robados al ciudadano.

c. Desde el año 2015 hay un estudio de CONATEL que tiene como objetivo establecer los lineamientos regulatorios necesarios para promover el desarrollo de la Banca Móvil a beneficio de los usuarios, esta propuesta actualmente se encuentra en discusión en el Congreso Nacional de la República y se ha vuelto necesaria debido al incremento de las diferentes transacciones electrónicas que tienen relación con dinero.

Sin embargo y a pesar de los logros obtenidos, no existe en CONATEL actualmente una propuesta relacionada con exigencia de regulación o control de tráfico anómalo en los servicios de datos que prestan los operadores de telecomunicaciones y que pueden evitar ciberataques que pongan en riesgo la seguridad de la información de los diferentes usuarios de servicio de telecomunicaciones.

4.2.2 Marco Regulatorio para Seguridad de la Información

Debido a las relaciones y convenios que CONATEL tiene con las instituciones de regulación en los países de Latinoamérica, especialmente con el caso de Costa Rica y Colombia, existe una propuesta de creación de un marco regulatorio con el objetivo principal de proteger la información del ciudadano hondureño. Este proyecto ha venido surgiendo desde hace un par de años siendo sus principales colaboradores, la Organización de los Estados Americanos (OEA), La Corporación de Internet para la Asignación de Nombres y Números (ICANN, de sus siglas en inglés) y el Banco Interamericano de Desarrollo (BID) (¿Ciberseguridad, estamos preparados en América Latina?).

En palabras de la Lic. Libby Rivas, Honduras carece de un marco legislativo para la seguridad de las TIC; su legislatura está actualmente llevando a cabo reformas al código penal que introducirían leyes contra la delincuencia cibernética y en los últimos meses se ha promulgado una legislación parcial respecto a la privacidad, la protección de datos y la protección de la libertad de expresión. La Dirección de Gestión de Telecomunicaciones de CONATEL lidera actualmente un proyecto en conjunto con la Dirección Nacional de Inteligencia que permitirá implementar en el país un Centro de Respuesta ante incidentes de Seguridad Informática (CSIRT), el cual se encargará de poder monitorear el país en materia de seguridad de la información y en conjunto con otros CSIRT a nivel mundial poder estar presto a las diferentes

amenazas de seguridad de la información. Por otro lado, la Dirección Presidencial de Gestión por Resultados a cargo de la "Agenda Digital" del Estado de Honduras están implementando tecnologías de seguridad y normas internacionales, incluyendo ISACA, ISO 27002 e ITIL ("Information Technology Infraestructure Library" en inglés), para proteger mejor los activos nacionales. Sin embargo, la gestión de tecnologías de seguridad es descoordinada y a menudo se subcontrata con terceros y no existe una política en marcha para la divulgación de las violaciones a la seguridad.

En conclusión a pesar de los esfuerzos por diferentes entidades de gobierno como ser CONATEL, Dirección Nacional de Investigación e Inteligencia (DNII) o en promover una ley o marco regulatorio de seguridad de las TIC para las instituciones de gobierno, no existe actualmente ningún control de la seguridad de la información y en el caso de las instituciones representativas en esta tesis mucha de la seguridad de la información que promueven está relacionada con las exigencias requeridas por aquellas entidades internacionales o privadas con las cuales tienen convenios y colaboración laboral.

4.3 Análisis de situación en las IGSFH

4.3.1 Reseña de BCH

El Banco Central de Honduras se creó el 3 de febrero de 1950 mediante decreto legislativo número 53, inició operaciones el 1 de julio de ese mismo año bajo la titularidad del abogado Roberto Ramírez. Esto representó un avance extraordinario sobre la situación que imperaba en aquella época pues solamente existían dos bancos a nivel nacional que cubrían las actividades financieras del país además si bien el congreso nacional ya había aprobado el Lempira como moneda oficial todavía no se había instituido como patrón monetario hasta la fundación del Banco Central de Honduras (Ver organigrama en la URL: http://portalunico.iaip.gob.hn/).

Dentro de las principales funciones que el Banco Central tiene en este momento están las siguientes:

1. Formular y dirigir la política monetaria y emitir la normativa correspondiente al país.
2. Emitir las monedas y billetes de curso legal en el territorio nacional.

3. Habilitar los agentes cambiarios que podrán negociar divisas del territorio nacional.
4. Administrar las reservas monetarias internacionales.
5. Determinar el tipo de cambio de la divisa en función de la oferta y demanda.
6. Realizar operaciones de crédito para atender insuficiencia de liquidez de las instituciones del sistema financiero nacional.
7. Realizar operaciones de estabilización monetaria.
8. Ejercer las funciones de banquero agente fiscal y consejero económico financiero del Estado.
9. Elaborar y publicar las principales estadísticas macroeconómicas.

4.3.2 Reseña de SEFIN

La Secretaría de Finanzas es la institución del estado de Honduras responsable de la formulación, coordinación, ejecución y evaluación de las políticas relacionadas con las finanzas públicas y el presupuesto general de ingresos y egresos de la República; lo relativo a la deuda pública, la programación de la inversión pública, en un marco de legalidad y transparencia, para contribuir al desarrollo económico del país (Ver organigrama en la URL: http://portalunico.iaip.gob.hn/). Los objetivos estratégicos de la institución son los siguientes:

1. Mejorar la supervisión, el control y el análisis de la ejecución financiera de los fondos públicos para que las autoridades realicen los ajustes oportunos.
2. Mejorar el control de las franquicias aduaneras y las exoneraciones fiscales para aumentar la disponibilidad de recursos del estado.
3. Mantener la sostenibilidad del endeudamiento público, para conservar la credibilidad en los mercados financieros.
4. Mejorar el sistema nacional de inversión pública, enfatizando en el control de los proyectos de inversión para la toma oportuna de decisiones.

4.3.3 Reseña de la SAR

El Servicio de Administración de Rentas (SAR), es una entidad Desconcentrada adscrita a la Presidencia de la República, con autonomía funcional, técnica, administrativa y de seguridad

nacional, con personalidad jurídica propia, responsable del control, verificación, fiscalización y recaudación de los tributos, con autoridad y competencia a nivel nacional y con domicilio en la Capital de la República.

Mediante decreto ejecutivo número PCM 083-2015 de fecha 26 de noviembre de 2015, el Presidente de la República en consejo de Ministros decreto Suprimir y liquidar la Dirección Ejecutiva de Ingresos (DEI), creada mediante decreto legislativo 17-2010 de fecha 28 de marzo de 2010; en el mismo decreto PCM 083-2015 en su artículo 7 decreta que todas las atribuciones y solicitudes inherentes a las obligaciones tributarias estarán a cargo de un Comisionado Presidencial, razón por la cual, surge la Comisionada Presidencial de la Administración Tributaria, la cual hasta el 31 de diciembre de 2016, tuvo a su cargo la Administración tributaria, de conformidad al artículo 7 del decreto PCM 084-2015. A partir del 1 de enero de 2017, el Servicio de Administración inicia operaciones como el órgano responsable de administración tributaria (Ver organigrama en la URL: http://portalunico.iaip.gob.hn/).

4.4 Controles de Seguridad en Dispositivos Móviles

Con el fin de determinar el nivel de seguridad de BYOD en las IGSFH y el nivel de riesgo, se seleccionaron algunos de los controles más representativos en pérdida de la seguridad de la información en dispositivos móviles, además se escogieron algunos controles que ayudan a determinar el nivel de cumplimiento de políticas de seguridad en las instituciones objeto de estudio, los controles escogidos fueron los siguientes:

a. Robo/Extravío de dispositivos móviles, pérdida del dispositivo móvil con riesgo a que la información de la institución sea expuesta a terceros no autorizados.
b. Acceso a redes inalámbricas públicas, nivel de exposición de la información almacenada en los dispositivos móviles en redes públicas.
c. Acceso a Wi-Fi Corporativo, nivel de exposición de los recursos informáticos de la institución a dispositivos móviles traídos a la institución.
d. Correo Electrónico, controles que determinan la seguridad de la aplicación de correo electrónico de la institución instalado en el dispositivo móvil.

4.5 Análisis y resultados de la encuesta aplicada al usuario final

Se muestran a continuación el análisis de cada una de las preguntas formuladas en la encuesta que se aplicó a usuarios de dispositivos móviles.

- ¿Tiene usted un dispositivo móvil (Smartphone o Tablet)?

Esta primera pregunta se definió como una pregunta filtro, para poder basar nuestro estudio solamente en los usuarios que tienen un dispositivo móvil.

- ¿Esta su dispositivo móvil (Smartphone/Tablet) configurado con el correo electrónico de la institución donde labora?

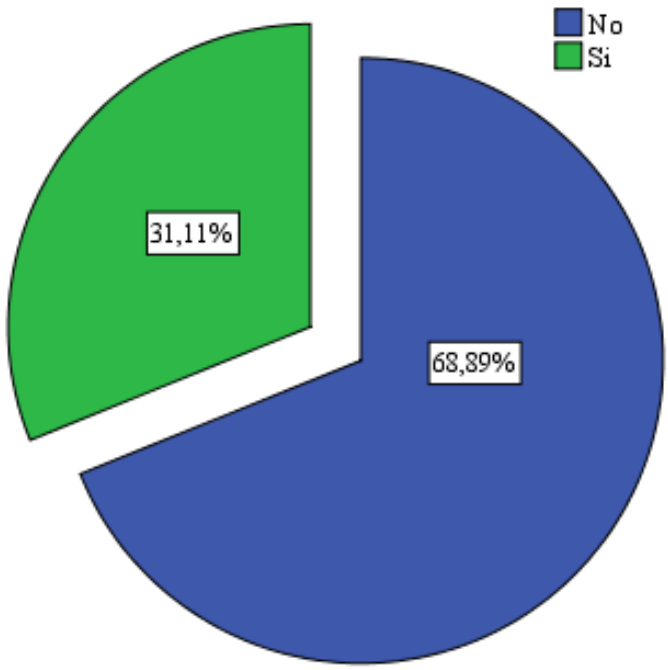

Grafico 4: Correo electrónico configurado en el dispositivo móvil

Fuente: (Elaboración propia)

Basado en los resultados que se obtuvieron de la pregunta 2 de la encuesta, se puede concluir que el 31.11% de los usuarios que laboran en estas instituciones, tienen el dispositivo

móvil conectado al correo electrónico de la institución. Lo que representa a su vez el porcentaje de dispositivos móviles que contienen información confidencial fuera de los controles físicos e informáticos de la institución.

- ¿En los últimos cinco (5) años ha sufrido de robo, hurto o extravío de algún dispositivo móvil?

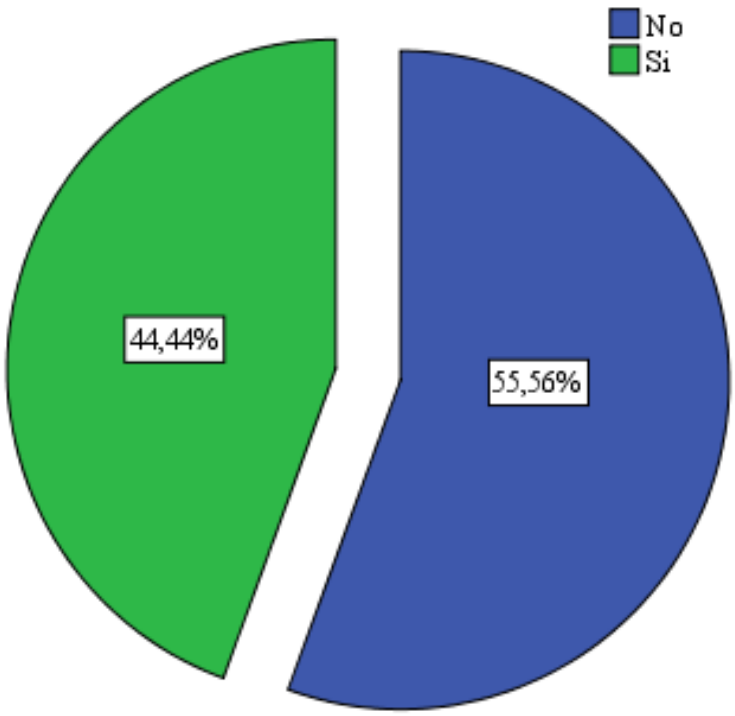

Grafico 5: Robo, hurto o extravió de dispositivo móvil

Fuente: (Elaboración propia)

Basado en los resultados que se obtuvieron de la pregunta 3 de la encuesta, se puede concluir que el 44.44% de los usuarios que tienen dispositivo móvil han sufrido de robo, hurto o extraviaron el dispositivo. Lo que indica que la información confidencial o personal almacenada en estos dispositivos fue expuesta a terceros por un lapso o fue perdida/robada totalmente.

- ¿Conecta su dispositivo móvil a redes inalámbricas públicas (Wi-Fi en Hoteles, Restaurantes, Aeropuertos, Centros Comerciales)?

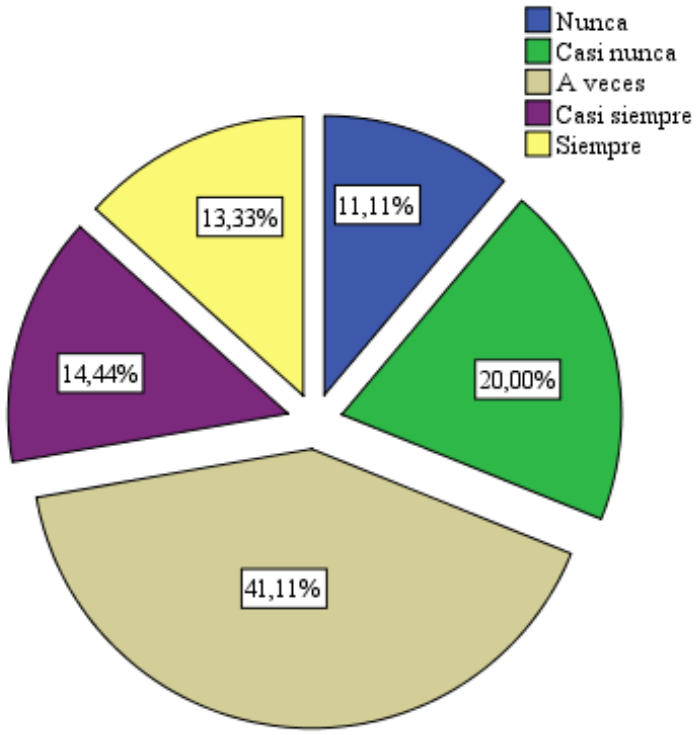

Grafico 6: Conexión a redes inalámbricas públicas

Fuente: (Elaboración propia)

Basado en los resultados que se obtuvieron de la pregunta 4 de la encuesta, se puede concluir que el 88.88% (suma de 41.11%, 14.44%, 13.33%, 20.00%) de los usuarios que tienen dispositivo móvil se conectan a redes inalámbricas públicas. Lo que indica que la información confidencial o personal almacenada en estos dispositivos está expuesta a robos informáticos, infección de virus o los dispositivos pueden ser atacados para ser utilizados como un punto de ataque una vez que se conectan a las redes Wi-Fi institucionales.

- ¿En un día laboral, con qué frecuencia revisa su correo electrónico institucional desde su dispositivo móvil?

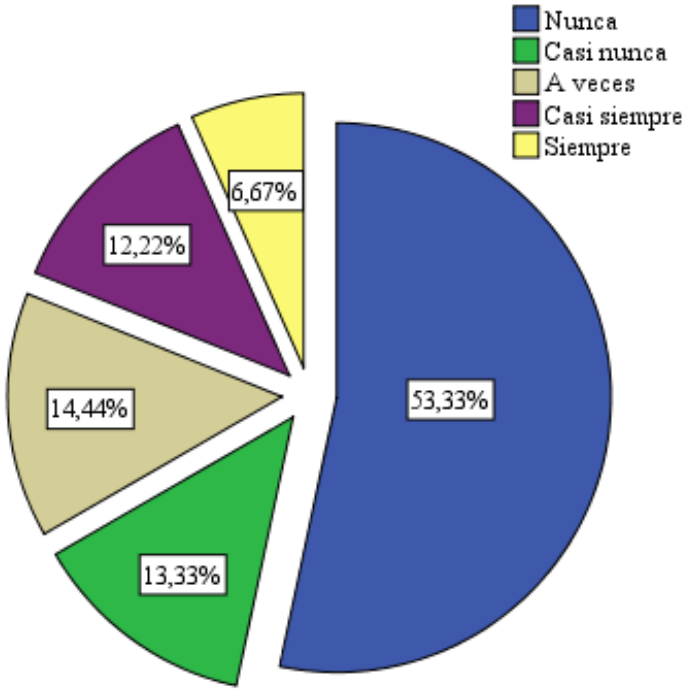

Grafico 7: Frecuencia en revisión del correo electrónico institucional en el dispositivo móvil

Fuente: (Elaboración propia)

Basado en los resultados que se obtuvieron de la pregunta 5 de la encuesta, se puede concluir que el 46.66% (suma de 14.44%, 13.33%, 12.22%, 6.67%) de los usuarios que tienen dispositivo móvil revisan su correo desde el dispositivo móvil. Lo que indica que hay una tendencia a utilizar el dispositivo móvil para realizar parte de su trabajo diario, y este, se está volviendo de una manera indirecta parte de los procesos de negocios de las instituciones.

- ¿Revisa en el dispositivo móvil archivos adjuntos que le envían a través del correo electrónico institucional?

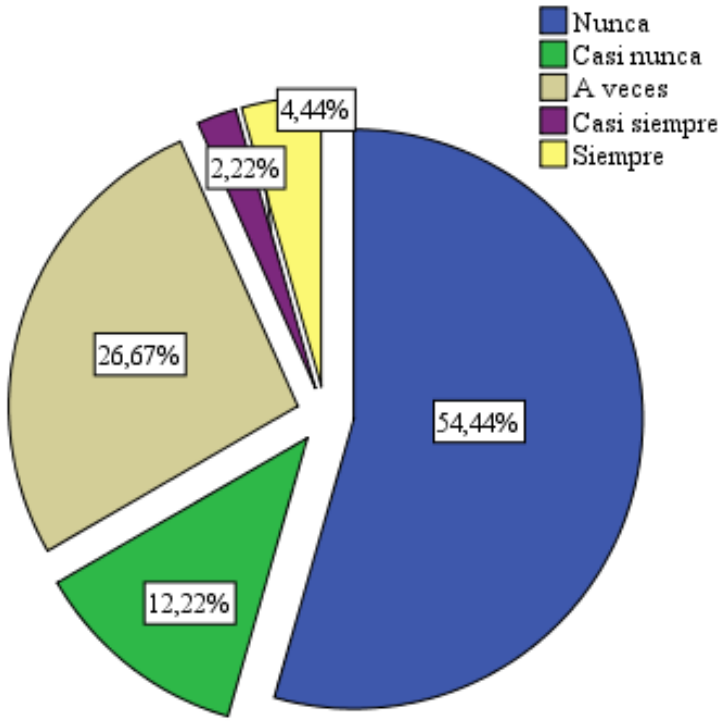

Grafico 8: Revisión de archivos adjuntos enviados a través del correo electrónico institucional

Fuente: (Elaboración propia)

Basado en los resultados que se obtuvieron de la pregunta 6 de la encuesta, se puede concluir que el 45.53% (suma de 26.67%, 12.22%, 4.44%, 2.20%) de los usuarios que tienen dispositivo móvil revisan archivos adjuntos que reciben a través del correo electrónico institucional desde el dispositivo móvil. Lo que indica que hay una tendencia a utilizar el dispositivo móvil para realizar parte del trabajo, y este se está volviendo de una manera indirecta parte de los procesos de negocios de las instituciones, lo que representa un riesgo a que la información confidencial de la institución almacenada en estos dispositivos no tenga de los controles físicos e informáticos que se les aplican a otros equipos dentro de las instituciones.

- ¿Le exigen en la institución donde labora reportar cuando su dispositivo móvil ha sido extraviado, hurtado o robado?

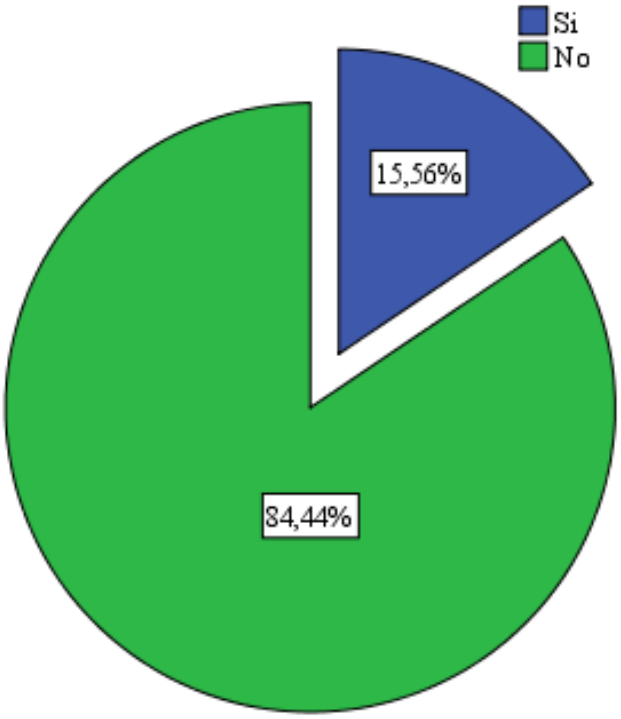

Grafico 9: Exigencia por parte de la institución cuando el dispositivo móvil es robado, hurtado o extraviado

Fuente: (Elaboración propia)

Basado en los resultados que se obtuvieron de la pregunta 7 de la encuesta, se observa que la mayoría de los usuarios encuestados indicaron que no se les exige reportar si han extraviado o han sufrido de hurto o robo de su dispositivo móvil. Por lo que se concluye que al suceder un evento de los antes mencionados no existe algún proceso que se inicie al reportar, por ejemplo, el robo del dispositivo móvil para proceder con el borrado de la información contenida en el dispositivo de manera remota o realizar un reseteo de fábrica remoto.

- ¿Conecta usted su dispositivo móvil a la red inalámbrica (Wi-Fi) de la institución donde labora?

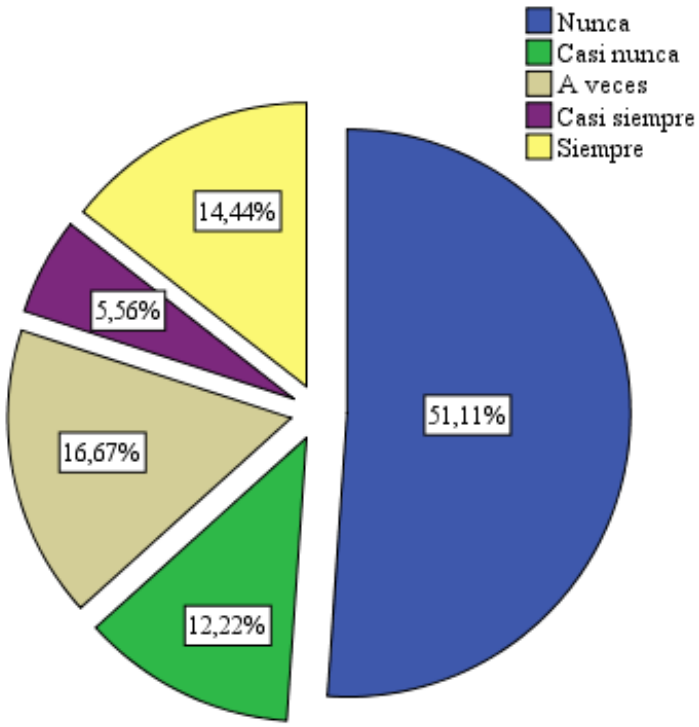

Grafico 10: Conexión del dispositivo móvil a la red inalámbrica institucional

Fuente: (Elaboración propia)

Basado en los resultados que se obtuvieron de la pregunta 8 de la encuesta, se puede concluir que el 48.89% (suma de 16.67%, 14.44%, 12.22%, 5.56%) de los usuarios indicaron que se conectan a la red inalámbrica institucional. Lo que indica que si estos dispositivos están infectados con virus exponen a la seguridad informática de la institución a robo de información utilizando este como punto de conexión, infectar de virus a otros dispositivos o los dispositivos pueden ser utilizados como un punto de conexión para un delincuente informático y lograr ingresar a la red interna.

- ¿En qué periodo se le exige que cambie la contraseña del correo electrónico institucional?

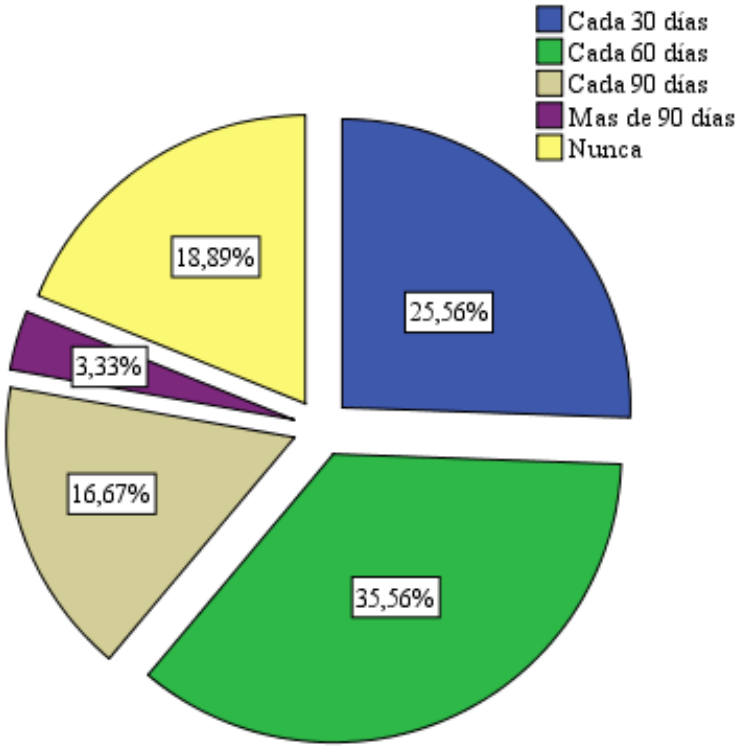

Grafico 11: Frecuencia del cambio de contraseña del correo electrónico institucional

Fuente: (Elaboración propia)

Basado en los resultados que se obtuvieron de la pregunta 9 de la encuesta, se puede concluir que existe una política que incluye el cambio de contraseña entre los 30 y 90 días, dado que el 77.79% (suma de 35.56%, 25.56%, 16.67%). Si bien, existen otras características para determinar si una contraseña es lo suficientemente segura para que sea difícil de predecir, el cambio de la contraseña es un factor importante cuando se relaciona con la frecuencia con que se conecta a redes inalámbricas públicas. Esto debido a que entre más frecuente se conecte a redes inalámbricas públicas, más alto es el riesgo de ser atacado por un hacker, y que este a su vez robe una contraseña que tiene una duración de más de 90 días.

- ¿Tiene su dispositivo móvil algún software para la protección de virus?

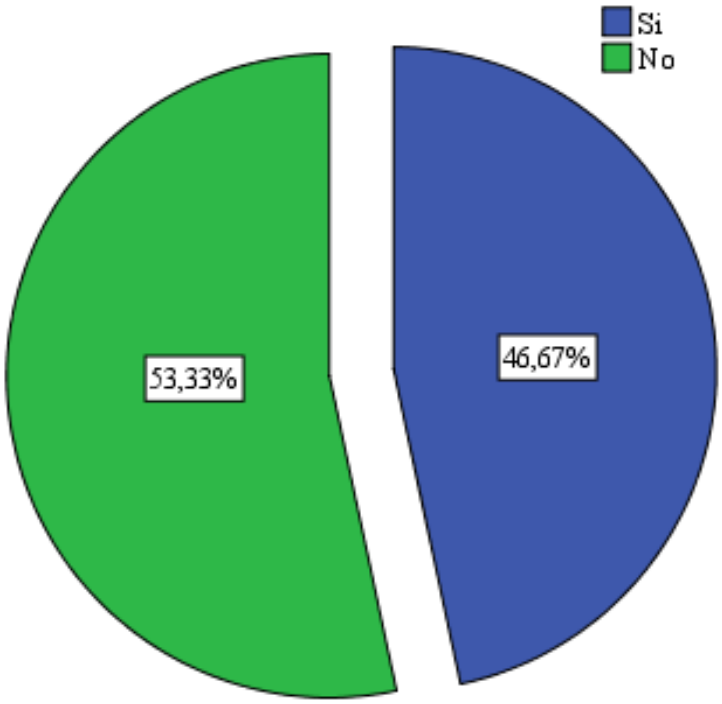

Grafico 12: Dispositivo móvil con software para la protección de virus

Fuente: (Elaboración propia)

Basado en los resultados que se obtuvieron de la pregunta 10 de la encuesta, se puede concluir que 53.33% de los usuarios indicaron que sus dispositivos no tienen un software antivirus. Lo que indica que todos estos dispositivos son vulnerables a la infección de un virus. Por otro lado, el 46.67% que respondió que sí, es un porcentaje bien alto a pesar que los dispositivos móviles no traen instalado un antivirus por defecto, y no existe una cultura de seguridad de la información que marque una tendencia de instalar antivirus por parte de los usuarios.

- ¿Le brindan en la institución charlas sobre seguridad en el manejo de la información?

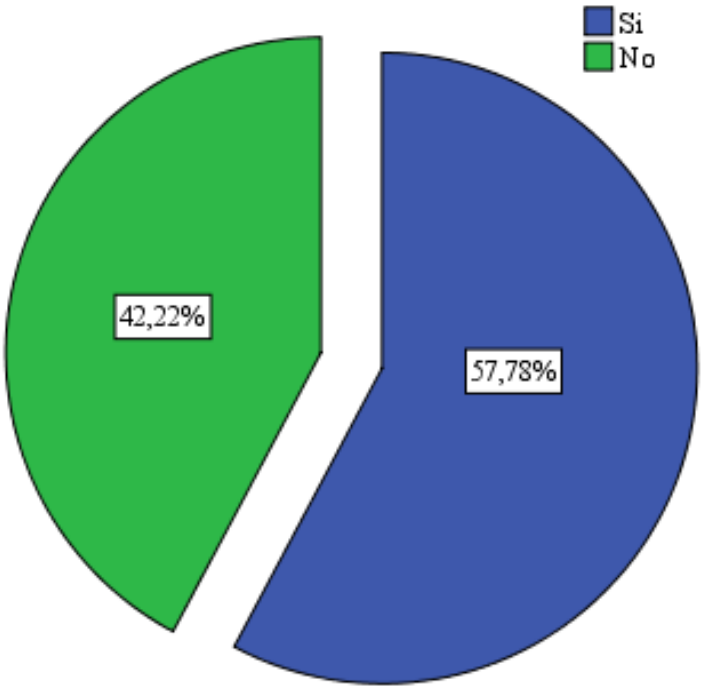

Grafico 13: Charlas de seguridad en el manejo de la información

Fuente: (Elaboración propia)

Basado en los resultados que se obtuvieron de la pregunta 11 de la encuesta, se observa que no existe una mayoría que indique que reciben charlas de seguridad en el manejo de la información, es decir que existen planes de capacitación para el manejo de la información, pero que estos deben ser más efectivos.

- ¿Ha firmado algún acuerdo de confidencialidad de la información en la institución donde labora?

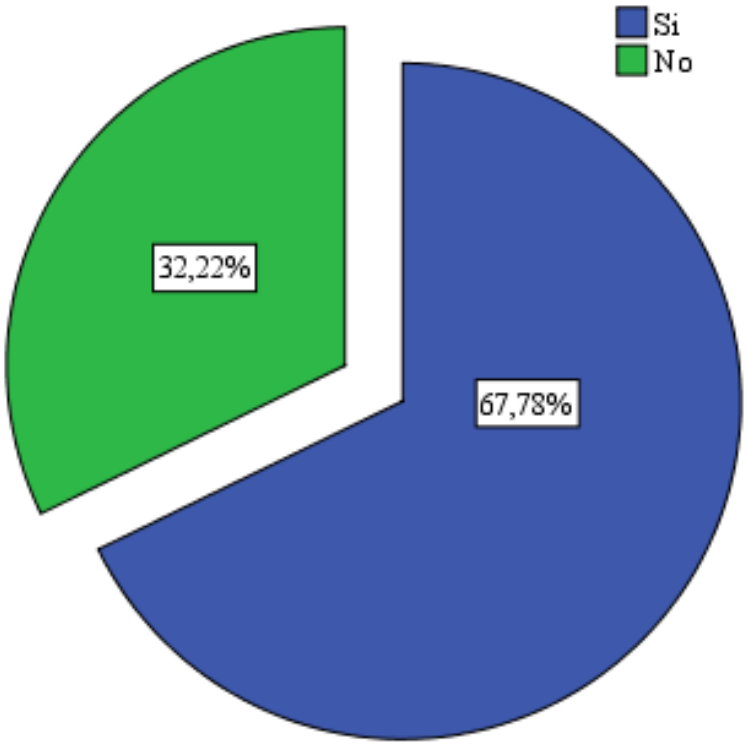

Grafico 14: Firma de acuerdo de confidencialidad

Fuente: (Elaboración propia)

Basado en los resultados que se obtuvieron de la pregunta 12 de la encuesta, se observa que la mayoría indicaron que firmaron un acuerdo de confidencialidad, lo que fortalece el tema de seguridad de la información a nivel institucional.

- ¿Se realizó algún registro de su dispositivo móvil antes de conectarlo a la red inalámbrica de la institución o al correo electrónico?

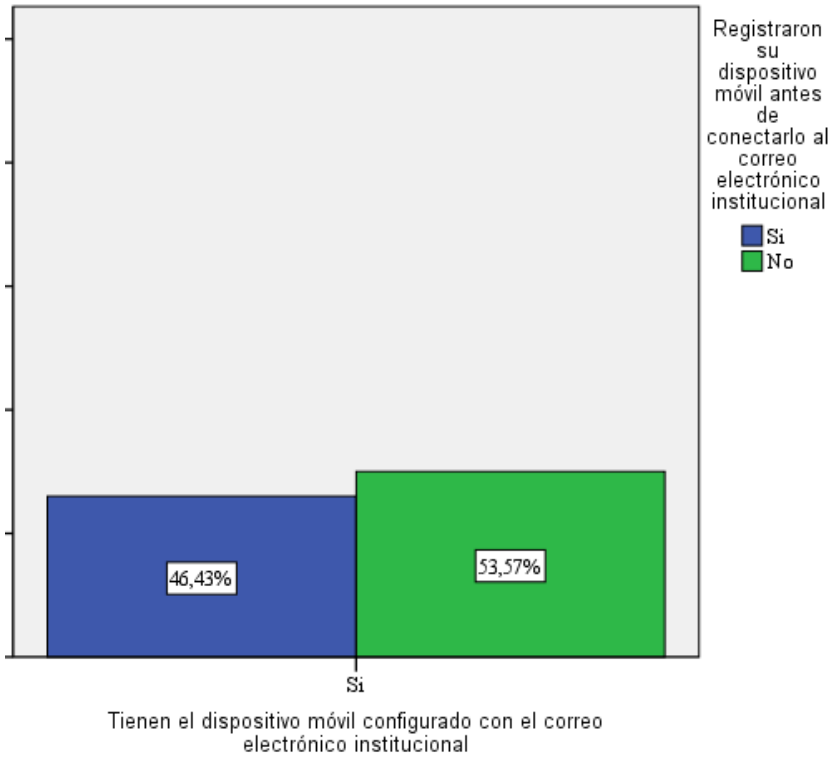

Grafico 15: Registro del dispositivo móvil antes de conectarlo al correo electrónico institucional

Fuente (Elaboración Propia)

Basado en los resultados que se obtuvieron de la pregunta 13 de la encuesta, se puede observar que las instituciones no registran todos los dispositivos que se conectan al correo electrónico.

- ¿Se realizó algún registro de su dispositivo móvil antes de conectarlo a la red inalámbrica de la institución o al correo electrónico?

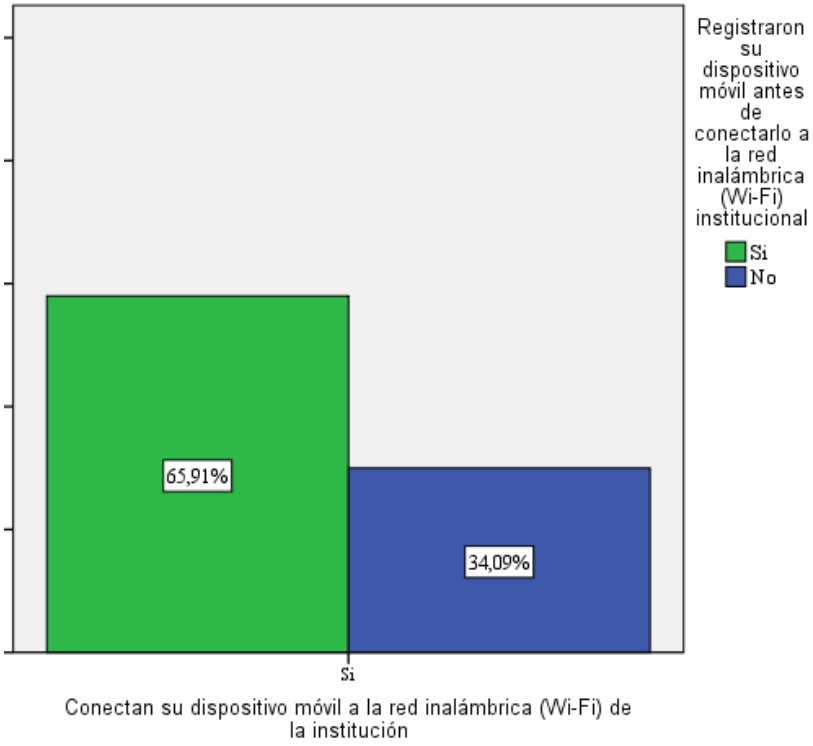

Grafico 16: Registro del dispositivo móvil antes de conectarlo a la red inalámbrica institucional

Fuente: (Elaboración propia)

Basado en los resultados que se obtuvieron de la pregunta 13 de la encuesta, se puede observar que las instituciones no registran todos los dispositivos que se conectan a la red inalámbrica institucional, ya que varios de los que respondieron que si se conectan a esta red también respondieron que no se les realizó registro del dispositivo.

- ¿Qué tan frecuente clasifican la información de su institución entre confidencial y pública?

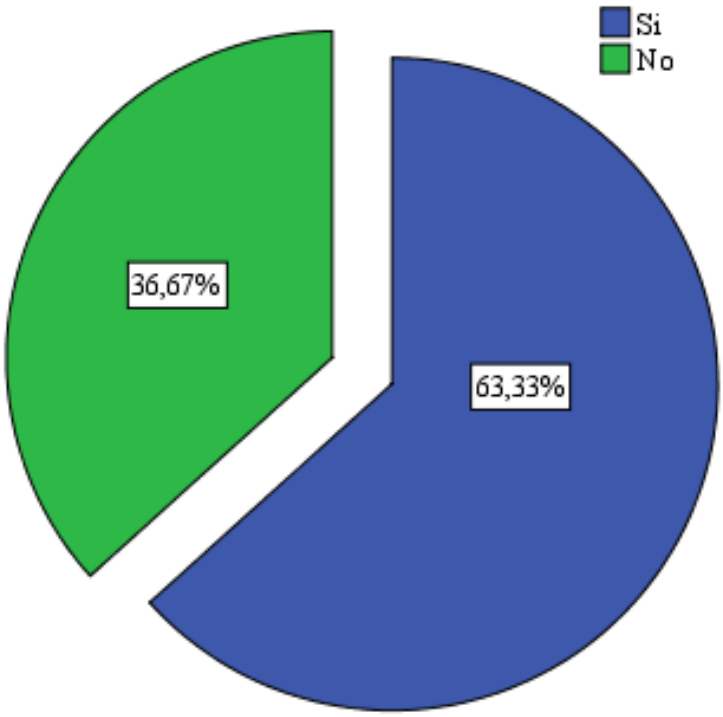

Grafico 17: Frecuencia de la clasificación de información entre confidencial y pública

Fuente: (Elaboración propia)

Basado en los resultados que se obtuvieron de la pregunta 14 de la encuesta, se puede concluir que 63.33% indicaron que se clasifica la información entre confidencial y pública. Lo que indica que se realizan el trabajo de clasificación de la información en un porcentaje significativo.

4.6 Análisis y relaciones entre resultados de la encuesta aplicada al usuario final

A continuación, se presenta el análisis de las relaciones que existen entre los resultados obtenidos.

4.6.1 Riesgos relacionados con el robo, hurto o extravío del dispositivo móvil

- Correo electrónico configurado en dispositivos robados, hurtados o extraviados

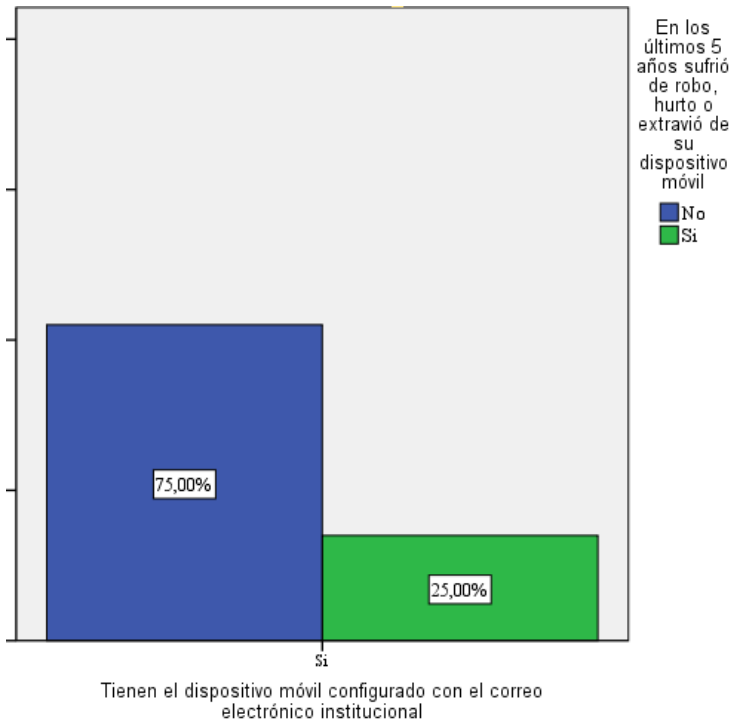

Grafico 18: Correo electrónico configurado en dispositivos robados, hurtados o extraviados

Fuente (Elaboración Propia)

El gráfico 18 muestra que la mayoría de usuarios que en los últimos cinco (5) años ha sufrido robo, hurto o extravío de sus dispositivos móviles no tenían configurado el correo electrónico institucional en su dispositivo. A pesar que es un porcentaje bajo de los que han tenido configurado el correo electrónico y les han robado el dispositivo, se recomienda que sea considerado al momento de aplicar controles.

- Archivos adjuntos en dispositivos robados, hurtados o extraviados con aplicación de correo electrónico configurada

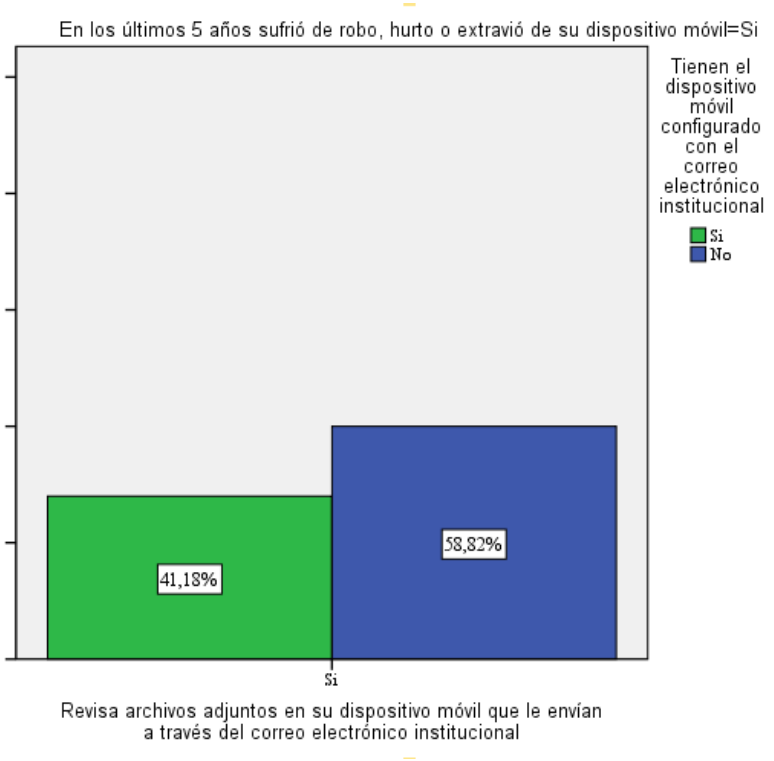

Grafico 19: Archivos adjuntos en dispositivos robados, hurtados o extraviados con aplicación de correo electrónico configurada

Fuente (Elaboración Propia)

El gráfico 19 muestra que una mayoría de usuarios que en los últimos cinco años ha sufrido robo, hurto o extravío de sus dispositivos móviles y tenían configurado el correo electrónico institucional en su dispositivo no descargan adjuntos del correo electrónico. El porcentaje de los que si lo hacen representan un porcentaje menos de la mitad y se recomienda su consideración para aplicar controles.

- Archivos adjuntos en dispositivos robados, hurtados o extraviados descargados del correo electrónico

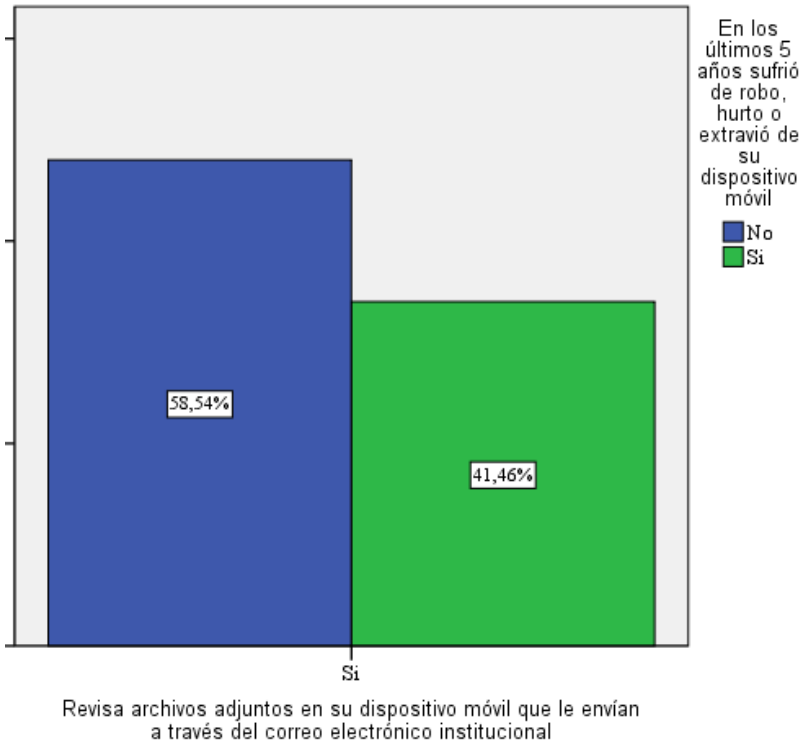

Grafico 20: Archivos adjuntos en dispositivos robados, hurtados o extraviados descargados del correo electrónico

Fuente (Elaboración Propia)

El gráfico 20 muestra los usuarios que en los últimos cinco años ha sufrido robo, hurto o extravío de sus dispositivos móviles, revisan el correo electrónico y descargan adjuntos del correo electrónico. El porcentaje de los que si lo hacen representan el 41.46% del total de la muestra.

- Dispositivos robados, hurtados o extraviados reportados en la institución con aplicación de correo electrónico instalada

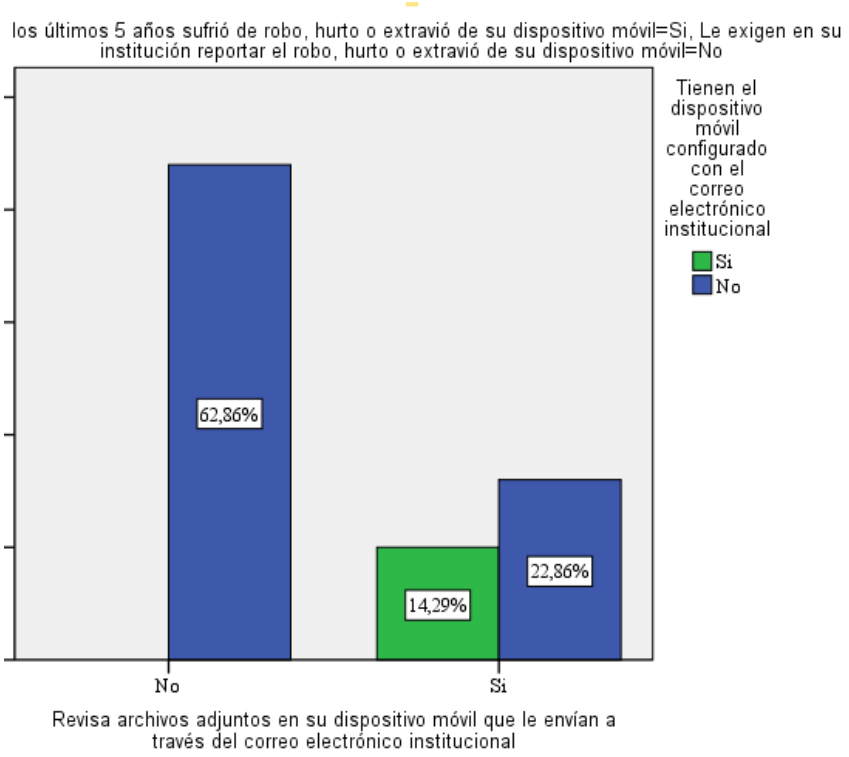

Grafico 21: Dispositivos robados, hurtados o extraviados reportados en la institución con aplicación de correo electrónico instalada

Fuente (Elaboración Propia)

El gráfico 21 muestra los usuarios que en los últimos cinco años ha sufrido robo, hurto o extravío de sus dispositivos móviles, la institución no les exige reportarlos y que tienen configurada la aplicación de correo electrónico, lo cual indica que el comportamiento de los usuarios es revisar archivos adjuntos en sus dispositivos con el correo electrónico configurado, o descargado a través de otros medios. Estos mismos usuarios les han sufrido de robo o pérdida y en la institución no les exigen reportarlo. Lo cual representa un riesgo a evaluar.

4.6.2 Riesgos relacionados con el control de activos (Dispositivos Móviles)

- Dispositivos robados, hurtados o extraviados que no han sido registrados en la institución

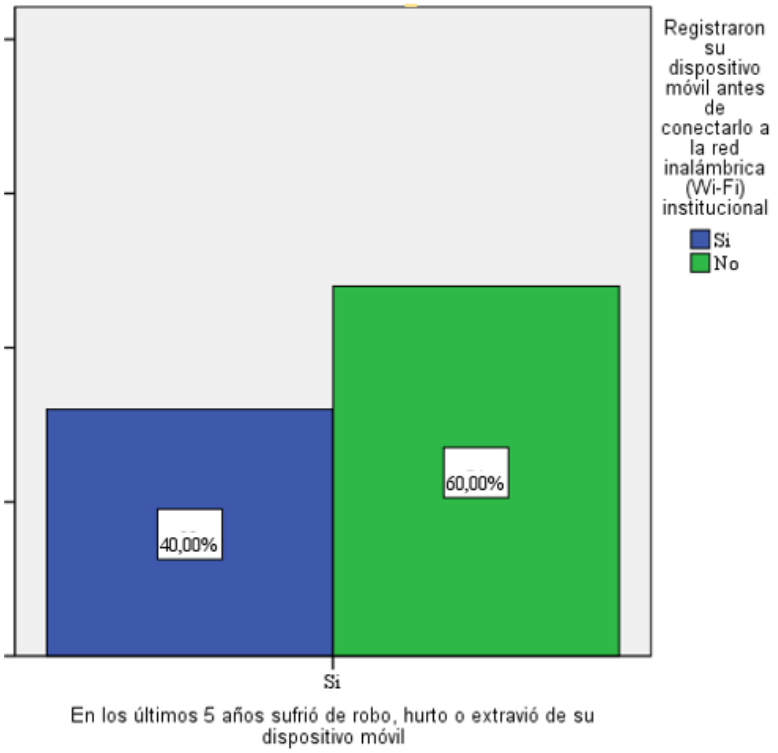

Grafico 22: Dispositivos robados, hurtados o extraviados que no han sido registrados en la institución

Fuente (Elaboración Propia)

El gráfico 22 muestra que los usuarios en un 26% no tenían su dispositivo registrado previo a conectarse a la red inalámbrica de la institución y han sufrido robo, hurto o extravío. Lo que indica que existe una falta de control para darle de baja a estos dispositivos.

- Dispositivos registrados en las instituciones previo a conectarlos a la red inalámbrica institucional

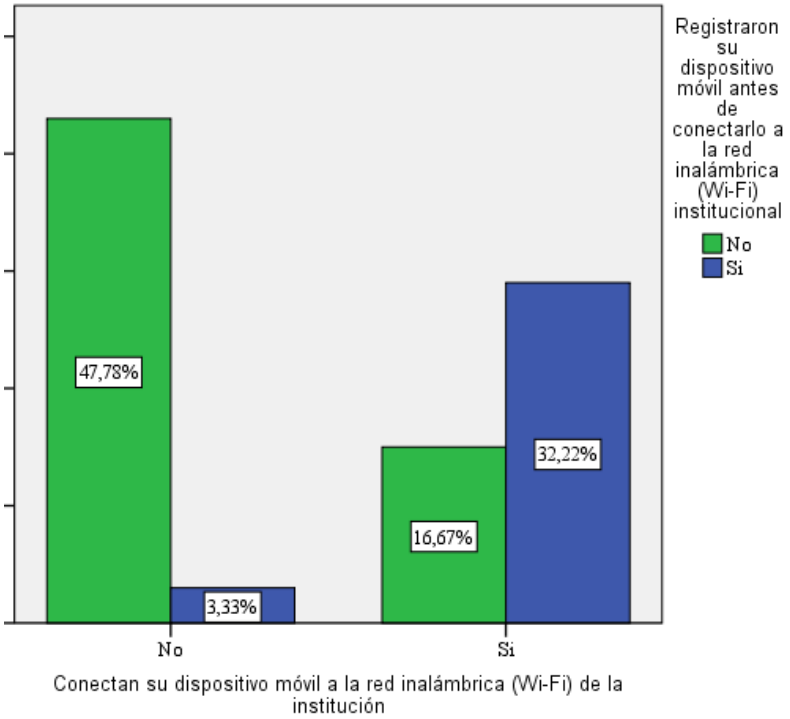

Grafico 23: Dispositivos registrados en las instituciones previo a conectarlos a la red inalámbrica institucional

Fuente (Elaboración Propia)

El gráfico 23 muestra los dispositivos que fueron registrados antes de enrolarlos a la red inalámbrica. El porcentaje de los que sí están conectados a la red inalámbrica y no fueron registrados representa un 16.67%. Lo que representa una falta de visión total de los equipos que se conectan a la red inalámbrica de la institución.

4.6.3 Riesgos relacionados con la conexión a redes inalámbricas públicas

Seguidamente se presenta el comportamiento de los usuarios y el riesgo al que se exponen cuando se conectan a redes inalámbricas públicas.

- Dispositivos que se conectan a redes inalámbricas públicas y a la red inalámbrica institucional

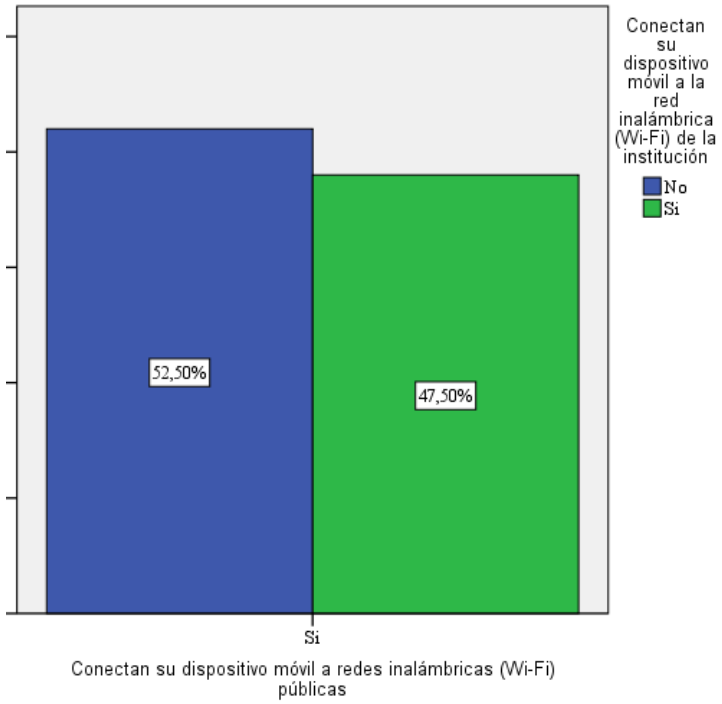

Grafico 24: Dispositivos que se conectan a Redes inalámbricas públicas y a la red inalámbrica institucional

Fuente (Elaboración Propia)

El gráfico 24 muestra los dispositivos que se conectan a redes públicas y se conectan a la red inalámbrica institucional. El porcentaje de los usuarios que conectan sus dispositivos en ambas redes representan un 47.50%. Este comportamiento puede llegar a debilitar la seguridad informática de la institución, lo anterior debido a que esto puede convertirse en una brecha de seguridad.

- Dispositivos que se conectan a redes inalámbricas públicas, a la red inalámbrica institucional y no cuentan con un software de protección o antivirus

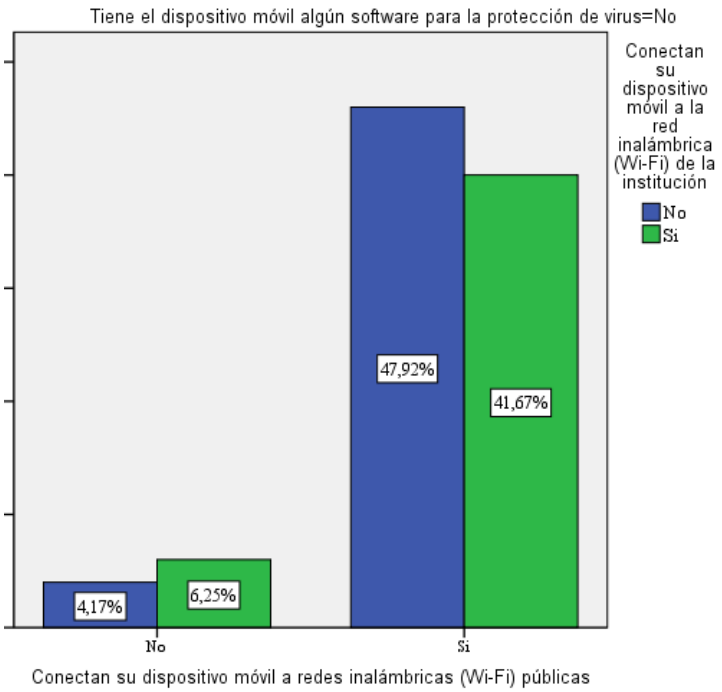

Grafico 25: Dispositivos que se conectan a Redes inalámbricas públicas, a la red inalámbrica institucional y no cuentan con un software de protección o antivirus

Fuente (Elaboración Propia)

El gráfico 25 muestra los dispositivos que se conectan a redes inalámbricas públicas, redes inalámbricas de la institución y no cuentan con un software de protección instalado, el porcentaje de usuarios con estas características representa un 47.67%. La característica de no contar con una protección antivirus, incrementa el riesgo de ataque al dispositivo y a la red inalámbrica institucional.

- Dispositivos que se conectan a redes inalámbricas públicas y tienen configurada la aplicación de correo electrónico

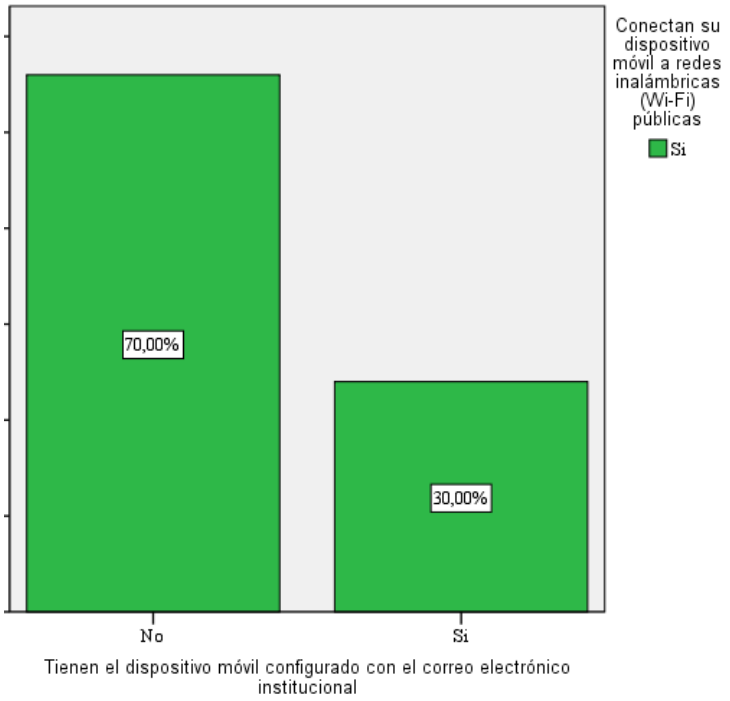

Grafico 26: Dispositivos que se conectan a redes inalámbricas públicas y tienen configurada la aplicación de correo electrónico

Fuente (Elaboración Propia)

El gráfico 26 muestra un 30% de los encuestados que conectan sus dispositivos a redes públicas y revisan su correo electrónico institucional en la aplicación instalada en su dispositivo, esto se considera una exposición riesgosa al robo de información a través de redes inalámbricas públicas.

4.6.4 Riesgos relacionados por falta de protección antes virus y software malicioso

Seguidamente se presenta la ausencia de antivirus en los dispositivos móviles de los usuarios y el riesgo al que se exponen.

- Dispositivos que se conectan a redes inalámbricas públicas y no tienen configurado un software de antivirus

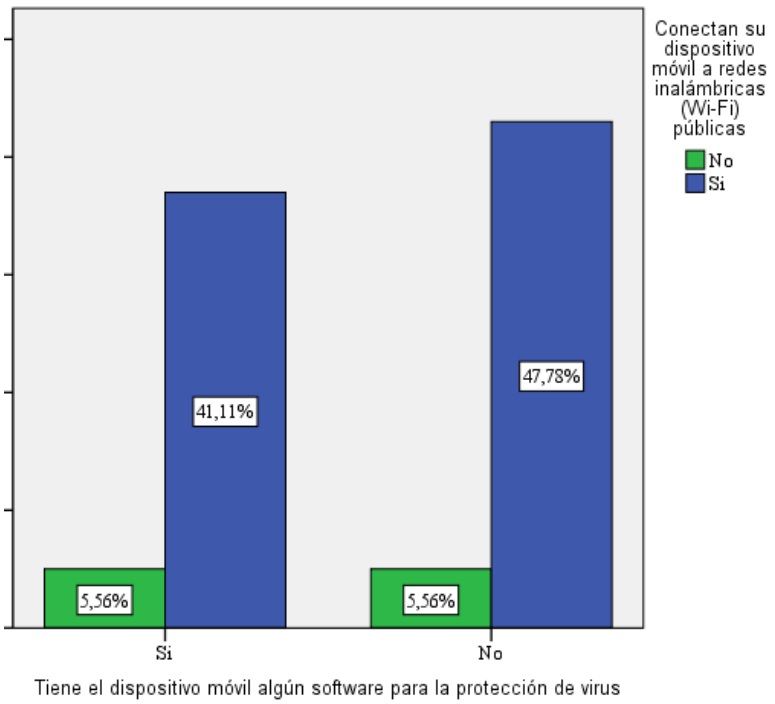

Grafico 27: Dispositivos que se conectan a redes inalámbricas públicas y no tienen configurado un software de antivirus

Fuente (Elaboración Propia)

El gráfico 27 muestra un 47.78% de los usuarios del total de la muestra conectan sus dispositivos a redes públicas, pero no tienen instalado un software de protección contra virus o software malicioso. El no contar con un software antivirus y conectarse a redes inalámbricas puede incrementar la posibilidad de que un ataque se materializa, debido a que el dispositivo no tiene un software para reducir este riesgo.

- Dispositivos que se conectan a redes inalámbricas públicas, no tienen configurado un software de antivirus y revisan el correo electrónico institucional

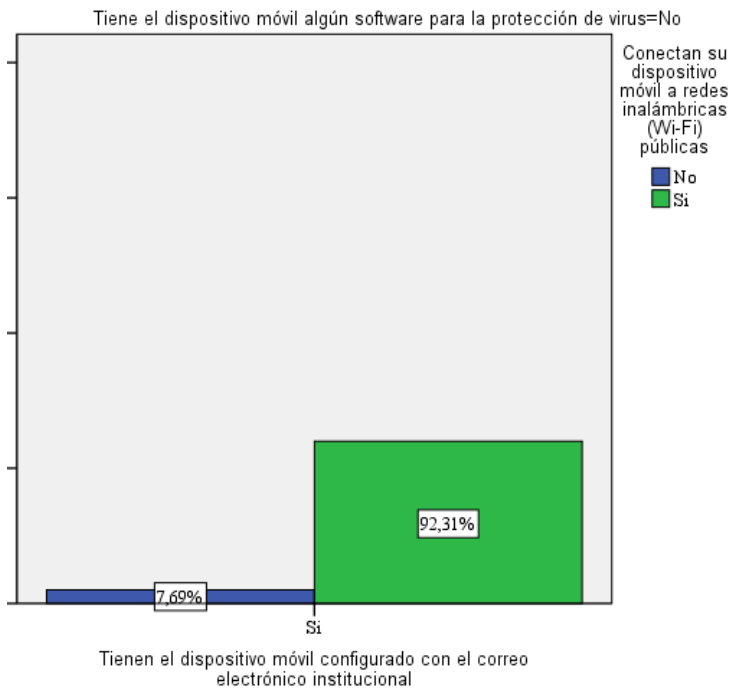

Grafico 28: Dispositivos que se conectan a redes inalámbricas públicas, no tienen configurado un software de antivirus y revisan el correo electrónico institucional

Fuente (Elaboración Propia)

El gráfico 28 muestra un 92.31% de los usuarios encuestados conectan sus dispositivos a redes públicas, no tienen instalado un software de protección contra virus o software malicioso y revisan el correo electrónico de la institución. Este comportamiento incrementa las posibilidades de que el robo de información a través de redes inalámbricas se materialice.

4.6.5 Riesgos relacionados con la administración de contraseñas en los dispositivos móviles

Seguidamente se presenta lo referente a la gestión de contraseñas tomando en cuenta el correo electrónico y los dispositivos móviles.

- Dispositivos que se conectan a redes inalámbricas públicas y el cambio de contraseña del correo electrónico está arriba de 90 días

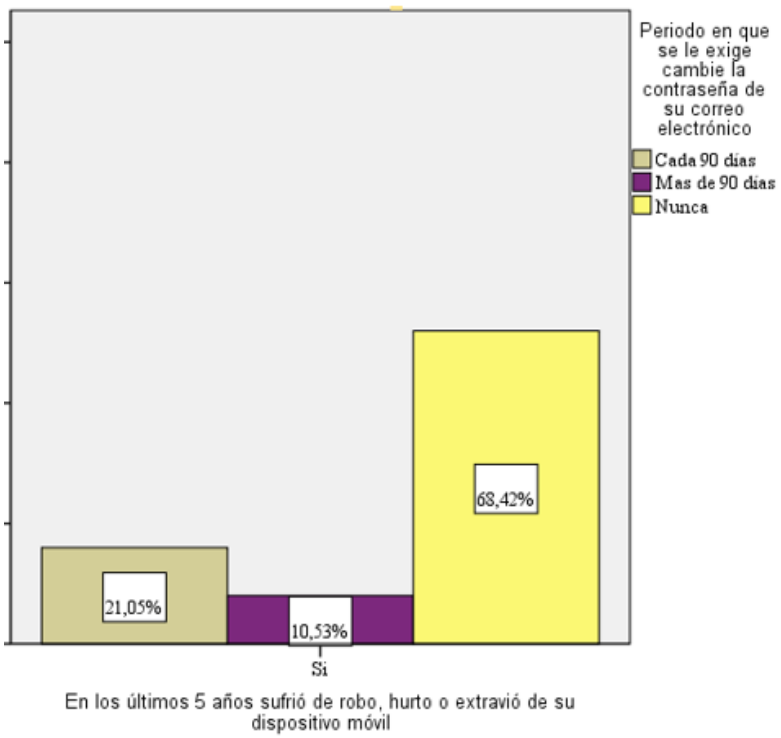

Grafico 29: Dispositivos que se conectan a redes inalámbricas públicas y el cambio de contraseña del correo electrónico está arriba de 90 días

Fuente (Elaboración Propia)

El gráfico 29 muestra un 21.05% de los usuarios encuestados que conectan sus dispositivos a redes públicas tienen cambio de contraseña de correo electrónico arriba de 90 días, y los que nunca la cambian representan un 68.42% de esta relación. La unión de estos factores representa, para un atacante, capturar la contraseña dentro de un periodo amplio de más de 90 días mientras se conecta a estas redes y así mismo utilizar estas contraseñas para delitos informáticos.

- Dispositivos que se conectan a redes inalámbricas públicas, no tienen configurado un software de antivirus y con cambio arriba de 90 días

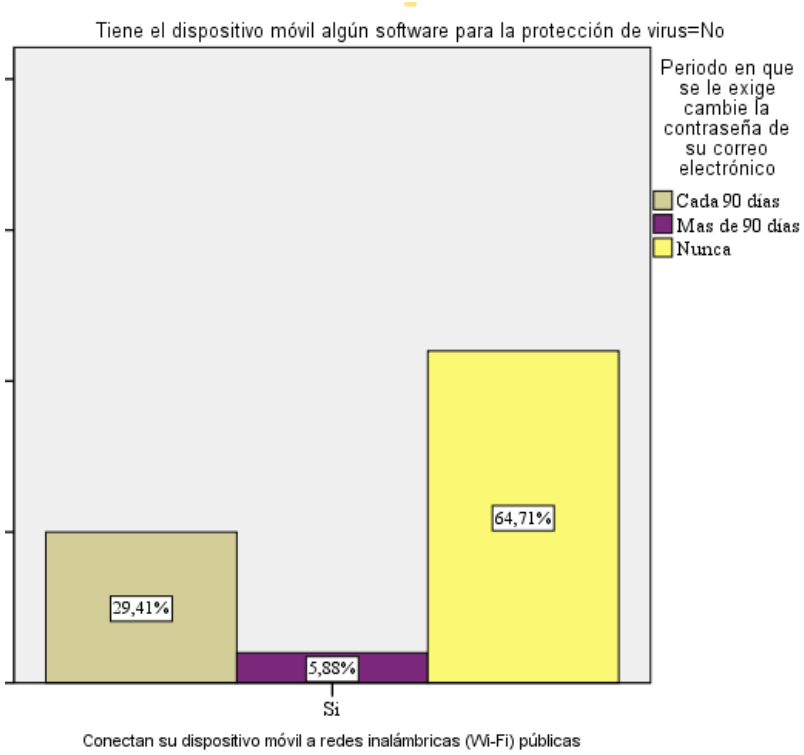

Grafico 30: Dispositivos que se conectan a redes inalámbricas públicas, no tienen configurado un software de antivirus y con cambio arriba de 90 días

Fuente (Elaboración Propia)

El gráfico 30 muestra un 29.41% de los usuarios encuestados que conectan sus dispositivos a redes públicas tienen cambio de contraseña de correo electrónico arriba de 90 días, y los que nunca la cambian representan un 64.71% de esta relación. La unión de estos factores representa, para un atacante, capturar la contraseña dentro de un periodo amplio de más de 90 días mientras se conecta a estas redes y así mismo utilizar estas contraseñas para delitos informáticos. Pero sumado a este comportamiento el factor de la falta de un antivirus en el dispositivo, incrementa el riesgo de que se materialice un ataque.

4.7 Controles de Seguridad en las IGSFH

Aunque las instituciones objeto de estudio de esta tesis cuentan con un nivel de seguridad de la información debido al conjunto de regulaciones con las que deben cumplir, fue necesario determinar si los controles de seguridad de la información se cumplen de acuerdo a estándares de seguridad reconocidos. Se agregaron a la encuesta realizada algunas preguntas relacionadas con asuntos de seguridad que cada usuario o empleado de las instituciones debe conocer obligatoriamente, dando como resultado la información mostrada en la tabla 10.

Tabla 10. Resultados de las preguntas relacionadas con la seguridad

Control consultado	Estado actual	Recomendación
Reporte de dispositivos extraviados, hurtados o robados	Se observa que la mayoría de los usuarios encuestados indicaron que no se les exige reportar si han extraviado o han sufrido de hurto o robo de su dispositivo móvil.	Es recomendable un procedimiento de reporte de dispositivos móviles que permita realizar el borrado de la información contenida en el dispositivo de manera remota o realizar un reseteo de fábrica remoto en caso que el dispositivo sufriera cualquiera de los eventos mencionados.
Charlas continuas sobre seguridad en el manejo de la información	Se observa que una cantidad considerable de usuarios indicó que no reciben charlas de seguridad en el manejo de la información.	Los planes de capacitación para el manejo de la información deben ser más efectivos y planificados de acuerdo a las necesidades de seguridad de la información y comportamiento del usuario.
registro de los dispositivos móviles antes de conectarlos a la red inalámbrica de la institución o al correo electrónico.	Al basarse en la encuesta al usuario se puede observar que las instituciones no registran todos los dispositivos que se conectan al correo electrónico	Es necesario que se dé mayor énfasis el proceso de control de activos de la institución lo que incluye un adecuado registro de los dispositivos móviles que se conectan a los recursos de la institución.
Firma de acuerdos de confidencialidad de la información.	se observó que la mayoría de los usuarios encuestados indicaron que firmaron un acuerdo de confidencialidad, lo que fortalece el tema de seguridad de la información a nivel institucional.	Una tercera parte de los encuestados afirmó no haber firmado acuerdos de confidencialidad, lo que hace suponer que a pesar que existe el procedimiento o control no está propagado en todos los procesos del negocio o alguna de las instituciones encuestada no tiene cumplimiento de dicho control.
Qué tan frecuente clasifican la información de su institución entre confidencial y pública.	Basado en los resultados que se obtuvieron de la encuesta, una mayoría de los usuarios indicaron que se clasifica la información entre confidencial y publica.	Una mínima parte de los encuestados afirmó que en su institución no clasifican la información entre confidencial y pública, lo que hace suponer que a pesar que existe el procedimiento o control no está propagado en todos los procesos del negocio o alguna de las instituciones encuestada no tiene

Control consultado	Estado actual	Recomendación
		cumplimiento de dicho control.

Fuente: (Elaboración propia)

4.8 Matriz de Riesgos

Es importante aclarar que el alcance de esta tesis está orientado a encontrar un marco de referencia para control de BYOD, sin embargo, para poder llegar a alinear este marco las instituciones deben tener ya una metodología de análisis y administración del riesgo como parte de los procesos del negocio.

De acuerdo a la información recopilada de los expertos entrevistados existen varias metodologías para poder tener un procedimiento de administración del riesgo, el Ingeniero Iván Flores comentó que ISO27001 el estándar de seguridad de la información más reconocido contiene en su cláusula 6.1.2 un proceso para control de riesgo, por otro lado el Ing. Carlos Arteaga CISSP y asesor de la dirección del Banco Central de Honduras comentaba que las instituciones pueden inclusive profundizar en el asunto y estandarizar completamente el análisis y gestión del riesgo a través del ISO 31000.

En lo investigado se pudo observar que los requerimientos para el proceso de administración del riesgo contenido en la cláusula 6.1.2 del ISO 270001:2013 no son difíciles y básicamente consisten en los siguientes cinco pasos (Calder & Watkins, 2008):

- Definir como identificar los riesgos que pueden causar la perdida de confidencialidad, integridad o disponibilidad de la información.
- Definir como identificar los propietarios del riesgo
- Definir los criterios para la evaluación de las consecuencias y la evaluación de la probabilidad del riesgo
- Definir como el riesgo será calculado
- Definir los criterios para aceptación del riesgo

Tomando en consideración lo expuesto anteriormente del tema de evaluación del riesgo y en adición los análisis de cruces de variables previamente presentados, se puede inferir que el riesgo evaluado del comportamiento de la muestra tomada es consistente a lo expuesto en la tabla 11:

Tabla 11. Evaluación del riesgo

Amenaza	Riesgo	Probabilidad	Impacto	Valor del riesgo	Nivel del riesgo
Robo, hurto o extravío de dispositivos con correo electrónico Configurado	Acceso a información confidencial	2	6	12	Importante
Robo, hurto o extravío de dispositivos con correo electrónico Configurado y adjuntos descargados.	Acceso a Información Confidencial.	1	5	5	Apreciable
robo, hurto o extravío de dispositivos con adjuntos descargados desde portal web.	Acceso a Información Confidencial.	2	15	30	Muy grave
robo, hurto o extravío de dispositivos con correo electrónico configurado y no han sido reportados.	Acceso a Información Confidencial.	1	5	5	Apreciable
Dispositivos Robados, hurtados o extraviados que no han sido registrados en la institución previo a conectarse a la red inalámbrica.	Riesgo a convertirse en un vector de ataque a los recursos de la institución.	3	12	36	Muy grave
Dispositivos que no han sido registrados en la institución y se utilizan la aplicación de correo electrónico.	Falta de Visibilidad del comportamiento del dispositivo.	2	6	12	Importante

Amenaza	Riesgo	Probabilidad	Impacto	Valor del riesgo	Nivel del riesgo
Dispositivos que no han sido registrados en la institución y se conectan a la red inalámbrica.	Falta de Visibilidad del comportamiento del dispositivo.	2	6	12	Importante
Dispositivos que se conectan a redes inalámbricas públicas y a la red inalámbrica institucional.	Riesgo a convertirse en un vector de ataque a los recursos de la institución.	5	20	100	Muy grave
Dispositivos que se conectan a redes inalámbricas públicas y a la red inalámbrica institucional y no cuentan con un software de protección o antivirus.	Riesgo a convertirse en un vector de ataque a los recursos de la institución.	3	12	36	Muy grave
Dispositivos que se conectan a redes inalámbricas públicas y tienen configurada la aplicación de correo electrónico.	Acceso a información confidencial.	3	9	27	Muy grave
Dispositivos que se conectan a redes inalámbricas públicas y no tienen configurado un software antivirus	Riesgo a convertirse en un vector de ataque a los recursos de la institución.	5	15	75	Muy grave
Dispositivos que se conectan a redes inalámbricas públicas, no tienen configurado un software antivirus y revisan el correo institucional	Acceso a información confidencial	2	6	12	Importante
Dispositivos que se conectan a redes inalámbricas públicas y la contraseña del correo electrónico está arriba de 90 días	Acceso a información confidencial	3	9	27	Muy grave

Amenaza	Riesgo	Probabilidad	Impacto	Valor del riesgo	Nivel del riesgo
Dispositivos que se conectan a redes inalámbricas públicas no tienen software antivirus y el cambio de contraseña del correo electrónico está arriba de 90 días	Riesgo a convertirse en un vector de ataque a los recursos de la institución y acceso a información confidencial	3	12	36	Muy grave

Fuente: (Elaboración propia)

Las probabilidades se realizaron mediante el resultado del cuestionario.

Los valores establecidos en la tabla 11 fueron obtenidos de la matriz de riesgos presentada en la tabla 12.

Tabla 12. Matriz de riesgos

			Impacto				
			MUY BAJO **1**	BAJO **2**	MEDIO **3**	ALTO **4**	MUY ALTO **5**
Probabilidad	MUY ALTA		5	10	15	20	25
	ALTA		4	8	12	16	20
	MEDIA		3	6	9	12	15
	BAJA		2	4	6	8	12
	MUY BAJA		1	2	3	4	5

Fuente: (Gómez Fernández & Fernández Rivero, 2015)

Las descripciones de los valores de riesgo se presentan en la tabla 13.

Tabla 13. Descripción del riesgo

	Riesgo muy grave. Requiere medidas preventivas urgentes.
	Riesgo importante. Medidas preventivas obligatorias.
	Riesgo apreciable. Estudiar económicamente ai es posible introducir medidas preventivas para reducir el nivel de riesgo. Si no fuera posible, mantener las variables

	controladas.
	Riesgo marginal. Se vigilará aunque no requiere medidas preventivas de partida.

Fuente: (Gómez Fernández & Fernández Rivero, 2015)

En el presente estudio para determinar la probabilidad del riesgo se tomó en cuenta las escalas del estudio realizado en la tabla 14.

Tabla 14. Detalles de la probabilidad

Porcentaje de la muestra	Probabilidad
1 a 9	Muy baja
10 a 19	Baja
20 a 29	Media
30 a 39	Alta
40 a 50	Muy Alto

Fuente: (Gómez Fernández & Fernández Rivero, 2015)

4.9 Norma de Referencia para Control de BYOD

Durante la investigación de construcción de un marco para control de BYOD se pudo encontrar que ya existen a nivel internacional marcos basados en los estándares de seguridad más reconocidos, uno de los más interesantes y detallado encontrado es el marco para protección de BYOD de NIST llamado "Guía de Seguridad de Usuario para Teletrabajo y Trae Tu Propio Dispositivo (BYOD) (del inglés,"User's Guide to Telework and Bring Your Own Device (BYOD) Security", el cual contiene de forma detallada las mejores prácticas a seguir para la protección no solamente de los dispositivos móviles en los cuáles se basa esta tesis, sino también para redes domésticas y estaciones de trabajo especializadas para trabajo remoto. (CITA documento NIST).

Sin embargo, guiándose por lo mencionado por los expertos de seguridad en las entrevistas realizadas, la mayoría calificada estuvo de acuerdo en que una de las grandes ventajas de ISO 27000 es que es un estándar certificable, es decir, que alineando un proceso como BYOD a esta norma, puede probar a los clientes, asociados y terceros de una institución, inclusive fuera del país que su información puede estar realmente segura, a diferencia de NIST, que aunque es un

buen marco de seguridad su contexto aplica a instituciones federales de los Estados Unidos. Por otro lado, la norma ISO 27000 se enfoca en proteger todos los tipos de información de todos los procesos de la institución y no solamente aquellos almacenados o procesados en sistemas de TI. Esto no quiere decir que el marco de NIST para protección de BYOD queda descartado, por el contrario, es un excelente marco de apoyo para determinar cómo elaborar algunos procesos que ISO 27000 deja a criterio de la institución.

Durante el proceso de investigación también se encontró un marco de la Auditoria de Administración de Sistemas, Instituto de Redes y Seguridad (SANS Institute, en inglés) para el control de dispositivos de mano (del inglés, handheld) basado en la norma de ISO 27001:2005, el cuál fue un excelente aporte para poder conocer en detalle que debe llevar un marco de referencia para control de BYOD, pero se pudo constatar que el documento no ofrece lineamientos paso a paso de cómo proteger los dispositivos móviles en una institución, sino más bien se centra a que dominios y controles de la versión 2005 ya desfasada de ISO 27001 debe apegar cada proceso. Algo que es excelente para poder verificar si una institución está cumpliendo con la norma del 2005 al pie de la letra, pero que no muestra un proceso sencillo o fácil de implementar para una institución que desea asegurar BYOD. (https://www.sans.org/reading-room/whitepapers/pda/security-policy-handheld-devices-corporate-environments-32823).

El propósito de esta tesis, por otro lado, es ofrecer un marco que sea simple de utilizar tomando en cuenta que el objetivo principal es cambiar el comportamiento de los usuarios de BYOD, de acuerdo a lo mencionado por el experto en implementaciones de ISO 27001 Dejan Kosutic, “cuando es necesario cambiar el comportamiento de los usuarios y este cambio está muy relacionado con reglas adicionales de seguridad, es necesario entonces que estas reglas sean fácilmente entendibles y explicadas lo más breve posible” (“Secure & Simple A small-business guide to implementing ISO 27001 on your own”), por otro lado, tal como se mencionó en el inicio de esta tesis, en el marco teórico, de acuerdo a la Asociación de Auditoría y Control de Sistemas de Información (ISACA) en su informe de seguridad de dispositivos móviles, un marco deberá contener siempre una política que cumpla elementos de control, por ejemplo, aplicable a una variedad de dispositivos, administración centralizada, política simple y fácil de implementar, y mantener flexibilidad de administración y manejo (ISACA,2010).

Durante las entrevistas con los expertos, tanto el Ing. Carlos Arteaga como el Ingeniero Ivan Flores detallaron que dominios y controles de ISO 27001:2013 se pueden utilizar siendo estos los siguientes:

1. A.6.2.1 Política de dispositivos móviles: Según este control se debe adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles, es decir que la norma también debe estar basada en la identificación de riesgos.
2. A.6.2.2 Teletrabajo: Cuando se permita el teletrabajo, deben aplicarse los mismos niveles de seguridad que en el trabajo local. El control requiere la implementación de medidas de seguridad para acceso, procesamiento y almacenamiento de la información, una norma de BYOD adecuada debe cubrir estas tres (3) áreas.
3. A.8.1.2 Propiedad de los activos: Toda la información y activos del inventario asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la Organización.
4. A.8.1.3 Uso aceptable de activos: Este control tiene como finalidad definir cómo va ser utilizado cada activo dentro de la organización.
5. A.8.1.4 Devolución de activos: Todos los empleados y usuarios de terceras partes deberían devolver todos los activos de la organización que estén en su posesión/responsabilidad una vez finalizado el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo
6. A.8.2.3 Manejo o administración de activo: Este control describe como se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
7. A.9.3.1 Uso de información confidencial para la autenticación: Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad de la organización en el uso de información confidencial para la autenticación.
8. A.9.4.3 Gestión de contraseñas de usuario: Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar contraseñas de calidad.

9. A.11.2.6 Seguridad de los equipos y activos fuera de las instalaciones: Se debería aplicar la seguridad a los activos requeridos para actividades fuera de las dependencias de la organización y en consideración de los distintos riesgos.
10. A.11.2.8 Equipo informático de usuario desatendido: Los usuarios se deberían asegurar de que los equipos no supervisados cuentan con la protección adecuada
11. A.11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla: Se debería adoptar una política de puesto de trabajo despejado para documentación en papel y para medios de almacenamiento extraíbles y una política de monitores sin información para las instalaciones de procesamiento de información.
12. A.12.2.1 Controles contra el código malicioso: Se deberían implementar controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios
13. A.12.3.1 Copias de seguridad de la información: Se deberían realizar y pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida.
14. A.12.5.1 Instalación del software en sistemas en producción: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operacionales.
15. A.12.6.2 Restricciones en la instalación de software: Se deberían establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios
16. A.13.2.1 Políticas y procedimientos de transferencia de la información: Este control exige el uso de documentación que describa como es transferida la información a través de cualquier equipo de comunicación, incluidos todos aquellos usuarios de dispositivos móviles. Este marco propuesto cubre estos requerimientos para control de BYOD sin necesidad de tener una política por separado.
17. A.13.2.3 Mensajería electrónica: Este control trata sobre cómo se debe proteger la información enviada en la mensajería electrónica.
18. A.13.2.4 Acuerdos de confidencialidad y secreto: se deberían identificar, revisar y documentar de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de información.

19. A.18.1.2 Derechos de propiedad intelectual (DPI): Se deberían implementar procedimientos adecuados para garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y utilizar productos software originales.

Aunque existen muchos más controles de la norma ISO 27001 que pueden ser aplicados a BYOD, los mencionados por los expertos y descritos anteriormente, son los involucrados directamente en la construcción del marco propuesto y cumpliendo estos los demás controles son implicados de forma predeterminada cubriendo las siguientes características del marco:

1. Riesgos principales involucrados en el uso de dispositivos móviles.
2. Cuáles aplicaciones móviles son obligatorias, cuales son permitidas y cuales no son permitidas para el proceso y almacenamiento de información de la empresa.
3. Que servicios son permitidos para almacenar información confidencial de la institución.
4. Que controles de acceso son necesarios utilizar en los dispositivos móviles.
5. Si fuera necesario respaldo de la información o configuración de cada dispositivo, con qué frecuencia se realizará y donde se almacenará.
6. Que tipos de mensajes no son permitidos.
7. Cuáles serán los lineamientos para protección física de los dispositivos móviles.
8. A que redes los usuarios de dispositivos móviles tienen permitido conectarse y que tipo de protección utilizaran cuando haya transferencia de información.
9. Definición de quien es el propietario de los datos que son almacenados en los dispositivos móviles.
10. Que personal de la institución tiene permitido o no permitido utilizar dispositivos móviles.
11. Qué tipo de dispositivos móviles en particular son permitidos y no permitidos en la institución.
12. Como serán manejadas las brechas de seguridad que han sido reportadas.
13. Qué departamento será el responsable por la capacitación de los usuarios en el uso de BYOD.
14. ¿Si los usuarios utilizarán sus dispositivos móviles personales en procesos del negocio, tendrán algún reembolso?

15. Si la institución hará uso de algún software para poder brindar características especiales a la administración de los dispositivos enrolados, cuáles serán esas características, ¿Se hará uso de un ambiente controlado para bloquear aplicaciones no deseables?, ¿Se manejará rastreo o monitoreo en tiempo real del comportamiento del dispositivo?, si el software tiene la capacidad de manipular la información ¿Qué derechos tendrá? ¿Será únicamente derecho de acceso o podrá editar y borrar la información del dispositivo?

Generalmente las instituciones al identificar los riesgos y vincularlos con los dominios y controles de la norma de seguridad de ISO270001:2013 lo que hacen es estructurar la documentación, una de las maneras más comunes es relacionar cada sección con una política, y esta política tiene procedimientos, y cada procedimiento tiene instrucciones de trabajo detallados que cubren cada control. En el caso de esta norma de BYOD nos dejamos llevar por dos reglas importantes, primero, analizar los riesgos adecuadamente y ordenarlos de acuerdo a la gravedad o importancia, para centrarnos en aquellos que necesitan un tratamiento obligatorio.

En la tabla 15 la cual contiene la matriz de riesgos ordenada de acuerdo al estudio realizado en las IGSFH, se puede observar un ejemplo práctico de cómo podemos aplicar los controles de ISO27001:2013 y las características expuestas anteriormente, las cuales dan a conocer lo que el marco debe contener:

Tabla 15. Ejemplo para aplicar los controles

Amenaza	Riesgo	Valor del riesgo	Nivel del riesgo	Controles a aplicar	Características para mitigación del riesgo
Dispositivos que se conectan a redes inalámbricas públicas y a la red inalámbrica institucional.	Riesgo a convertirse en un vector de ataque a los recursos de la institución.	100	Muy grave	A.6.2.1 A.6.2.2 A.11.2.6 A.11.2.8 A.13.2.1 A.13.2.4	- Protección contra riesgos de uso de dispositivos móviles. - Revisar niveles de seguridad para teletrabajo. - Medidas de seguridad para activos fuera de la institución - Políticas y procedimientos para la transferencia de la información. - Se deben manejar acuerdos de confidencialidad para protección de la información.

Amenaza	Riesgo	Valor del riesgo	Nivel del riesgo	Controles a aplicar	Características para mitigación del riesgo
Dispositivos que se conectan a redes inalámbricas públicas y no tienen configurado un software antivirus	Riesgo a convertirse en un vector de ataque a los recursos de la institución.	75	Muy grave	A.6.2.1 A.6.2.2 A.11.2.6 A.11.2.8 A.12.2.1 A.13.2.1 A.13.2.4	- Protección contra riesgos de uso de dispositivos móviles. - Revisar niveles de seguridad para teletrabajo. - Medidas de seguridad para activos fuera de la institución - Protección adecuada contra el código malicioso. - Políticas y procedimientos para la transferencia de la información. - Se deben manejar acuerdos de confidencialidad para protección de la información.
Dispositivos Robados, hurtados o extraviados que no han sido registrados en la institución previa a conectarse a la red inalámbrica.	Riesgo a convertirse en un vector de ataque a los recursos de la institución.	36	Muy grave	A.6.2.1 A.8.1.2 A.8.1.4 A.8.2.3 A.11.2.6 A.11.2.8 A.12.3.1 A.13.2.4	- Protección contra riesgos de uso de dispositivos móviles. - Inventario de información y activos que describa la propiedad de los mismos. - Procedimiento para devolución de los activos donde se incluya que sucede con los extraviados, dañados, etc. - Control para implementar un procedimiento para administración de activos - Control para protección de los activos fuera de las instalaciones y activo que funcionará de forma desatendida - Se deberá mantener un procedimiento para respaldo de la información de los activos. - Se deben manejar acuerdos de confidencialidad para protección de la información
Dispositivos que se conectan a redes inalámbricas públicas y a la red inalámbrica institucional y no cuentan con un software de protección o antivirus.	Riesgo a convertirse en un vector de ataque a los recursos de la institución.	36	Muy grave	A.6.2.1 A.6.2.2 A.11.2.6 A.11.2.8 A.12.2.1 A.13.2.1 A.13.2.4	- Protección contra riesgos de uso de dispositivos móviles. - Revisar niveles de seguridad para teletrabajo - Control para protección de los activos fuera de las instalaciones y activo que funcionará de forma desatendida - Protección adecuada contra el código malicioso - Políticas y procedimientos para la transferencia de la

Amenaza	Riesgo	Valor del riesgo	Nivel del riesgo	Controles a aplicar	Características para mitigación del riesgo
					información - Se deben manejar acuerdos de confidencialidad para protección de la información
Dispositivos que se conectan a redes inalámbricas públicas no tienen software antivirus y el cambio de contraseña del correo electrónico está arriba de 90 días	Riesgo a convertirse en un vector de ataque a los recursos de la institución y acceso a información confidencial	36	Muy grave	A.6.2.1 A.6.2.2 A.9.3.1 A.9.4.3 A.11.2.6 A.11.2.8 A.12.2.1 A.13.2.1 A.13.2.4	- Protección contra riesgos de uso de dispositivos móviles. - Revisar niveles de seguridad para teletrabajo. - Se debe fortalecer la política de gestión de contraseñas de los sistemas de información - Control para protección de los activos fuera de las instalaciones y activo que funcionará de forma desatendida - Protección adecuada contra el código malicioso - Políticas y procedimientos para la transferencia de la información - Se deben manejar acuerdos de confidencialidad para protección de la información
Robo, hurto o extravío de dispositivos con adjuntos descargados desde portal web.	Acceso a Información Confidencial.	30	Muy grave	A.6.2.1 A.8.1.2 A.8.1.4 A.8.2.3 A.11.2.6 A.11.2.8 A.12.3.1 A.13.2.4	- Protección contra riesgos de uso de dispositivos móviles. - Inventario de información y activos que describa la propiedad de los mismos. - Procedimiento para devolución de los activos donde se incluya que sucede con los extraviados, dañados, etc. - Control para implementar un procedimiento para administración de activos. - Control para protección de los activos fuera de las instalaciones y activo que funcionará de forma desatendida. - Se deberá mantener un procedimiento para respaldo de la información de los activos. - Se deben manejar acuerdos de confidencialidad para protección de la información.

Amenaza	Riesgo	Valor del riesgo	Nivel del riesgo	Controles a aplicar	Características para mitigación del riesgo
Dispositivos que se conectan a redes inalámbricas públicas y tienen configurada la aplicación de correo electrónico.	Acceso a información confidencial.	27	Muy grave	A.6.2.1 A.6.2.2 A.8.2.3 A.9.3.1 A.9.4.3 A.11.2.6 A.11.2.8 A.12.2.1 A.12.3.1 A.13.2.1 A.13.2.4	- Protección contra riesgos de uso de dispositivos móviles. - Revisar niveles de seguridad para teletrabajo. - Control para implementar un procedimiento para administración de activos. - Se debe fortalecer la política de gestión de contraseñas de los sistemas de información. - Control para protección de los activos fuera de las instalaciones y activo que funcionará de forma desatendida. - Se deberá mantener un procedimiento para respaldo de la información de los activos. - Protección adecuada contra el código malicioso. - Se deberá mantener un procedimiento para respaldo de la información de los activos. - Políticas y procedimientos para la transferencia de la información. - Se deben manejar acuerdos de confidencialidad para protección de la información.
Dispositivos que se conectan a redes inalámbricas públicas y la contraseña del correo electrónico está arriba de 90 días	Acceso a información confidencial	27	Muy grave	A.6.2.1 A.6.2.2 A.9.3.1 A.9.4.3 A.11.2.6 A.11.2.8 A.12.2.1 A.13.2.1 A.13.2.4	- Protección contra riesgos de uso de dispositivos móviles. - Revisar niveles de seguridad para teletrabajo. - Se debe fortalecer la política de gestión de contraseñas de los sistemas de información. - Control para protección de los activos fuera de las instalaciones y activo que funcionará de forma desatendida. - Protección adecuada contra el código malicioso. - Políticas y procedimientos para la transferencia de la información. - Se deben manejar acuerdos de confidencialidad para protección de la información.

Amenaza	Riesgo	Valor del riesgo	Nivel del riesgo	Controles a aplicar	Características para mitigación del riesgo
Dispositivos que no han sido registrados en la institución y se utilizan la aplicación de correo electrónico.	Falta de Visibilidad del comportamiento del dispositivo.	12	Importante	A.6.2.1 A.6.2.2 A.8.2.3 A.9.3.1 A.9.4.3 A.11.2.6 A.11.2.8 A.12.2.1 A.12.3.1 A.13.2.1 A.13.2.4	- Protección contra riesgos de uso de dispositivos móviles. - Revisar niveles de seguridad para teletrabajo. - Control para implementar un procedimiento para administración de activos. - Se debe fortalecer la política de gestión de contraseñas de los sistemas de información. - Control para protección de los activos fuera de las instalaciones y activo que funcionará de forma desatendida. - Protección adecuada contra el código malicioso. - Se deberá mantener un procedimiento para respaldo de la información de los activos. - Políticas y procedimientos para la transferencia de la información. - Se deben manejar acuerdos de confidencialidad para protección de la información.
Dispositivos que no han sido registrados en la institución y se conectan a la red inalámbrica.	Falta de Visibilidad del comportamiento del dispositivo.	12	Importante	A.6.2.1 A.6.2.2 A.8.2.3 A.9.3.1 A.12.2.1 A.12.3.1 A.13.2.1 A.13.2.4	- Protección contra riesgos de uso de dispositivos móviles. - Revisar niveles de seguridad para teletrabajo. - Control para implementar un procedimiento para administración de activos. - Se debe fortalecer la política de gestión de contraseñas de los sistemas de información. - Protección adecuada contra el código malicioso. - Se deberá mantener un procedimiento para respaldo de la información de los activos. - Políticas y procedimientos para la transferencia de la información. - Se deben manejar acuerdos de confidencialidad para protección de la información.

Amenaza	Riesgo	Valor del riesgo	Nivel del riesgo	Controles a aplicar	Características para mitigación del riesgo
Robo, hurto o extravío de dispositivos con correo electrónico Configurado	Acceso a información confidencial	12	Importante	A.6.2.1 A.8.1.2 A.8.1.4 A.8.2.3 A.11.2.6 A.11.2.8 A.12.3.1 A.13.2.4	- Protección contra riesgos de uso de dispositivos móviles. - Inventario de información y activos que describa la propiedad de los mismos. - Procedimiento para devolución de los activos donde se incluya que sucede con los extraviados, dañados, etc. - Control para implementar un procedimiento para administración de activos. - Control para protección de los activos fuera de las instalaciones y activo que funcionará de forma desatendida. - Se deberá mantener un procedimiento para respaldo de la información de los activos. - Se deben manejar acuerdos de confidencialidad para protección de la información
Dispositivos que se conectan a redes inalámbricas públicas, no tienen configurado un software antivirus y revisan el correo institucional	Acceso a información confidencial	12	Importante		
Robo, hurto o extravío de dispositivos con correo electrónico Configurado y adjuntos descargados.	Acceso a Información Confidencial.	5	Apreciable	A.6.2.1 A.8.1.2 A.8.1.4 A.8.2.3 A.11.2.6 A.11.2.8 A.12.3.1 A.13.2.4	- Protección contra riesgos de uso de dispositivos móviles. - Inventario de información y activos que describa la propiedad de los mismos. - Procedimiento para devolución de los activos donde se incluya que sucede con los extraviados, dañados, etc. - Control para implementar un procedimiento para administración de activos. - Control para protección de los activos fuera de las instalaciones y activo que funcionará de forma desatendida. - Se deberá mantener un

Amenaza	Riesgo	Valor del riesgo	Nivel del riesgo	Controles a aplicar	Características para mitigación del riesgo
					procedimiento para respaldo de la información de los activos. - Se deben manejar acuerdos de confidencialidad para protección de la información
Robo, hurto o extravío de dispositivos con correo electrónico configurado y no han sido reportados.	Acceso a Información Confidencial.	5	Apreciable	A.6.2.1 A.8.1.2 A.8.1.4 A.8.2.3 A.11.2.6 A.11.2.8 A.12.3.1 A.13.2.4	- Protección contra riesgos de uso de dispositivos móviles. - Inventario de información y activos que describa la propiedad de los mismos. - Procedimiento para devolución de los activos donde se incluya que sucede con los extraviados, dañados, etc. - Control para implementar un procedimiento para administración de activos. - Control para protección de los activos fuera de las instalaciones y activo que funcionará de forma desatendida. - Se deberá mantener un procedimiento para respaldo de la información de los activos. - Se deben manejar acuerdos de confidencialidad para protección de la información

Fuente: (Elaboración propia)

La segunda regla en la cual basamos este marco de referencia está basada en la cuestión de que tan extensiva realizar la documentación, decidimos entonces crear una política que contuviera todos los controles relacionados con BYOD en un solo documento. Esto es debido a que ISO27001 no establece una norma que mencione que controles van con que procedimientos o políticas, en otras palabras, tenemos la libertad de poder adaptar la documentación a las necesidades de la institución, por supuesto, si cada institución recibe la propuesta realizada en esta tesis y decide que es mejor crear un procedimiento para cada control, está en la total libertad de llevarlo a cabo.

Sin más preámbulos, en el anexo 3 se presenta el documento de política para el marco de referencia para control de BYOD propuesto para las Instituciones Gubernamentales del Sector Financiero de Honduras.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- Los controles existentes en las IGSFH no se pueden enumerar, debido a que por temas de confidencialidad no se pudo realizar la entrevista al encargado de seguridad de cada institución, por lo que fue necesario seleccionar controles recomendados por los expertos entrevistados. Los controles recomendados fueron investigados mediante una encuesta aplicada a empleados, y de acuerdo a los resultados de la encuesta, estos controles tienen oportunidades mejora para mitigar el riesgo al exponer la información sensible almacenada en los dispositivos.

- La entrevista con expertos proporcionó un panorama amplio de los controles de seguridad que deben aplicarse en las IGSFH, y así mismo indicaron que las mejores prácticas internacionales deben ser fuertemente consideradas para control del BYOD. Se concluye que el estándar ISO27001 es el estándar recomendado por la mayoría de los expertos, este estándar cubre áreas de negocio y técnicas, así mismo el recurso humano, lo que lo hace un estándar que engloba toda la organización y no solamente la parte tecnológica como software y hardware.

- Al procesar los datos estadísticos obtenidos a través de la encuesta, se pudo observar que los usuarios exponen contantemente la información sensible de la institución, cuando estos tienen patrones como conectar sus dispositivos móviles sin antivirus y con información institucional a redes inalámbricas públicas. Patrones como el antes expuesto indica que los usuarios no están conscientes de los riesgos a los que exponen la información.

- Las mejores prácticas pueden encontrarse en la norma de Referencia para Control de BYOD en la página 92 de este documento. Estas prácticas son bien conocidas en

el ámbito internacional, y tienen una lista amplia de controles a aplicar, por lo anterior se tomaron los controles más significativos y recomendados por los expertos en relacionado a la tendencia BYOD y así brindar un marco de referencia para las IGSFH para su control.

- El marco de referencia que el gobierno hondureño está implementando para el control de BYOD, no se pudo investigar de primera mano, esto debido a ser este un tema confidencial para las instituciones, pero con la encuesta aplicada a los empleados y la entrevista a expertos, se puede tener una visión del marco que están aplicando, el cual considera factores tecnológicos, recurso humano y políticas. Pero estos controles deben más eficientes en su aplicación, y por ende se presenta un marco de referencia para que sea considerado por las IGSFH.

5.2 Recomendaciones

- Para el análisis del riesgo se recomienda incluir en el cuestionario una pregunta relacionada con el nivel jerárquico que el encuestado tiene. Es decir, si el encuestado es operativo, táctico o estratégico. Esta pregunta puede determinar en qué nivel jerárquico enfocar controles de seguridad más críticos, y también que usuarios no deberían tener conexión a los servicios informáticos de la institución.

- Realizar un análisis del impacto positivo en la productividad que genera el uso de BYOD en las IGSFH. Este análisis determinara si es factible que los usuarios utilicen el dispositivo móvil personal para temas de laborales y por ende se determina el presupuesto que se debe considerar para la plataforma tecnológica, políticas y recurso humano para el control de dispositivos móviles.

- El análisis de riesgos debe realizarse a nivel de proceso de negocio, considerando la necesidad o no de que el dispositivo móvil personal realmente represente un valor agregado al proceso, probablemente, en este análisis, no todos los procesos requieren que un usuario mantenga conectado su dispositivo móvil al correo electrónico institucional.

- La Norma de Referencia para Control de BYOD y la Política de BYOD presentada en este documento, deben ser complementarias para su aplicación. Así mismo no se deben descartar otras normas como la del NIST.

- Debido a que el estudio se enfoca a la protección de la información confidencial gubernamental almacenada en dispositivos móviles, se recomienda que este análisis se amplié a otras secretarias del gobierno y que la aplicación del marco de referencia presentado se realice a nivel nacional. A su vez que este marco sea administrado por la secretaria o las secretarias encargadas de la seguridad nacional.

5.3 Líneas Futuras

- Esta investigación puede continuar para los próximos años en periodos considerables, de acuerdo a la evolución tecnológica, penetración del internet a nivel nacional y el incremente en uso de dispositivos móviles para temas laborales. Lo anterior con el objetivo de conocer la evolución del comportamiento de los usuarios a través del tiempo y poder tener métricas de control.
- Realizar una nueva versión de esta investigación para que un segundo grupo de alumnos pueda continuar aplicando la encuesta a instituciones privadas y realizar el mismo análisis. Así se podrá desarrollar una comparativa entre el nivel de control que tienen las instituciones privadas contra el nivel de control que tienen las instituciones públicas, y aplicar las mejoras que apliquen.
- El marco de referencia presentado podría ser utilizado para ser impartido en una clase de la Maestría de Gestión de Tecnologías de la información, con el objetivo de que las nuevas generaciones de maestrantes conozcan de primera mano el uso de dispositivos móviles en las IGSFH y los controles que se deben aplicar en estas.
- Puede ser útil extender este tipo de estudio y propuesta de un marco de referencia a otras áreas tecnológicas que se apliquen al gobierno de Honduras como ser seguridad informática en nuevas tendencias como el uso de Computación en la Nube (Cloud Computing, en inglés), lo anterior es considerado para fortalecer la seguridad del gobierno en diferentes temas tecnológicos.

REFERENCIAS

Ali, S. M., Soomro, T. R., & Brohi, M. N. (2013). MAPPING INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY WITH OTHER INFORMATION TECHNOLOGY STANDARDS AND BEST PRACTICES. *Journal of Computer Science*, 7.

Brownlee, T. (2013). *The Global BYOD Management Services Ecosystem* (p. 16). Forrester Research Inc. Recuperado a partir de https://www.business.att.com/content/whitepaper/Forrester-The_Global_BYOD_Management_Services_Ecosystem_1.6.14-1.6.15.pdf

Calder, A., & Watkins, S. (2008). *IT Governance A Manager's Guide to Data Security and ISO 27001/ISO 27002* (4th ed.). London: Kogan Page.

Center, P. R. (2010a). Millennials: Confident. Connected. Open to Change. *Pew Research Center's Social & Demographic Trends Project*, 149.

Center, P. R. (2010b). Millennials: Confident. Connected. Open to Change. *Pew Research Center's Social & Demographic Trends Project*, 149.

Company, N. (2016a). Millennials Are Top Smartphone Users [Market Research]. Recuperado el 27 de mayo de 2017, a partir de http://www.nielsen.com/us/en/insights/news/2016/millennials-are-top-smartphone-users.html

Company, N. (2016b). Millennials Are Top Smartphone Users [Market Research]. Recuperado el 27 de mayo de 2017, a partir de http://www.nielsen.com/us/en/insights/news/2016/millennials-are-top-smartphone-users.html

CONATEL. (2017). Desempeño del Sector de Telecomunicaciones Primer Trimestre 2017. Recuperado el 21 de septiembre de 2017, a partir de http://www.conatel.gob.hn/doc/indicadores/2017/Desempe%C3%B1o_del_Sector_De_Telecomunicaciones_1T2017.pdf

Disterer, G., & Kleiner, C. (2013). BYOD Bring Your Own Device. *Procedia Technology*, *9*, 43–53. https://doi.org/10.1016/j.protcy.2013.12.005

FORTINET INC. (2017). *Secure Access Solutions* (p. 8). USA: FORTINET INC. Recuperado a partir de https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/SG-SAA-Enterprise-Network.pdf

Gartner, I. (2014a). Gartner outlined key predictions around mobility. Recuperado el 28 de mayo de 2017, a partir de http://www.gartner.com/newsroom/id/2939217

Gartner, I. (2014b). Gartner outlined key predictions around mobility. Recuperado el 28 de mayo de 2017, a partir de http://www.gartner.com/newsroom/id/2939217

Gómez Fernández, L., & Fernández Rivero, P. P. (2015). *Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad*. España: AENOR.

GSMA, A. (2016). *La Economía Móvil América Latina 2016* (p. 74). United Kingdom: GSM Association. Recuperado a partir de https://www.gsmaintelligence.com/research/?file=6762be5b756dbff2b0cbaa1d59838d7b&download

Hernandez Sanpieri, R., Fernandez-Collado, C., & Baptista Lucio, P. (2006). *Metodologia de la Investigacón* (4ta ed.). Mexico: McGraw-Hill Interamericana.

Hom, E. J. (2012, febrero 8). Mobile Device Security: Startling Statistics on Data Loss and Data Breaches. Recuperado el 28 de mayo de 2017, a partir de

http://www.channelpronetwork.com/article/mobile-device-security-startling-statistics-data-loss-and-data-breaches

IBSG, C. (2012). *BYOD: A Global Perspective Harnessing Employee-Led Innovation* (Survey Report) (p. 21). Cisco. Recuperado a partir de http://www.cisco.com/c/dam/en_us/about/ac79/docs/re/BYOD_Horizons-Global.pdf

IDC. (2016a). Smartphone Vendor Market Share 2016 Q3. Recuperado el 28 de mayo de 2017, a partir de https://www.idc.com/promo/smartphone-market-share/vendor

IDC. (2016b). Smartphone Vendor Market Share 2016 Q3. Recuperado el 28 de mayo de 2017, a partir de https://www.idc.com/promo/smartphone-market-share/vendor

IDC. (2016c). Worldwide Tablet Market Forecast 2016. Recuperado el 28 de mayo de 2017, a partir de http://www.idc.com/getdoc.jsp?containerId=prUS41962916

IDC. (2016d). Worldwide Tablet Market Forecast 2016. Recuperado el 28 de mayo de 2017, a partir de http://www.idc.com/getdoc.jsp?containerId=prUS41962916

ISACA. (2010a). *Securing Mobile Devices* (p. 10). USA: ISACA.

ISACA. (2010b). *Securing Mobile Devices* (p. 10). USA: ISACA.

Kaspersky, L. (2016a). *Consumer Security Risks Survey 2016 Connected but not Protected* (Consumer Security Risks Survey) (p. 24). Kaspersky. Recuperado a partir de https://press.kaspersky.com/files/2016/10/B2C_survey_2016_report.pdf

Kaspersky, L. (2016b). *Consumer Security Risks Survey 2016 Connected but not Protected* (Consumer Security Risks Survey) (p. 24). Kaspersky. Recuperado a partir de https://press.kaspersky.com/files/2016/10/B2C_survey_2016_report.pdf

Lopez, E. J. (2014, marzo 1). Juan Orlando Hernández gobernará con un “superministro” y 7 sectoriales. Recuperado el 11 de junio de 2017, a partir de

http://www.laprensa.hn/honduras/tegucigalpa/440979-98/juan-orlando-hernandez-gobernara-con-un-superministro-y-7-sectoriales

Malhotra Page, N. K. (2013). *Marketing Research: An Applied Orientation* (6a ed.). Nueva Jersey: Prentice Hall.

National Institute of Standards and Technology. (2014a). *Framework for Improving Critical Infrastructure Cybersecurity* (p. 41). USA: National Institute of Standards and Technology.

National Institute of Standards and Technology. (2014b). *Framework for Improving Critical Infrastructure Cybersecurity* (p. 41). USA: National Institute of Standards and Technology.

Willis, D. A. (2014). *Bring Your Own Device: The Results and the Future* (No. G00250384) (p. 17). USA: Gartner Inc. Recuperado a partir de https://www.gartner.com/doc/2730217/bring-device-results-future

ANEXOS

ANEXO 1: PREGUNTAS DE LA ENTREVISTA CON EL EXPERTO DE SEGURIDAD DE LA INFORMACIÓN

1. ¿Cuál es su opinión del BYOD?
2. ¿Cuál es su opinión respecto a que los usuarios(as) que se conecten a la red inalámbrica empresarial con sus propios dispositivos?
3. ¿Cuáles son los beneficios más sustanciales del BYOD para una empresa?
4. ¿Cuáles son los beneficios más sustanciales del BYOD para un usuario(a)?
5. ¿Cuáles son los riesgos más significativos del uso del BYOD?
6. ¿Considera usted que el BYOD debería ser utilizado por los empleados(as) de las IGSFH? ¿Por qué?
7. ¿Qué controles básicos recomendaría para el uso del BYOD en las IGSFH?
8. ¿Qué controles óptimos recomendaría para el uso del BYOD en las IGSFH?
9. ¿Considera usted que debería existir una política de seguridad de la información que respalde los controles para BYOD? ¿Por qué?
10. Desde un punto de vista como usuario y experto en temas de BYOD: ¿Firmaría usted un documento que habilite a su empresa a controlar su dispositivo móvil remotamente?
11. ¿Estaría de acuerdo en que su empresa borre toda la información de su Smartphone o Tablet, si esta fuera extraviada?
12. ¿Cuál es su opinión de los empleados(as) que usan BYOD?
13. ¿Cree usted que un usuario(a) esté dispuesto a firmar un documento que habilite a su empresa a controlar su dispositivo móvil?

ANEXO 2: ENCUESTA A EMPLEADOS

1. ¿Tiene usted un dispositivo móvil (Smartphone o Tablet)?

   Si

   No
2. ¿Esta su dispositivo móvil (Smartphone/Tablet) configurado con el correo electrónico de la institución donde labora?

   Si

No

3. ¿En los últimos cinco (5) años ha sufrido de robo, hurto o extravío de algún dispositivo móvil?

   Si

   No

4. ¿Conecta su dispositivo móvil a redes inalámbricas públicas (Wi-Fi en Hoteles, Restaurantes, Aeropuertos, Centros Comerciales)?

   Nunca

   Casi nunca

   A veces

   Casi siempre

   Siempre

5. ¿En un día laboral, con qué frecuencia revisa su correo electrónico institucional desde su dispositivo móvil?

   Nunca

   Casi nunca

   A veces

   Casi siempre

   Siempre

6. ¿Revisa en el dispositivo móvil archivos adjuntos que le envían a través del correo electrónico institucional?

   Nunca

   Casi nunca

   A veces

   Casi siempre

   Siempre

7. ¿Le exigen en la institución donde labora reportar cuando su dispositivo móvil ha sido extraviado, hurtado o robado?

   Nunca

   Casi nunca

   A veces

Casi siempre

Siempre

8. ¿Conecta usted su dispositivo móvil a la red inalámbrica (Wi-Fi) de la institución donde labora?

   Nunca

   Casi nunca

   A veces

   Casi siempre

   Siempre

9. ¿En qué periodo se le exige que cambie la contraseña del correo electrónico institucional?

   Cada 30 días

   Cada 60 días

   Cada 90 días

   Nunca

10. ¿Tiene su dispositivo móvil algún software para la protección de virus?

    Si

    No

11. ¿Le brindan en la institución charlas sobre seguridad en el manejo de la información?

    Si

    No

12. ¿Ha firmado algún acuerdo de confidencialidad de la información en la institución donde labora?

    Si

    No

13. ¿Se realizó algún registro de su dispositivo móvil antes de conectarlo a la red inalámbrica de la institución o al correo electrónico?

    Si

    No

14. ¿Clasifican la información de su institución entre confidencial y pública?

    Si

    No

ANEXO 3: POLITICA BYOD

[Logo de la Institución]*

[Nombre de la institución]*

Política Trae tu propio dispositivo (BYOD)

ID Documento:	<Compatible con la nomenclatura de los documentos de la institución>
Versión:	
Fecha de la versión:	
Creado por:	
Aprobado por:	
Nivel de confidencialidad:	

*Campo obligatorio

Fecha	Versión	Creado por	Descripción de la modificación
DD-MM-AAAA	0.1		<Descripción básica del documento>

Tabla de Contenido de la Política BYOD

Objetivo, Alcance y Usuarios

El objetivo de este documento es definir cómo [nombre de la Institución] retendrá el control sobre su información mientras se accede a dicha información a través de dispositivos que no pertenecen a la organización.

Este documento se aplica a todos los dispositivos personales que tienen la capacidad de almacenar, transferir o procesar cualquier tipo de información sensible clasificada en las políticas de seguridad de la institución. Aunque esta política ha sido desarrollada con el objetivo de proteger dispositivos como teléfonos inteligentes y Tablets la misma puede ser utilizada para control de otros dispositivos como los ordenadores personales, unidades de memoria USB, cámaras digitales, etc. En esta política se identificará a estos dispositivos como BYOD.

Los usuarios de este documento son todos los empleados de [nombre de la Institución].

Documentos de Referencia

- Norma ISO/IEC 27001, puntos A.6.2.1, A.6.2.2, A.8.1.2, A.8.1.3, A.8.1.4, A.8.2.3, A.9.3.1, A.9.4.3, A.11.2.6, A.11.2.8, A.11.2.9, A.12.2.1, A.12.3.1, A.12.5.1, A.12.6.2, A.13.2.1, A.13.2.3, A.13.2.4, A.18.1.2

Reglas de Seguridad para el uso de BYOD

Las reglas de la presente Política aplican para todos los BYOD, ya sea de uso personal o que se utilicen para trabajar, dentro o fuera de las instalaciones de la organización.

1. Política de la institución

[Nombre de la institución] adhiere al uso generalizado de BYOD para actividades laborales; por ejemplo, [Correo electrónico, WhatsApp].

Los datos de la institución que se almacenan, transfieren o procesan en BYOD siguen perteneciendo a la institución, y la institución mantiene el derecho a controlar esos datos, aunque no sea propietaria del dispositivo.

2. Quiénes pueden utilizar BYOD y para qué

El [Encargado de la seguridad de la información] creará una lista de cargos y/o personas a quienes se les permite utilizar BYOD junto con las aplicaciones y bases de datos a las cuales pueden acceder con sus propios dispositivos.

El [Encargado de la seguridad de la información] creará una lista de aplicaciones prohibidas para BYOD.

3. Qué dispositivos están permitidos

El [Encargado de la seguridad de la información] creará una Lista de dispositivos aceptados que pueden ser utilizados como BYOD, junto con [antivirus, bloqueo de pantalla con contraseña, cifrado de información] para cada dispositivo.

4. Uso aceptable

Lo siguiente es obligatorio para todos los BYOD:

- [describir cómo se debe realizar la creación de copias de seguridad para información de la institución]

- [detallar qué software de seguridad debe ser instalado; por ej., software antivirus, prevención de intrusiones, software para administración de dispositivos móviles, etc.]
- [describir el método de encriptación que se utilizará y para qué]
- [describir el método de autenticación que se utilizará]
- [describir el método seguro de conexión a la red de la institución]
- Cuando se utilicen BYOD fuera de las instalaciones de la institución, no deben ser dejados desatendidos y, si es posible, deben estar físicamente resguardados bajo llave.
- Cuando se utiliza BYOD en lugares públicos, el propietario debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas.
- Se deben instalar periódicamente parches y actualizaciones.
- La información clasificada debe contar con protección adicional de acuerdo con la [Política de Clasificación de la información].
- Notificar al [Encargado de la seguridad de la información] antes de eliminar, vender o entregar un BYOD a terceros para su reparación.

No se permite hacer lo siguiente con los BYOD:

- Permitir el acceso a cualquiera que no sea el empleado propietario del dispositivo.
- Instalar aplicaciones que están enumeradas en la Lista de aplicaciones prohibidas para BYOD.
- Almacenar material ilegal en el dispositivo.
- Instalar software sin licencia.
- Conectarse por Bluetooth con cualquier tipo de dispositivo.
- [Conectarse a redes Wi-Fi desconocidas, si aplica, determinar la manera de protección].
- Almacenar claves localmente, excepto cuando se utilicen las siguientes aplicaciones: [detallar las aplicaciones permitidas en las que se puede almacenar claves]
- Almacenar localmente la siguiente información: [detallar información sensible]
- Transferir datos de la institución a otros dispositivos no permitidos.

5. Derechos especiales

[Nombre de la institución] tiene el derecho de ver, editar y borrar todos los datos de la institución que se encuentran almacenados, transferidos o procesados en BYOD.

El [Encargado de la seguridad de la información] está autorizado a configurar cualquier BYOD en conformidad con la presente política y a controlar su uso a través de [especificar el nombre del software para gestión de dispositivos móviles].

[Nombre de la Institución] tiene el derecho de realizar el borrado completo de todos los datos del BYOD si considera que es necesario para la protección de los datos de la institución, sin el consentimiento del propietario del dispositivo.

6. Reembolso

[Nombre de la institución] no abonará a los empleados (los propietarios de BYOD) ningún costo por el uso del dispositivo con fines laborales.

[Nombre de la institución] abonará lo siguiente:

- Todo nuevo software que necesite ser instalado para uso de la institución.
- Costos de telecomunicaciones (cargos de teléfono y datos): [definir un porcentaje] de las facturas mensuales del propietario.

7. Violaciones de seguridad

Todas las violaciones de seguridad relacionadas con BYOD deben ser reportadas inmediatamente al [Mesa de ayuda]. Además, todas las debilidades que aún no se hayan convertido en incidentes deben ser reportados por medio de los mismos canales dentro de 1 día hábil.

8. Capacitación y concienciación

El [Encargado de la seguridad de la información] está a cargo de la capacitación de los empleados nuevos y existentes sobre el uso adecuado de los BYOD, como también de concientizar sobre las amenazas más comunes.

Gestión de Registros Guardados en Base a este Documento

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
[Lista de usuarios habilitados para BYOD y a qué pueden acceder]	[Colocar acá la ubicación donde estará almacenado el	[cargo]	Solamente el [cargo] puede editar y publicar nuevas versiones de la Lista.	La lista que ya no tiene validez debe ser archivada

	Archivo]			por [3 años].
[Lista de dispositivos BYOD aceptados y sus configuraciones]	[Colocar acá la ubicación donde estará almacenado el Archivo]	[cargo]	Solamente el [cargo] puede editar y publicar nuevas versiones de la Lista.	La lista que ya no tiene validez debe ser archivada por [3 años].
[Lista de aplicaciones prohibidas para BYOD]	[Colocar acá la ubicación donde estará almacenado el Archivo]	[cargo]	Solamente el [cargo] puede editar y publicar nuevas versiones de la Lista.	La lista que ya no tiene validez debe ser archivada por [3 años].

Validez y Gestión de Documentos

Este documento es válido hasta el [fecha].

El propietario de este documento es el [cargo], que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año. El [Encargado de la seguridad de la información] revisará la Lista de usuarios habilitados, la Lista de dispositivos aceptados y la Lista aplicaciones prohibidas cada 3 meses.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de incidentes relacionados con el uso de BYOD.
- Cantidad de empleados que utilizan BYOD sin autorización.

[Encargado de control de documentación]
[Nombre]

_____
[firma]