FACULTAD DE POSTGRADO
TRABAJO FINAL DE GRADUACIÓN

ANÁLISIS DE IMPLEMENTACIÓN DE UNA NORMATIVA DE PROTECCIÓN DE DATOS EN LAS EMPRESAS DE HONDURAS

SUSTENTADO POR:

CARLOS ROBERTO VELÁSQUEZ VARGAS
SCARLETH REGINA FORTIN AGUILAR

PREVIA INVESTIDURA AL TÍTULO DE

MÁSTER EN
GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN

TEGUCIGALPA, FRANCISCO MORAZÁN, HONDURAS, C.A.

ABRIL, 2019

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA

UNITEC

FACULTAD DE POSTGRADO

AUTORIDADES UNIVERSITARIAS

RECTOR

MARLON ANTONIO BREVÉ REYES

SECRETARIO GENERAL

ROGER MARTÍNEZ MIRALDA

DECANO DE LA FACULTAD DE POSTGRADO

CLAUDIA MARÍA CASTRO VALLE

ANÁLISIS DE IMPLEMENTACIÓN DE UNA NORMATIVA DE PROTECCIÓN DE DATOS EN LAS EMPRESAS DE HONDURAS

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

MÁSTER EN

GESTIÓN DE TECNOLOGIAS DE INFORMACIÓN

ASESOR

JORGE RAÚL MARADIAGA CHIRINOS

MIEMBROS DE LA TERNA:

RAFAEL ALBERTO RIVERA
CARLOS HUMBERTO PÉREZ
ALFONSO DE JESÚS ALFONSO

FACULTAD DE POSTGRADO

ANÁLISIS DE IMPLEMENTACIÓN DE UNA NORMATIVA DE PROTECCIÓN DE DATOS EN LAS EMPRESAS DE HONDURAS

Carlos Roberto Velásquez Vargas
Scarleth Regina Fortín Aguilar

Resumen

Para el 2019, el robo de datos personales es uno de los diez riesgos más graves a nivel mundial, por esta razón, es de suma importancia contar con medidas que regulen la protección de los mismos. En Honduras, éste es un tema poco explorado, por lo tanto, la población no cuenta con un respaldo que los proteja ante una situación en la que su información personal sea expuesta, como producto de ataques cibernéticos o de algún error por parte de las empresas que manejan los datos.

Esta es una investigación que se llevó a cabo, mediante el análisis de la situación de Honduras y el estudio de diferentes estándares y normativas a nivel internacional con respecto a la protección de datos personales. Es por eso, que se elabora una propuesta de cómo se puede implementar varias medidas que regulen éste tema, en las empresas de los diferentes sectores del país.

Palabras claves: Protección de datos, Ciberataques, Normativa, Robo de Datos.

GRADUATE SCHOOL

ANALYSIS OF THE IMPLEMENTATION OF A DATA PROTECTION RULES IN THE COMPANIES OF HONDURAS

Carlos Roberto Velásquez Vargas
Scarleth Regina Fortín Aguilar

Abstract

By 2019, the theft of personal data is one of the ten most dangerous risks worldwide, which is why it is of utmost importance with the measures that regulate their protection. In Honduras, this is a little explored issue, therefore, the population does not have a backup that is protected against a situation in which their personal information is exposed, as a result of cyber attacks or some error by companies who handle the data.

This is an investigation that has been carried out, through the analysis of the situation in Honduras and the study of different international standards and norms regarding the protection of personal data. That is why it is a proposal of how you can implement several measures that regulate this issue in companies in different sectors of the country.

Palabras claves: Data Protection, Cyber Attacks, Normative, Data Theft.

DEDICATORIA

A Dios, la razón de mi existir, quien bendice mi vida, me guía a lo largo de mi existencia, me da fortaleza cuando me siento débil y me sustentó para continuar en este proceso de obtener uno de mis más grandes sueños.

A mis padres Dagoberto y Sonia, quienes me han inculcado el ejemplo del esfuerzo, valentía, sacrificio y trabajo duro, a no temer ante ninguna circunstancia, ya que siempre tengo a Dios y a ellos a mi lado. Los amo con todo lo que soy.

A mis hermanos Edwin y Yareli por siempre acompañarme en cada etapa de mi vida, porque sé que puedo contar con su amor, sus consejos y su apoyo incondicional.

A mis sobrinos Raquel, Rebeca y Santiago, quienes con sus sonrisas y ocurrencias me dan fuerzas para continuar en cualquier reto que se me presente.

Atentamente, Scarleth Fortín.

Dedicado al forjador de mi camino: Dios, que con su amor y bondad me permite cumplir una meta más en mi vida; a mis padres Carlos y Cecilia que nunca han dejado de creer en lo que soy capaz de lograr; quienes desde muy pequeño me enseñaron a esforzarme y a perseguir mis sueños, a ser una persona simple y a vivir la vida, como si no existieran límites. Con todo el amor sincero.

Carlos Velásquez.

AGRADECIMIENTO

Agradezco a Dios, por acompañarme en el transcurso de este proceso, brindándome los medios necesarios para mantenerme espiritual y económicamente.

A mis padres, por ser pilar fundamental en mi vida, y siempre decirme las palabras exactas que necesitaba escuchar, por darme fuerza, esperanza y, sobre todo, por tener fe en mí.

A mis hermanos, por llenarme de alegría día con día y ser ese apoyo constante que siempre necesitaré en mi vida.

A mis sobrinos, por ser mi fuerza y mi impulso al anhelar convertirme en un modelo a seguir para ellos.

A Carlos Velásquez, quien me acompañó durante un recorrido muy largo y difícil, por haber sido un apoyo en los momentos donde parecía que no podíamos más, gracias por culminar esta etapa conmigo ¡lo logramos!

A mi asesor Jorge Maradiaga, por su tiempo, su guía, conocimiento y por todo el apoyo que nos brindó a lo largo de todo el proceso.

A todos los docentes de UNITEC, que compartieron sus conocimientos y experiencias profesionales en todas las clases impartidas.

Atentamente, Scarleth Fortín.

El amor es el motor que mueve cada pieza del universo, agradezco el amor que Dios me ha dado toda vida, a mis padres que con su apoyo incondicional se convirtieron en promotores de mi sueño; a mi familia por cada palabra de ánimos durante ésta etapa, a mis amigos que muchas veces me dieron las fuerzas que me faltaron y a Scarleth Fortín, mi compañera de ésta aventura, quien me animó a emprender ésta etapa juntos, me hace sentir el hombre más orgulloso del planeta; gracias por haber volado conmigo.

Carlos Velásquez

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

GLOSARIO DE TÉRMINOS

Término	Definición
Bitcoins	Es una red consensuada que permite un nuevo sistema de pago y una moneda completamente digital.
Buffer Overflow	Se lleva a cabo cuando un programa informático excede el uso de cantidad de memoria asignado por el sistema operativo, escribiendo en el bloque de memoria contiguo. Estos fallos son utilizados por ciberdelincuentes para lograr ejecutar código arbitrario en un equipo, de manera que en muchos casos logran tomar control del equipo víctima o ejecutar un ataque de Denegación de Servicios.
DDOS	Ataque de denegación de servicios distribuido, se lleva a cabo generando un gran flujo de información desde varios puntos de conexión hacia un mismo punto de destino.
DIRECCIÓN IP	Es un número que identifica, de manera lógica y jerárquica a una interfaz en red de un dispositivo que utilice el protocolo IP, que corresponde al nivel de red del modelo TCP/IP.
DOS	Ataque de denegación de servicios, tiene como objetivo inhabilitar el uso de un sistema, una aplicación o una máquina, con el fin de bloquear el servicio para el que está destinado.
Dumpster Diving	Es la práctica de bucear en la información "basura" generada por corporaciones en las que se ha participado, donde el ciberdelincuente

	busca información que puede ser valiosa o relevante para causar daños a terceros.
EIPD	Evaluaciones de impacto en la Protección de Datos
IDS	(Intrusion detection system) Sistema de detección de intrusos.
INE	Instituto Nacional de Estadísticas
Ingeniería Social	Es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos.
ISACA	(Information Systems Audit and Control Association) Asociación de Auditoría y Control de Sistemas de Información
ISO 29100	Marco de referencia de alto nivel para la protección de datos personales.
IT	**(**Information Technology) Tecnología de la Información
Network Mappers	Se utiliza para descubrir y visualizar la conectividad de red física y virtual a través de un grupo de tareas interrelacionadas que facilitan la creación de un mapa de red, incluidos diagramas de flujo, diagramas de red, detección de topología e inventarios de dispositivos.
Network Scanners	Es una aplicación que está específicamente centrada a la administración de sistemas de redes y especializada en el escaneo de éstas.
Password Filtering	Técnica empleada por hackers para robarse la información de contraseñas de usuarios en los sitios web.
Paypal	Procesa transacciones para particulares, compradores y vendedores

	online, sitios de subastas y otros usos comerciales.
PII	(Personally identifiable information) Información personal de identificación.
Port Mappers	El mapeador de puertos es el protocolo que asigna el número o la versión de un programa de llamada a procedimiento remoto de Informática en Red a un puerto utilizado para redes por esa versión del programa.
Port Scanners	Es un explorador de redes que permite encontrar con rapidez los puertos abiertos de los equipos conectados a la red e identificar las versiones de los programas que se están ejecutando en los puertos detectados.
RGPD	Reglamento General de Protección de Datos
Session Hijacking	Se refiere a que un atacante consigue el identificador de sesión entre una página web y un usuario, de forma que puede hacerse pasar por este y acceder a su cuenta en esa página web.
Sniffing	Es una aplicación especial para redes informáticas, que permite capturar los paquetes que viajan por una red.
Vulnerability Scanners	Es un programa de computadora diseñado para evaluar computadoras, redes o aplicaciones para detectar debilidades conocidas.
UE	Unión Europea

Tabla 1. Glosario de términos

CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1 Introducción

El reglamento general de protección de datos está revolucionando globalmente la manera en que las empresas administran y almacenan la información de los datos personales de los clientes; este reglamento entró en vigor a partir de mayo de 2018 en la Unión Europea afectando potencialmente cualquier organización dentro y fuera de ésta región, desde pequeñas empresas hasta grandes organizaciones que incluyan cualquier actividad económica y ofrezcan servicios abiertos al público en general.

Éste reglamento establece requisitos mínimos sobre la forma en que los datos personales son almacenados y procesados; ésta información puede ser la ubicación domiciliar, número de identidad, dirección IP, etnia social, identidad cultural y cualquier dato personal que permita identificar a una persona.

En éste documento podremos encontrar un marco de referencia para aliviar los esfuerzos de lograr la implementación y el cumplimiento del reglamento general de protección de datos en Honduras y lo que implicaría su aplicación en el país basados en la norma ISO 29100, ya que el impacto que el reglamento ha causado a nivel global ha ejercido una significativa presión para que los demás países deban actualizarse e incluirse en éste marco de referencia que ofrece beneficios y mayor protección a la identidad de las personas.

1.2 Antecedentes del Problema

Desde la década de los 80’s donde apareció el primer virus informático, los ciberataques y nueva aparición de virus informáticos no ha cesado. Hoy en día las diversas amenazas que existen y que afectan la ciberseguridad son virus, spam, violaciones a la seguridad de datos, y donde el

robo de identidad de usuarios no ha sido la excepción para éstos atacantes que pueden ser desde piratas informáticos o hackers hasta grandes empresas dedicadas a realizar trabajos de éste tipo.

Se presume que son más de 370 millones las víctimas de ataques cibernéticos cada año y decenas de miles los virus que circulan y atacan los sistemas.

El ciberataque de mayor relevancia en la historia llegó a afectar a Yahoo! en el año 2013 cuando se alcanzó a robar la información de las cuentas de todos sus usuarios contabilizando la cantidad estimada de 3,000 millones de usuarios y que al final generó problemas económicos y afectó la reputación de la empresa.

Uber, quienes son una compañía dedicada a alquiler de vehículos con conductor reveló que en noviembre de 2017 robaran la información de 57 millones de usuarios quien después fue afectada con duras críticas por esconder la información durante algún tiempo.

Así como éstas empresas, se han conocido empresas que también sufrieron daños en el robo de datos, todos somos vulnerables y estamos expuestos a ser víctimas de éste tipo de delitos y de ésta modalidad que ha trascendido significativamente en los últimos años.

1.3 Definición del Problema

Las reglas generales de protección de datos no es algo que sólo afecta a la Unión Europea, quienes son pioneros en la implementación de este marco; su implementación tiene un impacto mundial que exige a empresas ubicadas fuera de la región a utilizar los estándares establecidos.

En nuestra región, incluyendo a Honduras la protección efectiva de datos personales no es una realidad todavía, en Latinoamérica la mayoría de países carecen de un marco regulatorio enfocado en la protección de datos personales en donde efectivamente la información de las personas se encuentre protegida; la poca inversión tecnológica, las pobres leyes que establecen los

entes reguladores generan una vulnerabilidad en la ciberseguridad nacional, aumentando de una manera significativa el riesgo que hay de la apropiación ilícita de la información de las empresas.

Mientras Honduras carezca de los estándares adecuados para la protección de datos personales estaremos renunciando al pleno desarrollo del comercio electrónico, al ejercicio de los derechos y seguiremos estando sumergidos en un país donde la inseguridad es uno de los mayores problemas a los que nos enfrentamos día con día.

1.4 Objetivos del Proyecto

1.4.1 Objetivo General

- Realizar un análisis basado en las principales normativas de protección de datos personales de mayor importancia a nivel internacional, y de ésta forma, poder determinar cuál es la apropiada para implementar bajo un contexto empresarial público y privado de Honduras.

1.4.2 Objetivos Específicos

1. Analizar las diferentes normativas referentes a la protección de datos que han sido implementadas a nivel internacional.
2. Determinar el estado actual de la protección de los datos en Honduras, y evaluar el impacto que traerá consigo la normativa en los sectores públicos y privados del país.
3. Evaluar los principios claves de aplicación de la normativa más viable, para garantizar una efectiva protección de datos personales en el contexto empresarial del país.

1.5 Justificación

“Desde cuando se revelaron las actividades de vigilancia internacional a países extranjeros en 2013, varios países de la región comenzaron a analizar o a crear marcos de políticas destinadas a proteger los datos personales y la privacidad, y ha aumentado la conciencia relacionada con los riesgos cibernéticos” (Maciel et al., 2016).

La implementación del reglamento general de protección de datos surge en Europa en mayo de 2018 como una medida de seguridad ante los constantes robos de identidad y las vulnerabilidades que presentan las empresas hoy en día donde como consecuencia se producen robos de información y ciberataques que afectan la identidad de las personas, violando sus datos personales y poniendo en riesgo los derechos y libertades de las personas.

La aparición de esta ley sustituirá cualquier directiva de protección de datos vigentes en Honduras, tal como ha sucedido con otros países de la región que han implementado ésta ley, es necesario adoptar éste estándar como una guía protección para cada uno de los ciudadanos y habitantes del país permitiendo controlar quien tiene acceso a los datos que puedan identificar a una persona, así como el aumento de la transparencia, igualdad y dignidad que merece cada persona en el país.

La aplicabilidad del reglamento general de protección de datos se pretende evaluar desde el punto de vista de las normas ISO 29100 como una guía para definir una estrategia para la protección de los datos que en un futuro cercano llegará a implementarse en Honduras.

CAPÍTULO II. MARCO TEÓRICO

2.1 Anatomía de un ataque informático

Jorge Mieres (2009) afirma que, un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización. (Debilidades de seguridad comúnmente explotadas, 2009, p. 4)

> "Conocer las diferentes etapas que conforman un ataque informático brinda la ventaja de aprender a pensar como los atacantes y a jamás subestimar su mentalidad. Desde la perspectiva del profesional de seguridad, se debe aprovechar esas habilidades para comprender y analizar la forma en que los atacantes llevan a cabo un ataque". (Debilidades de seguridad comúnmente explotadas, Jorge Mieres, 2009)

Jorge Mieres (2009) sustenta que existen cinco etapas por las cuales suelen pasar los ataques informáticos en el momento en que éstos se llevan a cabo:

Fase 1: Reconocimiento; en ésta etapa involucra la obtención de información con respecto a una potencial víctima que puede ser una persona natural o una persona jurídica. Por lo general, durante esta fase se recurre a diferentes recursos de Internet como ser Google, entre tantos otros, para recolectar datos del objetivo. Entre algunas de las técnicas utilizadas en este primer paso son la Ingeniería Social, el Dumpster Diving ó el sniffing.

Fase 2: Exploración, en esta segunda etapa se utiliza la información que se obtuvo en la fase uno para vigilar el blanco y tratar de capturar información clave sobre el sistema víctima como ser direcciones IP, nombres de dominios, datos de autenticación, contraseñas, entre otros. Entre

las herramientas que un atacante puede emplear durante la exploración se encuentra el network mappers, port mappers, network scanners, port scanners, y vulnerability scanners.

Fase 3: Obtener acceso, en la etapa tres se comienza a materializar el ataque a través de la explotación de las vulnerabilidades y defectos del sistema o "Flaw exploitation" como se conoce en inglés, descubiertos durante las fases de reconocimiento y exploración. Algunas de las técnicas que el atacante puede utilizar son ataques de Buffer Overflow, ataque de denegación de servicios (DoS), Distributed Denial of Service (DDos), Password filtering y Session hijacking.

Fase 4: Mantener el acceso; una vez que el atacante ha conseguido acceder al sistema, éste buscará implantar herramientas que le permitan mantener el acceso para poder volver a acceder en el futuro desde cualquier lugar donde tenga acceso a Internet. Para ello, suelen recurrir a utilidades backdoors, rootkits y virus troyanos.

Fase 5: Borrar huellas, ésta es la última fase, una vez que el atacante logró obtener y mantener el acceso al sistema, intentará borrar todas las huellas que fue dejando durante la intrusión para evitar ser detectado por el profesional de seguridad o los administradores de la red. En consecuencia, buscará eliminar los archivos de registro, conocidos también como logs o alarmas del Sistema de Detección de Intrusos (IDS). (Debilidades de seguridad comúnmente explotadas, 2009, p. 5-6)

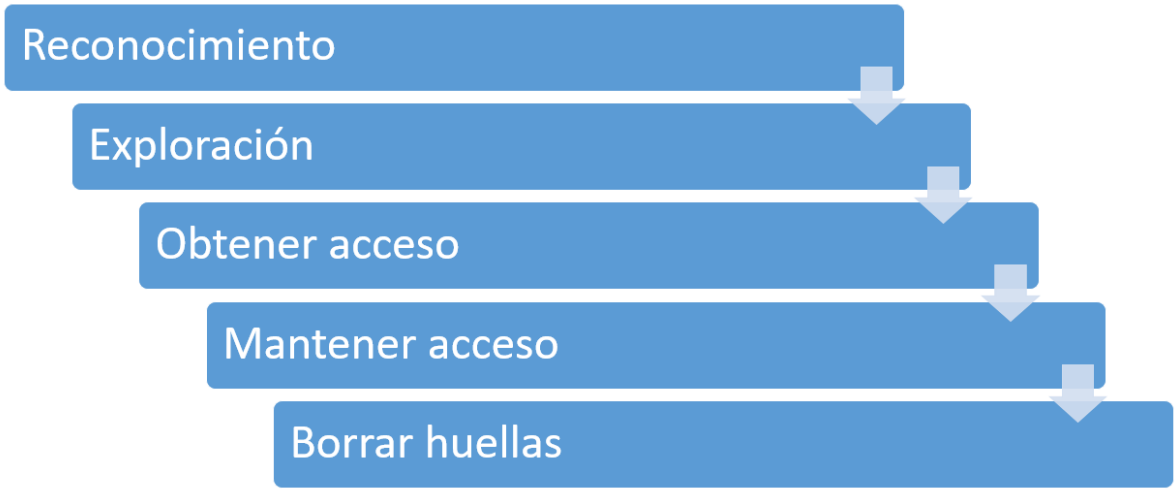

Figura 1. Anatomía de un ataque cibernético

Fuente: (Elaboración propia).

2.2 Ciberamenazas a la privacidad de los usuarios y organizaciones

En los últimos años se ha visto como aparecen cada día noticias relacionadas con divulgación de información privada relevante, afectando la integridad de las personas y la reputación o confiabilidad en las organizaciones; ésta información va desde publicaciones intimas, información personal, fotografías y datos de clientes o empleados obtenida a través del robo o secuestro de la información; en donde la preocupación y el interés de las personas u organizaciones ha despertado para comenzar a protegerse en el mundo del internet .

A pesar de la preocupación que hay entre las personas que utilizan a diario el internet, muchos de ellos desconocen los peligros y son incapaces de identificarlos al momento de compartir su información en la web, y por ende no tienen idea de cómo mitigar los riesgos de ataques cibernéticos y cómo enfrentarse a ellos; aunque la naturaleza de los ataques cibernéticos ha ido cambiando constantemente, así como los objetivos de los ataques.

"Los robos más importantes de información pueden afectar a tres tipos de aspectos:

- Económico: si te roban las contraseñas o tienen acceso a sistemas online como bancos, Paypal, bitcoins…
- Lúdico: se refiere a la pérdida de fotografías, acceso a información sensible como repositorios en la nube…
- De "imagen": si roban cuentas de las redes sociales, pueden llegar a suplantar la identidad y dañarla".

(Ciberseguridad, la protección de la información en un mundo digital, septiembre 2016).

Los constantes avances tecnológicos y la nueva era de la digitalización en los servicios y la economía conforman grandes retos, los cuales llevan a que los usuarios y organizaciones se vean obligados a enfrentarlos, donde se debe incluir una vasta especialización mediante recurso humano y concientización de la forma en la que se vive día con día en éste mundo globalizado donde las ciberamenazas cada vez son mayores.

"Es posible que el usuario considere que no tiene ninguna información relevante que pueda ser utilizada por delincuentes. Eso suele ser una percepción falsa, ya que los atacantes pueden querer acceder a las libretas de contactos para realizar spam masivo personalizado y atacar a terceras personas, o bloquear el ordenador y pedir un rescate por recuperar la información, pues, aunque la información no sea de valor para terceras personas, sí lo será para el propio usuario…. Es necesario que los usuarios sean conscientes de las nuevas normas de juego que imponen Internet y las nuevas tecnologías y conozcan tanto los mecanismos más importantes que utilizan los atacantes como cuáles de nuestras identidades pueden ser interesantes para ellos. (Ciberseguridad, la protección de la información en un mundo digital, septiembre 2016)

La imagen que se presenta a continuación representa las actitudes de los usuarios ante la seguridad y a la privacidad, basados en los factores voluntariedad y sensibilidad de la información.

Figura 2. Actitud ante la seguridad y privacidad de la información.

Fuente: ("Ciberseguridad, la protección de la información en un mundo digital ", septiembre 2016).

Por otra parte, el problema de la ciberseguridad en las empresas es similar a la de los usuarios, por ejemplo, la pérdida sentimental que representa para una persona el perder información privada, en una empresa representa la pérdida de confiabilidad y el riesgo reputacional cuando es víctima de un ataque cibernético, donde ha perdido el activo más importante: su información; lo que impide el desarrollo de las actividades diarias de la empresa y hasta pueden llegar a perder grandes cantidades de dinero, cabe mencionar los ataques cibernéticos a las empresas pueden ser ataques a su red privada o ataques a su infraestructura; por lo tanto las empresas poseen mayor conciencia ante éste tipo de eventualidades.

Los ciberataques a las empresas tienen un impacto económico considerablemente superior al de los ataques hacia las personas, es por esa razón que las empresas optan por implementar planes relacionados a la seguridad tecnológica. Sin embargo, empresas pequeñas y medianas presentan dificultades al momento de poner en marcha dichos planes, ya que el tema económico impide que puedan desarrollarse y obtener recursos para llevar a cabo este tipo de tecnologías satisfactoriamente.

En el año 2015, INE presentó datos relacionados a las empresas pequeñas con políticas de seguridad informática establecidas, donde se muestra que las empresas que poseen menos de diez empleados tan sólo una tiene una política de seguridad.

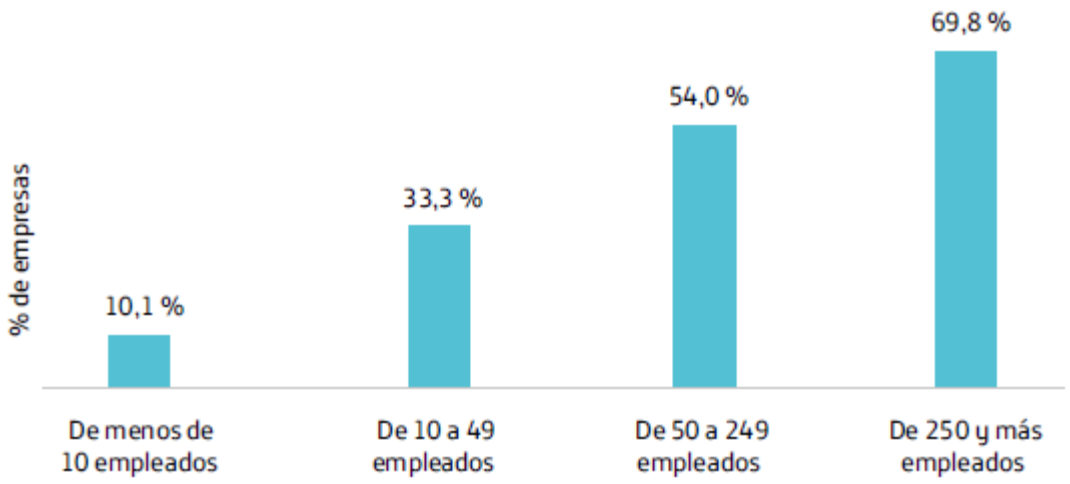

Figura 3. Empresas que tienen una política de seguridad establecida.

Fuente: (INE, 2015).

Los datos son desalentadores, y muestran la ardua labor que aún falta por hacer para lograr la concientización de las empresas en la importancia de tener establecida una política de seguridad informática; es necesario que ésta conciencia vaya más allá de creer que tener un antivirus instalado lo es todo, sino que es importante tener una estrategia y política que aplicar en el día a día; tomando en cuenta que entre más grande es la empresa o más relevancia tiene entre la sociedad más aspectos deben tomar en cuenta para los planes de seguridad y el seguimiento de las políticas debe ser más riguroso.

Uno de los principales peligros por el que las empresas se preocupan a la hora de tener aplicadas las políticas de seguridad es evitar la destrucción de los datos que estas utilizan en las operaciones diarias, un aspecto que es considerado en un 94,7 %; después la revelación de datos confidenciales, el cual se considera por tan solo el 77,9 % de las empresas de menos de 10 empleados y por el 85,5 % de las empresas con más de 250 empleados que tienen planes de seguridad.

La frecuencia con la que las empresas dan seguimiento a estas políticas, dos de cada tres empresas revisaron los planes en un periodo de doce doces meses anteriores y tan solo una baja porción de ellas lo hizo hace más de veinticuatro, lo que da a conocer que existe un interés por actualizarse en temas que tienen que ver con la seguridad informática.

Las empresas más grandes realizan revisiones de estos planes con mayor frecuencia, posiblemente al disponer más habitualmente de empleados expertos en IT.

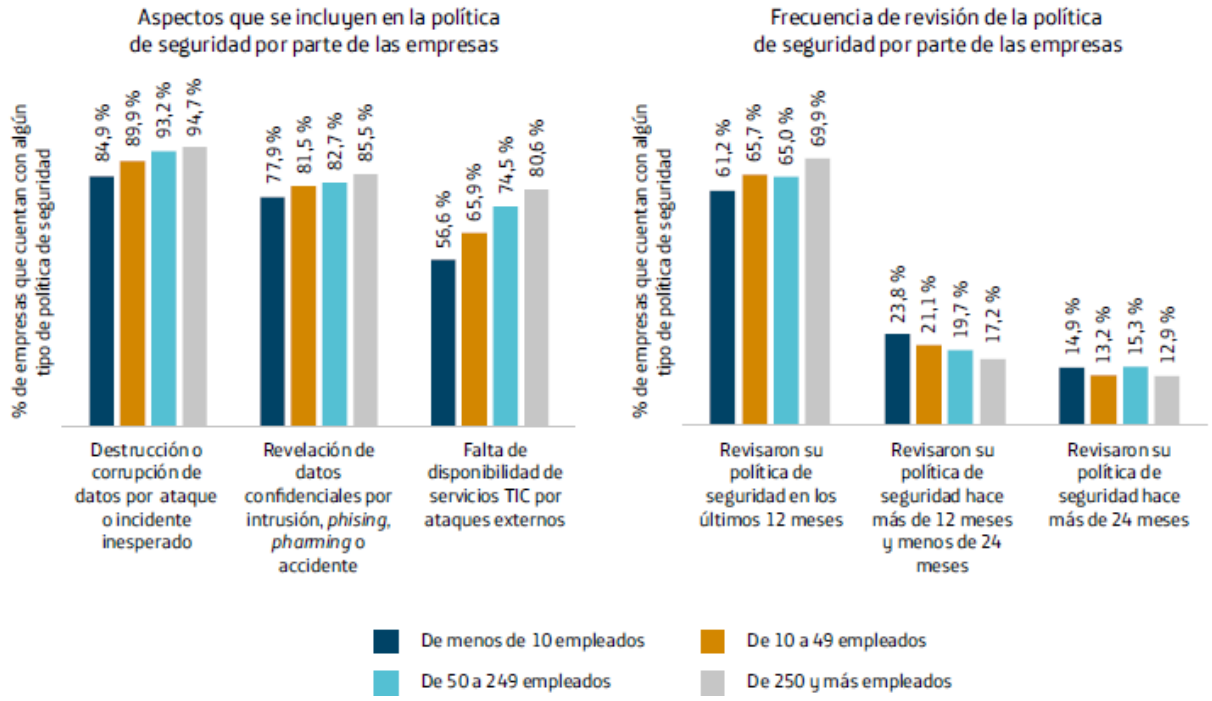

Figura 4. Medidas de Seguridad en las Empresas.

Fuente: (INE, 2015).

2.3 Casos de ciberataques y robos de información

2.3.1 Ciberataque a SONY Pictures en 2014

Durante el lapso de una semana, la empresa productora cinematográfica SONY Pictures fue víctima de un ataque cibernético; revelando información confidencial e información de películas que estaban próximas a estrenar.

Sony Pictures es una de las productoras más grandes e importantes del cine a nivel mundial; en 2014 pasó a convertirse en una víctima más de los cibercriminales que burlaron todos los niveles de seguridad en la empresa apoderándose de sus bases de datos, revelando información confidencial y películas sin estrenar, dañando la imagen y ocasionando pérdidas económicas en su víctima.

El suceso ocurrió cuando el grupo de hackers conocidos como #GOP accedió a través de la intranet de Sony Pictures accediendo a grandes volúmenes de información, contraseñas, y acceso anticipado a un catálogo de películas próximas a estrenar; éste grupo de hackers expuso al mundo las pobres políticas de seguridad que se manejaban en la empresa; a tal punto que se dio a conocer que la información "confidencial" de la empresa se encontraba en documentos de texto y archivos de Excel, considerando que por la sensibilidad de la información se creía que ésta podía encontrarse cifrada o encriptada para su uso.

Aunque no se dio a la luz pública cuales fueron las condiciones que exigieron los hackers para la liberación de éste secuestro de información; una de las consecuencias que arraigó este incidente fue la divulgación de cinco películas que la empresa aún no había estrenado, ocasionando en primera instancia pérdidas económicas en la organización.

Las consecuencias para Sony Pictures trascendieron en otra serie de incidentes, pues liberaron información personal de muchos empleados de la empresa, como ser lo salarios de algunos ejecutivos incluyendo el CEO de la compañía, quien gana 3 millones de Dólares al año, incluyendo quejas y condiciones de algunos empleados, además de información de domicilio, hay números de seguro social de muchos otros empleados.

Aunque se presume que el ataque cibernético podría tratarse de una represalia de Corea del Norte, a raíz del estreno de una película cómica donde se hace referencia al gobierno de dicho país, éste no se quedó de brazos cruzados generando fuertes reclamos ante las Naciones Unidas. Ante las sospechas del origen del ciberataque sobre el gobierno norcoreano, éste desmintió alegando no estar relacionado con el incidente, que tiempo después estudios de informática forense descubrió que la compilación de los programas que ocasionaron el ataque fueron de fechas previas al robo, relacionando también las amenazas que el gobierno hizo a Sony en su momento por haber

producido esa película.

Si de algo hay que estar seguros es que Sony Pictures tenía un pobre nivel de seguridad y políticas que, aunque existían no se aplicaban; ocasionando el peor ataque cibernético hacia la industria del cine de todos los tiempos y uno de los más catastróficos incidentes de la historia.

2.3.2 Violación de seguridad en Universidad de Valladolid, España 2019

El 10 y 11 de enero de 2019, la Universidad de Valladolid sufrió un ataque y de robo de información personal a través de la página web del Servicio de Relaciones Internaciones.

A pesar de que el alcance del ataque aún no se hiciera público por motivos de seguridad; la Universidad de Valladolid informó a la Agencia Española de Protección de Datos y se interpuso una denuncia formal ante las Fuerzas y Cuerpos de Seguridad del Estado; quienes han remitido a la Brigada de Delitos Tecnológicos.

Las personas responsables de llegar a las conclusiones y detalles del ataque cibernético aseguran estar trabajando intensamente para llegar a dar con el origen y motivos del mismo; los protocolos de la política de seguridad de la información de la Universidad se hicieron cumplir en el momento que se comenzó a sospechar de que estaban siendo víctimas del ataque, donde se procedió a bloquear y poner en cuarentena la máquina afectada y se preparó un informe dirigido al ente Español de Protección de Datos, así como identificar las personas afectadas y la clasificación del riesgo al que están expuestos.

La Universidad de Valladolid ha indicado que éste incidente es causado por una vulnerabilidad existente, pero no existe evidencia alguna de haber causado daños mayores.

2.3.3 Mayor robo de contraseñas de la historia.

En el mes de enero de 2019, más de 700 millones de contraseñas fueron robadas por cibercriminales, donde un masivo filtrado de datos ha expuesto la información de correo electrónico y contraseñas de millones de usuarios y ha pasado a ser el mayor robo de contraseñas en la historia.

El ataque no proviene de una sola fuente, donde se reportan que cientos de miles de datos pertenecen a una recopilación de cerca de 2000 bases de datos que incluyen contraseñas que están visibles y vulnerables debido a la violación de seguridad por las que fueron robadas.

A diferencia de lo que usualmente sucede en los robos de información, en lugar de colocar en venta los datos, éstos fueron compartidos en diversos foros de piratas informáticos y sitios de descargas; con ésta enorme cantidad de contraseñas robadas, Colletion#1 es uno de los robos de datos más grandes registrados en la historia, solamente superado por el robo al tan conocido Yahoo que afectó a 3 mil millones de usuarios.

Según Troy Hunt, un experto en el tema de la ciberseguridad web, la lista se encontraba alojada en el sitio MEGA y fue repartida en más de 12000 archivos particionados donde sumaban un total de 87 GB; en diversos medios de comunicación se dio a conocer la noticia donde se recomendó a las personas cambiar sus contraseñas.

Hasta el momento, de los detalles exactos sobre la lista expuesta se ha conocido poco; pero las alarmas quedan abiertas para que los usuarios actualicen sus claves y no ser víctimas de ésta filtración.

2.3.4 Protección de datos en Facebook y Whatsapp.

En septiembre de 2017, la Asociación Española de Protección de Datos impuso una multa de 1.2 millones de euros a Facebook por vulnerar normativas de protección de datos personales; a partir de ese momento se consideró que las políticas aplicadas al tema de privacidad eran poco claras y muy genéricas ya que trataba datos especialmente protegidos sin consentimiento de las personas además de conservar excesiva información personal.

Un mes después, se multó con 150 mil euros por el servicio de chat de ésta red social en donde éste servicio permitía que pudiera verse de manera pública los métodos de conexión de los usuarios, sin opción a cambiar por parte del dueño de la cuenta.

A los últimos antecedentes se suma la multa de 300 mil euros a Facebook y a Whatsapp, en esta ocasión los datos personales de los usuarios fueron utilizados de la aplicación de mensajería de la empresa sin un consentimiento adecuado tras su compra.

En total, la empresa Facebook ha sido duramente golpeada económicamente, donde todas estas sanciones suman 1.65 millones de euros aproximadamente por parte de la Agencia Española de Protección de Datos.

El último antecedente reportado ha sido donde nuevamente la Agencia Española de Protección se unió para investigar a Facebook en 2018 donde se presumen la posible fuga de datos de 136,985 usuarios españoles.

La red social lo confirmó días después, en donde casi 137 mil cuentas de usuarios españoles fueron afectadas donde se llegó a saber por un análisis interno realizado; se determinó que 44 personas españolas habían descargado una aplicación llamada *thisisyourdigitallife*, que dio el acceso a Digital Analytica a toda la información personal de miles de usuarios y la de sus contactos,

donde posteriormente esos datos fueron utilizados por la consultora para afinar con perfiles psicológicos para modificar el voto hacia la campaña de Donald Trump en 2016.

Facebook intentó mitigar lo ocurrido mostrando un mensaje en la página de inicio y en los muros de cada persona con el siguiente mensaje: “Protección de tu información. Comprendemos la importancia de proteger tus datos. Ahora podrás controlar más fácilmente con qué aplicaciones compartes información. Puedes ir cuando quieras a la sección “Aplicaciones y sitios web” de la configuración para ver las aplicaciones y los sitios web en los que iniciaste sesión con Facebook. También puedes eliminar aquellos que ya no quieras que estén conectados con Facebook.”

Además, se creó un panel de configuración donde cada persona tiene el derecho a elegir qué datos sensibles desean que Facebook trate, como, por ejemplo, la etnia, creencias religiosas y reconocimiento facial, entre otros.

Por otra parte, debido al cambio en las políticas de protección de datos, Whatsapp por ser perteneciente a Facebook también preparó un cambio en sus políticas de condiciones de uso del servicio en donde la edad mínima requerida para el uso de la aplicación ha pasado de 13 a 16 años de edad; ésta medida se toma a consecuencia de las filtraciones que se han producido con la red social, Whatsapp también indica que en caso de no tener la edad mínima se deberá tener la autorización de los padres o el tutor del menor.

2.3.5 Robo de datos personales en la Banca Tailandesa

En agosto de 2018, el Banco de Tailandia reportó el hurto de datos personales de aproximadamente 120 mil clientes mediante un ciberataque a dos de sus más grandes e importantes filiales a nivel nacional; según la página oficial del banco, todo aquel que recientemente aplicó a un crédito o préstamo debía presentarse con sus documentos personales y declaraciones bancarias, así como constancia de ingresos.

El presidente de la firma Krung Bank Thai, Payong Srivanich, afirmó que los atacantes utilizaron técnicas de pirateo modernas y avanzadas para robar la información personal de las personas que habían aplicado a créditos en línea recientemente. Payong también afirmó que expertos de seguridad de la información del Krung Bank Thai detuvieron el ciberataque de manera inmediata después de que la división de Seguridad Informática de la empresa sospechara de movimientos que dieron indicio de que estaban siendo víctimas de un ciberataque.

Por otra parte, el presidente de Kasikornbank, Pipit Aneaknithi, confirmó más tarde que los piratas informáticos obtuvieron datos de 3000 usuarios coporativos que utilizan el servicio de sucursales electrónicas en línea, en donde afirmó que parte de la información robada incluyen nombres de compañías y detalles de los contactos, sin embargo, no hubo ningún tipo de desviación de fondos o robo de dinero como suele de darse en la mayor parte de ciberataques a los bancos a nivel mundial.

Por su parte, el presidente de la Asociación de Banqueros de Tailandia expresó que con los grandes avances tecnológicos es necesario buscar niveles más avanzados de ciberseguridad, obteniendo mejores niveles de protección vigilancia, así como aplicar políticas mayores y mejores políticas en las empresas, con el fin de minimizar los riesgos que existen hoy en día.

2.4 Contexto de la protección de datos

2.4.1 Definición de dato personal

Ramón Oró (2015) afirma que, es toda aquella información que pudiera vincularse a una persona, tanto si esta información hace referencia a su identidad, a sus características o su comportamiento, como si la información se utiliza para determinar o influir en la manera de tratar o evaluar a la persona.

Cualquier información, sea cual sea su naturaleza, el formato, o el contenido, referida a una persona. Desde el punto de vista de la naturaleza, es dato personal todo tipo de afirmación sobre una persona, tanto si esta información es objetiva, como si son opiniones o evaluaciones subjetivas.

Con relación al formato, el concepto de datos personales incluye informaciones disponibles en cualquiera de las formas alfabética, numérica, gráfica, fotográfica, sonora o audiovisual. Incluso no es necesario que la información esté recogida en una base de datos o en un fichero estructurado porque también son datos personales los contenidos en un texto libre, escrito en formato digital, ya sea en una página web o en un mensaje de correo electrónico. Y en cuanto al contenido, son datos personales las informaciones referidas a cualquier aspecto de la vida de una persona, independientemente de su posición o capacidad. (La protección de datos, 2015, p. 52)

Algunos ejemplos de información de identificación personal (PII por sus siglas en inglés, personally identifiable information) son: nombre completo, dirección de residencia, números de tarjetas de crédito, edad, entre otras que se mencionan a continuación:

Ejemplos de Identificación Personal (PII)
Historia Criminal
Información clínica
Datos financieros y números de tarjeta de pago
Identificadores biométricos
Fechas de nacimiento
Información de discapacidades
Datos de recursos humanos y salarios
Perfiles financieros
Posiciones GPS
Direcciones IP
Nombres y apellidos
Direcciones de correo electrónico
Creencias religiosas o filosóficas
Orientación sexual

Tabla 2. Ejemplos de información de identificación personal.

Fuente: Elaboración Propia.

2.4.2 Origen

Luego de la Segunda Guerra Mundial, el mundo entero estaba impactado por el acontecimiento ocurrido, es por eso que el 10 de diciembre de 1948, la Asamblea General de las Naciones Unidas adoptó la "Declaración Universal de Derechos Humanos", en el mismo, se detalla lo siguiente:

> "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques." (Declaración Universal de los Derechos Humanos, Comisión de Derechos Humanos,1948)

Años más tarde, exactamente en 1950, el Convenio Europeo para la protección de los derechos humanos y las libertades fundamentales, afirma en el octavo capítulo:

> "1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás". (Convenio Europeo de Derechos Humanos , 4 de noviembre 1950)

Sin embargo, ninguno de los 2 tratados internacionales habla específicamente sobre la protección de datos personales, pero sí sobre la protección de la vida privada.

2.4.3 Avances y situación actual de la Protección de Datos en Latinoamérica

La tabla que a continuación se presenta, muestra la realidad de algunos países de Latinoamérica en lo que respecta a la protección de datos personales, así como las leyes vigentes y el interés por implementar leyes de éste ámbito.

No.	País	Situación Actual
1	Argentina	La República de Argentina implementó un sistema de Protección de Datos personales por la Ley 25.326, también conocida como Ley Habeas Data con el fin de regular las actividades de las bases de datos que registran información de carácter personal, su objeto es garantizar a las personas el control del uso de los datos personales ofreciéndole a los ciudadanos la opción de oposición a negarse a facilitar una información personal en caso de que no sea obligatorio hacerlo. Derecho a obtener información o indicios de existencia de sus datos personales en cualquier archivo, institución bancaria o base de datos; así como la finalidad y el destino para la cual se está haciendo uso de su información; así como la debida supresión o actualización de información personal.
2	Chile	El 15 de mayo de 2018, el senado de Chile aprobó una reforma constitucional de protección de datos personales en dicho país donde el objetivo es elevar a rango constitucional el derecho en que todos los ciudadanos del país puedan tener al fin sus datos personales debidamente protegidos.

		Ésta reforma modifica la constitución chilena y no la ley sobre la vida privada que se encuentra actualmente vigente en el país, ya que el proyecto de ley se encuentra en proceso aun e implica crear un organismo regulador llamado Agencia de Protección de Datos Personales basados en el RGPD implementado en la Unión Europea. Este organismo será el encargado de velar por la seguridad de los datos personales de los ciudadanos y regular el uso que las empresas hacen de la información de sus clientes. Las autoridades del Consejo Para La Trasparencia (CPLT) manifiestan que dentro de aproximadamente 3 o 4 años se debería pasar de una cultura de desprotección de los datos a una cultura de proyección de datos personales.
3	México	La República de México ha adoptado el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal también conocido como el Convenio 108; el cual fue adoptado por el Consejo de Europa en 1981 y reformado en el año 2001. Es el primer y único instrumento internacional vinculante en la materia, y también el primer instrumento europeo en ser abierto a países no miembros de la Unión Europea. El objetivo del convenio está basado en la creación de un marco jurídico en lo que a la protección de datos personales concierne, reconociendo la necesidad de conciliar ese cuidado con el flujo transfronterizo de los datos y promoviendo la cooperación internacional.

		El instrumento es vinculante para los 53 países que lo han adoptado, y establece diversos principios que tendrán que ser reconocidos en las legislaciones locales de los Estados firmantes. De acuerdo con los resultados de la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2017, "en México existen más de 71.3 millones de usuarios de Internet, quienes representan 63.9% de la población mayor a seis años. De ésta, 76.6% lo ha utilizado para acceder a redes sociales, 50.2% para descargar software, 47.7% para realizar compras o pagos y 15.7% para acceder a servicios en la nube" (Instituto Nacional de Estadística y Geografía (INEGI) 2018. Dado que estas actividades se sujetan a la solicitud de información que permita la identificación del usuario, más de 75% de cibernautas en México han dejado algún dato personal llámese identificación, sensible, patrimonial o biométrico en sitios virtuales. Aunque México ya cuenta con una ley especializada en protección de datos personales tanto para el ámbito privado, conocida como Ley Federal de Protección de Datos Personales en Posesión de los Particulares como para el público, la firma del Convenio 108 es un ejemplo claro de la importancia que tiene para México defender el derecho humano a la protección de datos personales.
4	Cuba	Cuba avanza en la informatización de los procesos de la sociedad cubana.

		Y con las oportunidades también llegan los grandes desafíos, entre los cuales resulta de alto impacto la protección de los datos personales. Tal como sucede en Iberoamérica con la escasez de regulaciones específicas o cuerpos legislativos de mayor peso, como pueden ser las leyes y decretos leyes, Cuba tiene pendiente el marco jurídico-legal que ampare la protección de los datos en medio de lo que resulta ya inevitable para el país como ser el trasiego de datos personales, vital para mejorar los servicios ciudadanos en línea.
5	Costa Rica	En fecha 7 de julio de 2011, a través de la Ley 8969, en el diario oficial la Gaceta se promulgó la Ley de Protección de la Persona frente al tratamiento de sus datos personales creando así la Agencia de Protección de Datos de los Habitantes, conocida como PROHAB, la cual garantiza que las personas sin importar su nacionalidad, residencia, tengan un pleno derecho a la autodeterminación informativa en relación con su vida o actividades privadas y demás derechos de la personalidad. Asimismo, orienta a los ciudadanos a ejercitar sus derechos y a las entidades públicas o privadas que gestionan bases de datos a cumplir con las obligaciones que establece la ley 8969 antes mencionada. Con lo anterior, se pretende actualizar la normativa costarricense sobre Protección de Datos Personales a la corriente de tendencias internacionales en la materia, a través de la aclaración de aspectos que en su momento suscitaron inquietudes respecto a la Ley y su aplicación, así como

		coadyuvar a las instituciones públicas y privadas a cumplir con las garantías, derechos otorgados y la simplificación de los trámites que corresponden, garantizando mayor fluidez en la transferencia y comercialización de datos, mejor control y competencia en la protección de datos personales.

Tabla 3. Situación Actual en Países de Latinoamérica

Fuente: ("Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?", 2016).

2.5 Reglamento General de Protección de Datos

En 2016, se adoptó el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, que entró en vigor el 25 de mayo de 2018 para reemplazar la Directiva 95/46/CE con el fin de implementar un reglamento legalmente vinculante que se considerará la ley de protección de datos de la UE. La ley de protección de datos de la UE brinda a una gran gama de derechos a los interesados que pueden hacerse valer contra las empresas que tratan datos personales. Esos derechos limitarán la capacidad de las empresas de tratar datos personales de los interesados en forma legal en muchas de las maneras que se solían utilizar en el pasado. Los nuevos derechos pueden tener un impacto significativo en el modelo de negocios de una empresa. Ese cambio a un modelo proteccionista que se enfoca en la privacidad individual representa una transformación importante de los requisitos para la protección de datos personales de los individuos de toda Europa.

Debido a las multas significativas por incumplimiento y a los esfuerzos de conformidad claramente más proactivos planificados por el supervisor de protección de datos de la UE, el RGPD en verdad impulsa la toma de medidas no solo por parte de todas las empresas que realizan negocios en Europa (incluido el Reino Unido después del brexit, la UE y los países del Espacio

Económico Europeo), sino también por parte de todas las empresas con oficinas en Europa, trabajadores en Europa (incluso si no residen en la zona en forma permanente), y clientes, pacientes y todo tipo de consumidores de Europa. Un requisito significativo del RGPD es que las empresas conduzcan evaluaciones de impacto en protección de datos (EIPD) para identificar y reducir los riesgos de protección de datos dentro de proyectos y sistemas, y también la probabilidad de daños de privacidad a los interesados.

2.5.1 Requisitos e impacto de RGPD

El RGPD incluye los siguientes cambios generales, en comparación a la Directiva 95/46/CE de Protección de Datos de la UE.

- El alcance territorial aumenta con aplicación extraterritorial.
- Se pueden multar a los responsables del tratamiento de datos.
- Los requisitos y condiciones para el consentimiento se consolidan y se vuelven más rigurosos.
- Si existe alguna infracción, se debe notificar a los interesados y autoridades de supervisión dentro de las 72 horas a partir de la identificación.
- El derecho de acceso se aplica a los datos personales, informes o cualquier actividad relacionada. ("Evaluaciones de Impacto en Protección de Datos del RGPD, ISACA", 2017).

Figura 5. Determinar si el RGPD se aplica a una empresa.

Fuente: ("Territorial scope of the GDPR (Flowchart)" de Varankevich, Siarhei, LinkedIn, 17 de febrero de 2017).

2.6 ISO/IEC 29100:2011 Marco de Referencia para la Protección de Datos Personales

Muchas empresas se han visto realmente afectadas en términos de responsabilidad legal, robo de identidad y costos de recuperación, debido a varios incidentes relacionados con la seguridad de la información. Es por eso, que, en respuesta a tales sucesos, en el año 2011 ISO (Organización Internacional de Estandarización), desarrolló el marco de privacidad ISO/IEC 29100 y la arquitectura del marco de privacidad ISO 29101, con el fin de brindar un marco de mayor nivel para la seguridad personal.

Las diferentes organizaciones, pueden utilizar los estándares en el diseño, implementación, operación y mantenimiento de sus sistemas de tecnologías de la información, permitiendo proteger los datos y de esta manera, mejorar los programas de privacidad de la organización a través de mejores prácticas de la industria.

Este estándar internacional provee una estructura general para la protección de información de identificación personal, con el objetivo de ayudar a las organizaciones a definir los mecanismos de protección relacionados a la privacidad de datos**.**

El marco establecido en la norma ISO / IEC 29100: 2011 es tanto aplicable a las personas como para las organizaciones si están utilizando sistemas o servicios de información y/o tecnologías de la comunicación que requieran controles de privacidad para el procesamiento de información de identificación personal.

A pesar de que existen estándares relacionados a la seguridad, como ser, ISO 27001, ISO 27002 e ISO 27108) ISO/IEC 29100 se enfoca al tratamiento de la información personal identificable.

2.6.1 Características y ventajas principales

- Proporciona un marco de privacidad que puede ser empleado para salvaguardar PII.
- Provee los controles necesarios para mitigar los riesgos significativos que plantean a la PII.
- Contiene información útil tanto para personas como por organizaciones que utilizan sistemas o servicios de información y/o tecnologías de la comunicación que se requieran controles de privacidad para el procesamiento de información de identificación personal.
- Es aplicable tanto por empresarios individuales tanto como por las multinacionales.

2.6.2 Principios de Privacidad

El estándar ISO/IEC 29100, cuenta con once principios de privacidad que han sido desarrollados para tener en cuenta los factores legales, reglamentarios, comerciales, contractuales y más. Es importante destacar, que todos estos principios fueron desarrollados por varios países, y diferentes organizaciones internacionales alrededor del mundo.

1. Elección y consentimiento

   El proveedor de los datos tiene la opción de poder elegir o no, el procesamiento de los datos por medio de un consentimiento, a su vez, se le debe notificar sobre los derechos de participación y acceso.

2. Propósito de legitimidad y especificación

El propósito de la forma en que se procesan los datos, debe cumplir con las leyes aplicables, y antes de que el titular proporcione la información, debe ser informado sobre dicha especificación.

3. Limitación de la recolección

   La recolección de datos, debe ser limitada únicamente a las necesidades del propósito que se ha especificado.

4. Minimización de datos

   Se debe de conceder acceso a los datos, solamente al personal que lo requiera. También se deben desechar los datos cuyos objetivos ya hayan expirado.

5. Limitación de uso, retención y divulgación

   Los datos personales proporcionados, deben estar limitados según los propósitos específicos, explícitos y legítimos por los que fueron establecidos.

6. Precisión y calidad

   Se debe garantizar que los datos son precisos, actualizados, relevantes, completos y confiables para el propósito de su uso. De igual forma, establecer controles al momento de recolectar y realizar periódicamente revisiones para la validación de los datos almacenados.

7. Honestidad, transparencia y aviso

   Si existe cualquier cambio en la forma en la que se procesan los datos, se debe notificar al titular de la información.

8. Participación y acceso individual

   El titular debe contar con el beneficio de poseer acceso para revisar sus datos en el momento que él disponga, se deben definir procesos para que puedan ejercer sus derechos de forma eficiente.

9. Responsabilidad y rendición de cuentas

   La implementación de políticas de privacidad debe ser asignada a un responsable dentro de la organización. Si llega a existir el caso que se produzca una brecha de seguridad y los datos del titular se vean afectados, se debe informar a éste. Capacitar al personal que tenga acceso a los datos proporcionados y gestionar cómo se maneja a los involucrados a través de consideraciones contractuales.

10. Seguridad de la información

    Se debe garantizar la confidencialidad, disponibilidad e integridad de los datos personales al implementar controles estratégicos, y así poder protegerlos contra accesos no autorizados, divulgación, pérdida o destrucción, entre otros riesgos.

11. Cumplimiento de la privacidad.

    Por medio de auditorías periódicas, verificar los niveles de protección de los controles de seguridad que existan, realizar monitoreo del cumplimiento de los requerimientos de la privacidad.

Estos principios son usados para guiar, diseñar, desarrollar e implementar controles de privacidad, además se pueden utilizar como un punto de referencia en el monitoreo y medición de la evaluación del desempeño.

2.6.3 Elementos básicos de Privacidad

Los elementos básicos del marco de privacidad ISO/IEC 29100, está basado en el WG5 en la ISO/IEC/FIDIS/ITU-T Joint Workshop en los Estándares del Manejo de Identidad. (Lucern, Suiza 2007).

En la siguiente figura, se identifica a los proveedores y receptores de PII como los actores. Los proveedores de PII, pueden ser los usuarios de cualquier sistema de tecnología de la información o los dueños de los datos como tal, ellos establecen las preferencias de privacidad y los proveedores de aplicaciones o administradores son conocidos como receptores de PII.

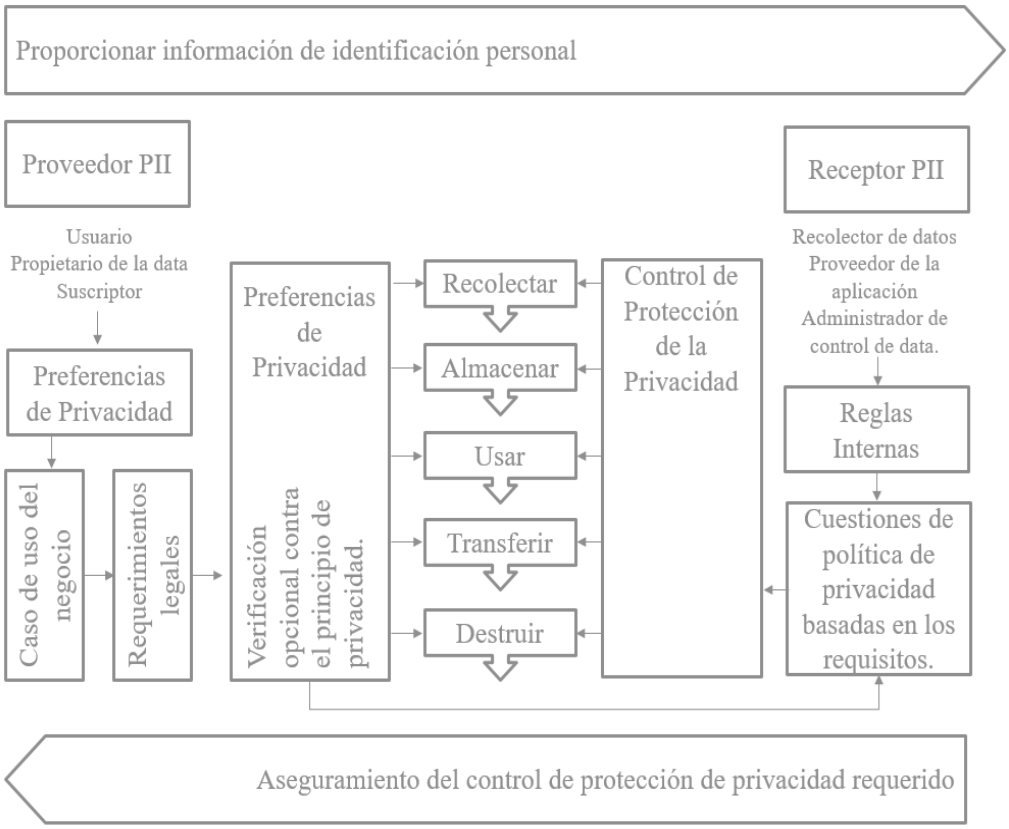

Figura 6. Elementos básicos de ISO/IEC 29100

Fuente: ("ISO 29100 How can organizations secure its privacy network?" Eric Lachapelle, Bardha Ajvazi, Fitim Rama de PECB, 27 de octubre de 2015).

2.7 PCI – DSS Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago

Las PCI-DSS definen un conjunto mínimo de requisitos para la protección de los datos de los titulares de las tarjetas de pago, se elaboraron para fomentar y mejorar la seguridad de los datos y así poder facilitar la adaptación de medidas de seguridad que sean uniformes alrededor del mundo. Estas normas, proveen referencias de requisitos técnicos y operativos, a continuación, se encuentran los 12 requisitos:

Desarrollo y mantenimiento de redes y sistemas seguros.	1. Instalar y mantener una configuración de firewall para proteger los datos del titular de la tarjeta. 2. No utilizar contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.
Proteger los datos del titular de la tarjeta.	3. Proteger los datos del titular de la tarjeta que fueron almacenados. 4. Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.
Mantener un programa de administración de vulnerabilidad.	5. Utilizar y actualizar con regularidad los programas o software antivirus. 6. Desarrollar y mantener sistemas y aplicaciones seguras.

Implementar medidas sólidas de control de acceso.	7. Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa. 8. Identificar y autenticar el acceso a los componentes del sistema. 9. Restringir el acceso físico a los datos del titular de la tarjeta.
Supervisar y evaluar las redes con regularidad.	10. Rastrear y supervisar todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas. 11. Probar con regularidad los sistemas y procesos de seguridad.
Mantener una política de seguridad de información.	12. Mantener una política que aborde la seguridad de la información para todo el personal.

Tabla 4. Requisitos de normas de seguridad de datos de la PCI.

Fuente: ("Requisitos y procedimientos de evaluación de seguridad v3.0, noviembre 2013).

Los encargados del cumplimiento, son las principales marcas de tarjetas de pago que establecieron las PCI DSS y el Consejo de Normas de Seguridad de PCI:

- American Express
- Discover Financial Services
- JCB International

- MasterCard Worlwide
- Visa Inc.

La Corporación “Tecnología Transaccional” ofrece el estándar de seguridad de datos para la industria de tarjetas de pago, un mecanismo donde están yendo todas las instituciones financieras de todo el mundo, y el país no es la excepción.

Cada vez la tecnología ha hecho que las diferencias en la implementación, el uso y la seguridad sean un estándar.

El estándar de seguridad de datos fue desarrollado por las compañías de tarjetas más importantes, como una guía que ayude a las organizaciones que procesan, almacenan o transmiten datos de tarjetahabientes, a asegurar dicha información, con el objetivo de evitar los fraudes en las tarjetas de débito y crédito.

2.8 TIBER –EU Threat Intelligence-based Ethical Red Teaming

El Banco Central Europeo (BCE) desarrolló en mayo de 2018 un simulador de ataques cibernéticos para servicios financieros, llamado European Framework for Threat Intelligence-Based Ethical Red Teaming (TIBER-EU), que es el primer marco a nivel de Europa para pruebas controladas contra ataques cibernéticos en el sistema financiero.

La iniciativa por la que se desarrolló ésta aplicación fue debido a que las entidades del sistema financiero en Europa son de las más castigadas por los cibercriminales, por eso el Banco Central Europeo encontró la necesidad de mitigar los riesgos e incidentes que se dan muy a menudo en los bancos, bolsas financieras y otras instituciones.

El marco TIBER-EU funciona realizando pruebas basadas en inteligencia que imita todo

tipo de tácticas, técnicas y procedimientos empleados por cibercriminales que son una amenaza latente en la sociedad; las pruebas que se llevan a cabo también se basan en las funciones críticas y los sistemas de las entidades, como ser las personas, procesos y tecnologías. Esto ayuda a la entidad a evaluar las capacidades de protección, nivel de detección y qué tan rápida es la respuesta obtenida frente a posibles ataques cibernéticos.

Finalmente, se conoce que éste marco fue diseñado para las autoridades y entidades europeas que forman el sistema financiero central, incluyendo empresas que realizan actividades transfronterizas que entran en éste ámbito regulatorio regido por varias autoridades. El marco TIBER-EU puede ser empleado en cualquier empresa del sector financiero, así como para entidades de otros sectores. (How to implement the European framework for Threat Intelligenc-based Ethical Red Teaming, 2018)

2.9 OCDE: Protección de la Privacidad y Flujos Transfronterizos de Datos Personales

En 1980, la Organización para la Cooperación y el Desarrollo Económico (OCDE) decidió elaborar directrices sobre la política internacional de la privacidad y los flujos transfronterizos de datos personales ante la llegada de la tecnología de la información a múltiples áreas de la vida cotidiana.

Estas directrices fueron adoptadas como parte de una recomendación del Consejo de la OCDE apoyando los tres principios que reúnen a los países de la OCDE:

- Democracia pluralista
- Respeto de los derechos humanos
- Economías de mercado abiertas

2.10 Prevención de Pérdida de Datos.

El DLP o medida de prevención de datos, es una estrategia donde se asegura que usuarios no envían información sensible o crítica fuera de la red empresarial, ésta terminología es también empleada para describir productos de aplicaciones que son gestionados a través del administrador de red para controlar que datos pueden ser transferidos por los usuarios finales.

La implementación de ésta medida en las empresas está siendo fuertemente impulsada por amenazas internas y por leyes estatales de privacidad, las cuales tienen ciertos componentes de protección de información, así como de acceso.

Las aplicaciones de software de DLP están basados en un conjunto de reglas de negocio que verifican el contenido de los archivos que pueden contener información crítica o sensible; el software puede ser útil para identificar el contenido bien definido, por ejemplo, datos de cuentas bancarias, información de cédulas de identidad, etc. Mencionando que, para implementar con éxito el DLP es necesario involucrar al personal de todos los niveles de gestión de la creación de reglas de negocio.

Finalmente, un usuario que de manera intencional o actividad intente divulgar información considerada como sensible podrá ser sancionado gracias al monitoreo que se realiza dentro del flujo de datos de la red.

CAPÍTULO III. METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Enfoque de la investigación

El siguiente capítulo consiste en determinar la metodología que se va a utilizar durante la investigación y desarrollo del documento; el enfoque determinado ayudará a responder la pregunta de investigación definida en el documento sobre cómo implementar un marco regulatorio para la protección de datos personales en las empresas del país, la categorización de la metodología es determinante ya que servirá de soporte a la comprobación y recomendaciones que se harán para el tema de investigación.

3.1.1 Enfoque Cualitativo

El entorno en el cual se desarrolla la investigación, aporta información que servirá de futuras referencias para la implementación de un reglamento para regular la protección de datos en las empresas de Honduras.

La investigación tiene un enfoque cualitativo y los expertos lo definen:

> … se enfoca a comprender y profundizar los fenómenos, explorándolos desde la perspectiva de los participantes en un ambiente natural y en relación con el contexto. El enfoque cualitativo se selecciona cuando se busca comprender la perspectiva de los participantes (individuos o grupos pequeños de personas a los que se investigará) acerca de los fenómenos que los rodean, profundizar en sus experiencias, perspectivas, opiniones y significados, es decir, la forma en que los participantes perciben subjetivamente su realidad. También es recomendable seleccionar el enfoque cualitativo cuando el tema del estudio ha sido poco explorado, o no se ha hecho investigación al respecto en algún grupo social específico. El proceso cualitativo inicia con la idea de investigación. (Sampieri, Collado, & Lucio, 2014).

3.2 Tipo de alcance de la investigación

El tipo de alcance de la presente investigación es exploratorio y descriptivo, ya que no se medirán datos en sí, sino que se propone realizar una propuesta de un marco regulatorio que contenga elementos claves y que mayor se adecue a la situación actual del país, si bien hay muchas normas que han sido ampliamente estudiadas, las cuales regulan la protección de datos a nivel internacional, en Honduras no existe un marco regulatorio que haga tal cosa.

3.3 Diseño de la investigación

En éste documento investigativo se recompilará información basados en las experiencias de los casos de éxito en cuanto a la implementación del reglamento general de protección de datos personales en los países que han incluido el reglamento para brindar los beneficios necesarios a los ciudadanos y optimizar los niveles de ciberseguridad; además de brindar recomendaciones basados en el criterio de los expertos quienes gracias a su experiencia aportarán el valor necesario al tema de investigación para conocer la situación actual del país y las ventajas que poseen las normativas internacionales vigentes.

3.4 Técnicas e instrumentos aplicados

3.4.1 Revisión de Documentos

Con el objetivo de introducirse y explorar el ambiente, se llevó a cabo la recolección de datos, con el fin de analizarlos y convertirlos en información que permita generar una propuesta de acuerdo al ambiente y condiciones de Honduras, siendo un procedimiento usual en el proceso de recolección y análisis de los datos según lo manifiesta(Hernandez Sampieri, 2014, pág. 396).

3.4.2 Revisión de Casos de Estudio

Al tratarse de un estudio cualitativo, es fácil adaptarlo a los casos de estudio ya que son temas únicos y que ameritan un profundo análisis y un acercamiento más real al contexto de la situación a investigar.

El estudio de casos, es una investigación empírica que estudia un fenómeno contemporáneo dentro de su contexto de la vida real, especialmente cuando los límites entre el fenómeno y su contexto no son claramente evidentes. Una investigación de estudio de casos trata exitosamente con una situación técnicamente distintiva en la cual hay muchas más variables de interés que datos observacionales y, como resultado, se basa en múltiples fuentes de evidencias, con datos que deben converger en un estilo de triangulación; además, se beneficia del desarrollo previo de proposiciones teóricas que guían la recolección y el análisis de datos. (Monje, 2010)

3.4.3 Entrevistas

Las entrevistas se aplican a expertos del país, se utilizaran entrevistas abiertas semi estructuradas, con el fin de observar el panorama general en el país, las preguntas incluyeron interrogantes de ejemplificación en otros países, que sirven de referente a Honduras en contraste de diferencias y similitudes, este tipo de entrevista permite que sea más íntima, flexible y abierta (Hernandez Sampieri, 2014, pág. 396).

Las entrevistas semiestructuradas según (Yuni & Urbano 2006, Sampieri 2010) se basan en una guía de asuntos, un listado tentativo de temas o preguntas y el entrevistador tiene la libertad de introducir preguntas adicionales para precisar conceptos u obtener más información sobre los temas deseados (es decir, no todas las preguntas están predeterminadas). Se busca relevar el conocimiento, expresado en forma de respuestas y de ese modo hacerlo accesible para interpretar.

3.5 Matriz metodológica

A continuación, se presenta una secuencia lógica de los elementos investigativos para que el problema, los objetivos, la metodología, instrumentos, variables e indicadores mantengan una correlación y así poder puntualizar resultados congruentes.

Nombre del Proyecto	Problema	Pregunta	Objetivo General	Objetivos Específicos	Metodología	Instrumentos
Análisis de implementación de una normativa de protección de datos en las empresas de Honduras.	Inexistencia de un marco regulatorio para la protección de datos en las empresas privadas y públicas de Honduras.	¿Cómo implementar un marco regulatorio para la protección de datos en las empresas del país?	Realizar un análisis basado en las principales normativas de protección de datos personales de mayor importancia a nivel internacional, y	Analizar las diferentes normativas referentes a la protección de datos, que han sido implementadas a nivel internacional. Determinar el estado actual de la protección de los datos en Honduras, y evaluar el impacto que traerá	Cualitativa	Revisión de documentos Revisión de casos de estudio Entrevistas a expertos

			de ésta forma, poder determinar cuál es la apropiada para implementar bajo un contexto empresarial público y privado de Honduras.	consigo las normativas en los sectores públicos y privados del país. Evaluar los principios claves de aplicación de la normativa más viable, para garantizar una efectiva protección de datos personales en el contexto empresarial del país.		

Tabla 5. Matriz metodológica de la investigación
Fuente: Elaboración propia.

CAPÍTULO IV. RESULTADO Y ANÁLISIS

4.1 Resultados de las Entrevistas

En base a la metodología presentada en el capítulo III de esta investigación, se presenta una propuesta para la implementación de un estándar que regule la protección de datos personales en las instituciones de Honduras.

4.1.1 Entrevistas Realizadas

Según el tema a analizar en la investigación, se planteó el instrumento de la entrevista a diferentes expertos en el área, con preguntas enfocadas a obtener la información necesaria para alinear las respuestas con el planteamiento del problema.

No.	Código de Instrumento	Nombre de Entrevistado	Lugar de Trabajo	Puesto Actual	Área de Especialización	No. de Anexo
1	ESPD-01	Sandy Karina Palma Rodríguez	Secretaría de Estado en los Despachos de Gobernación, Justicia y Descentralización	Jefe de la Unidad de Transparencia y Acceso a la información pública	Ing. En Informática / Ciberseguridad / Protección de Datos / Acceso a la Información	Anexo No. 1

2	ESPD-02	Alfonso de Jesús Alfonso	Grupo LAFISE-Honduras	Oficial de Seguridad de la Información	Dirección Estratégica en TI/Seguridad de la Información	Anexo No. 2
3	ESPD-03	Alvin Onam Rubio	Banco Central de Honduras	Administrador de Telecomunicaciones	Seguridad de Redes	Anexo No. 3
4	ESPD-04	Roberto Rodezno	BAC Credomatic Honduras	Jefe de Seguridad Informática	Seguridad de TI	Anexo No. 4
5	ESPD-05	Edy Javier Milla	Banco Central de Honduras	Jefe de Telecomunicaciones	Mg. Seguridad Informática	Anexo No.5
6	ESPD-06	Iván Roland Flores	Consultor	Consultor Informática Empresarial	CRMs ERP ISO27001	Anexo No. 6

Tabla 6. Lista de personas entrevistadas
Fuente: Elaboración propia.

4.1.2 Análisis de Muestreo Casos de Expertos

En la siguiente sección se plantea el resultado del análisis a las entrevistas aplicadas a expertos en el tema.

4.1.2.1 Descripción y análisis de Entrevista No. 1

Se entrevistó a la Ingeniera Sandy Karina Palma Rodríguez, Ingeniera en informática quien funge actualmente como jefe de la Unidad de Transparencia y Acceso a la Información Pública, la cual gracias a su experiencia se ha convertido en especialista en temas de ciberseguridad, protección de datos y acceso a la información; siendo así una referente nacional en éstos temas, impartiendo seminarios y charlas con el fin de hacer llegar el mensaje de la importancia de estos temas a muchas personas.

Menciona que existen diversas leyes a nivel nacional en las que se regula el acceso a la información personal de los habitantes, entre ellas está la ley de transparencia y acceso a la información pública, el código de ética del Servidor Publica, la Ley de Comisión de Bancas y Seguros, la misma Constitución de la República y que actualmente se encuentra en proceso de aprobación de ley en el Congreso Nacional una propuesta de protección de datos personales.

Afirma que todas las normativas que entran en cumplimiento a nivel internacional con cumplimiento obligatorio para el país, deben ser abarcadas y tomadas en consideración para evitar sanciones internacionales; hablando un poco del entorno nacional, menciona que toda ley una vez entrada en vigor en Honduras, debe ser cumplida a totalidad y una vez implementada las empresas deben acoplarse al cumplimiento de la misma, aplicando las debidas sanciones en caso de que éstas leyes no se cumplan, para lo cual, debe existir una comisión interventora encargada de vigilar el cumplimiento de la misma.

Recomienda la implementación de una ley constitucional, no un reglamento; el mismo debe ser autónomo del poder del estado y sus autoridades deben ser elegidas en audiencias públicas por el Congreso Nacional de la República, los países de los cuales se pueden tomar como referencia para la aplicación de una Ley de Protección de Datos pueden ser los países de la Unión Europea, Chile, Colombia, México y Perú.

Seguidamente, recomienda algunas medidas para reducir el impacto del uso indebido de los datos en Honduras, adherirnos al convenio de Budapest, así como la creación de una política nacional de seguridad de la información, también la creación del ente regulador y la comisión de protección de protección de datos de carácter constitucional.

4.1.2.2 Descripción y análisis de Entrevista No. 2

El Ingeniero Alfonso de Jesús Alfonso Pineda, especialista en Seguridad de la Información y dirección estratégica de TI, quien actualmente funge labores como Oficial de Seguridad de Información del prestigioso Grupo Lafise- Honduras; menciona conocer el GDPR y la Ley de Acceso a la Información Pública como leyes que obligan a las empresas a proteger la información personal de sus usuarios; donde la implementación de leyes de éste tipo en el país es algo requerido por todos los sectores; menciona que actualmente existe el Adhoc pero que sólo algunas empresas lo ponen en práctica aplicándolo solamente como una guía de buenas prácticas y recomendaciones.

Agrega que todo aquel cliente que posee información en Honduras afecta, ya que no les permite a las empresas locales cotizar en bolsas estadounidenses u otros mercados por la falta de estar apegados a diferentes normas al igual que la ventaja económica en comparación a otros países.

A nivel de protección de datos Honduras se encuentra muy baja, señala, pues hasta el momento no conoce leyes que contemplen dicho tema, por lo que, si se llegara a formar una comisión o un comité podrían verse involucradas entidades como la Comisión Nacional de Bancos y Seguros, el Instituto de Acceso a la Información Pública, el Poder Judicial y el Registro Nacional de las Personas; tomando en cuenta que el tiempo que tardó Colombia sería una referencia viable a tomar como parámetro en cuanto al tiempo de implementar regulaciones de éste tipo.

El presupuesto que el Estado destina para proteger la información es muy baja, comparado con el que se destina en la empresa privada, agregando que el fortalecimiento de las políticas internas a nivel de empresa y las leyes nacionales, además de una correcta clasificación de información personal y un marco jurídico adecuado podrían ayudar al país a alcanzar un nivel adecuado de protección de datos.

4.1.2.3 Descripción y análisis de Entrevista No. 3

El Ingeniero Alvin Onam Rubio, quien labora para el Banco Central de Honduras en el puesto de Administrador de Telecomunicaciones y especializado en la parte de Seguridad de Redes conoce normativas como:

- California Online Privacy Protection Act of 2003.
- Children's Online Privacy Protection Act of 1998.
- Cuarta Enmienda a la Constitución de los Estados Unidos.
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

- General Data Protection Regulation (GDPR).

- Payment Card Industry Data Security Standar.

Señala que desde el punto de vista de protección de datos personales es muy factible que las empresas públicas y privadas implementen normativas como éstas, ya que el país se encuentra con índices muy bajos en el tema.

Las normativas implementadas a nivel internacional afectan a países como el nuestro, indica, pues los reglamentos orientados a la protección de datos tienen impacto internacional como por ejemplo la cadena hotelera Marriot, que está establecida en Honduras, cuando atiene a personas de nacionalidad española se ven obligados a cumplir con el GDPR, así como los bancos que manejan tarjetas de crédito se deben apegar a PCI-DSS.

Afirma que el Registro Nacional de las Personas, el Instituto de la Propiedad y la CONATEL son los entes gubernamentales que apropiadamente se pueden involucrar para integrar una comisión y que el tiempo que tome el implementar una ley de este tipo depende en gran manera del interés mostrado por el gobierno de la república; en donde se puede tomar a España como referente ya que son los pioneros en la implementación de leyes en cuanto a protección de datos se refiere.

Menciona que a largo plazo se deberían elaborar leyes en las que obliguen a las empresas la aplicación de los controles correctos para la protección de información, evaluando los controles y realizando el debido seguimiento con auditorias con el fin de verificar que se están aplicando las leyes y en caso de no ser así, aplicar las sanciones correspondientes.

4.1.2.4 Descripción y análisis de Entrevista No. 4

Roberto Rodezno, Ingeniero en sistemas que labora en BAC Credomatic como jefe de Seguridad Informática describe que conoce del anteproyecto de ley que está en proceso de aprobación por el Congreso Nacional y la GDPR, la cual se implementó en los países de la Unión Europea. Recomienda que, para la implementación de lo mencionado anteriormente, se realice un estudio de factibilidad para considerar el impacto que tendrá, ya que es un tema muy amplio y deben considerarse muchos puntos importantes; como ser, el impacto del incumplimiento de la regulación, la creación de un programa que sea capaz de gestionar todo lo relacionado a la protección de la información, la creación de unidades de supervisión y regulación del cumplimiento de las normativas, así como validar temas de certificación y cumplimientos de organizaciones especializadas en el tema.

Cualquier incidente en nuestro país, quedaría impune o no controlada, por lo que, para implementar una ley, los entes que más apropiados le han parecido para conformar una comisión son el Congreso Nacional de la República, IAIP, el Poder Legislativo, organizaciones especializadas en temas de protección de datos, Comisión Nacional de Bancos y Seguros y entes internacionales.

Menciona que los países que pueden servir como guía para futuras regulaciones son Chile, México, Estados Unidos de América, Colombia y Costa Rica, en América; y de Europa son España, Inglaterra, Suiza y Alemania; señalando que un plazo de 3 a 5 años puede ser un plazo de tiempo para la implementación de leyes de ésta índole, aunque todo depende del interés y debida importancia que el gobierno preste al tema.

4.1.2.5 Descripción y análisis de Entrevista No. 5

El Ingeniero Iván Flores, que actualmente se dedica como consultor de informática empresarial y especializado en CRMs ERP ISO27001 afirma conocer la GDPR de Europa como marco regulatorio de protección de datos personales, señalando que en el país sería factible la implementación de leyes de éste tipo, aunque podría tomar de 1 a 2 años implementarlo.

Las normativas como la GDPR de Europa tienen impacto en Honduras, ya que se requiere cumplirla al realizar transacciones de negocios con entidades de la Unión Europea; el poco apoyo legal hace que el país tenga cifras muy bajas en relación a la protección de datos personales, por lo que, el instituto de Acceso a la Información Pública, el Ministerio Público, el Instituto de la Propiedad, Secretarías de Finanzas, Seguridad, Salud pueden ser los entes gubernamentales apropiados para integrar un comité para manejar éste tema.

Los países como la Unión Europea, México y Costa Rica son países que recomienda utilizar como referencia al momento de implementar una ley de protección de datos personales, donde las medidas que se pueden tomar para reducir el impacto del uso indebido de datos son analizar el GDPR y aplicarla al contexto empresarial antes de que se vuelva ley, y basados en los principios como conocer su inventario de información personal que posee en sus archivos y computadoras, reduzca sus archivos y mantenga únicamente la información que necesita para manejar el negocio, guarde con claves la información que mantiene, deseche (correctamente) la información que ya no necesita, elabore un plan para responder a las violaciones de seguridad.

4.1.2.6 Descripción y análisis de Entrevista No. 6

El Ingeniero Edy Javier Milla, fue el sexto experto entrevistado, especialista en el área de Seguridad Informática que actualmente labora como Jefe de Telecomunicaciones en el Banco Central de Honduras, expresa que si conoce estándares que obliga a las empresas a proteger la información personal de sus usuarios; mencionando La Ley del Registro Nacional de las personas donde se hace referencia a la clasificación de los datos que son públicos, la Constitución de la República donde menciona el hábeas data y derecho a la intimidad personal, familiar y la propia imagen; y la Ley de Justicia Constitucional que garantiza la libertad personal, integridad e intimidad de las personas.

Agrega que, si llegase a existir una ley, toda empresa debe estar en la obligación a cumplirla a su cabalidad; agrega que que también existen leyes de cumplimiento obligatorio en un sector específico, si una empresa tiene su propia ley, se debe analizar si ampara la protección de datos en ella; mencionando que es de mucha importancia analizar la aplicabilidad de las normas internacionales en el país, ya que Honduras posee ciertos tratados internacionales donde si no llega a cumplirlos parcialmente, puede caer en multas y sanciones costosas o la suspensión de apoyo económico, de ser necesario.

Honduras se encuentra baja –menciona- en términos de protección de datos, por lo que de implementar una ley que regule la protección de datos personales en las empresas del país podría demorar un periodo de tiempo de 3 a 5 años; dependiendo de la voluntad e interés del Estado en llevar a cabo un proyecto de éste tipo, donde países como Argentina, Colombia, Chile, México y Costa Rica podrían servir como referencia.

Los entes gubernamentales más apropiados que considera para estar involucrados en formar un comité para administrar éste tema son el Registro Nacional de las Personas, la Secretaria de Coordinación General del Gobierno, el Poder Judicial, Colegio de Abogados, Representante de la sociedad Civil, Representante de la sociedad Privada.

En cuanto al tema del presupuesto, explica que el mismo varia de una entidad a otra, tomando como referencia los procesos de las dependencias del estado, buscando algún proyecto destinado a la Seguridad de la Información.

Finalmente, las medidas que recomienda para reducir el impacto del uso indebido de los datos son, el cumplimiento de la ley, aplicar controles de seguridad en las empresas y concientización de la importancia del tema.

4.2 Resultados de la Investigación

4.2.1 Comparación entre los estándares y normas mundialmente aceptados.

A continuación, se presenta una comparación entre dos diferentes estándares existentes a nivel internacional y que han sido analizados en el presente estudio, en el cual se muestran los principios de privacidad más importantes y así poder determinar cuál metodología es la más adecuada para la implementación en las instituciones del país.

PRINCIPIOS DE PRIVACIDAD DE ISACA	RGPD	ISO 29100:2011
1. Elecciones y consentimiento	Aviso y consentimiento	Consentimiento y elecciones
2. Especificación de la finalidad legítima y de las Restricciones de uso	Toma de decisiones automatizada y finalidad legítima	Legitimidad y especificación de finalidades; y uso, retención y limitación de la divulgación
3. Información personal y ciclos de vida de la información sensible	Privacidad inherente, EIPD, Salvaguardas y consentimiento del afectado	Limitación de la recopilación, datos necesarios y no excesivos
4. Precisión y calidad	Rectificación de datos y calidad de datos	Precisión y calidad
5. Apertura, transparencia y aviso	Transparencia y derechos del afectado	Apertura, transparencia y aviso
6. Participación individual	Acceso del afectado	Acceso y participación individual
7. Responsabilidad	Tratamiento de datos, Delegados de la protección de datos y responsables del tratamiento	Responsabilidad
8. Salvaguardas de seguridad	Salvaguardas de seguridad durante el ciclo de vida de datos	Seguridad de la información
9. Supervisión, medición y presentación de informes	Informes y registros sobre el tratamiento, derecho al olvido y portabilidad de datos	Cumplimiento de privacidad

10. Prevención de daños	Legitimidad, acceso del afectado, portabilidad y EIPD	N/A
11. Gestión de terceros y proveedores	Gestión de encargados del tratamiento	N/A
12. Gestión de violaciones de seguridad	Gestión de violaciones de seguridad y notificaciones	N/A
13. Seguridad y privacidad inherentes	Responsabilidades del responsable del tratamien-to, toma de decisiones automatizada y protección de datos predeterminada	N/A
14. Circulación libre de infor-mación y restricciones legítimas	Derechos de los interesados, legalidad, transferencia de datos, normas corpora-tivas vinculantes	N/A

Figura 7. Principios de privacidad de ISACA aplicados a estándares de privacidad.

Fuente: (“Evaluaciones de Impacto en Protección de Datos del RGPD, ISACA”, 2017).

4.2.2 Análisis de la Situación Actual de Honduras

Según los resultados de las entrevistas realizadas a expertos en el tema, la situación de Honduras en términos de protección de datos personales es **muy baja**.

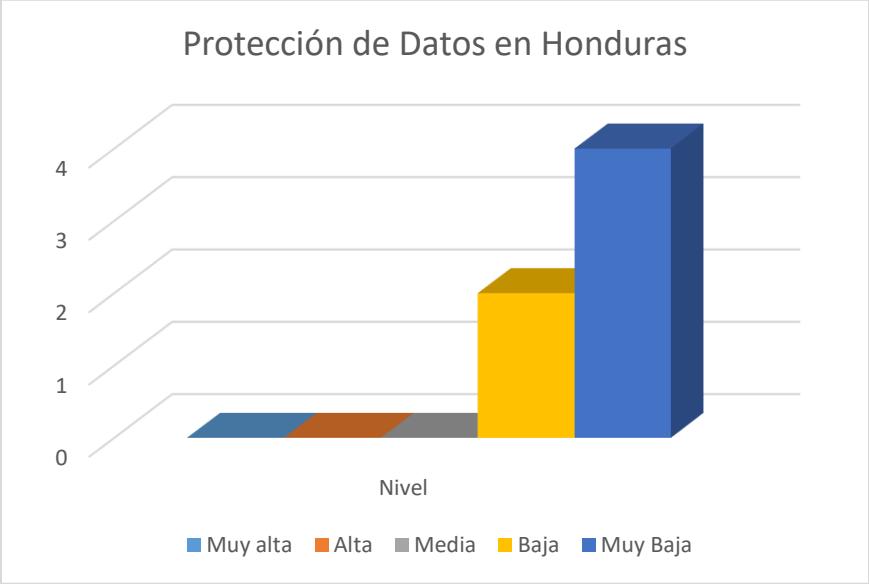

Figura 8.Protección de datos en Honduras
Fuente: Elaboración propia.

Según los datos oficiales del Observatorio de la Ciberseguridad en América Latina y el Caribe compuesta por la Organización de los Estados Americanos y el Banco Interamericano de Desarrollo mencionan que la falta de una política nacional de seguridad cibernética o un equipo de respuesta a incidentes, el Gobierno de Honduras tiene una capacidad limitada para abordar de manera proactiva las amenazas a su seguridad cibernética.

El gobierno ha llegado a adoptar una serie de medidas, entre ellas trabajar para renovar su estrategia de seguridad nacional para incluir los temas de seguridad y delincuencia cibernética; asistir a foros internacionales ofrecidos por la Organización de los Estados Americanos y otras instituciones en cuestiones de planificación de gestión de crisis; e incorporar programas digitales

en organismos como la Comisión Nacional de Telecomunicaciones y la Dirección Presidencial de Gestión por Resultados a cargo de la Agenda Digital del Estado.

Así mismo, las partes interesadas de la Infraestructura Crítica Nacional están implementando tecnologías de seguridad y normas internacionales, incluyendo ISACA, ISO 27002 e ITIL, 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 (Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?, 2016).

El informe de ciberseguridad 2016 indica:

> 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. La Dirección Nacional de Información Criminal de la Policía Nacional es la única entidad del país responsable de investigar los delitos cibernéticos, pero carece de un laboratorio forense digital o estadísticas nacionales sobre delincuencia cibernética (Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?, 2016).

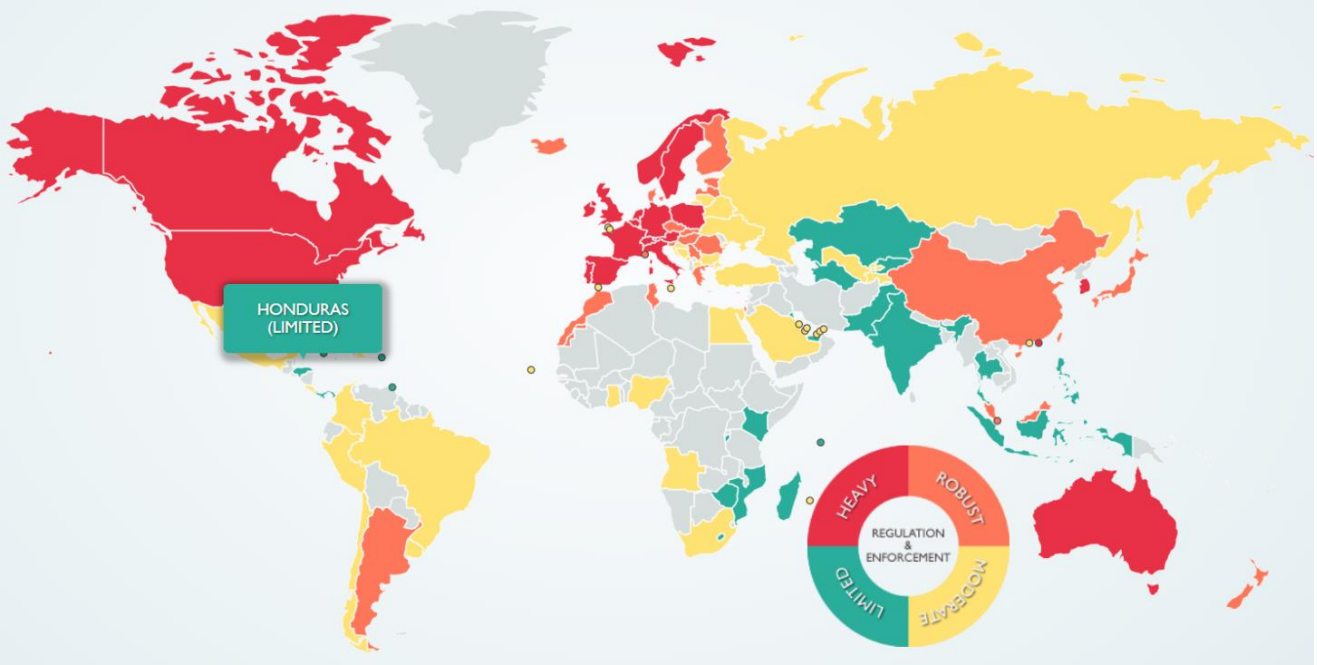

Figura 9. Honduras a nivel mundial en protección de datos
Fuente: ("DLA Piper Global Data Protection Laws of the World - World Map", s/f).

4.2.2.1 Leyes existentes en Honduras

Por lo anterior, éstas son las únicas leyes que regulan el acceso a la información pública:

- Constitución Nacional de Honduras: el artículo 182 proporciona la protección constitucional de Habeas Data, que otorga a las personas el derecho de acceder a cualquier archivo o registro, privado o público, electrónico o escrito a mano, que contenga información que pueda producir daños al honor personal y a la privacidad de la familia. También es un método para evitar la transmisión o divulgación de dichos datos, rectificar datos inexactos o engañosos, actualizar datos, requerir confidencialidad y eliminar información falsa. Esta garantía no afecta el secreto de las fuentes periodísticas.

- Ley del Registro Civil (artículo 109, Decreto 62-2004). Esta Ley se refiere únicamente a la información personal pública contenida en los archivos del Registro Civil.
- Ley de Transparencia y de Acceso a la Información Pública (artículo 3.5, Decreto 170-2006). Esta ley permite el acceso de cualquier persona a toda la información contenida en entidades públicas, excepto la que se clasifica como "Confidencial". También extiende la Protección Constitucional de los Datos de Hábeas y prohíbe la transmisión de información personal que pueda causar cualquier tipo de discriminación o daño moral o económico a las personas.
- Reglas sobre la Ley de Transparencia y de Acceso a la Información Pública (Artículo 42, Acuerdo 001-2008). Proporcionar una definición de las bases de datos que contengan información personal confidencial y requiere el consentimiento del interesado antes del uso por parte de un tercero.
- Además, en el Congreso de Honduras se está discutiendo una Ley de Protección de Privacidad de Datos y Datos de Hábeas. (Law in Honduras - DLA Piper Global Data Protection Laws of the World, s/f).

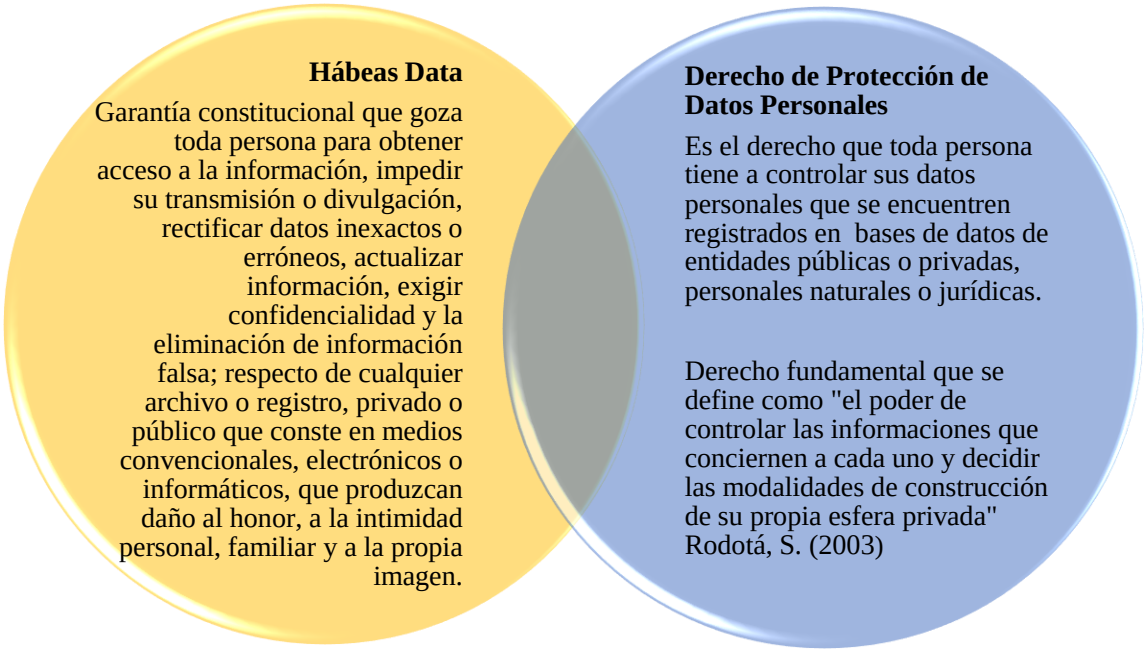

Figura 10. Diferencias entre Hábeas Data y Derecho de protección de datos personales.
Fuente: ("Análisis comparativo de legislaciones sobre protección de datos personales y hábeas data - Dr. Lester Ramírez Irías", 21 de enero de 2014).

4.2.2.2 Origen y evolución de la protección de datos en Honduras

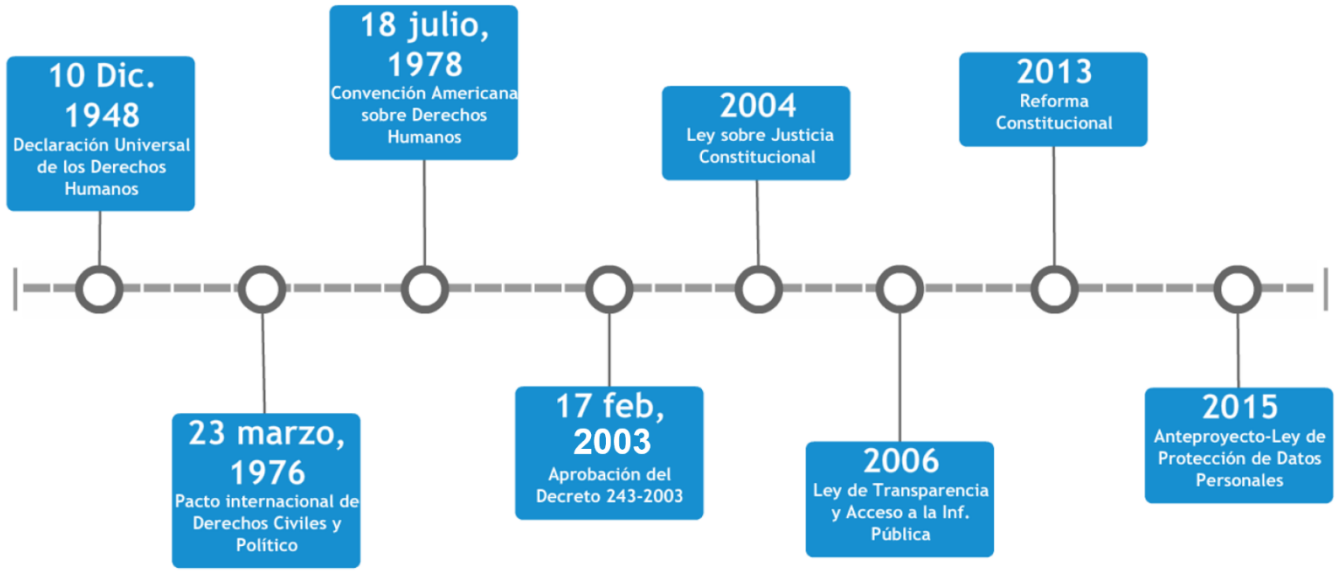

Figura 11. Origen y evolución de la protección de datos personales en Honduras
Fuente: Elaboración Propia.

Manzanares Vaquero, Gustavo Adolfo (2015) afirma: A pesar de que la Ley de Transparencia y Acceso a la Información Pública reconoce en su artículo 25 que los Datos Personales serán protegidos siempre y de que ya contamos con una garantía constitucional que nos permite ejercer una protección más efectiva sobre nuestros Datos, no es menos cierto que es necesario contar con una norma legal que reconozca en forma expresa los Derechos de los titulares de los datos personales como lo son, el de acceso, rectificación, cancelación y oposición, así como al recurso ante una autoridad independiente y especializada dotada de facultades sancionatorias.

"El sector privado proporciona un contraejemplo en términos de mentalidad en seguridad cibernética. Con el apoyo del gobierno, algunas organizaciones privadas del sector financiero en Honduras han establecido políticas de alto nivel y pautas de seguridad cibernética para sus organizaciones. Estos documentos proporcionan una política de seguridad cibernética en general para los empleados dentro de estas organizaciones. Sin embargo, aún no se han implementado, de manera efectiva, medidas para proteger la privacidad de los empleados" (Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?, 2016, p. 82).

4.2.3 Propuesta de una normativa de Protección de Datos

Todas las organizaciones a nivel mundial, tanto las que residen dentro de la Unión Europea como las que están ubicadas extraterritorialmente y operan con empresas europeas, se ven obligadas a cumplir con el Reglamento General de Protección de Datos.

En Honduras existen empresas que dentro de sus bases de datos cuentan con información personal de clientes de la UE. Aprovechando la coyuntura, y como resultado del análisis realizado en esta investigación, la propuesta de implementación de un marco regulatorio en el país, es el Reglamento General de Protección de Datos (RGPD) aplicado al contexto empresarial, mientras se apruebe en su totalidad la Ley de Protección de Datos de Honduras (la cual lleva 69 de sus 96 artículos aprobados).

Esta norma es aplicable a todas aquellas empresas que pertenezcan al sector público o privado que procesen datos de carácter personal. Es importante señalar, que se aplica a todo el espectro de la gestión de datos (desde la recopilación hasta la eliminación de datos).

4.2.3.1 Beneficios del RGPD

- Facilidad al comercio internacional.
- Aumento de la confianza de los clientes hacia las empresas.
- Reorganización de datos y su categorización.
- Depuración en la base de datos.
- Mejora la imagen y reputación como empresa.
- Mejora en seguridad de la información.

4.2.3.2 Medidas de Responsabilidad Activa

- Medidas de seguridad: Las empresas no deben conformarse con las acostumbradas medidas de seguridad, de ahora en adelante deben tener en cuenta lo siguiente:
    - La seudonimización, que es una técnica que desvincula los datos personales de la persona a la que identifican.
    - Cifrado de datos, para impedir el acceso a los datos personales, a personas que no estén autorizadas.
    - Confidencialidad, integridad, disponibilidad y resiliencia permanente de los sistemas y servicios de tratamiento.
    - La capacidad de restaurar la disponibilidad y el acceso a datos personales, en caso que existiera un incidente físico o técnico.
    - El proceso de verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y de la organización para garantizar la seguridad del tratamiento.
- Quiebras de seguridad: Los responsables están en la obligación de comunicar las violaciones de seguridad que se produzcan en sus sistemas, y en las que se dé destrucción, pérdida, alteración de los datos ya sea accidental o intencional. Cada empresa debe contar con mecanismos de detección y alertas de las violaciones, a su vez, deben tener un plan de contingencia para reaccionar ante las quiebras de seguridad.

  Con respecto a la comunicación de las violaciones, la empresa debe notificar a la autoridad de control correspondiente inmediatamente y si no fuera así, tiene un

plazo de 72 horas para comunicarlo.

- Evaluaciones de impacto sobre la protección de datos (EIPD), permite identificar y analizar los riesgos de un producto o servicio que pueda afectar la protección de datos de los afectados, de igual forma, se determina como gestionar dichos riesgos mediante las medidas correspondientes para mitigarlos.

    - Creación de la figura "Delegado de Protección de Datos (DPD, en inglés DPO – Data Protection Officer) (artículos 37-39), el cual cubre la necesidad de las empresas de contar con una persona que tenga los conocimientos especializados en protección de datos personales, siendo la figura que rinde cuentas ante el cumplimiento de la normativa. (Wolters Kluwer, 2018, p16)

4.2.3.3 Análisis GAP

Estado Actual (Objetivos)	**Métricas**	**Plan de Acción (Factores Claves para el cambio)**	**Estado Deseado**
Se requiere el análisis de qué datos se tratan, cuál es su finalidad, y que tipo de operaciones de tratamiento llevan a cabo.	Establecimiento de controles de auditoría interna.	Seguimiento y control de indicadores que miden los procesos de integridad y confidencialidad de la información personal de sus clientes.	Responsabilidad Proactiva por parte de la empresa, al exigir una actitud diligente y consciente frente al tratamiento de datos.

El interesado podría solicitar la confirmación, si se están tratando o no datos personales que le conciernen.		Disponibilidad, responsabilidad y actuar con diligencia al momento de presentar los datos personales que posee la empresa sobre un determinado cliente.	Derecho a obtener una copia de los datos personales que se están tratando.
Se requiere el borrado de la información personal, cuando el interesado lo solicite.		Adoptar medidas técnicas para informar a otros responsables de la solicitud de borrado.	Manifestación de los derechos de borrado o cancelación.
Elección del encargado de tratamiento.	Códigos de conducta o certificaciones.	Ofrecer medidas técnicas y organizativas apropiadas.	El responsable deberá garantizar que se cumple según el reglamento.
Se requiere tomar medidas organizativas y técnicas para integrar en los tratamientos,		Adoptar medidas que garanticen que solo se traten los datos necesarios.	Protección de datos desde el inicio de diseño de un tratamiento.

garantías que permitan aplicar los principios de privacidad.			
Notificación de quiebras de seguridad.	Cuando está la certeza que se ha producido una violación a la seguridad y se tiene el conocimiento sobre su origen y alcance.	Se debe notificar: la naturaleza de la violación, qué tipos de datos fueron afectados, medidas aplicadas para solucionar la violación.	Alertar a los afectados para que puedan tomar medidas de protección a las consecuencias.
Elaboración de la evaluación de impacto sobre la protección de datos.	EIPD, volumen de datos y la variedad de datos tratados, duración de la actividad de tratamiento.	Realizar una EIPD sobre aquellos tratamientos que signifiquen un alto riesgo para los derechos de los interesados.	Identificar la forma de mitigar los posibles riesgos en términos de tecnología disponible.
Se requiere la figura de un DPD (Delegado de Protección de	Cualificaciones profesionales, conocimiento de leyes	Elección de un DPD que permita asesorar al responsable o	Tener un punto de contacto para los interesados en todo lo

Datos)	y la práctica de protección de datos.	encargado en todo lo se relacione con la normativa.	que tenga que ver con protección de sus datos.

Tabla 7. Análisis GAP
Fuente: Elaboración Propia.

4.2.3.4 Pasos a seguir para cumplir el RGPD

Figura 12. Pasos a seguir para el cumplimiento del RGPD.
Fuente: Elaboración Propia.

4.2.3.5 Artículos del RGPD aplicables al contexto empresarial de Honduras

No. Artículo de RGPD	Descripción
Artículo 4, apartado 1, 2, 4, 5, 7, 8, 11, 12.	Definiciones
Artículo 5, apartado 1 y 2	Principios
Artículo 6, apartado 1	Licitud del tratamiento
Artículo 7, apartado 1 - 4	Condiciones para el consentimiento
Artículo 8, apartado 1 y 2	Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información.
Artículo 9, apartado 1, 2.1, 2.2	Tratamiento de categorías especiales de datos personales.
Artículo 13, apartado 1, 2	Información y acceso a los datos personales.
Artículo 14, apartado 1-5	Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado.
Artículo 15, apartado 1	Derecho de acceso del interesado
Artículo 16	Derecho de rectificación
Artículo 17, apartado 1	Derecho de supresión
Artículo 18, apartado 1	Derecho a la limitación del tratamiento

Artículo 20, apartado 1	Derecho a la portabilidad de los datos
Artículo 21, apartado 1, 2 y 3	Derecho de Oposición
Artículo 24, apartado 1	Responsabilidad del responsable del tratamiento
Artículo 25, apartado 1 y 2	Protección de datos desde el diseño y por defecto.
Artículo 28, apartado 1, 2	Encargado del tratamiento
Artículo 30, apartado 1, 2	Registro de las actividades de tratamiento
Artículo 32, apartado 1, 2, 4	Seguridad del tratamiento
Artículo 34, apartado 1, 3	Comunicación de una violación de la seguridad de los datos personales al interesado.
Artículo 35, apartado 1, 2, 3, 7, 8, 9, 11	Evaluación de impacto relativa a la protección de datos.
Artículo 37, apartado 1, 2, 3, 5, 6	Designación del delegado de protección de datos.
Artículo 38, apartado 1, 2, 3, 4, 5, 6	Posición del delegado de protección de datos.
Artículo 39, apartado 2	Funciones del delegado de protección de datos.

Tabla 8. Artículos del RGPD aplicables al contexto empresarial de Honduras.
Fuente: Elaboración Propia.

4.2.3.6 Factores de Éxito

Objetivo	Factor de Éxito
Fortalecer el comercio internacional entre Honduras y el resto del mundo.	Contar con una normativa que permita proteger los datos de los clientes del sector empresarial, de ésta forma, se genera un alto sentido de confianza y permitiría la facilidad de establecer negocios internacionales.
Contar con expertos en la materia, que puedan brindar asesoramiento sobre los pasos a seguir para adaptarse a una normativa.	Crear una carrera de "Derecho Informático" en las instituciones educativas de nivel superior. También se podría agregar al pensum académico de las carreras afines a la informática, clases en las que se oriente a este tema.
Gestionar el riesgo.	Implementar un proceso de gestión de riesgos, el cual permita una valoración que sea objetiva y realizar un tratamiento adecuado mediante la aplicación de medidas para su mitigación.
Mantener los sistemas monitorizados.	Contar con una herramienta de monitorización que permita configurar alertas para detectar incidentes en tiempo real.
Reaccionar de forma rápida a las brechas de	Notificar a las autoridades de control y a los usuarios que han sido afectados, según la

seguridad.	infracción ocurrida y así evitar ser sancionados.
Contemplar las acciones que se deben ejecutar, después de un incidente de seguridad.	Crear un plan de respuesta ante incidentes.
Evaluar y mejorar la eficacia de los procesos de gestión de la seguridad y del cumplimiento de la normativa aplicable.	Realizar auditorías periódicas para asegurar el cumplimiento de la normativa de forma continua.
Garantizar la correcta gestión de la seguridad y el cumplimiento de las obligaciones.	Implementar un sistema de gestión que permita a la empresa optimizar recursos, reducir costos y mejorar en el cumplimiento de sus objetivos.

4.2.3.7 Perfil del Delegado de Protección de Datos DPO

Para cumplir con el Reglamento General de Protección de Datos, se requiere la designación de un DPO o Delegado de Protección de Datos que sea el encargado de supervisar la estrategia de la seguridad en la organización, las empresas cuya actividad principal sea el tratamiento masivo de datos, así como toda aquella organización que se encargue del tratamiento a gran escala de categorías de datos personales que se encuentran especialmente protegidas o de datos relacionados con condenas e infracciones; es decir, cualquier empresa que se encuentre especialmente protegida se ve en la necesidad de tener un recurso de éste tipo en sus filas, ya que realizan funciones de mucha importancia como ser brindar información y asesorar los responsables, cooperar con las autoridades de control y será ésta persona la referencia para los titulares de datos o afectados por su tratamiento para el ejercicio de sus derechos o reclamaciones.

Es necesario definir un perfil requerido en cuanto a los conocimientos y habilidades que debe poseer el DPO, se investigó en LinkedIn el perfil de diferentes DPO quienes la mayoría reúne los siguientes conocimientos:

- Ingeniero en sistemas o Ingeniero Técnico en Informática.
- Consultor RPGD.
- Gestión de las TIC.
- Especializaciones o certificaciones en Derecho Informático Empresarial.
- Conocimientos sobre Ciberseguridad.
- Experiencia en Seguridad de la Información, Protección de Datos y Comercio Electrónico.
- Consultor, técnico en auditoría.

4.2.3.8 Organismo Regulador de Protección de Datos en Honduras

A lo largo de la investigación, se llevó a cabo un análisis de la situación actual de algunos países de Latinoamérica en lo que respecta a la implementación de leyes de protección de datos, por lo que se pudo observar que la mayoría de los países vieron la necesidad de la creación de un ente regulatorio encargado de velar por la seguridad de datos personales, aplicando las medidas y directrices necesarias para el cumplimiento de la ley, y brindando asesoramiento sobre cualquier aspecto que la ley contemplada.

En Honduras, también será necesario aplicar la misma metodología para alcanzar el éxito de la implementación de un marco regulatorio como el de los demás países que se estudiaron; los organismos para conformar dicha comisión pertenecen al sector gubernamental, los cuales, basados en la naturaleza de sus funciones para con el Estado, y bajo las recomendaciones brindadas

en las entrevistas por los expertos del tema, se consideran debidamente oportunas y capaces de llevar la gestión de manera eficaz las siguientes organizaciones:

- Instituto de Acceso a la Información Pública
- Registro Nacional de las Personas
- Instituto de la Propiedad
- Ministerio Público
- Secretaría de Seguridad
- Comisión Nacional de Telecomunicaciones
- Cancillería de la República
- Comisión Nacional de Bancos y Seguros

4.2.3.9 Implementación de LDP en Honduras

La adopción del LDP o prevención de pérdida de datos como estrategia de que los usuarios no exporten o envíen información crítica fuera de la red corporativa de las empresas es una forma efectiva de prevención mientras se implementa la Ley de protección de Datos Personales de manera oficial en el país; de manera que se evite la perdida de información y fuga de datos de las empresas.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

1. Después de realizar el respectivo análisis, se determinó que el Reglamento General de Protección de Datos es el más favorable para la implementación de sus mejores prácticas en el contexto empresarial de Honduras. Cada artículo que conforma dicho reglamento fue objeto de estudio para establecer cuáles de ellos podrían ser aplicables actualmente, según la situación actual del país.
2. Como resultado de entrevistas a expertos en el tema, y de realizar un profundo análisis de la situación actual de Honduras, es evidente la necesidad de una normativa que regule la protección de datos personales en el país; si bien es cierto, existe una garantía constitucional relacionada al Hábeas Data, en la cual, toda persona puede tener acceso a su información, sin embargo, no puede controlar lo que se hace con ella, como es el caso del derecho de protección de datos personales.
3. El Reglamento General de Protección de Datos no solamente es aplicable a las entidades que tengan su sede en la Unión Europea, sino que, si la empresa está establecida fuera, y ofrece productos o servicios a habitantes de esta región, está en la obligación de cumplir con la normativa. En vista a lo anterior, se brinda la propuesta de implementar el RGPD al contexto empresarial de Honduras, en tanto se apruebe la Ley de Protección de Datos en el país.
4. Si las reglas que el RGPD dicta, apoyan al establecimiento de un nuevo estándar mundial, es inaplazable que el gobierno de Honduras considere éste estándar como la guía para la protección de sus propias ciudadanías; esto no es una cuestión de transparencia en su información específicamente, sino de igualdad, libertad,

autonomía y dignidad.

5. Los lineamientos establecidos en el RGPD y que como buenas prácticas se recomendaron en el documento, establecerían un cambio de cultura en las empresas públicas y privadas del estado de Honduras, las administraciones públicas que obligan a tener en consideración la privacidad de datos en todos los aspectos y decisiones que afecten al tratamiento de datos personales.

6. Siguiendo el RGPD como un marco de referencia para aplicación en la protección de datos personales en Honduras, se puede decir que no se trata solamente de una cuestión de cumplimiento legal o jurídico, sino que se encuentra vinculada directamente con el modelo de negocios de muchas de las empresas más grandes a nivel global y que operan en la web.

5.2 Recomendaciones

1. Se recomienda la creación de una Agencia de Protección de Datos en Honduras, pudiendo ser la misma conformada por entidades como el Instituto de Acceso a la Información Pública, Registro Nacional de las Personas, Comisión Nacional de Bancos y Seguros y el Instituto de la Propiedad, que garanticen un sentido de protección y autodeterminación en relación a las actividades privadas y demás derechos de las personas.

2. Entretanto la Ley de Protección de Datos en Honduras sea aprobada, las empresas del país pueden implementar la práctica de Prevención de Pérdida de Data, DLP por sus siglas en inglés. Con ésta estrategia se puede asegurar que el usuario final no envíe información confidencial o sensible fuera de la red empresarial.

3. Concientizar a las autoridades correspondientes y a la población de Honduras sobre la importancia del tema de la Protección de Datos Personales, ya que se encuentra en una escala muy baja según datos aportados por las partes expertas que fueron entrevistadas en el documento de investigación, el obtener el apoyo del Estado o el nivel ejecutivo es clave para lograr avanzar en el tema, ya que se le daría la importancia debida y así se podría desarrollar un sentido de responsabilidad en las empresas por proteger los datos de los ciudadanos.

4. El modelo de RGPD está siendo exportable a Latinoamérica, por ésta razón muchos países de la región están en proceso de implementación y análisis del tema, Honduras no sería la excepción, puesto que se podría aprovechar los beneficios que la misma ley ofrece a los ciudadanos; es por ello recomendable que aborden procesos de reforma legislativa a mediano plazo siguiendo el marco de referencia

de como se ha hecho en Europa con el fin de enfrentar los nuevos retos que plantean las tecnologías emergentes.

5. Establecer el modelo de regulación tomando como principio clave, la gestión de riesgos. De ésta manera, tener la oportunidad de adoptar aquellas medidas técnicas y organizativas que consideren apropiadas para garantizar la integridad y confidencialidad de toda aquella información que se considere de índole personal y demostrar el cumplimiento de los principios establecidos en el Reglamento.

REFERENCIAS BIBLIOGRÁFICAS

Agencia Española de Protección de Datos, Agencia Vasca de Protección de Datos, & Autoridad Catalana de Protección de Datos. (s/f). Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento.

DLA Piper Global Data Protection Laws of the World - World Map. (s/f). Recuperado de https://www.dlapiperdataprotection.com/index.html?t=world-map&c=HN

Eduardo Marín. (2014). El ataque a Sony Pictures es el mayor "hackeo" que ha sufrido la industria del cine.

El Mundo Financiero. (2018). Roban información personal de 120.000 clientes de la banca tailandesa.

European Central Bank. (2018). How to implement the European framework for Threat Intelligence-based Ethical Red Teaming.

Grant Thornton. (2017, octubre). El Reglamento General de Protección de Datos (RGPD).

ISACA. (2017). Evaluaciones de Impacto en Protección de Datos del RGPD.

ISACA. (s/f). Adopción del RGPD utilizando COBIT 5.

Jose Luis Piñar Mañas. (s/f). *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad.*

Law in Honduras - DLA Piper Global Data Protection Laws of the World. (s/f). Recuperado el 19 de noviembre de 2018, de https://www.dlapiperdataprotection.com/index.html?c=HN&c2=&t=law

Lester Ramírez Irías. (2014, enero 21). Análisis Comparativo de Legislaciones sobre Protección de Datos Personales y Hábeas Data.

Observatorio de la Ciberseguridad en América Latina y el Caribe. (2016). Ciberseguridad

¿Estamos preparados en América Latina y el Caribe?

Organización para la Cooperación y el Desarrollo Económico. (s/f). Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales.

Parlamento Europeo, & Consejo de la Unión Europea. (2016, abril 27). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. Recuperado de https://www.boe.es/doue/2016/119/L00001-00088.pdf

PCI (Industria de tarjetas de pago) Normas de seguridad de datos - Requisitos y procedimientos de evaluación de seguridad. (2013).

Pulido, E. Z. (s/f). LA PROTECCIÓN DE DATOS PERSONALES EN ESPAÑA: EVOLUCIÓN NORMATIVA Y CRITERIOS DE APLICACIÓN, 508.

Ramón Oró. (s/f). *La Protección de Datos* (Primera). UOC.

Rebollo Delgado, Lucrecio. (s/f-a). *El derecho a la protección de datos en España y Argentina: orígenes y regulación vigente.*

Rebollo Delgado, Lucrecio. (s/f-b). *Introducción a la Protección de Datos*.

VietnamPlus. (2018). Hackers roban datos de cientos de miles clientes en ciberataques contra bancos en Tailandia.

Wolters Kluwer. (2018). *Cómo sobrevivir al GDPR* (Primera). BOSCH.

ANEXOS

Entrevista Semiestructurada

Protección de Datos Personales en Honduras

Anexo No. 1

Datos Generales	
Nombre Completo:	**Sandy Karyna Palma Rodríguez**
Puesto Actual:	**Jefe de la Unidad de Transparencia y Acceso a la Información Pública**
Área de Especialización:	**Ing. En Informática / Ciberseguridad / Protección de Datos / Acceso a la Información**

1. **¿Conoce algún estándar, normativa o ley que obligue a las empresas a proteger la información personal de sus usuarios?**

   Si/No

   En caso de su respuesta ser si, especifique cuales.

   R// Si

   - Ley de Transparencia y Acceso a la Información Pública
   - Código de Ética del Servidor Pública
   - Ley de la Comisión Nacional de Bancas y Seguros
   - Constitución de la República
   - NOTA: Actualmente se encuentra en proceso de aprobación la ley de protección de datos en el Congreso Nacional de la Republica. el borrador de la propuesta que se

presentó al congreso está aquí: https://cei.iaip.gob.hn/doc/Ley%20de%20Proteccion%20de%20Datos%20Personales.pdf

2. **¿Qué factibilidad hay, para que en las empresas de los sectores públicos y privados del país se implementen dichas normativas para la protección de datos personales?**

   Las leyes son de carácter obligatorio su implementación y cumplimiento, por lo que su factibilidad, no es una opción. Una vez que esta exista debe de cumplirse en su totalidad, en caso contrarios estas cuentan con marco normativo sancionatorio.

3. **¿Las normativas y reglamentos a nivel internacional afectan a países como Honduras? ¿Por qué?**

   Lo convenios, convenciones, tratados, resoluciones tanto de la ONU, OEA, CIDH, si nuestro país lo ratifica toda esta es de cumplimiento obligatorio, pero existen unos que, aunque no sea ratificado por el país se debe cumplir como ser la CARTA UNIVERSAL DE LOS DDHH, LA CARTA INTERAMERICANA DE LOS DDHH, etc. Y las resoluciones de las Corte IDH y la CIJ, son de cumplimiento obligatorio sino implica una sanción para el país

4. **¿Actualmente, cómo está Honduras en términos de protección de datos?**

   Muy Alta

   Alta

   Media

Baja

Muy Baja

Respuesta// Baja

5. **Si a una persona le roban sus datos en nuestro país ¿qué contemplan las leyes existentes?**

   Si se comprueba el delito, puede ir hasta prisión, dependiendo como le impongan los cargos.

6. **¿Qué entes gubernamentales serían los ideales para estar involucrados en una comisión o comité conformado de manera oficial para manejar este tema?**

   - Registro nacional de las personas
   - Instituto de Acceso a la Información Pública
   - Secretaría de Seguridad
   - CONATEL
   - HONDUTEL
   - Secretaría de Gobernación
   - Instituto de la Propiedad
   - Cancillería de la Republica
   - Sociedad Civil
   - CONADEH
   - Ministerio Publico
   - Poder Judicial

7. **¿En cuánto tiempo aproximadamente, se podría implementar un reglamento que regule la protección de los datos personales en las empresas del país?**

   No debe ser un reglamento, debe ser una Ley y que asigne una institución de protección de datos, con carácter constitucional, que no dependa de ningún poder del estado y que sus autoridades sean elegidas en audiencias públicas por el congreso nacional de la república. Y que los que propongan estos sean, de diferentes sectores, auto propuestos, CONADEH, sociedad civil, gobierno, poder judicial, algo así como los del TSC, TSE, MP. En entre otros, con independencia administrativa y de decisión.

8. **¿Cuáles países podrían ser de referencia en este tema para futuras regulaciones en el país?**

   - La Unión Europea – Con su Reglamento General de Protección de Datos (es una ley)
   - Chile la protección de datos personales está regulada legalmente desde el año 1999, mediante la ley 19.628 sobre protección de datos de carácter personal.
   - Colombia, la ley 1581 de 2012 y el decreto 1377 de 2013 regulan la forma en la que se deben proteger los derechos de los titulares de los datos personales y las obligaciones que nacen para quienes los recolectan y administran.
   - México, la ley federal de protección de datos personales en posesión de los particulares (vigente desde el 6 de julio de 2010) y su reglamento (en vigor desde el 22 de diciembre de 2011) son las principales fuentes de derecho que, de manera conjunta, tienen como finalidad regular el tratamiento legítimo, controlado e

informado de los datos personales, para garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

- Perú desde el 2011 cuenta con una regulación específica en materia de protección de datos personales. La ley 29733 y sus normas reglamentarias aprobadas por decreto supremo (003-2013-JUS)

9. ¿Cuál es el presupuesto anual que se destina para la protección de la información en una empresa?

No existe una respuesta a esta pregunta de forma concreta. Tomando en cuenta que la información es el activo más importante, debería ser fundamental contar con una Política de Seguridad de la Información (Ciberseguridad) institucional, y crear un plan de acción de detalle cómo implementar la política y cuáles son los procedimientos, costos, recursos humanos y económicos destinados para la protección de los activos (datos, información, físico, rrhh, etc).

10. ¿Qué medidas se pueden tomar para reducir el impacto del uso indebido de datos?

A. Como país:

- Aprobar la Ley de protección de datos que se encuentra en discusión en el congreso nacional.
- Adherirnos al convenio de Budapest.
- Crear una política nacional de seguridad de la información (Ciberseguridad) enlazada con la ley de protección de datos.
- Crear el ente de protección de datos con carácter constitucional.

- Crear el ente / comisión de implementación de la política ciberseguridad con carácter constitucional.
- Nota: los dos últimos incisos aquí podría ser la misma institución.

B. Como empresa (privada o individual si lo del inciso anterior no se hace)
    a. Crear una estrategia de seguridad de la información institucional.
    b. Un plan de la implementación, seguimiento y mejora continua.
    c. El apoyo de los tomadores de decisiones, es fundamental para esto. La protección de datos y la inversión en tecnología van de la mano y es fundamental para lograrlo.

Anexo No. 2

Datos Generales	
Nombre Completo:	**Alfonso de Jesús Alfonso Pineda**
Puesto Actual:	**Oficial de Seguridad de Información – Grupo Lafise Honduras**
Área de Especialización:	• **Dirección Estratégica en Tecnologías de Información** • **Seguridad de la Información**

1. **¿Conoce algún estándar, normativa o ley que obligue a las empresas a proteger la información personal de sus usuarios?**

   Si/No

   En caso de su respuesta ser si, especifique cuales:

   - GDPR
   - Ley de Acceso a la Información Pública

2. **¿Qué factibilidad hay, para que en las empresas de los sectores públicos y privados del país se implementen dichas normativas para la protección de datos personales?**

En mi concepto es requerido y es algo que viene siendo requerido por todos los sectores. Actualmente está Adhoc pero creo se puede formalizar ya que solo cada empresa o institución lo hace solo en base a las mejores prácticas.

3. **¿Las normativas y reglamentos a nivel internacional afectan a países como Honduras? ¿Por qué?**

   Los clientes extranjeros con información en Honduras nos afectan, no nos permite a nuestras empresas cotizar en bolsas estadounidenses u otros mercados por ausencia de estar apegados como país a dichas normas. No hay ventaja económica respecto a otros países. Ejm vrs Colombia quien si las tiene.

4. **¿Actualmente, cómo está Honduras en términos de protección de datos?**

   Muy Alta

   Alta

   Media

   Baja

   Muy Baja

5. **Si a una persona le roban sus datos en nuestro país ¿qué contemplan las leyes existentes?**

   No contemplado

6. **¿Qué entes gubernamentales serían los ideales para estar involucrados en una comisión o comité conformado de manera oficial para manejar este tema?**

    - **CNBS**
    - **Instituto de Acceso a la Información Pública**
    - **Poder Judicial**
    - **RNP**

7. **¿En cuánto tiempo aproximadamente, se podría implementar un reglamento que regule la protección de los datos personales en las empresas del país?**

    La ley en Colombia Tardó 3 años, ese puede ser un buen parámetro.

8. **¿Cuáles países podrían ser de referencia en este tema para futuras regulaciones en el país?**

    Colombia definitivamente, Costa Rica está trabajando también.

9. **¿Cuál es el presupuesto anual que se destina para la protección de la información en una empresa?**

    200,000 $ en promedio, eso en empresa privada, el estado invierte mucho menos.

10. **¿Qué medidas se pueden tomar para reducir el impacto del uso indebido de datos?**

    Políticas Internas y Leyes Nacionales, Clasificación de Datos de Carácter Personal, Marco Jurídico Adecuado.

Anexo No. 3

Datos Generales	
Nombre Completo:	**Alvin Onam Rubio**
Puesto Actual:	**Administrador de Telecomunicaciones**
Área de Especialización:	**Seguridad de Redes**

1. ¿Conoce algún estándar, normativa o ley que obligue a las empresas a proteger la información personal de sus usuarios?

Si/No

En caso de su respuesta ser si, especifique cuales.

- California Online Privacy Protection Act of 2003 (CalOPPA).
- Children's Online Privacy Protection Act of 1998 (COPPA).
- Cuarta Enmienda a la Constitución de los Estados Unidos.
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
- General Data Protection Regulation (GDPR).
- Payment Card Industry Data Security Standar (PCI-DSS).

2. **¿Qué factibilidad hay, para que en las empresas de los sectores públicos y privados del país se implementen dichas normativas para la protección de datos personales?**

   Desde un punto de vista de protección de los datos personales y la importancia que tiene el tema a nivel internacional, es altamente factible. No obstante, recomendaría evaluar otras variables como el costo/beneficio, leyes nacionales, tratados internacionales, nivel de madurez actual versus el deseado, entre otros. Debido que, al revisar todas estas variables se podría determinar que empresas aplican y que empresas no aplican a la protección de datos personales.

3. **¿Las normativas y reglamentos a nivel internacional afectan a países como Honduras? ¿Por qué?**

   Si afectan. Los reglamentos relacionados con la protección de los datos personales tienen un impacto internacional, debido a la globalización brindada por el Internet, no obstante, hay normativas y reglamentos que son de cumplimiento obligatorio para algunos sectores. Ejemplo: El Hotel Marriot, por ser una cadena de hoteles que atiende extranjeros de nacionalidad española se ven en la obligación de cumplir con el GDPR. Los bancos que manejan tarjetas de crédito deben apegarse al PCI-DSS.

4. **¿Actualmente, cómo está Honduras en términos de protección de datos?**

   Muy Alta

   Alta

Media

Baja

Muy Baja

5. **Si a una persona le roban sus datos en nuestro país ¿qué contemplan las leyes existentes?**

   Este sería un tema legal, y debería iniciar un proceso apegados a las leyes vigentes.

6. **¿Qué entes gubernamentales serían los ideales para estar involucrados en una comisión o comité conformado de manera oficial para manejar este tema?**

   - Registro Nacional de las Personas.
   - Instituto de la Propiedad.
   - Comisión Nacional de Telecomunicaciones.

7. **¿En cuánto tiempo aproximadamente, se podría implementar un reglamento que regule la protección de los datos personales en las empresas del país?**

   Considero que esta pregunta debe hacerse a un abogado. Por otra parte, considero que esto dependerá en gran medida del interés del congreso en impulsar un reglamento para este tipo de propuestas.

8. **¿Cuáles países podrían ser de referencia en este tema para futuras regulaciones en el país?**

España.

9. **¿Cuál es el presupuesto anual que se destina para la protección de la información en una empresa?**

   Es un dato complejo, varia del rubro, el país, cantidad y tipo de información procesada. Pero ciertamente las empresas hoy en día, se están viendo obligadas por las nuevas leyes de protección de la información a invertir más en esta área.

10. **¿Qué medidas se pueden tomar para reducir el impacto del uso indebido de datos?**

    - En el largo plazo: Elaboración de leyes que obliguen a los sectores en la aplicación de los controles correctos y efectivos para la protección de la información, esto detonará un gran esfuerzo y una gran inversión por parte de los sectores. Una vez creadas las leyes deben de evaluarse los controles y hacer auditorías de que estos controles se están aplicando correctamente. Multas que vayan acorde a los beneficios que generó el uso indebido de los datos, por ejemplo: Si una empresa por negligencia o a propósito filtró información que le generó utilidades, la multa debe ir acorde a esas utilidades.

    - En el corto plazo: Generar conciencia en la población, alfabetizar a los ciudadanos en este tema. Es importante que el usuario final entienda lo importante que es la protección de sus datos.

Anexo No. 4

Datos Generales	
Nombre Completo:	**Roberto Rodezno**
Puesto Actual:	**LSO**
Área de Especialización:	**Seguridad de TI**

1. **¿Conoce algún estándar, normativa o ley que obligue a las empresas a proteger la información personal de sus usuarios?**

   Si/No

   En caso de su respuesta ser si, especifique cuales.

   Localmente se conoce de:

   http://congresonacional.hn/index.php/2018/04/23/ley-de-proteccion-de-datoscn-evitara-que-datos-personales-de-los-hondurenos-sigan-siendo-vendidos-por-empresas-privadas/

   Internacional: DGPR en Europa Principalmente, HIPAA, FATCA (principalmente en los servicios financieros) en UUEE

   http://www.comunica-web.com/verarticulo-reglamento-general-proteccion-datos-que-es_929.php

   Otra referencia local:

https://portalunico.iaip.gob.hn/

https://cei.iaip.gob.hn/doc/Ley%20de%20Proteccion%20de%20Datos%20Personales.pdf

https://arsa.gob.hn/descargas/acuerdo0242018.pdf

2. **¿Qué factibilidad hay, para que en las empresas de los sectores públicos y privados del país se implementen dichas normativas para la protección de datos personales?**

   Inicialmente debería de haber un estudio de Factibilidad para considerar un resultado, en base a un criterio personal, se considera poco Factible para los sectores mencionados.

3. **¿Las normativas y reglamentos a nivel internacional afectan a países como Honduras? ¿Por qué?**

   Si, afectan por todos los convenios público-privados que se tienen en marcos regulatorios y/o comerciales.

4. **¿Actualmente, cómo está Honduras en términos de protección de datos?**

   Muy Alta

   Alta

   Media

   Baja

   Muy Baja

5. **Si a una persona le roban sus datos en nuestro país ¿qué contemplan las leyes existentes?**

   No se conoce ley publicada y un caso de aplicación de la misma, por lo anterior quedaría impune o no controlada, se adjunta un caso que podría relacionar con el tema no directamente, pero si hacer referencia del proceder local.

   https://www.laprensa.hn/honduras/1146210-410/maccih-denuncia-pacto-impunidad-congreso-blindar-corrupcion

6. **¿Qué entes gubernamentales serían los ideales para estar involucrados en una comisión o comité conformado de manera oficial para manejar este tema?**

   a. Congreso Nacional
   b. IAIP
   c. Poder Legislativo
   d. Organizaciones especializadas en protección de datos
   e. CNBS
   f. Entes Internacionales (Unión Europea, USAID, etc.)

7. **¿En cuánto tiempo aproximadamente, se podría implementar un reglamento que regule la protección de los datos personales en las empresas del país?**

   Dependiendo de la factibilidad y disposición de los entes gubernamentales, se visualizaría a mediano plazo (3 a 5 años)

8. **¿Cuáles países podrían ser de referencia en este tema para futuras regulaciones en el país?**

    - Americanos: Chile, México, Estados Unidos, Colombia y Costa Rica
    - Europeos: España, Inglaterra, Suiza y Alemania

9. **¿Cuál es el presupuesto anual que se destina para la protección de la información en una empresa?**

    Varia de Sector a sector, Importancia de la misma, del volumen de datos, normalmente un presupuesto que no sobrepasa del 1% de su presupuesto

10. **¿Qué medidas se pueden tomar para reducir el impacto del uso indebido de datos?**

    - Validar el impacto de un incumplimiento a una normativa o regulación.
    - Tener un programa que regule, gestione y administre todo lo relacionado a la protección de los datos.
    - Crear unidades de supervisión y regulación del cumplimiento de las normativas o políticas públicas aprobadas.
    - En las empresas privadas, validar temas de certificaciones y cumplimientos de organizaciones especializadas en el tema.

Anexo No. 5

Datos Generales	
Nombre Completo:	**Edy Javier Milla**
Puesto Actual:	**Jefe de Telecomunicaciones BCH**
Área de Especialización:	**Mg. Seguridad Informática**

1. ¿Conoce algún estándar, normativa o ley que obligue a las empresas a proteger la información personal de sus usuarios?

Si/No

En caso de su respuesta ser si, especifique cuales:

- Ley del Registro Nacional de las Personas, en su artículo 109 menciona cuales son los datos que son públicos, como ser: nombres y apellidos, número de identidad, fecha de nacimiento o fallecimiento, sexo, domicilio (excepto la dirección de la vivienda), profesión, ocupación u oficio, nacionalidad y estado civil.

- Constitución de la República, en el artículo 76 y 182 hace referencia a la garantía del habeas data y el derecho a la intimidad personal, familiar y a la propia imagen.

- Ley sobre Justicia Constitucional, en el artículo 13, hace mención al deber del estado de garantizar la libertad personal y la integridad e intimidad de la persona.

2. **¿Qué factibilidad hay, para que en las empresas de los sectores públicos y privados del país se implementen dichas normativas para la protección de datos personales?**

   Si existe una ley en el país, toda empresa tiene la obligación de cumplir con ella. Es importante mencionar, que también existen leyes de cumplimiento obligatorio en un sector específico, si una empresa tiene su propia ley, se debe analizar si ampara la protección de datos en ella.

3. **¿Las normativas y reglamentos a nivel internacional afectan a países como Honduras? ¿Por qué?**

   En cada normativa internacional se debe estudiar si obliga directamente a otro gobierno a cumplir con las regulaciones existentes en su país. Por otra parte, Honduras tiene tratados internacionales, y si el país no cumple con algún aspecto de las regulaciones, puede caer incluso en una demanda internacional contra el Gobierno de Honduras, se podría hablar también de la suspensión del apoyo económico por incumplimiento a normativas.

4. **¿Actualmente, cómo está Honduras en términos de protección de datos?**

   Muy Alta

   Alta

   Media

   Baja

   Muy Baja

5. **Si a una persona le roban sus datos en nuestro país ¿qué contemplan las leyes existentes?**

   Para brindar una mejor perspectiva de este punto, se les recomienda entablar una entrevista con un experto en leyes del país.

6. **¿Qué entes gubernamentales serían los ideales para estar involucrados en una comisión o comité conformado de manera oficial para manejar este tema?**

   - Registro Nacional de las Personas
   - Secretaría de Coordinación General del Gobierno
   - Poder Judicial
   - Colegio de Abogados
   - Representante de la Sociedad Civil
   - Representante de la Empresa Privada

7. **¿En cuánto tiempo aproximadamente, se podría implementar un reglamento que regule la protección de los datos personales en las empresas del país?**

   Según la implementación de leyes anteriores en el país, es probable que se cumpla en un período de 3 a 5 años. Todo depende de la voluntad al avanzar en este tema.

8. **¿Cuáles países podrían ser de referencia en este tema para futuras regulaciones en el país?**

- Argentina
- Colombia
- Chile
- México
- Costa Rica

9. **¿Cuál es el presupuesto anual que se destina para la protección de la información en una empresa?**

   Varía de una entidad a otra. Como referencia se podría mencionar los procesos de todas las dependencias del estado que se encuentran en www.honducompras.com, se puede buscar algún proyecto destinado a la seguridad de la información, y cuál fue su costo.

10. **¿Qué medidas se pueden tomar para reducir el impacto del uso indebido de datos?**

- Cumplimiento de la ley
- Controles de seguridad de las empresas
- Concientización y socialización del tema.

Anexo No. 6

Datos Generales	
Nombre Completo:	**Ivan Roland Flores**
Puesto Actual:	**Consultor Informatica Empresarial**
Área de Especialización:	**CRMs ERP ISO27001**

11. ¿Conoce algún estándar, normativa o ley que obligue a las empresas a proteger la información personal de sus usuarios?

Si

En caso de su respuesta ser si, especifique cuales.

La GDPR de Europa.

12. ¿Qué factibilidad hay, para que en las empresas de los sectores públicos y privados del país se implementen dichas normativas para la protección de datos personales?

Es bastante factible pero tomará tiempo considerable (1-2 años) implementarlo.

13. ¿Las normativas y reglamentos a nivel internacional afectan a países como Honduras? ¿Por qué?

La GDPR de Europa se requeire cumplir al realizar transacciones de negocios con entidades de la UE.

14. ¿Actualmente, cómo está Honduras en términos de protección de datos?

Muy Alta

Alta

Media

Baja

Muy Baja <<<<

15. Si a una persona le roban sus datos en nuestro país ¿qué contemplan las leyes existentes?

Hay poco apoyo legal. En 2018 se inició la aprobación de la una ley.

16. ¿Qué entes gubernamentales serían los ideales para estar involucrados en una comisión o comité conformado de manera oficial para manejar este tema?

a) Instituto de Acceso a la Información Pública
b) Ministerio Público
c) Instituto de la Propiedad
d) Secretarías de Finanzas, Seguridad, Salud.

17. ¿En cuánto tiempo aproximadamente, se podría implementar un reglamento que regule la protección de los datos personales en las empresas del país?

Estimación de 1-2 años implementarlo

18. ¿Cuáles países podrían ser de referencia en este tema para futuras regulaciones en el país?

Union Europea. Mexico. Costa Rica.

19. ¿Cuál es el presupuesto anual que se destina para la protección de la información en una empresa?

Estimo que actualmente es menos del 1/20 del 1% del presupuesto operativo. Eso debe incrementarse a ½ a ¼ del 1%

20. ¿Qué medidas se pueden tomar para reducir el impacto del uso indebido de datos?

Analizar el GDPR y aplicarla al contexto empresarial antes que se vuelva ley, sin embargo, hay algunos principios base aplicables de acurdo a la FTC y a la GDPR:

- Conozca su inventario de información personal que posee en sus archivos y computadoras.
- Reduzca sus archivos y mantenga únicamente la información que necesita para manejar el negocio.
- Guarde con claves la información que mantiene.
- Deseche (correctamente) la información que ya no necesita.
- Elabore un plan para responder a las violaciones de seguridad.