Universidad Católica de Santa María

Facultad de Ciencias e Ingenierías Físicas y Formales

Escuela Profesional de Ingeniería de Sistemas

PROPUESTA DE UNA METODOLOGÍA PARA LA IMPLEMENTACIÓN DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES APLICADO A UNA EMPRESA DEL SECTOR TEXTIL: MICHELL Y CÍA S.A.

Tesis presentada por los Bachilleres:

García Tenorio, Maryori Flor de Jazmín

Urquizo Pinto, Jeanpierre Ricardo

Para optar el Título Profesional de

Ingeniero de Sistemas

Especialidad en Sistemas de Información

Asesor:

Mg. Rosas Paredes, Karina

Arequipa- Perú

2019

FACULTAD DE CIENCIAS E INGENIERIAS FISICAS Y FORMALES

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

INFORME DICTAMEN DE BORRADOR TESIS

VISTO

El Borrador de TESIS titulado:

PROPUESTA DE UNA METODOLOGIA PARA LA IMPLEMENTACION DE LA LEY DE PROTECCION DE DATOS PERSONALES APLICADO A UNA EMPRESA TEXTIL : MICHELL y CIA S. A.

Presentado por (el) (la) (los) Bachiller (es):

MARYORI FLOR DE JAZMÍN GARCIA TENORIO

JEANPIERRE RICARDO VERGIZO PINTO

Nuestro dictamen es:

Es favorable

OBSERVACIONES: Ninguna

Arequipa, 30 de Setiembre de 2019

COD: 1631

1568

PRESENTACIÓN

Señor Decano de la Facultad de Ciencias e Ingenierías Físicas y Formales.
Señor Director del Programa Profesional de Ingeniería de Sistemas.

Señores Miembros del Jurado Dictaminador de la Tesis

De conformidad con las disposiciones del Reglamento de Grados y Títulos de la Escuela Profesional de Ingeniería de Sistemas, pongo a vuestra consideración el presente trabajo de investigación titulado:

Propuesta de una Metodología para la Implementación de la Ley de Protección de Datos Personales aplicado a una Empresa del Sector Textil: Michell y Cía. S.A.

El trabajo de investigación fue realizado aplicando los conocimientos adquiridos durante nuestra formación universitaria, el mismo que al ser aprobado nos permitirá optar por el Título Profesional de Ingeniero de Sistemas.

DEDICATORIA

Maryori Flor de Jazmín García Tenorio

A Dios que hace posible el logro de una más de mis metas.

A mi padre, por ser la persona que jamás me abandona y me anima a seguir adelante para nunca rendirme hasta cumplir mis sueños más anhelados.

A mi madre, por inculcarme el valor del respeto, la humildad, la generosidad, el amor y la fé en Dios.

A ambos, por ser mi principal motor y estar siempre dispuestos a ayudarme a crecer profesionalmente y brindarme su apoyo incondicional y sobre todo por nunca cortarme las alas dejándome decidir sobre lo que deseo en mi futuro.

A mi hermano, por haber sido siempre mi mayor ejemplo a seguir y una de mis mayores motivaciones por su inteligencia, capacidad y esfuerzo.

A mi compañero de tesis, amigo y alguien muy especial en mi vida, Jeanpierre Urquizo Pinto, porque a pesar de todo nunca perdimos de vista la meta trazada de culminar este proyecto que emprendimos juntos para terminarlo juntos.

Jeanpierre Ricardo Urquizo Pinto

Dedico este proyecto a Dios por que sin el nada sería posible
A mis padres por su esfuerzo y cariño sacaron adelante todo mi camino a la Universidad, por ellos soy lo que soy hoy en día.
A mi hermana por su constante apoyo y cariño.
A mi compañera, amiga y alguien muy especial en mi vida, Maryori Garcia Tenorio por apoyarme a culminar este proyecto, por estar presente cuando más la necesitaba y por acompañarme en este camino.

AGRADECIMIENTO

A nuestra asesora de Tesis, Mg. Karina Rosas Paredes por su apoyo en el desarrollo del presente informe y al Mg. Oscar Ramírez Valdez por su asesoramiento durante la implementación del proyecto.

También agradecemos a los directivos de la empresa MICHELL Y CIA S.A., en especial al gerente administrativo, y al gerente de tecnologías de la información, por permitirnos desarrollar este proyecto, paciencia y tiempo dedicado para la llevar a cabo el proyecto de la mejor manera.

INTRODUCCION

En los últimos años la tecnología ha evolucionado permitiendo generar, transmitir y almacenar gran cantidad de información. Sin embargo, este proceso incontrolable ha dejado a las personas totalmente desprotegidas del uso que se pueda dar a su información (González, Ruiz & Pollo, 2016). Esto se vuelve un verdadero problema cuando la información manipulada es de carácter personal, debido a que en ocasiones puede existir uso excesivo de información que puede producir perjuicios a las personas, por lo tanto, se ha vuelto una necesidad poder controlarlo.

Como consecuencia, en varios países del mundo se ha decretado la ley de protección de datos personales, reconocida en el Perú como la Ley N°29733 para proteger la información personal que están en manos de otros.

La protección de datos personales representa el reconocimiento de un derecho humano porque todo individuo tiene derecho a que su intimidad sea resguardada de abusos que se puede generar manipulando sus datos personales que se encuentran en bancos de datos, tanto públicos como privados (Richter, 2015).

Actualmente, en nuestro país son pocas las empresas textiles que cumplen con lo establecido en la Ley N°29733, y otras empresas han sido rechazadas en la etapa de inscripción de sus bancos de datos personales por no tener los controles adecuados en sus bancos de datos. El hacer caso omiso a esta ley puede ocasionar consecuencias negativas para una organización como son: los riesgos de pérdida de información, sabotaje, manipulación de información no permitida, y el pago de multas que la ley de protección de datos personales sustenta y que a su vez puede llegar a ser sumamente perjudicial tanto para la empresa como para la Gerencia de TI.

Considerando la problemática anterior, la presente investigación propone una metodología que permita a las empresas textiles implementar la ley de protección de datos personales garantizando que el proceso de registro de sus bancos de datos sea correcto y que sus procedimientos y políticas de seguridad de la información estén orientados a tener un sistema de gestión de la seguridad de la información conforme al estándar internacional ISO 27001:2012 y la Directiva de Seguridad que complementa a la ley de protección de datos personales.

RESUMEN

La presente investigación se ha efectuado considerando la ley de protección de datos personales formulándose una propuesta de una metodología para implementar la ley de protección de datos personales a una empresa del sector textil como Michell y Cía. S.A.

Una de las actividades principales es el proceso de registro de los bancos de datos personales ante el registro nacional de protección de datos personales y asegurar el cumplimiento de los niveles adecuados de seguridad para cada banco de datos personales con la Directiva de Seguridad establecida por la autoridad nacional de protección de datos personales.

La presente propuesta está estructurada en cuatro fases: (a) planeamiento, donde se identifica áreas involucradas y posibles bancos de datos, (b) recopilación y registro de los bancos de datos, en el cual se hace un listado de todos los bancos de datos identificados para su posterior inscripción ante el registro nacional de protección de datos personales, (c) elaboración y ejecución de políticas y procedimientos, y finalmente (d) la obtención del consentimiento del titular, en el cual se determina mecanismos para obtener el consentimiento de los titulares de datos personales.

Luego de ejecutar las fases descritas anteriormente, se obtendrá un documento que consolide todos los procedimientos de seguridad de la información requeridos por la Empresa Michell y Cía. S.A., para culminar con la elaboración de un formato y un procedimiento que permitan obtener el consentimiento del titular de los datos personales.

Palabras claves:

Seguridad de información. LPDP, banco de datos, datos personales, derechos ARCO.

ABSTRACT

The present investigation was carried out considering the law of protection of personal data formulating a proposal of a methodology to implement the law of protection of personal data to a company of the textile sector like Michell and Company. S.A.

One of the main activities is the process of registering the personal data banks with the national registry for the protection of personal data and ensuring compliance with the security directive established by the national authority for the protection of personal data.

The present proposal is structured in four phases: (a) planning, identifying areas involved and possible data banks, (b) collecting and registering data banks, listing all databases (c) elaboration and implementation of policies and procedures, and (d) obtaining the consent of the holder, in which mechanisms are established to obtain the consent of the holders of personal data.

After executing the phases described above, you will obtain a document that consolidates all the information security procedures required by Michell and Cía. S.A., to culminate with the elaboration of a format and a procedure that allow obtaining the consent of the holder of the personal data.

Key words:

Information security LPDP, data bank, personal data, ARCO rights.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CAPITULO I

1. PLANTEAMIENTO TEÓRICO

1.1 PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1.1 Planteamiento del Problema

Antes de ver la metodología veamos que es el derecho a la privacidad de la información, para aclarar este problema tenemos 2 conceptos:

"Es el derecho a quedarse solo" (Arce Janáriz, 1996), "El derecho del individuo a ser protegido contra la intrusión en su vida personal o asuntos, o los de su familia, por medios físicos directos o por publicación de información", (Comité Calcutt, Reino Unido, 1997).

Hay una gran variedad de temas concernientes al manejo de los datos de las personas no solo en el ámbito informático, sino en el ámbito legal, las empresas tienen un alto grado de responsabilidad para realizar tratamiento de todo tipo de documentos, así como la tecnología que utiliza para realizar este manejo de información, esto no es tan simple como parece ya que la empresa debe generar soportes que sean manejables y a la vez seguros.

El articulo 2 numeral 6 de la Constitución Política del Perú sostiene que "Toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten a la intimidad personal y familiar" (Congreso, 1993).

Sin embargo, existen empresas que no cumplen con la finalidad de la Ley de Protección de Datos Personales: Garantizar el derecho fundamental de la protección de datos personales, con un adecuado tratamiento.

Es nuestra responsabilidad como ingenieros de sistemas y responsable de la información a nivel empresarial, conocer toda información acerca de la

seguridad de los datos en cada empresa en la que laboramos, es cada vez más crítico las sanciones y procesos que se llevan a cabo por incumplimiento de la Ley de Protección de Datos Personales (Ley 29733). Esto genera preocupación no solo en las personas sino también en las organizaciones que no saben cómo aplicar estas medidas adecuándolas a sus procesos, tanto estratégicos, core o de soporte que incluyan información de personas naturales.

Esta ley especifica claramente que su ámbito "La presente Ley es de aplicación a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional. Son objeto de especial protección los datos sensibles (Ministerio de Justicia y Derechos Humanos, 2011b).

Este flujo de información ha tomado una tremenda importancia económica para fines de marketing, por ejemplo, para llegar más eficiente a determinados públicos objetivos. Pero el mayor uso implica peligro de mala utilización y vulnerabilidad del derecho a la intimidad o privacidad.

También tenemos el caso de la sanción a la empresa limeña Dorimuth Travel Service S.A. Por exponer información sensible, por su falta de seguridad la empresa fue sancionada con la más grande multa que se ha registrado (50 UIT), lo que causa no solo problemas económicos también la confianza de los clientes disminuyo drásticamente.

Como consecuencia a lo mencionado se decretó la ley de protección de datos personales (LPDP), que permite garantizar la protección de los datos personales mediante el control inequívoco de su uso. Además, para que dé una adecuada protección a la privacidad permitiendo la posibilidad de uso de los sistemas automatizados.

En el mundo existen leyes reguladoras que protegen la información personal en diferentes aspectos, el más claro ejemplo es Directiva Protección Datos EU en la Unión Europea y la Ley Orgánica de Protección de Datos Personales en España. Así mismo, en el Perú está reconocida como la Ley N°29733 y es una obligación de las empresas adecuarse a ella.

El problema principal es que de las 2’124,280 empresas (INEI, 2016) que existen en nuestro país, ya sea por los pocos años de haber sido decretada la Ley, no tienen o tienen poco conocimiento de la implementación de la ley de protección de datos, sus beneficios y consecuencias que se pueden generar.

Uno de los mayores perjuicios que puede acarrear no cumplir lo establecido por la Ley, es el pago de multas o sanciones que son categorizadas por el nivel de gravedad, esto puede ser sumamente grave para pequeñas y hasta para medianas empresas.

Además, en la actualidad existen empresas que han sido rechazadas por no haber llevado a cabo un registro y cumplimiento satisfactorio de la Ley de Protección de Datos, provocando hasta el cierre de la empresa.

Para esto se propone una metodología para la implementación de la ley de protección de datos personales aplicado a una empresa del sector textil: Michell y Cía. S.A.

1.1.2 Objetivos de la Investigación

a. General

Proponer una metodología para implementar la ley de protección de datos personales aplicado a una empresa del sector textil y privado– MICHELL Y CIA S.A. que permita garantizar la seguridad de los datos personales preservando su confidencialidad, disponibilidad e integridad a través de sus respectivos controles de seguridad en el tratamiento de los datos personales.

b. Específicos

a) Crear una Metodología para poder implementar la Ley de Protección de Datos Personales en una Empresa textil, considerando Fases y Actividades en su desarrollo.

b) Identificar los bancos de datos personales utilizados por la Empresa MICHELL Y CIA S.A. de conformidad con la Ley N°29733 y su reglamento.

c) Obtener la resolución de inscripción de los Bancos de Datos provista por el Registro Nacional de Datos Personales.

d) Identificar, establecer e implementar medidas de seguridad de información para cada banco de datos personales de acuerdo al nivel de protección correspondiente aplicando la Directiva de Seguridad de Información que está alineado a la NTP ISO/IEC 27001:2008 EDI Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información.

e) Elaborar un procedimiento para el ejercicio de los derechos ARCO.

f) Elaborar procedimientos para recabar los consentimientos de los titulares de los datos personales, y así poder realizar algún tratamiento con sus datos personales.

g) Desarrollar un sistema web que pueda ayudar a la gestión y validación de las solicitudes ARCO, incidencias relacionadas al tratamiento de datos personales y backups que contengan datos personales.

1.1.3 Preguntas de Investigación

1. ¿Existe una metodología que permita implementar eficientemente la Ley de Protección de Datos Personales?
2. ¿Qué es y qué contiene un Banco de Datos?
3. ¿Qué procedimientos y controles se aplica para asegurar el cumplimiento de la Ley de Protección de datos personales?
4. ¿Qué tan efectivos son los procedimientos aplicados a la Ley de Protección de Datos Personales?
5. ¿Cuál es el proceso completo que se debe seguir para obtener la resolución de inscripción de Bancos de Datos en el Ministerio de Justicia?

1.1.4 Línea y Sub-Línea de Investigación

- Línea: Sistemas de Información y Bases de Datos
- Sub-Línea: Seguridad de Información

1.1.5 Palabras Clave

Ley, Datos Personales, Banco de Datos, Metodología, LPDP, Ministerio de Justicia de Arequipa.

1.1.6 Solución Propuesta

a. Justificación e Importancia

Es obligación de toda persona natural, persona jurídica u organización que realiza un tratamiento de datos personales esté sujeta y deba adecuarse a la ley de protección de datos personales. Sin embargo, aún existen muchas de ellas que no cumplen con esta ley por diversos motivos como desconocimiento, no poder llevar a cabo una adecuada implementación, temor al riesgo que puede implicar o simplemente por no adoptar medidas de seguridad dentro de la empresa.

Por tales motivos, la ley conlleva a sanciones por parte de la Autoridad Nacional de Protección de Datos Personales que van desde 0.5 UIT a 100 UIT (Semana Económica, 2015) siendo calificadas por el agravio de los datos vulnerados, intencionalidad del acto, omisión del infractor y la recurrencia.

Es importante que las organizaciones protejan su información confidencial haciendo uso de medidas y controles de seguridad asociados a la Directiva de Seguridad de Información que forma parte de la ley de

protección de datos personales para evitar este tipo de multas que pueden ser provocadas por el propio titular de los datos personales o ante visitas inopinadas que deseen perjudicar a la empresa.

Como consecuencia, se propone una metodología para saber cómo implementar la ley de protección de datos personales, garantizando la adecuación de las medidas de seguridad en una empresa textil a los procedimientos de seguridad establecidos en la Directiva de Seguridad de Información, viéndose beneficiados tanto la empresa como el titular de los datos personales al no exponer su información a terceros evitando un trato inadecuado.

b. Descripción de la Solución

La metodología para implementar la ley de protección de datos personales a una empresa textil, permite identificar de forma rápida sus bancos de datos, elaborar y hacer un seguimiento de sus procedimientos y políticas de seguridad de información, así como obtener los consentimientos por parte de los titulares de los datos personales para poder hacer uso de su información.

La metodología se llevó a cabo a través de la ejecución de cuatro fases descritas a continuación:

Primero se realizó la fase de Planeamiento donde se identificó al titular de los bancos de datos personales, se determinó el alcance de la implementación de la LPDP dentro de la empresa, también se identificó nombres de posibles bancos de datos y las áreas involucradas que implica realizando un cuadro, así mismo se define a los responsables para cada área y se hace una planificación para llevar a cabo las entrevistas. También se realizó un listado de los softwares que administra la empresa para conocer si alguno de ellos manipula o almacena información personal, y finalmente se definió un plan de acción, breve capacitación y la distribución para los recabadores de bancos de datos.

En la segunda fase se elaboró un listado de interrogantes para entrevistar a cada área, a partir de ello se define a los responsables de cada banco de datos personales para luego recopilar un listado de todos los datos personales filtrados por banco de datos identificado e identificar los sistemas impactados (sistemas que involucren datos personales) que existe en la empresa. Finalmente, se estableció un listado de todos los bancos de datos personales previamente evaluados por los recabadores para proceder a registrarlos ante la Dirección Nacional de Protección de Datos Personales.

Luego se elaboró y modificó los procedimientos y políticas de seguridad de la empresa para ser adecuados a la Directiva de Seguridad de la Información.

Finalmente, se debe obtener los consentimientos de los titulares de los datos personales estableciendo diversos mecanismos de obtención, haciendo adecuaciones de materia legal en los contratos y haciendo uso de formatos que me permita obtener el consentimiento.

Terminada la investigación se elaboró un documento denominado "Manual de Procedimientos y Políticas de la LPDP" a la empresa para garantizar el seguimiento del cumplimiento de los procedimientos y políticas de seguridad asociados a la ley de protección de datos personales. Así como también un sistema web que permita validar el cumplimiento de la misma.

1.2 FUNDAMENTOS TEÓRICOS

1.2.1 Estado del arte

Se debe reconocer los riesgos que podría implicar para los derechos fundamentales el creciente uso de la tecnología. Temerosos de ello, desde comienzos de los años setenta, varios países adoptaron leyes sobre protección

de los datos personales para reglamentar el tratamiento automatizado y no automatizado de la información personal y sensible de cualquier persona (Cerda Silva, 2011).

En Europa, se dictó en el año 1995 la directiva 95/46/CEE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. España y Portugal tienen influencia de dos zonas, la Unión Europea y Latinoamérica. En España, la privacidad viene regulada por el artículo 18.4 de la Constitución Española según el cual "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Además, existe una legislación para proteger la privacidad de los ciudadanos, basada en la Ley Orgánica de Protección de Datos Personales. En Portugal la privacidad se sustenta sobre la Ley de Protección de Datos Personales 67/98 del 26 de octubre que se encuentra adaptada a la directiva europea (Sanchez et al., 2011).

En Latinoamérica, también se ha demostrado una inquietud por la privacidad de información personal, reglamentando dicha ley denominándola de diversas maneras. En Argentina, la privacidad viene protegida por la Ley N°25326. En Brasil, es la Ley N°9.507/97 como Habeas Data. En Chile, no existe norma expresa, pero la construcción jurídica de protección de datos personales se basa en el artículo 19 N°4 de la Constitución Política de la República y en la Ley 19 628 "Protección de la vida privada". En Costa Rica, está previsto y en trámite legislativo la "Ley de protección de la persona frente al tratamiento de sus datos personales". En Ecuador, la privacidad se garantiza mediante el artículo 23 y 94 de la constitución de 1998 y el artículo 9 de la Ley de Comercio Electrónico. El Salvador, Nicaragua, Uruguay, Venezuela y Panamá no existen normas específicas para proteger la privacidad, sin embargo, los cuatro primeros garantizan su privacidad mediante los siguientes artículos en su constitución. En el Salvador a través del artículo 2 de la Constitución, en Nicaragua a través de los artículos 5 y 26 de su constitución, en Uruguay a través de los artículos 10,28 y 72 de su constitución de 1967, y en Venezuela mediante los artículos 28,60 y 281 de la constitución de 1999 (Sanchez et al., 2011)

En América del Norte, de igual manera existe preocupación de la privacidad destacando la legislación de USA. En Estados Unidos Mexicanos la privacidad se sustenta en la Ley Federal de Transparencia y Acceso a la Información Pública.

Otros países como Japón, Australia y Malasia han desarrollado leyes específicas que se están modificando para adaptar a los cambios que las mejoras tecnológicas conllevan (Sánchez et al., 2011).

El Perú no ha sido la excepción. La privacidad se garantiza a través de los artículos 2 y 200 de la constitución política de 1993 y también por su Ley N°29733, Ley de Protección de Datos Personales, aprobada en el año 2013 y puesta en vigencia a través del Decreto Supremo N°003-2013-JUS, la cual constituye de 6 Títulos, 131 Artículos, 3 Disposiciones Complementarias Finales y 03 Disposiciones Complementarias Transitorias (Ministerio de Justicia y Derechos Humanos, 2013a).

Según el artículo N°1 del reglamento de la presente ley nos dice que el objetivo es el garantizar el derecho fundamental a la protección de datos personales, regulando un adecuado tratamiento, tanto por las entidades públicas, como por las instituciones pertenecientes al sector privado.

Por lo tanto, el cumplimiento de esta ley es obligatorio para cualquier empresa pública o privada, ya que es importante que conozcan la información personal que gestionan de sus recursos humanos, clientes, proveedores u otros, y los controles de seguridad que deben ser adoptadas.

Sin embargo, muchas veces se cree que el actual marco legal no aborda adecuadamente la privacidad de información personal. Específicamente, que la ley de protección de datos personales no ha seguido el ritmo de la tecnología informática y se concluye que no se protege adecuadamente los intereses de la privacidad de los individuos.

Para cualquier empresa, el implementar la ley de protección de datos personales considera implantar controles de seguridad porque esto supone obtener importantes mejoras como dar a conocer y controlar riesgos a los que puede estar expuesto. Sin embargo, es común que las empresas no cuenten con

un sistema de gestión de la seguridad de la información, o en caso la tuviesen no tengan documentación elaborada del mismo. Aunque la mayoría de las empresas pueden trabajar con las TICS normalmente, es primordial disponer de guías, métricas y herramientas que permitan evaluar la seguridad de la empresa en cualquier momento.

Actualmente, existe una norma internacional emitida por la Organización Internacional de Normalización (ISO). La norma puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización (Vilca, 2015).

Según el Instituto Nacional de Competencia y de la Protección de Propiedad Intelectual (INDECOPI, 2013), "define que la implementación de un Sistema de Gestión de Seguridad de Información (SGSI), permite proteger y reducir los riesgos que puedan afectar a los activos de la empresa. El Sistema de Gestión de Seguridad de Información permite proteger la información asegurando su confidencialidad, integridad y disponibilidad para brindar la confianza a las instituciones, empleados, clientes; permitiendo responder oportunamente a los incidentes que puedan afectar a la empresa"

Por ello, la Autoridad Nacional de Protección de Datos Personales elaboró la Directiva de Seguridad de Información como documento facilitador del cumplimiento de la ley de protección de datos personales, la cual está orientado y adecuado a la ISO 27001, la cual se encarga de implementar un sistema de gestión de seguridad de información.

Esta DSI orienta sobre las condiciones y requisitos que se deben tener en cuenta para el cumplimiento del reglamento de la LPDP y brinda lineamientos para determinar las medidas organizativas, medidas legales y medidas técnicas que debe cumplir la empresa, o como ellos lo denominan, el titular del banco de datos.

El objetivo principal de la DSI es garantizar la seguridad de los datos personales mediante medidas de seguridad que debe adoptar cada banco de datos (Ministerio de Justicia y Derechos Humanos, 2013a).

Actualmente, no todas las empresas se han adecuado al reglamento de la ley, esto se debe a muchos factores como el desconocimiento de la misma, falta de recursos y de tiempo, o muchas veces por no tener ningún tipo de medida de seguridad de información.

Sin embargo, existen algunos manuales que pueden servir de apoyo a las empresas. Tejedor y Pascual (2005) elaboraron un manual documentario de protección de datos de carácter personal dirigido a empresas para un mejor entendimiento del tema el cual busca aportar ciertas soluciones útiles a los empresarios.

También, la Universidad Politécnica de Valencia (2005) en España, elaboró un manual interno de la protección de datos de carácter personal, el cual recoge un resumen de la política, normas, reglas, estándares, procedimientos y otras consideraciones a tener en cuenta en el manejo de los datos de carácter personal contenidos en sus bancos de datos.

Mientras que Sánchez et al. (2011) pusieron gran enfoque en los datos personales de pacientes en hospitales, los cuales son considerados altamente sensibles. De tal forma que desarrollaron un software denominado www.citasalud.es, siendo la primera solución integral de gestión de esperas hospitalarias que permite racionalizar el flujo de los pacientes dentro de los hospitales, a partir del registro de los mismos mediante DNI o tarjeta Sanitaria, cumpliendo debidamente la protección de la información personal.

Así mismo, El “Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes” referido también como Memorándum de Montevideo, contiene una serie de recomendaciones dirigidas a organismos gubernamentales, a legisladores, a jueces, pero también a la sociedad y a la industria de las redes sociales para que en el ámbito de sus respectivas competencias, se comprometan a trabajar a favor de la protección de los menores y de sus datos (Gregorio & Ornelas, 2011).

Cabe recalcar que la Unión Europea adoptó una directiva comunitaria para requerir "un nivel adecuado de protección" por terceros países, a efectos de autorizar la transferencia de datos personales hacia ellos y ha socavado su propósito a cualquier lugar a que ésta exporte datos personales (Cerda Silva, 2011).

Se puede confirmar que el alcance de proteger la información personal es a nivel mundial, por lo que la existencia de manuales y documentación sirve de gran apoyo al momento de implementar esta ley, incluso herramientas que permitan proteger en cierta magnitud la información personal.

Sin embargo, el hecho de conocer los marcos de referencia para salvaguardar la información no asegura que se implemente de forma exitosa. Es por esto que se requiere adicionalmente una metodología que de manera eficaz y eficiente aplique los marcos de referencias.

A raíz de ello, en el año 2014 se elaboró una propuesta metodológica usando la NTP /ISO 27001:2008 en la implementación de un Sistema de Gestión de Seguridad de la Información en una entidad del Estado para mejorar la seguridad de los activos de información y mitigarlos (Suca Ancachi, 2014).

Y en el año 2017 se elaboró un trabajo donde se desarrolló la descripción de servicios informáticos, los procesos de tecnologías de información y las mejoras respectivas basándolas en COBIT 5 y la NTP 27001:2014 (Fernández Vargas & Mayta Aguilar, 2017).

Así mismo, también existen metodologías enfocada en procesos reconocidas internacionalmente que son muy usadas al momento de implantar un sistema de Gestión de Seguridad de Información en una organización, entre estas tenemos al Ciclo de Deming, OCTAVE, MAGERIT Y CRAMM. Estas tres últimas están enfocadas al análisis y gestión de riesgos en sistemas de información.

OCTAVE se centra en el estudio de riesgos organizacionales y se focaliza principalmente en los aspectos relacionados con el día a día de las empresas. La evaluación inicia a partir de la identificación de los activos relacionados con la información, definiendo este concepto como los elementos

de TI que representan valor para la empresa (sistemas de información, software, archivos físicos o magnéticos, personas, entre otros). De esta forma, OCTAVE estudia la infraestructura de información y, más importante aún, la manera como dicha infraestructura se usa en el día a día (Gómez, Pérez, Donoso, & Herrera, 2010).

MAGERIT es una metodología española para la gestión y análisis de riesgos de los sistemas de la información que en sus tres libros "Método", "Catalogo de elementos" y "Guía de técnicas" sirve como fuente de revisión de definiciones y lo correspondiente a la estimación de riesgos (Ramírez & Ortiz, 2011).

CRAMM puede definirse como una metodología para el análisis y gestión de riesgos, orientado a proteger la confidencialidad, integridad y disponibilidad de un sistema y sus activos. Conformado por tres etapas: Identificación y valoración de activos, evaluación de amenazas y vulnerabilidades y finalmente con la selección y recomendación de contramedidas (Cordero Torres, 2015).

Sin embargo, hasta el momento no existe ninguna metodología que me indique paso a paso las actividades que deben ser ejecutadas para implementar la ley de protección de datos personales y su normativa, además incluyendo las medidas de seguridad adecuadas que serán adoptadas por cada banco de datos personales.

1.3 MARCO METODOLÓGICO

1.3.1 Bases Teóricas de la Investigación

Para la presente investigación los conceptos previos a conocer fueron los siguientes.

Un banco de datos está compuesto por todo tipo de información aportada por las mismas personas para determinados objetivos (Ministerio de Justicia, 2014).

Datos personales es toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados (Ministerio de Justicia y Derechos Humanos, 2011a) y un banco de datos personales es el conjunto organizado de éstos, automatizados o no, independiente de su medio de almacenamiento.

Se conoce como titular de datos personales a la persona a quien corresponde la información y como titular de banco de datos personales a la persona que determina la finalidad y el tratamiento de los datos personales y las medidas de seguridad que se deben adoptar. (Ministerio de Justicia y Derechos Humanos, 2011a).

También es importante conocer los principios rectores los cuales han sido considerados en los procesos de tratamiento de datos personales por parte de titulares y responsables de los bancos de datos. Entre estos principios tenemos al (a) principio de legalidad, (b) principio de consentimiento, (c) principio de finalidad, (d) principio de proporcionalidad, (e) principio de calidad, (f) principio de seguridad, (g) principio de disposición de recurso, y el (h) principio de nivel de protección adecuado (Ministerio de Justicia y Derechos Humanos, 2011a).

Así como también comprender los derechos que toda persona tiene y la potestad de controlar la información personal que comparte con terceros. Estos derechos son (a) el derecho de información, (b) de acceso, (c) de actualización, (d) a impedir el suministro, (e) de oposición, (f) al tratamiento objetivo, (g) a la tutela, (h) a ser indemnizado, (i) contraprestación, y (j) limitaciones (Ministerio de Justicia y Derechos Humanos, 2013b).

Sin embargo, también existen los derechos ARCO donde sus siglas corresponden a (a) el derecho al acceso, (b) a la rectificación, (c) a la cancelación, y (d) a la oposición (Ministerio de Justicia y Derechos Humanos, 2013b). Los derechos ARCO fueron indispensables para la obtención de los consentimientos y para atender posibles reclamos de titulares de datos personales.

Cada dato personal que está contenido o destinado a ser contenido en un banco de datos personal debe estar protegido ante cualquier uso indebido en conformidad a la ley de protección de datos personales, esto se logra a través de la Directiva de Seguridad de Información que complementa dicha ley, la cual nos brinda medidas de seguridad organizativas, legales y técnicas que debe adoptar cada banco de datos (Autoridad Nacional de Protección de Datos Personales APDP, 2013).

Cada uno de estos conceptos fueron fundamentales al implementar la metodología debido a que su finalidad es proteger los datos personales y eso se logró adecuando los procedimientos y políticas de la empresa a la ley de protección de datos personales a través de la Directiva de Seguridad de Información; así mismo los derechos del titular del dato personal fueron establecidos a través de los procedimientos de la obtención del consentimiento del mismo.

1.3.2 Alcances y Limitaciones

a) Alcances.

La investigación tiene como alcance proponer una metodología para implementar la ley de protección de datos personales en una empresa del sector textil en nuestro caso: Michell & CIA S.A.

La metodología considera la identificación de todos los bancos de datos hasta la adecuación de procedimientos y políticas de seguridad de la información de la empresa textil con la ley de protección de datos personales.

El desarrollo de la metodología considerará fases, actividades y entregables y además se desarrollará una herramienta de software que permita el control y la gestión de la seguridad y protección de datos personales.

b) Limitaciones.

La metodología propuesta no aplicará a otros países sin la debida adecuación a sus regulaciones y requerimientos.

1.3.3 Aporte

1. Las empresas textiles podrán cumplir de forma efectiva la ley de protección de datos personales evitando posibles rechazos en la inscripción de los bancos de datos ante la Autoridad Nacional de Datos Personales.

2. Las empresas textiles podrán adoptar un nivel de seguridad de información adecuado para sus bancos de datos personales.
3. La gestión de la seguridad de la información mejorará a través de los procedimientos y políticas ajustados a la Directiva de Seguridad de Información que forma parte de la LPDP.
4. Controlar efectivamente y reducir el pago de multas establecidas por la Autoridad Nacional de Datos Personales.
5. Desarrollar un sistema web basado en la normativa de la LPDP que permita automatizar, registrar y validar los procesos de control de la información personal.
6. Brindar una nueva metodología de implementación de la LPDP para todo tipo de empresa con algunas mínimas modificaciones según sea su rubro.

1.3.4 Tipo y Nivel de Investigación

El tipo es una investigación aplicada, ya que los resultados obtenidos a partir de ella pretenden aplicarse o utilizarse en forma inmediata para resolver alguna situación problemática en la empresa. El nivel, es aplicativa, porque con la metodología propuesta se busca solucionar problemas y reconstruir procesos en base a descubrimientos ya realizados.

1.3.5 Población y Muestra Metodológica

Para este trabajo se tomará un método de muestreo no probabilístico, el muestreo por cuotas. En este método los investigadores pueden formar una muestra que involucre a individuos que representan a una población y que son seleccionados tomando como referencia ciertas características o cualidades.

Para este caso el marco poblacional sujeto al estudio son todos los trabajadores administrativos de la empresa.

Al dividir a toda la población en subgrupos se tomará en cuenta las siguientes características: (a) participación en el comité de ley de protección de datos personales, (b) nivel de responsabilidad en su área, (c) alto nivel de tratamiento físico de datos personales, y (d) alto nivel de tratamiento lógico de datos personales.

En este caso, el marco poblacional abarca las siguientes instancias (a) área de recursos humanos, (b) el área legal, (c) área de ventas, (d) área de exportaciones e importaciones, (e) área de tecnologías de información, (f) área de vigilancia, (g) área de logística, (h) área de negocios electrónicos, (i) área de finanzas, (j) área de contabilidad, y (e) caja.

Y la muestra se determinó dividiendo la población descrita en grupos en base a las siguientes variables clave:

1. Participación en el Comité de Ley de Protección de Datos Personales.

2. Nivel de responsabilidad del área.

3. Alto nivel de tratamiento físico de datos personales.

4. Alto nivel de tratamiento lógico de datos personales.

1.3.6 Métodos, Técnicas e Instrumentos empleados

Para la implantación de la metodología se llevaron a cabo los siguientes métodos y técnicas:

Entrevista

Es una técnica de recopilación de información, en una reunión formal, con la que obtendremos información acerca de los procesos que incluyan datos personales, el objetivo de la entrevista es encontrar lo que es importante y significativo para los informantes, su propósito es obtener descripciones del

marco de trabajo del entrevistado para su posterior análisis y posterior mejora en la creación de nuevos procesos que cumplan con la Ley de protección de Datos Personales.

Encuesta

Técnica de adquisición de información mediante un cuestionario, a través de la cual se puede conocer la opinión de los entrevistados acerca del conocimiento que tienen y cuanto ha mejorado el uso de la información con los nuevos procedimientos.

También permite obtener y elaborar datos de modo rápido y eficaz, y se puede definir como una técnica que utiliza un conjunto de procedimientos estandarizados de investigación mediante los cuales se recoge o se analiza una serie de datos de una muestra de casos representativa de una población o universo más amplio del que se pretende explorar, describir, predecir y/o explicar una serie de características (Rodríguez et al., 2016).

Análisis Documental

Obtenemos datos e información de fuentes secundarias como el material informativo en la página web del Ministerio de Justicia (https://www.minjus.gob.pe/material-informativo-dp/), así como también en la página del congreso de la republica (http://www.pcm.gob.pe/transparencia/Resol_ministeriales/2011/ley-29733.pdf).

Y como herramienta principal se utilizó la Directiva de Seguridad que proporciona la Autoridad Nacional de Datos Personales, en donde se respeta los ocho principios rectores señalados en la Ley N°29733, Ley de Protección de Datos Personales, los cuales son: (a) legalidad, (b) consentimiento, (c) finalidad, (d) proporcionalidad, (e) seguridad, (f) calidad, (g) disposición de recurso y (h) nivel de protección adecuado.

CAPITULO II

2. MARCO TEÓRICO

En este capítulo se verá el marco teórico. El marco teórico fundamenta la presente investigación proporcionando al lector un mejor entendimiento del tema.

Así mismo se encontrarán los principales conceptos que refieren a la seguridad de la información y a la ley de protección de datos personales.

2.1 CONCEPTOS RELACIONADOS A LA SEGURIDAD DE LA INFORMACION

2.1.1 Dato

Según la Real Academia Española la palabra “dato” tiene 2 conceptos fundamentales:

- Es el antecedente necesario para llegar al conocimiento exacto de algo o para deducir las consecuencias legítimas de un hecho.
- Es un documento, testimonio, fundamento.

2.1.2 Información

Es el conjunto de datos procesados y que tienen un significado (relevancia, propósito y contexto), y que por lo tanto son de utilidad para quién debe tomar decisiones, al disminuir su incertidumbre. Los datos se pueden transforman en información añadiéndoles valor:

- Contextualizando: se sabe en qué contexto y para qué propósito se generaron.
- Categorizando: se conocen las unidades de medida que ayudan a interpretarlos.

- Calculando: los datos pueden haber sido procesados matemática o estadísticamente.
- Corrigiendo: se han eliminado errores e inconsistencias de los datos.
- Condensando: los datos se han podido resumir de forma más concisa (agregación).

Por tanto, la información es la comunicación de conocimientos o inteligencia, y es capaz de cambiar la forma en que el receptor percibe algo, impactando sobre sus juicios de valor y sus comportamientos (Carrión., 2016).

2.1.3 Seguridad De La Información

Es la preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad (Comite Tecnico de Normalizacion de Codificacion e Intercambio Electronico de Datos, 2007).

2.1.4 Evento de seguridad de la información

Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las contingencias, o una situación desconocida previamente que puede ser relacionado con la seguridad (Report, 2008).

2.1.5 Gestión De La Seguridad De La Información (ISO 27001)

La Organización Internacional de Estandarización (ISO) y la Comisión Internacional de Electrotecnia (IEC) formaron el sistema especializado de estándares internacionales. La ISO 27001 es el estándar internacional que especifica la gestión de la seguridad de la información.

El objetivo del estándar ISO 27001 es definir los requerimientos para establecer, implementar, mantener y contantemente mejorar el sistema de seguridad de la información (ISOTools Excellence, 2003). Algunos factores que pueden influir esta gestión sol las necesidades y objetivos, procesos, tamaño y estructura de la organización. Todas las partes tanto internas como externas pueden usar el estándar ISO 27001 para evaluar el desempeño de satisfacción de la empresa con su propia información.

2.1.6 Lineamiento

Una descripción que aclara que se debiera hacer y cómo, para lograr los objetivos establecidos en las políticas (Provided, No, & Licensee, 2013).

2.1.7 Disponibilidad

Es la propiedad de estar disponible cuando lo requiera una entidad autorizada. La información debe encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Es también el acceso a la información por personas autorizadas cuando lo requieran, evitando interrupciones debido a cualquier imprevisto, esto implica también prevención de ataque de denegación de servicio (NTC 5411-1:2006).

2.1.8 Confidencialidad

Es la propiedad de que la información no sea divulgada a personas, entidades o procesos no autorizados.

Es el acceso a la información únicamente por personas que cuentan con la debida autorización (NTC 5411-1:2006).

2.1.9 Integridad

Propiedad de salvaguardar por la exactitud y completitud de los activos. Busca mantener la información libre de alteraciones sin autorización, de tal manera que se mantenga intacta como fue generada, sin ser manipulada ni modificada por personas o procesos no autorizados (NTC 5411-1:2006).

2.1.10 Organización Interna

El objetivo de la organización interna es gestionar la seguridad de la información sin el apoyo de la estructura administrativa. La gestión debe asegurar la seguridad incluyendo la clara dirección de la organización, el compromiso, tareas específicas y el desempeño de coordinación en cuanto a seguridad de la información (Universidad de Miami 2006).

2.1.11 Activo

Cualquier cosa que tenga valor para la organización (ISO 13335-1:2004).

2.1.12 Amenaza

Una causa potencial de un incidente no deseado el cual puede resultar dañino para un sistema u organización (ISO 13335-1:2004).

2.1.13 Vulnerabilidad

La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas. (ISO/IEC 13335-1:2004).

2.1.14 Riesgo

Probabilidad de que una amenaza explote una vulnerabilidad del activo impactando adversamente en la empresa.

Combinación de consecuencias de un evento determinado y la probabilidad de ocurrencia asociada (ISO/IEC Guía 73:2002).

2.1.15 Control de riesgo

Medios para gestionar el riesgo, incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal (ISO/IEC Guía 73:2002).

Las responsabilidades de seguridad de la información deben ser bien definidas y claras de acuerdo a las políticas establecidas.

2.1.16 Impacto

Cambio adverso en el nivel de los objetivos del negocio logrados (ISO/IEC Guía 73:2002).

2.1.17 Partes Externas

El objetivo de las partes externas es mantener la seguridad de la información en la organización y dar las facilidades de gestión y acceso (ISO/IEC 1799 2005, 14).

2.1.18 Estimación Cualitativa de Riesgos

Incluye diferentes escenarios de posibilidad de riesgo, evaluación de impacto y la efectividad de probables soluciones y contingencias (Harris 2003, 72.). Este análisis contiene el juicio, la intuición y la experiencia. Por ejemplo: Técnica de Delphi, lluvia de ideas, reuniones, encuestas, cuestionarios, listas de verificación, entrevistas (Steward – Chapple – Gibson 2012). Los equipos de análisis de riesgo analizarán el estado de la empresa y decidirán la mejor técnica para manejar cada caso.

2.1.19 Estimación Cuantitativa de Riesgos

El análisis cuantitativo usa números reales y significativos en todos los elementos del proceso de análisis de riegos. Los elementos incluyen costos de garantía, el impacto, el valor de los activos, la frecuencia de casos, las probabilidades, etc. Este análisis provee porcentajes específicos de casos y riesgos. Para determinar el total de riesgos, cada elemento debe ser contabilizado (Sosa, 2012).

2.2 CONCEPTOS RELACIONADOS A LA LEY DE PROTECCIÓN DE DATOS PERSONALES

2.2.1 Dato Personal

Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados (Ministerio de Justicia y Derechos Humanos, 2011a).

2.2.2 Dato Sensible

Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual (Ministerio de Justicia y Derechos Humanos, 2011a).

2.2.3 Titular de los datos personales

La persona natural o jurídica a la que se refiere la información (Ministerio de Justicia y Derechos Humanos, 2011a).

2.2.4 Banco De Datos

Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso (Ministerio de Justicia y Derechos Humanos, 2011a).

2.2.5 Ley De Protección De Datos Personales (LPDP)

En el año 2011 sale por primera vez la LPDP en nuestro país. Para el año 2013 aprueban su reglamento a través del DECRETO SUPREMO Nº 003-2013-JUS, obligando a someterse a ella tanto las entidades públicas como privadas.

Esta ley que consta de un título preliminar con disposiciones generales, 7 títulos, 40 artículos y 11 disposiciones complementarias finales, tiene como objetivo principal garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen (Ministerio de Justicia y Derechos Humanos, 2011a).

Su fiscalización está a cargo de la Dirección General de Protección de Datos Personales**,** quien cumple funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadora, y sancionadora.

Entonces, las entidades públicas y privadas tienen la obligación de garantizar la protección de los datos personales que contienen, para evitar acceso y uso inadecuado por parte de terceros no autorizados.

2.2.6 Autoridad Nacional de datos personales (APDP)

Nace con la dación de la ley de protección de datos personales, a través del ministerio de justicia que dispuso que le corresponda realizar todas las acciones necesarias para velar por el cumplimiento de la legislación vinculada con la protección de datos personales y por el respeto de sus principios rectores (Ministerio de Justicia y Derechos Humanos, 2014).

2.2.7 Registro Nacional de Bancos Personales

Unidad de almacenamiento a cargo de la autoridad nacional de datos personales, se encarga de inscribir los bancos de datos personales de administración pública o privada, además da publicidad de la existencia de banco de datos personales, sus finalidades y la identidad y domicilio de sus titulares (Ministerio de Justicia y Derechos Humanos, 2014).

2.2.8 La Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales

La Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, garantizan el derecho fundamental de acceso a la información pública y el derecho a la protección de datos personales, velando por el cumplimiento de las normas sobre la materia. Ejerce funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras (Ministerio de Justicia y Derechos Humanos, 2019).

Figura 1 La Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales

Fuente: Ministerio de Justicia

La Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales cuenta con las siguientes unidades orgánicas:

a. Dirección de Transparencia y Acceso a la Información Pública

La Dirección de Transparencia y Acceso a la Información Pública es la unidad orgánica que fomenta la cultura de la transparencia y acceso a la información pública a través de recomendaciones y capacitaciones, supervisa el cumplimiento de las normas, directivas y lineamientos en materia de transparencia y acceso a la información pública. Así como también emite opiniones técnicas sobre la materia. Depende jerárquicamente de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (Ministerio de Justicia y Derechos Humanos, 2019).

b. Dirección de Protección de Datos Personales

La Dirección de Protección de Datos Personales es la unidad orgánica que resuelve en primera instancia los procedimientos sancionadores sobre protección de datos personales, resuelve en primera instancia los procedimientos trilaterales de tutela, administra el Registro Nacional de Protección de Datos Personales. Depende jerárquicamente de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (Ministerio de Justicia y Derechos Humanos, 2019).

c. Dirección de Fiscalización e Instrucción

La Dirección de Fiscalización e Instrucción es la unidad orgánica responsable de fiscalizar el cumplimiento de las obligaciones y prohibiciones establecidas en la Ley de Protección de Datos Personales y su Reglamento, así como de iniciar los procedimientos sancionadores por infracción a las disposiciones sobre Protección de Datos Personales e instruir el procedimiento sancionador. Depende jerárquicamente de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (Ministerio de Justicia y Derechos Humanos, 2019).

2.2.5 Directiva de Seguridad de Protección de Datos Personales

Orienta sobre las condiciones, los requisitos y las medidas técnicas que se deben tomar en cuenta para el cumplimiento de la ley de protección de datos personales y su reglamento.

Las condiciones muestran recomendaciones que generan impacto favorable para la implementación de requisitos, habilitando un entorno apropiado para los procesos relacionados.

Los requisitos se basan en condiciones que deben de ser demostrables, para considerar que se ha cumplido con la directiva.

Se basa en tipo de tratamiento en las cuales se les asigna un color en la siguiente imagen:

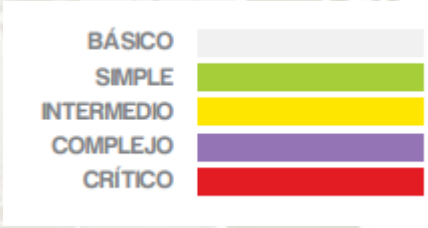


Figura 2 Categorización de los Bancos de Datos Personales

Fuente: Ministerio de Justicia

2.2.6 Derecho Fundamental a la Protección de Datos Personales

Es el derecho que toda persona tiene a controlar la información personal que comparte con terceros, así como el derecho a que esta utilice de forma apropiada, de tal forma que no la perjudique (Ministerio de Justicia y Derechos Humanos, 2013b).

2.2.7 Responsable de seguridad

Rol asignado a una persona que coordina y controla la implementación de las medidas se seguridad en un banco de datos personales (Autoridad Nacional de Protección de Datos Personales APDP, 2013).

2.2.8 Usuarios de sistemas de información

Persona natural que tiene acceso a un sistema de información que realiza tratamiento de datos personales. Pueden ser administradores de sistemas, administradores de banco de datos, personal de soporte o titulares de banco de datos personales (Autoridad Nacional de Protección de Datos Personales APDP, 2013).

2.2.9 Derechos ARCO

Nace con la ley de protección de datos personales, permite que las personas puedan controlar su información personal, para ello, la LPDP prevé derechos que permite a las personas exigir que sus datos personales sean tratados adecuadamente. Estos derechos son: Acceso, Rectificación, Cancelación y Oposición (Ministerio de Justicia y Derechos Humanos, 2013b).

2.2.10 Derecho de Acceso

Se refiere al derecho que toda persona tiene a obtener la información que sobre sí mismo sea objeto de tratamiento en bancos de datos de administración pública o privada, la forma en la que fueron obtenidos, las razones que motivaron su obtención y a solicitud de quien se realizó su recopilación, así como las trasferencias que se realizaron o que se piensa hacer con ellos en el futuro. (Ministerio de Justicia y Derechos Humanos, 2013b).

2.2.11 Derecho de Rectificación

Es el derecho del titular de los datos a que se modifiquen o rectifiquen los datos que resulten ser parcial o totalmente inexactos, incompletos, erróneos o falsos (Ministerio de Justicia y Derechos Humanos, 2013b).

2.2.12 Derecho de Cancelación

El titular de los datos podrá solicitar la cancelación de sus datos cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la que hayan sido obtenidos; hubiere vencido el plazo establecido para su tratamiento; sea revocado su consentimiento y en los que no están siendo tratados conforme a la ley (Ministerio de Justicia y Derechos Humanos, 2013b).

2.2.13 Derecho de Oposición

Es el derecho que permite que toda persona tiene la posibilidad de oponerse por un motivo legítimo y fundado, referido a una situación concreta, a estar registrado en un banco de datos o al tratamiento de su información, siempre que una ley disponga lo contrario (Ministerio de Justicia y Derechos Humanos, 2013b).

CAPITULO III

3. METODOLOGÍA DE IMPLEMENTACIÓN DE LA LPDP

3.1 DESCRIPCIÓN DE LA METODOLOGÍA

La presente metodología está conformada por cuatro fases que abarca desde la identificación de los bancos de datos personales, su correspondiente inscripción al RNPDP a través del portal del ministerio de justicia, asegurando un nivel adecuado de seguridad del banco de datos para finalmente culminar con la obtención de los consentimientos de los titulares.

Figura 3 Metodología de Implementación de LPDP

Fuente: Elaboración Propia

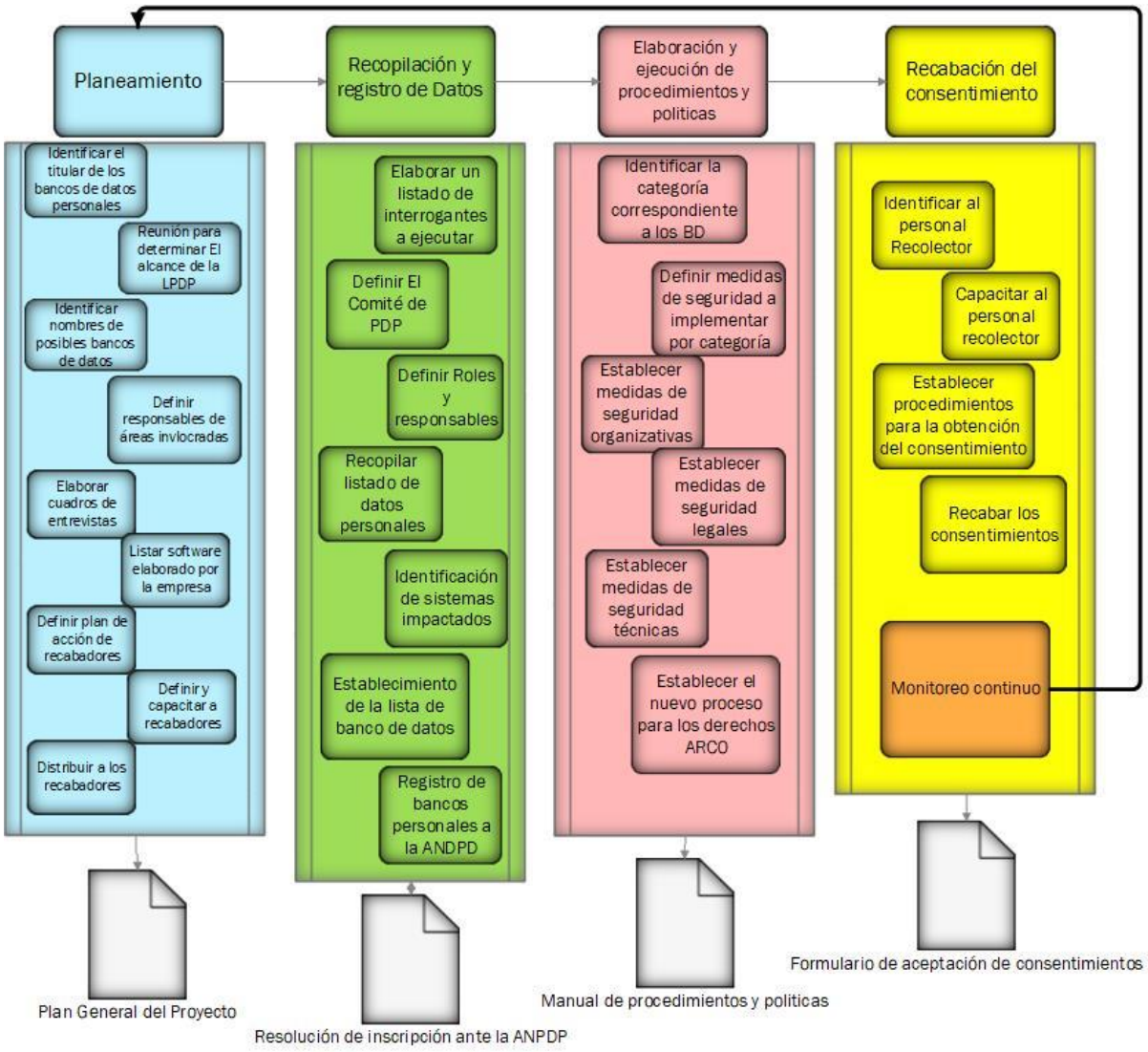


Figura 4 Metodología detallada de la LPDP

Fuente: Elaboración Propia

3.2 FASES DE LA METODOLOGÍA

3.2.1 Planeamiento

En la fase de planeamiento se describe todos los lineamientos para la implementación de la LPDP, es decir, aclara lo que se debe hacer y cómo hacerlas para garantizar el objetivo de la metodología. Además, en esta fase de

define el alcance de la implementación de la LPDP y el plan de acción para los recabadores de bancos de datos.

3.2.2 Recopilación y Registro

La fase de Recopilación y Registro tiene como principal objetivo la inscripción de los bancos de datos personales ante el RNPDP. Para esto se ejecutó una serie de pasos para cumplir dicho objetivo.

3.2.3 Elaboración y Ejecución

La siguiente fase nos permite adecuar los procedimientos y políticas de seguridad actuales de la empresa a lo reglamentado en la LPDP. Incluyendo el procedimiento y modelo de formato de los derechos ARCO.

3.2.4 Obtención del Consentimiento

Finalmente, se identifica y capacita al personal recolector de los consentimientos de los titulares de los datos personales, y se establecen mecanismos de obtención de los mismos.

3.3 APLICACIÓN DE LA METODOLOGÍA

Tabla 1 *Planeamiento*

Identificación del titular de los Bancos de Datos Personales	Gerente de TI, Recolector 1, Recolector 2.
Llevar a cabo reunión para determinar el alcance de la LPDP	Gerente de TI.
Identificar nombres de posibles bancos de datos y las áreas involucradas	Recolector 1, Recolector 2.
Definir a los responsables de cada área involucrada	Gerente de TI, Jefe de Proyectos de TI.
Elaborar un cuadro de planificación de entrevistas a cada área involucrada	Jefe de Proyectos de TI, Recolector 1, Recolector 2.
Listar los softwares administrados por la empresa	Recolector 1, Recolector 2.
Definir plan de acción de Recabadores de bancos de datos	Recolector 1, Recolector 2.
Definir y Capacitar a los Recabadores de bancos de datos	Gerente de TI, Jefe de Proyectos de TI.
Distribución de recabadores de bancos de datos	Jefe de Proyectos de TI.

Fuente: Elaboración Propia

3.3.1 Planeamiento

a. Identificación del titular de los Bancos de Datos Personales

El primer paso a realizar es el identificar al titular de los bancos de datos personales a inscribir ante el RNPDP a través de la página web del ministerio de justicia.

El titular es aquella entidad pública, persona jurídica o natural que realiza un tratamiento de datos personales, también es responsable de determinar la finalidad de sus bancos de datos, sus datos personales contenidos en éstos, su tratamiento y las medidas de seguridad a adoptar.

Para identificar al titular nos hicimos las siguientes preguntas:

- ¿La empresa textil es una entidad pública, persona jurídica o persona natural?

Es identificada como persona jurídica al ser una empresa privada.

- Como persona jurídica. ¿Realiza algún tratamiento de datos personales?
  Si realiza tratamiento de datos personales.

Al realizar tratamiento de datos personales está sujeta a la LPDP y se estableció a la empresa textil Michell y Cía. S.A. como titular de los bancos de datos personales.

b. Llevar a cabo reunión para determinar el alcance de la LPDP

Una vez identificado al titular de los bancos de datos, se determina el alcance de la implementación de la LPDP dentro de la entidad.

Par ello se llevó a cabo una reunión donde intervinieron el Gerente Administrativo, el Gerente de Tecnologías de las Información y el Jefe de Proyectos de Tecnologías de Información; en el cual nos brindaron información general de la empresa, dándonos a conocer que está compuesto por las siguientes compañías:

- Mundo Alpaca
- Sol Alpaca
- Michell (Tops e Hilados)
- Mallkini
- Mfh Knits
- Michell Carpets

Finalmente, se acordó únicamente abarcar dentro de la entidad a Sol Alpaca, Mundo Alpaca y Michell (Tops e Hilados) excluyendo a MFH Knits y Michell Carpets porque forman parte de otra empresa.

c. Identificar nombres de posibles bancos de datos y las áreas involucradas

Los nombres adecuados para los posibles bancos a identificar son:

- Colaboradores
- Postulantes
- Clientes
- Proveedores
- Video vigilancia
- Marketing y Publicidad

d. Definir a los responsables de cada área involucrada

Como responsable de cada área se propuso a aquella persona que conozca en su totalidad o en gran mayoría el proceso y procedimientos de su área de trabajo.

Tabla 2 *Responsable de cada Área Involucrada*

Área	Responsable
Recursos Humanos	Jefe de Recursos Humanos
Medicina Ocupacional	Médico Ocupacional
Comercial	Secretaria de Gerencia Comercial
Negocios Electrónicos	Jefa de Negocios Electrónicos
Exportaciones e Importaciones	Jefa de Exportaciones e Importaciones
Logística – Sol Alpaca	Jefe de Logística – Sol Alpaca
Logística Nacional	Jefe de Logística
Finanzas	Asistente de Finanzas
Caja	Asistente de Caja
Contabilidad	Jefe de Contabilidad
Vigilancia	Jefe de Vigilancia
Bienestar Social	Jefa de Bienestar Social

Fuente: Elaboración Propia

e. Elaborar un cuadro de planificación de entrevistas a cada área involucrada

Una vez que se haya definido a los responsables de cada área se realiza un cuadro de planificación de las entrevistas indicando la fecha, área involucrada y su responsable (encargado de atender la entrevista).

f. Listar los softwares administrados por la empresa

Los softwares administrados por la empresa son los siguientes:

- Sistema ERP de Michell
- SQL Oracle Developer
- Office 365
- Navegadores (Chrome, Firefox y IE 11)

g. Definir plan de acción de Recabadores de bancos de datos

Se desarrolló un plan de acción para llevar a cabo las entrevistas. Las acciones a llevar cabo se detallan a continuación.

1. Realizar una breve presentación del contenido y objetivo de la LPDP, además señalando la importancia de su implementación dentro de la empresa.
2. Explicar y diferenciar los datos personales y sensibles.
3. Identificar el o los bancos de datos personales que se manipula en cada área involucrada.
4. Realizar una serie de interrogantes.
5. Identificar los datos personales que manipula para luego ser contenidos en los bancos de datos personales ya identificados.
6. Completar el formulario de inscripción de una persona jurídica proporcionado por el Ministerio de Justicia a través de su página web.

h. Definir y Capacitar a los Recabadores de bancos de datos

Para este punto, los recabadores deben ser personas que tengan conocimiento suficiente de lo que trata la (a) ley de protección de datos personales,

(b) su alcance y sus limitaciones y (c) sus principios rectores. También, algunos otros conceptos como: (a) banco de datos, (b) datos personales y (c) datos sensibles.

En este caso nosotros fuimos los recabadores, encargados de implementar la LPDP dentro de la empresa.

i. Distribución de recabadores de bancos de datos

Los recabadores fueron distribuidos con la finalidad de abarcar todas las áreas de la empresa para extraer información de los bancos de datos a inscribir y de sus datos personales contenidos.

3.3.2 Recopilación y Registro de bancos

Tabla 3 *Recopilación y Registro de Datos*

Elaborar un listado de interrogantes ejecutadas en cada entrevista.	Recolector 1, Recolector 2.
Definir un Comité de Protección de Datos Personales	Gerente de TI, Jefe de Proyectos TI, Recolector 1, Recolector 2.
Definir roles y responsabilidades del Comité de Protección de Datos Personales	Gerente de TI, Jefe de Proyectos TI, Recolector 1, Recolector 2.
Recopilar un listado de los datos personales por banco de datos.	Jefe de Proyectos TI, Recolector 1, Recolector 2.
Identificación de los sistemas impactados.	Jefe de Proyectos TI, Recolector 1, Recolector 2.
Establecimiento de la lista de bancos de datos personales.	Asesor Legal, Gerente de TI, Jefe de Proyectos TI, Recolector 1, Recolector 2.
Registro de los bancos de datos personales ante la Dirección Nacional de Protección de Datos.	Asesor Legal, Gerente de TI.

Fuente: Elaboración Propia

a. Ejecución de entrevista a responsable de cada área

Luego de identificar las áreas involucradas y sus responsables, se inició a ejecutar las entrevistas a cada uno de ellos.

Para su ejecución se elaboró una serie de interrogantes claves que nos permitieron recopilar gran cantidad de información requerida para la inscripción de los bancos de datos personales de la empresa.

Las interrogantes formuladas fueron las siguientes:

- ¿Cuál es su puesto en la empresa?
- ¿Qué procesos realiza y cuáles son sus funciones? Respuesta detallada.
- ¿Qué tipo y cuáles son los datos personales que gestiona?
- ¿Qué métodos y herramientas usa para la obtención de los datos personales?
- ¿Cómo y dónde almacenan los datos personales?
- ¿Cuál es la finalidad de la manipulación de los datos personales?
- ¿Realizan transferencia de datos personales, sea nacional o internacional? ¿Por qué? Y ¿Cuál es el destino?
- ¿Qué medidas de seguridad física tienen implementado?
- ¿Qué medidas de seguridad lógica tienen implementado? (Sólo área de TI).
- ¿Cuentan con algún documento de seguridad de información? (Sólo área de TI).

En base a estas interrogantes realizadas a cada representante obtenemos la situación actual de la empresa respecto a las medidas de seguridad de información que gestionan e información requerida de los bancos de datos personales identificados para implementar la LPDP dentro de la empresa.

b. Definir un Comité de Protección de Datos Personales

Luego de entrevistar a los responsables de cada área se debe definir un comité en el cual serán partícipes:

1. Los recolectores de información.

- Practicantes de Tecnologías de Información con conocimientos en la Ley 29733, Ley de Protección de Datos Personales.

2. Los responsables para cada banco de datos personales encontrado.

Tabla 4 *Responsable de seguridad de cada Banco de Datos*

Banco de Datos	Puesto
Colaboradores	Jefe de División de Personal y Recursos Humanos
Postulantes	Jefe de División de Personal y Recursos Humanos
Clientes	Gerente Comercial
Visitantes	Gerente Administrativo
Video Vigilancia – Sol Alpaca	Dirección Sol Alpaca
Video Vigilancia – Plantas	Gerente Administrativo
Proveedores	Jefe de Logística

Fuente: Elaboración Propia

3. El encargado del ejercicio de los Derechos ARCO.
   - Jefe de Proyectos de Tecnologías de Información

c. Definir roles y responsabilidades del Comité de Protección de Datos Personales

1. Los recolectores de información.

Tabla 5 *Roles y Responsabilidades del recolector de información*

ROLES Y RESPONSABILIDADES DEL RECOLECTOR DE INFORMACION	
1	Ser responsable de elaborar el listado de interrogantes para llevar a cabo las entrevistas.
2	Ser responsable de llevar a cabo las entrevistas a cada responsable de área para obtener información de cada proceso.
3	Ser responsable de identificar los procesos clave en donde deben implementarse medidas de seguridad relacionadas a la LPDP.
4	Ser responsable de identificar claramente los bancos de datos personales que pudieran existir en la empresa.
5	Ser responsable de capacitar al personal necesario sobre la seguridad de información y la LPDP.

Fuente: Elaboración Propia

2. Los responsables para cada banco de datos personales encontrado.

Tabla 6 *Roles y Responsabilidades del Responsable de Seguridad del Banco de Datos*

ROLES Y RESPONSABILIDADES DEL RESPONSABLE DE SEGURIDAD DEL BANCO DE DATOS PERSONALES	
1	Ser responsable de garantizar y hacer cumplir las medidas de seguridad tanto físicas como lógicas para la protección de los datos personales contenidos en el Banco de Datos Personales a su cargo.
2	Ser responsable del contenido del banco de datos personales bajo su cargo.
3	Ser responsable por el tratamiento adecuado de la información de datos personales, según y únicamente para la finalidad determinada para el Banco de Datos Personales a su cargo.
4	Ser responsable de analizar y establecer posibles acciones a tomar ante el ejerció de los derechos del titular de datos personales (Derecho de Acceso, Rectificación, Cancelación y oposición), coordinando dichas acciones con Seguridad de la Información y Legal, garantizando así el cumplimiento de los derechos del titular de datos personales.
5	Ser responsable de revisar periódicamente que los privilegios de acceso a los datos personales correspondan al personal autorizado, esta revisión debe generar un registro de revisión que lo evidencie, por lo menos de manera anual.
6	Ser responsable de autorizar el acceso y tratamiento de datos personales contenidos en la información a su cargo o la transferencia de estos, tanto de manera interna como externa.
7	Ser responsable de autorizar la recuperación de información que contenga datos personales desde sus copias de respaldo.
8	Ser responsable de definir y designar los roles necesarios al personal que considere para la protección de la información que contenga datos personales.

Fuente: Elaboración Propia

Nota: Es importante mencionar que en caso no hubiera un responsable de seguridad definido, se entiende que este rol recae sobre el titular del banco de datos personales.

3. El encargado del ejercicio de los Derechos ARCO.

Tabla 7 *Roles y Responsabilidades del Encargado del Ejercicio de Derechos ARCO*

ROLES Y RESPONSABILIDADES DEL ENCARGADO DE LOS DERECHOS ARCO	
1	Ser responsable de recibir y recepcionar las solicitudes del ejercicio de los derechos ARCO.
2	Ser responsable de comunicar oportunamente las solicitudes al responsable de seguridad de los bancos de datos personales.
3	Ser responsable de responder los correos notificados por la Autoridad Nacional de Protección de Datos personales.

Fuente: Elaboración Propia

d. Recopilar un listado de los datos personales por banco de datos

En cada área que se entrevistó se identificó los bancos de datos que manipula y los datos personales contenidos en éstos. Estos datos personales fueron

identificados tanto físicamente (papel u hoja) como virtual (bases de datos, Excel, entre otros).

Los datos identificados por cada banco de datos se muestran a continuación clasificada en cinco aspectos.

Identificativo: Cualquier información que permite identificar a una persona.

Personal: Cualquier información relacionada a características personales.

Económico/Seguros: Cualquier información relacionada a los ingresos económicos y los seguros.

Social: Cualquier información de carácter social.

Sensible: Están constituidos por

- Datos biométricos que por sí mismos pueden identificar a la persona.
- Datos referidos al origen racial y étnico.
- Opiniones o convicciones políticas, religiosas filosóficas o morales y la afiliación sindical.
- Información relacionada a la salud o a la vida sexual.

Tabla 8 *Datos Personales de Colaboradores*

IDENTIFICATIVO	**PERSONAL**	**ECONÓMICO/ SEGUROS**	**SOCIAL**	**SENSIBLE**
Nombres	Estado Civil	Créditos, Préstamos, Avales	Aficiones y hábitos personales.	Vida Sexual
Apellidos	Fecha de nacimiento	Datos Bancarios	Características de vivienda	Vida afectiva o familiar
N° DNI	Nacionalidad	Historial de créditos		Información relativa a la salud física o metal
N° RUC	Sexo	Información Tributaria		Ingresos económicos
N° de Pasaporte	Profesión	Seguros		Huella
Dirección de Domicilio	Edad	Planes de pensiones / jubilación		Afiliación Sindical
Teléfono	Datos Académicos			Condición del Trabajador (Apto/ No Apto)
Correo electrónico	Datos de Derechohabientes			Resultado de Evaluación Médica
Imagen	Datos de persona de contacto			Motivo de accidente y diagnóstico.
Firma	Talla de Zapato			Motivo cese
N° de Brevete	Estatura			
N° Carnet Seguro de Salud	Peso			
N° Carnet de Extranjería	Anamnesis			

N° Libreta Militar	Grupo Sanguíneo			
Código interno del Trabajador	Puesto de Trabajo			
	Grado de Instrucción			
	Número de Hijos			
	Nombre de Hijos			
	Edad de Hijos			
	Sexo de Hijos			

Fuente: Elaboración propia

Tabla 9 *Datos personales de postulantes*

IDENTIFICATIVO	**PERSONAL**	**SOCIAL**	**SENSIBLE**
Nombres	Estado civil	Aficiones y hábitos personales	Convicciones filosóficas o morales
Apellidos	Fecha de nacimiento		Convicciones religiosas
N° DNI	Nacionalidad		
N° RUC	Sexo		
N° Pasaporte	Profesión		
Dirección de Domicilio	Edad		
correo electrónico	Datos Académicos		
Imagen			
Firma			
Carne de extranjería			
Teléfono			

Fuente: Elaboración propia

Tabla 10 *Datos* personales *de clientes*

IDENTIFICATIVO	**PERSONAL**	**ECONÓMICO/ SEGUROS**
Nombres	Nacionalidad	Créditos, Préstamos y Avales.
Apellidos	Sexo	Datos Bancarios
N° DNI	Datos de persona de Contacto	Historial de Créditos
N° RUC		Bienes Patrimoniales
Pasaporte		
Dirección de Domicilio		
Teléfono		
Correo electrónico		
Firma		
N° Fax		
Código de Cliente		
Nombre Comercial		
Razón Social		

Fuente: Elaboración propia

Tabla 11 *Datos* personales *de proveedores*

IDENTIFICATIVO	**PERSONAL**	**ECONÓMICO/ SEGUROS**
Nombres	Nacionalidad	Datos Bancarios
Apellidos	Datos de persona de Contacto	
N° DNI		
N° RUC		
Dirección de Domicilio		
Teléfono		
Correo electrónico		
Firma		
Código de proveedor		
N° Fax		
Razón social		

Fuente: Elaboración propia

Tabla 12 *Datos personales de vigilancia-Plantas*

IDENTIFICATIVO
Imagen

Fuente: Elaboración propia

Tabla 13 *Datos personales de vigilancia-Sol Alpaca*

IDENTIFICATIVO
Imagen

Fuente: Elaboración propia

Tabla 14 *Datos personales de visitantes*

IDENTIFICATIVO
Nombres
Apellidos
N° DNI
N° RUC

N° Pasaporte
Firma
Carne de extranjería

Fuente: Elaboración propia

e. Identificación de los sistemas impactados

Teniendo ya los datos personales contenidos en los bancos de datos y la lista de softwares administrados por la empresa, se identificó los softwares que son usados para la gestión de los datos personales.

a. Sistema de Michell
b. Microsoft Office (Excel, Word, Access, Outlook)
c. Oracle
d. Mozilla Firefox
e. Chrome

f. Establecimiento de la lista de bancos de datos personales

En este paso establecemos todos los bancos de datos personales encontrados haciendo una lista de los mismos.

1. Colaboradores
2. Postulantes
3. Clientes
4. Proveedores
5. Video Vigilancia - Plantas
6. Video Vigilancia - Sol Alpaca
7. Visitantes

g. Registro de los bancos de datos personales ante el RNPDP

Finalmente, luego de haber establecido los bancos de datos personales podemos completar los formularios de inscripción de los bancos de datos identificados para proceder a realizar su registro ante el RNPDP. (Anexo A).

3.3.3 Elaboración y Ejecución de Procedimientos y Políticas

Tabla 15 *Elaboración y Ejecución de Procedimientos y Políticas*

Identificar la categoría correspondiente a los bancos de datos personales	Jefe de Proyectos TI, Recolector 1, Recolector 2.
Definir las medidas de seguridad a implementar por categoría.	Jefe de Proyectos TI, Recolector 1, Recolector 2.
Establecer medidas de seguridad organizativas para cada banco de datos personales	Jefe de Proyectos TI, Recolector 1, Recolector 2.
Establecer medidas de seguridad legales para cada banco de datos personales	Gerente de TI, Asesor Legal, Recolector 1, Recolector 2.
Establecer medidas de seguridad técnicas para cada banco de datos personales	Gerente de TI, Jefe de Proyectos TI, Recolector 1, Recolector 2.
Establecer el nuevo proceso para garantizar los derechos ARCO	Recolector 1, Recolector 2.

Fuente: Elaboración Propia

a. Identificar la categoría correspondiente a los bancos de datos personales

Para cumplir con la tercera fase de la metodología primero debemos evaluar y categorizar a cada banco de datos personales encontrado de acuerdo a diversos criterios, tal como nos dice la Directiva de Seguridad. (Anexo B.)

Las categorías están definidas de la siguiente manera, además asociadas a un color en particular para diferenciarlas.

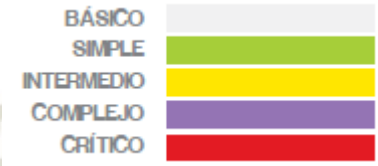


Figura 5 Categorías a tomar en cuenta por cada banco de datos personales

Fuente: Directiva de Seguridad

Tabla 16 *Detalle de categorías por criterios*

CRITERIOS						
CATEGORÍA	**Volumen de registros**	**Número de Datos**	**Periodo de Tiempo para la finalidad**	**Finalidad respaldada por alguna Ley**	**Múltiples Localizaciones**	**Tratamiento de Datos Sensibles**
Básico	No mayor a 50.	Menor a 5.	Mínimo.	No	No	No
Simple	No mayor a 100.	Indeterminado.	Inferior a 1 año.	No	No	No
Intermedio	Hasta 1000.	Indeterminado.	Superior a 1 año.	No	Si	Si.
Complejo	Más de 1000.	Indeterminado.	Superior a 1 año.	No	Si	Si
Crítico	Más de 1000.	Indeterminado.	Superior a 1 año.	Si	Si	Si

Fuente: Elaboración Propia

La categorización va a servir para definir las medidas de seguridad que deben ser adoptadas para cada banco de datos. Un banco de datos con categoría simple no requiere las medidas de seguridad que uno crítico o complejo, y por el contrario un banco de datos con categoría crítico requiere mayor seguridad que uno con categoría simple o básica. Por eso es muy importante que la categorización sea realizada con el mayor cuidado y veracidad.

Los resultados de la categorización de los bancos identificados en la empresa Michell y Cía. S.A. son los siguientes:

Tabla 17 *Resultado de categorización por cada banco de datos*

BANCO DE DATOS	CRITERIOS							
	Titular del Banco de Datos	**Volumen de registros**	**Número de Datos**	**Periodo de Tiempo para la finalidad**	**Finalidad respaldada por alguna Ley**	**Múltiples Localizaciones**	**Tratamiento de Datos Sensibles**	**CATEGORÍA**
Colaboradores	Persona Jurídica Michell y Cía. S.A.	Más de 1000.	53	Indeterminado (más de 1 año).	Si	Si	Si	**Crítico**
Clientes	Persona Jurídica Michell y Cía. S.A.	Más de 1000.	21	Indeterminado (más de 1 año).	No	Si	No	**Complejo**
Postulantes	Persona Jurídica Michell y Cía. S.A.	Más de 1000.	19	Indeterminado (más de 1 año).	No	Si	Si	**Complejo**
Proveedores	Persona Jurídica Michell y Cía. S.A.	Menos de 1000.	16	Indeterminado (más de 1 año)	No	Si	No	**Complejo**
Visitantes	Persona Jurídica Michell y Cía. S.A.	Más de 1000.	6	Más de 1 año.	No	No	No	**Complejo**
Video Vigilancia	Persona Jurídica Michell y Cía. S.A.	Menos de 1000.	1	Menos de 1 año.	No	No	No	**Intermedio**

Fuente: Elaboración Propia

b. Definir las medidas de seguridad a implementar por categoría

Las medidas de seguridad que debe adoptar cada banco de datos identificado están divididas como: (a) medidas organizativas, las cuales deben ser evaluadas y recibir el apoyo de directivos o funcionarios de la empresa; (b) medidas legales o jurídicas, cuyas medidas deben ser evaluadas por el asesor legal de la empresa para ser aplicadas; y (c) medidas técnicas, las cuales son evaluadas por el área de tecnologías de información de la empresa para ser aplicadas. Además, son estas medidas las más importantes y críticas para conseguir un nivel de seguridad apropiado para cada banco de datos personales.

Tabla 18 *Medidas* Organizativas *por categoría*

MEDIDAS ORGANIZATIVAS	**CATEGORIA**				
	Critico	**Complejo**	**Intermedio**	**Simple**	**Básico**
Definir un responsable de seguridad	X	X	X	X	X
Comunicar clara y oportunamente la Política de Seguridad de Información al interior de la organización.	X	X	X	X	X
Llevar control de asignación y retiro de privilegios y acceso a la información contenida en el banco de datos personales y su correspondiente registro de acceso.	X	X	Opcional	-	-
Realizar un control periódico del cumplimiento de las políticas de seguridad	X	X	X	-	-
Adecuación de los procesos del negocio involucrados en el tratamiento de datos personales a la Ley N° 29733, Ley de Protección de Datos Personales.	X	X	Opcional	-	-
Desarrollar un procedimiento de control de acceso a datos personales	X	X	X	-	-

Desarrollar un procedimiento de gestión de incidentes para la protección de datos personales	X	X	X	-	-

Fuente: Elaboración Propia

Tabla 19 *Medidas Legales* por *categoría*

MEDIDAS LEGALES	CATEGORIA				
	Critico	Complejo	Intermedio	Simple	Básico
Adecuar los contratos del personal y terceros relacionados al tratamiento de datos personales.	X	X	X	X	X
Desarrollar formatos de consentimiento para el tratamiento de datos personales, adecuados y de conformidad con la finalidad para la cual son acopiadas.	X	X	X	X	X
Desarrollar y mantener actualizado un documento de compromiso de confidencialidad en el tratamiento de datos personales.	X	X	Opcional	-	-

Fuente: Elaboración Propia

En el caso de las medidas de seguridad técnicas son divididas dependiendo del tipo de tratamiento inadecuado que se realice con los bancos de datos personales. Estos tipos de tratamientos son los siguientes:

1. Acceso no autorizado al banco de datos personales
2. Alteración no autorizada al banco de datos personales
3. Pérdida del banco de datos personales
4. Tratamiento no autorizado del banco de datos personales

Además, para garantizar la seguridad de los dato personales contenidos en cada banco se evalúa cuáles de estas medidas de seguridad técnicas permitirán preservar su confidencialidad, disponibilidad e integridad. Para ello, se agrega una nueva columna de seguridad de información en cada una de las siguientes tablas, en donde:

C: Confidencialidad

D: Disponibilidad

I: Integridad

Tabla 20 *Medidas Técnicas - Acceso no autorizado al banco de datos personales*

ACCESO NO AUTORIZADO AL BANCO DE DATOS PERSONALES	SI	CATEGORÍA DE BANCO CRITICO	CATEGORÍA DE BANCO COMPLEJO	CATEGORÍA DE BANCO INTERMEDIO	CATEGORÍA DE BANCO SIMPLE	CATEGORÍA DE BANCO BÁSICO
Gestión y uso de contraseñas en medios informáticos.	C	Requerido	Requerido	Requerido	Requerido	Requerido
Revisión y registro de los privilegios de acceso	C	Registro dentro del sistema	Registro dentro del sistema	Registro dentro del sistema	Registro en un cuaderno de seguridad.	Registro en un cuaderno de seguridad.
Ubicación física segura para el banco de datos (llave, cerradura, etc.)	C	Ambiente aislado con llave	Ambiente aislado con llave	Ambiente aislado con llave	Caja, cajón de un mobiliario con llave.	Caja, cajón de un mobiliario con llave.
Mecanismos de autenticación	C	Mecanismo de contraseñas u otro fuerte mecanismo de autenticación.	Mecanismo de contraseñas u otro fuerte mecanismo de autenticación.	Mecanismo de contraseñas u otro fuerte mecanismo de autenticación.	Mínimo una validación de acceso.	Mínimo una validación de acceso.
Autorización o Retiro de Acceso a un Usuario.	C					

Fuente: Elaboración Propia

Tabla 21 *Medidas Técnicas - Alteración no autorizada de datos personales*

ALTERACIÓN NO AUTORIZADA AL BANCO DE DATOS PERSONALES	SI	CATEGORÍA DE BANCO	CATEGORÍA DE BANCO	CATEGORÍA DE BANCO	CATEGORÍA DE BANCO	CATEGORÍA DE BANCO
		CRITICO	COMPLEJO	INTERMEDIO	SIMPLE	BÁSICO
Seguridad en el traslado de información	I	Requerido	Requerido	Requerido	Requerido	Requerido
Ubicación física que evite el acceso	C	Requerido	Requerido	Requerido	Requerido	Requerido
Encriptación y mecanismo de verificación	I	Requerido	Requerido	Requerido	Requerido	Requerido
Mecanismos seguros de eliminación	I	Requerido	Requerido	Requerido	Requerido	Requerido
Mecanismos seguros de generación de copias y reproducción de documentos	I	Requerido	Requerido	Requerido	Requerido	Requerido

Fuente: Elaboración Propia

Tabla 22 *Medidas Técnicas - A la pérdida de bancos personales*

A LA PÉRDIDA DEL BANCO DE DATOS PERSONALES	SI	CATEGORÍA DE BANCO	CATEGORÍA DE BANCO	CATEGORÍA DE BANCO	CATEGORÍA DE BANCO	CATEGORÍA DE BANCO
		CRITICO	COMPLEJO	INTERMEDIO	SIMPLE	BÁSICO
Copias de respaldo de los datos personales	D	Requerido	Requerido	Requerido	Opcional	Opcional
Técnicas de cifrado	C,I	Requerido	Requerido	Requerido	Opcional	Opcional
Ubicación física segura de las copias de respaldo	C	Requerido	Requerido	Requerido	Opcional	Opcional

Mecanismos de continuidad del tratamiento de los datos personales	D	Requerido	Requerido	Requerido	Opcional	Opcional
Autorización para la recuperación de la copia de respaldo	D	Requerido	Requerido	Requerido	Opcional	Opcional
Pruebas de verificación de integridad de los datos personales de la copia de respaldo	I	Requerido	Requerido	Requerido	Opcional	Opcional

Fuente: Elaboración Propia

Tabla 23 *Medidas Técnicas - Al tratamiento no autorizado de datos personales*

AL TRATAMIENTO NO AUTORIZADO DEL BANCO DE DATOS PERSONALES	SI	CATEGORÍA DE BANCO	CATEGORÍA DE BANCO	CATEGORÍA DE BANCO	CATEGORÍA DE BANCO	CATEGORÍA DE BANCO
		CRITICO	COMPLEJO	INTERMEDIO	SIMPLE	BÁSICO
Datos personales deben ser independizados	I	Requerido	Requerido	Requerido	Requerido	Requerido
Informar el tratamiento no autorizado	C	Requerido	Requerido	Requerido	Requerido	Requerido
Registrar los datos recuperados tras un incidente	C	Requerido	Requerido	Requerido	Requerido	Requerido
Mantenimiento preventivo y correctivo de equipos	D	Requerido	Requerido	Requerido	Opcional	Opcional
Poseer software de protección contra software malicioso (virus, troyanos, etc.)	C	Requerido	Requerido	Requerido	Opcional	Opcional

Almacenamiento seguro empleando mecanismos de control de acceso y cifrada	C	Requerido	Requerido	Requerido	Opcional	Opcional
Transporte de información personal mediante algún cifrado	C	Requerido	Requerido	Requerido	Requerido	Opcional
Seguridad en el flujo transfronterizo de datos personales.	D,C	Requerido	Requerido	Requerido	Requerido	No Aplica
Restringir el uso de equipos de fotografía, video, audio u otro	C	Requerido	Requerido	Requerido	Requerido	Opcional

Fuente: Elaboración Propia

c. Establecer medidas de seguridad organizativas para cada banco de datos personales

Tabla 24 *Medidas Organizativas de Seguridad*

EVALUACIÓN DE LAS MEDIDAS DE SEGURIDAD INDICADAS EN LA DIRECTIVA DE SEGURIDAD PARA LOS BANCOS DE DATOS DE MICHELL Y CIA. S.A.						
CRITERIO	**COLABORADORES**	**POSTULANTES**	**PROVEEDORES**	**CLIENTES**	**VIDEO VIGILANCIA**	**VISITANTES**
MEDIDAS ORGANIZATIVAS DE SEGURIDAD	**CRITICO**	**COMPLEJO**			**INTERMEDIO**	
Definir un responsable de seguridad	Jefe de Recursos Humanos	Jefe de Recursos Humanos	Jefe de Logística	Gerente comercial	Jefe de Retail Sol Alpaca	Gerencia Administrativa
Comunicar clara y oportunamente la Política de Seguridad de Información al interior de la organización.	La Política de Protección de Datos Personales es comunicada a toda la organización y publicada en nuestra página web. (Ver Capítulo IV)					
Llevar control de asignación y retiro de privilegios y acceso a la información contenida en el banco de datos personales y su	Se controla el acceso y se puede identificar al usuario a través de la base de datos Oracle.					

correspondiente registro de acceso.					
Realizar un control periódico del cumplimiento de las políticas de seguridad	Se realiza un control periódico cada 6 meses.				
Adecuación de los procesos del negocio involucrados en el tratamiento de datos personales a la Ley N° 29733, Ley de Protección de Datos Personales.	Se adecuaron los siguientes procesos: Reclutamiento de Personal. (Figura 27)	Se adecuaron los siguientes procesos: Selección de Personal. (Figura 28)	Se adecuaron los siguientes procesos: Adquisición de servicios a nivel Nacional e internacional. (Figura 29 y Figura 30)	Se adecuaron los siguientes procesos: Venta de productos en la Tienda virtual, Venta de productos en tiendas. (Figura 31 y Figura 32)	Se adecuaron los siguientes procesos: Recopilación de visitantes a la empresa. (Figura 33)
Desarrollar un procedimiento de control de acceso a datos personales	Existe una Política y Procedimiento de Control de Acceso y Privilegios. (Ver Capítulo IV)				
Desarrollar un procedimiento de gestión de incidentes para la protección de datos personales	Existe una Política y Procedimiento de Gestión de Incidencias. (Ver Capítulo IV)				

Fuente: Elaboración Propia

d. Establecer medidas de seguridad legales para cada banco de datos personales

Tabla 25 *Medidas Legales de Seguridad*

EVALUACIÓN DE LAS MEDIDAS LEGALES INDICADAS EN LA DIRECTIVA DE SEGURIDAD PARA LOS BANCOS DE DATOS DE MICHELL Y CIA. S.A.						
CRITERIO	**COLABORADORES**	**POSTULANTES**	**PROVEEDORES**	**CLIENTES**	**VIDEO VIGILANCIA**	**VISITANTES**
MEDIDAS LEGALES DE SEGURIDAD	**CRITICO**	**COMPLEJO**			**INTERMEDIO**	
Adecuar los contratos del personal y terceros relacionados al tratamiento de datos personales.	Ya fue adecuado.	No corresponde.	Ya fue adecuado.	Ya fue adecuado.	No corresponde.	No corresponde.
Desarrollar formatos de consentimiento para el tratamiento de datos personales, adecuados y de conformidad con la finalidad para la cual son acopiadas.	Si se ha desarrollado. (Ver Capítulo IV)					
Desarrollar un documento de compromiso de confidencialidad en el tratamiento de datos personales.	Si se ha desarrollado. El documento especifica que todo el personal colaborador que realice un tratamiento con datos personales de cualquiera de los bancos de datos se compromete a guardar confidencialidad. (Ver Capítulo IV)					

Fuente: Elaboración Propia

e. Establecer medidas de seguridad técnicas para cada banco de datos personales

Tabla 26 *Medidas Técnicas de Seguridad – Acceso No autorizado*

EVALUACIÓN DE LAS MEDIDAS TÉCNICAS INDICADAS EN LA DIRECTIVA DE SEGURIDAD PARA LOS BANCOS DE DATOS DE MICHELL Y CIA							
ACCESO NO AUTORIZADO AL BANCO DE DATOS PERSONALES		**CRITICO**	**COMPLEJO**			**INTERMEDIO**	
CRITERIO	**ESPECIFICACIONES**	**COLAB.**	**POST.**	**PROV.**	**CLI.**	**VIDEO VIG.**	**VISIT.**
Gestión y uso de contraseñas en medios informáticos.	**Cuando se utilice un servidor de autenticación, éste debe almacenar las contraseñas de manera cifrada.**	La base de datos Oracle almacena las contraseñas de manera cifrada automáticamente.					-
	Contraseñas deben ser alfanuméricas.	Las contraseñas cuentan con un formato determinado.					-
	Bloquear al usuario luego de cinco (05) intentos fallidos de autenticación consecutivos.	El sistema bloquea al usuario dependiendo del perfil configurado acorde a su rol de puesto de trabajo. Y por el momento son 05 intentos fallidos de autenticación consecutivos.					-
	Permitir a los usuarios cambiar su contraseña cuando él lo vea necesario.	Está permitido que los usuarios puedan cambiar su contraseña cuando lo considere necesario.					-
Revisión y Registro de los privilegios de acceso.	**Revisar que solo el personal autorizado pueda acceder a los datos personales.**	Cada usuario está con un rol asociado en la Base de datos, y cada rol tiene sus controles de accesos necesarios.					-
	Se debe registrar dicha verificación.	Se realiza dos revisiones cada seis meses y se guarda un registro de dicha revisión.					-

Mecanismos de autenticación.	**Los usuarios deben tener un identificador único de acceso asociado a perfiles de usuarios y los accesos autorizados para cada uno de ellos.**	Usuarios tienen un identificador único de acceso asociado a un rol específico y sus accesos autorizados.
¿Quién autoriza o retira algún acceso a un usuario? ¿Con qué autorización?	**Esta autorización o retiro de acceso a un usuario debe registrarse.**	Cuando se requiera dar permisos a un rol, debe ser autorizado por el jefe de área a quien corresponde el rol y notificar al área de sistemas o el encargado de seguridad lógica de los bancos de datos personales.
	El registro debe contener: Usuario, Fecha y Hora de autorización o retiro y Usuario que autoriza y/o retira.	Se hace un registro de autorización.

Fuente: Elaboración Propia

Tabla 27 *Medidas Técnicas de Seguridad - Alteración No Autorizada*

EVALUACIÓN DE LAS MEDIDAS TÉCNICAS INDICADAS EN LA DIRECTIVA DE SEGURIDAD PARA LOS BANCOS DE DATOS DE MICHELL Y CIA								
ALTERACIÓN NO AUTORIZADA AL BANCO DE DATOS PERSONALES		**CRITICO**	**COMPLEJO**			**INTERMEDIO**	
CRITERIO	**ESPECIFICACIONES**	**COLAB.**	**POST.**	**PROV.**	**CLI.**	**VIDEO VIG.**	**VISIT.**
Cuando se requiera eliminar información, ¿Se cuenta con mecanismos seguros de eliminación?	**Este mecanismo debe permitir el borrado total de la información** **No se debe poder recuperar la información.**	A nivel de base de datos, por lo general no eliminan ningún backup generado. En el caso de una computadora cuando va a hacer reasignado a otra persona se elimina y se formatea la Pc.					
¿Se cuenta con autorización previa para poder eliminar información de un medio informático removible?		Para poder eliminar información de un medio informático removible se cuenta con la autorización del encargado de seguridad lógica de los bancos de datos personales.					-
¿Quién es el encargado de poder eliminar información de un medio informático removible?		El responsable de las copias de seguridad dentro del área de sistemas.					-
¿Sólo personal autorizado puede generar copias y/o reproducciones de documentos que contienen información del banco de datos?		Solo personal autorizado puede generar y manipular documentos que contengan información de los bancos de datos personales.					

Fuente: Elaboración Propia

Tabla 28 *Medidas Técnicas de Seguridad - A la Pérdida del Banco de Datos*

EVALUACIÓN DE LAS MEDIDAS TÉCNICAS INDICADAS EN LA DIRECTIVA DE SEGURIDAD PARA LOS BANCOS DE DATOS DE MICHELL Y CIA							
A LA PÉRDIDA DEL BANCO DE DATOS PERSONALES		**CRITICO**	**COMPLEJO**			**INTERMEDIO**	
CRITERIO	**ESPECIFICACIONES**	**COLAB.**	**CLI.**	**PROV.**	**POST.**	**VIDEO VIG.**	**VISIT.**
¿Se realiza copias de respaldo de los datos personales para permitir su recuperación?		Se realizan copias de respaldo de la base de datos todos los días antes de terminar el día y a cada computadora personal de los colaboradores por lo menos 1 vez a la semana.			-		
¿La copia de respaldo está protegida mediante técnicas de cifrado?		Los backups de la base de datos Oracle están cifrados automáticamente. Pero los backups de las computadoras no están cifrados.					
¿La copia de respaldo se encuentra en un ambiente distinto a la del tratamiento de los datos personales?		Tienen copias de los backups realizados en todas las sedes de la empresa para casos de emergencias.			-		
¿Existen mecanismos que garanticen la continuidad del tratamiento de los datos personales?		Cuentan con UPS que duran alrededor de 20 min, también grupo electrógeno que puede durar hasta 4 horas para que se garantice el uso del sistema con normalidad.					
¿La recuperación de datos personales cuenta con la autorización del encargado del banco de datos?		La recuperación de los datos personales cuenta con la autorización del jefe de área correspondiente en coordinación con el encargado de la seguridad de los bancos de datos personales.					

¿Se realiza pruebas de recuperación de los datos personales para verificar la integridad de la copia de respaldo?	**Se debe documentar los resultados de las pruebas indicando:**	No se realiza actualmente.
	a) Fecha y hora de la prueba.	
	b) Nombre de la persona que realizó la prueba.	
	c) Banco de datos personales recuperado.	
	d) Archivo recuperado y fecha de los datos recuperados.	
	e) Tiempo de recuperación.	
	f) Resultados de las pruebas.	
	g) Acciones tomadas en caso de pruebas insatisfactorias	

Fuente: Elaboración Propia

Tabla 29 *Medidas Técnicas de Seguridad - Al Tratamiento No Autorizado*

<table>
<tr><th colspan="8">EVALUACIÓN DE LAS MEDIDAS TÉCNICAS INDICADAS EN LA DIRECTIVA DE SEGURIDAD PARA LOS BANCOS DE DATOS DE MICHELL Y CIA</th></tr>
<tr><th colspan="2">AL TRATAMIENTO NO AUTORIZADO DEL BANCO DE DATOS PERSONALES</th><th>CRITICO</th><th colspan="3">COMPLEJO</th><th colspan="2">INTERMEDIO</th></tr>
<tr><th>CRITERIO</th><th>ESPECIFICACIONES</th><th>COLAB.</th><th>POST.</th><th>PROV.</th><th>CLI.</th><th>VIDEO VIG.</th><th>VISIT.</th></tr>
<tr><td>Cuando un banco de datos no está automatizado, ¿Los datos personales de una persona están independizados de forma individual?</td><td></td><td colspan="6">Cada documento que incluye datos personales está almacenado y es gestionado de forma individual para cada persona.</td></tr>
<tr><td rowspan="5">¿Se informa inmediatamente al titular de los datos personales cuando se confirma un tratamiento no autorizado?</td><td>La información debe incluir:</td><td colspan="6" rowspan="5">Se encuentra especificado en el “Procedimiento de Gestión de Incidentes.”</td></tr>
<tr><td>a) Naturaleza del incidente.</td></tr>
<tr><td>b) Datos personales comprometidos.</td></tr>
<tr><td>c) Nombres de las personas involucradas en la resolución del incidente.</td></tr>
<tr><td>d) Recomendaciones al titular de datos personales.</td></tr>
</table>

	e) Medidas correctivas implementadas.	
	f) Consecuencias del incidente.	
	g) Recuperación de datos.	
Si se logra recuperar los datos personales tras un incidente, ¿Se registra los datos recuperados?	**Debe registrarse tras una recuperación de datos personales:**	Se encuentra especificado en el “Procedimiento de Gestión de Incidentes.”
	Nombre de la persona que realizó la recuperación.	
	Descripción y fecha de los datos restaurados.	
	Descripción de los datos restaurados en forma manual.	
¿Se realiza mantenimiento preventivo y correctivo a los equipos utilizados para el tratamiento de datos personales?		Se realiza mantenimiento preventivo y correctivo de los equipos, periféricos y servidores.
¿Solo personal autorizado realiza el mantenimiento preventivo y correctivo?		Sólo lo realizan técnicos capacitados.
¿Estos equipos cuentan con software de protección contra software malicioso (virus, troyanos, etc.) para proteger la integridad de los datos personales?		Cada computadora personal cuenta con su propio antivirus y a su vez los servidores Linux también cuentan con su propio antivirus. Adicionalmente en las plantas de la empresa no se está permitido el uso de usb.

¿El software es actualizado frecuentemente?		Los softwares se actualizan automáticamente.			
¿El transporte electrónico de datos personales se realiza mediante algún cifrado o protocolo de comunicación de cifrado?	**VPN, correo electrónico cifrado, FTP seguro, entre otros.**	Usan VPN, correo electrónico cifrado (Gmail), y también una aplicación denominada mensajero, la cual envía mensajes encriptados.			
Seguridad en el flujo transfronterizo de datos personales.		El flujo transfronterizo de información personal se hace únicamente por correo electrónico o vía telefónica.	-	El flujo transfronterizo de información personal se hace únicamente por correo electrónico o vía telefónica.	-
Cuando sucede un evento que afecte la confidencialidad, integridad y disponibilidad de los datos personales. ¿Es reportado inmediatamente al responsable del banco de datos personales?		Si sucede un evento de este tipo, se le informa inmediatamente al encargado de la seguridad de los bancos de datos personales.			

Fuente: Elaboración Propia

Tabla 30 *Controles adoptados para preservar la Seguridad de Información*

Controles de Seguridad	Confidencialidad	Disponibilidad	Integridad
Gestión de Contraseñas	x		
Revisión de privilegios de acceso	x		x
Usuarios deben contar con un identificador único de acceso	x		x
Autorización previa para autorizar o retirar privilegios a un usuario	x		x
Registro de autorización de acceso o retiro de privilegios a un usuario	x		
Mecanismos seguros de eliminación			x
Autorización previa para la eliminación de información de un medio informático removible	x		x
Acceso restringido a la generación de copias y reproducciones de documentos con datos personales	x		x
Copias de respaldo de los bancos de datos personales		x	x
Copias de respaldo guardados en ambientes distintos		x	
Mecanismos que garanticen la continuidad del negocio		x	
Pruebas de recuperación de las copias de respaldo			x
Política y Procedimiento de gestión de copias de respaldo		x	
Política y Procedimiento de gestión de incidentes			x
Mantenimiento preventivo y correctivo de equipos		x	

Mantenimiento preventivo y correctivo de servidores		x	
Contar con software de protección contra software malicioso			x
Actualización de software frecuentemente		x	
Transmisión de datos personales a través de algún protocolo de comunicación de cifrado	x		x

Fuente: Elaboración Propia

f. Establecer el nuevo proceso para garantizar los derechos ARCO

Es importante desarrollar e implementar un procedimiento que ayude a Michell y Cía. cumplir con los derechos que le corresponden a cualquier persona, pero en este caso se está hablando de los colaboradores, postulantes, clientes, proveedores, video vigilancia y visitantes de la empresa.

Para esto se ha propuesto un nuevo proceso de atención para los titulares de los datos personales cuando éste presente un reclamo o desee ejercer algunos de estos derechos.

1. El proceso inicia presentando una solicitud de derechos ARCO por el Reclamante a través del correo LPDP@michell.com.pe.
2. El comité envía el link con el formato correspondiente para ser llenado por el reclamante.
3. El reclamante envía el formato añadiendo un documento de identidad que lo identifique.
4. El Comité de Protección de Datos Personales recibe la solicitud para poder evaluar el tipo de solicitud
5. Se debe evaluar que cumpla con los requisitos de documentación.
6. Es obligatorio que para cada tipo de solicitud se adjunte un documento de identidad.
7. En caso que la solicitud sea de tipo Rectificación o Cancelación, el titular debe adjuntar todo documento que sustente lo solicitado.
8. El titular tiene hasta 7 días hábiles para completar su solicitud.
9. Luego de evaluar que la solicitud cumpla con los requisitos previos de documentación se procede a evaluar el tipo de solicitud, ya sea si es de Acceso, Rectificación, Cancelación u Oposición.
10. Finalmente, el titular recibe la respuesta a su solicitud por el correo electrónico que fue recibido.

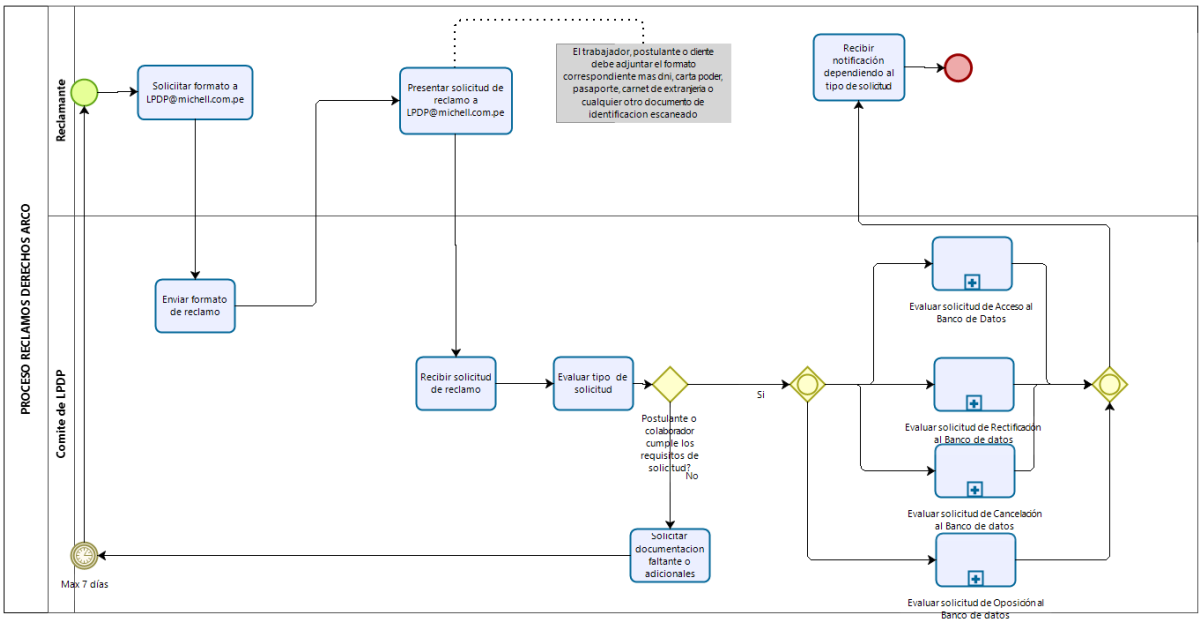


Figura 6 Proceso de Reclamos de Derechos ARCO

Fuente: Elaboración Propia

Como se puede visualizar en la imagen anterior, el proceso tiene cuatro subprocesos denominados:

- Evaluar solicitud de Acceso al Banco de Datos
- Evaluar solicitud de Rectificación al Banco de Datos
- Evaluar solicitud de Cancelación al Banco de Datos
- Evaluar solicitud de Oposición al Banco de Datos

A continuación, se detalla cada subproceso.

Evaluar solicitud de Acceso al Banco de Datos

1. El Comité de Protección de Datos Personales se encarga de recopilar la información solicitada.
2. En caso no se pueda recopilar información por parte del Comité de Protección de Datos Personales, se auxiliará con alguna persona responsable que pueda brindar la información requerida.

3. Caso contrario, se procede a recopilar la información sin ningún inconveniente.
4. Finalmente, se procede a notificar la información solicitada a través del correo electrónico por el que se recibió la solicitud.
5. El plazo máximo para dar respuesta a la solicitud es de 20 días hábiles después de recibida la solicitud.

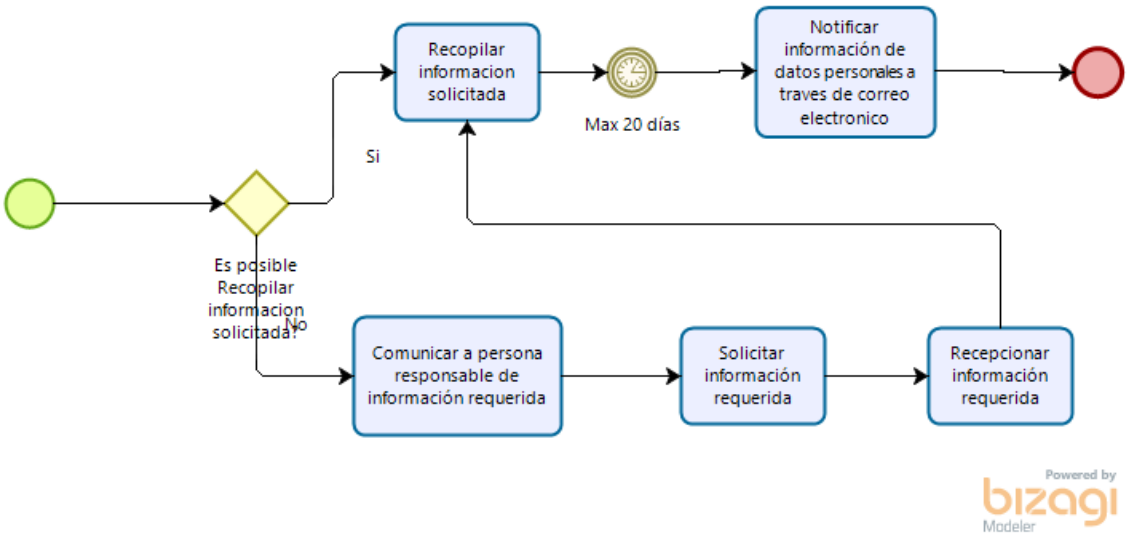


Figura 7 Acceso al Banco de Datos

Fuente: Elaboración Propia

Evaluar solicitud de Rectificación al Banco de Datos

1. El Comité de Protección de Datos Personales debe evaluar primeramente si los datos personales a rectificar han sido transferidos a otras sedes de la empresa previa a la solicitud.
2. En caso la información haya sido transferida, se debe comunicar a la sede transferida la petición del titular de la rectificación de sus datos personales.
3. Caso contrario, se empieza a evaluar si los datos personales pueden ser rectificados. Si área de Reclamos no puede realizar dicha rectificación

se puede auxiliar con el área de Sistemas para ejecutarla. De lo contrario se procede a ejecutar la rectificación sin ningún problema.

4. El plazo máximo de ejecutar la petición de rectificación por parte del titular es de 10 días hábiles después de recibida la solicitud.

   NOTA: El informar a la sede transferida la rectificación y ejecutarla en el sistema puede llevarse a cabo en paralelo para que la respuesta se notifique a tiempo.

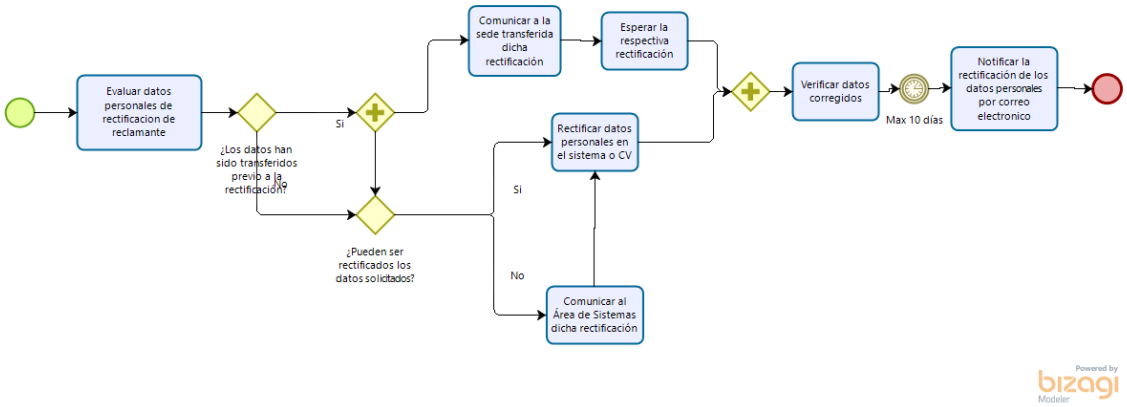


Figura 8 Rectificación al Banco de Datos

Fuente: Elaboración Propia

Evaluar solicitud de Cancelación al Banco de Datos

1. El Comité de Protección de Datos Personales primero debe evaluar si la solicitud de cancelación procede.
2. En caso la solicitud proceda:
3. Si es titular es colaborador, se registra la fecha de cese en el sistema para que sus datos personales no sean parte del tratamiento para cualquier tipo de gestión.
4. Si el titular es cliente/proveedor o colaborador, se cambia su estado a inactivo para que sus datos personales no sean parte del tratamiento para cualquier tipo de gestión.
5. Si el titular es postulante, se le hace entrega de su currículum vitae en físico.

6. En caso la solicitud no proceda, se notifica en la respuesta a la solicitud el motivo por el cual no procede. (Se puede adjuntar documentación que lo sustente).
7. Finalmente, se notifica la cancelación de cualquier tratamiento a los datos personales.
8. El plazo máximo de dar respuesta a la solicitud es de 10 días hábiles después de recibida la solicitud.

   Nota: El cancelar cualquier tipo de tratamiento a los datos personales del titular no significa el eliminarlo por completo en el sistema (se considera registrarlo como inactivo) ya que, por otra ley, para el caso de los colaboradores, se requiere tenerlos registrados.

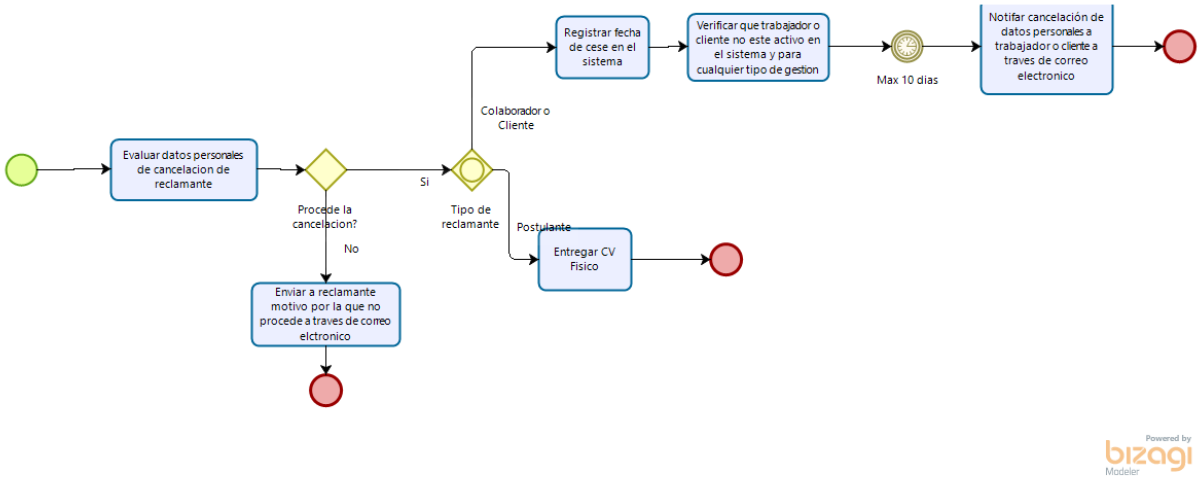


Figura 9 Cancelación al Banco de Datos

Fuente: Elaboración Propia

Evaluar solicitud de Oposición al Banco de Datos

1. El Comité de Protección de Datos Personales debe verificar si existe previo consentimiento de tratar sus datos personales para evaluar el motivo de oponerse a su tratamiento.
2. En el caso que exista dicho consentimiento, se procede a evaluar si dicho tratamiento causa algún tipo de perjuicio al titular.
3. En caso no cause perjuicio alguno, se corrobora si estos datos personales son necesarios por mandato legal.

4. Si efectivamente son necesarios se rechaza la solicitud notificando el motivo en su respuesta. (Se puede adjuntar documentación que lo sustente).
5. Caso contrario, se procede a ejecutar el paso 3.
6. Si no hay ningún problema se procede a ejecutar la petición. Si es colaborador, cliente o postulante, se cambia el estado a inactivo en el sistema; si es postulante, se le hace entrega de su currículum vitae físico.
7. Finalmente, se verifica que la solicitud haya sido ejecutada satisfactoriamente para proceder a notificar la respuesta a la solicitud.

   El plazo máximo para dar respuesta a la solicitud es de 10 días hábiles después de recibida la solicitud.

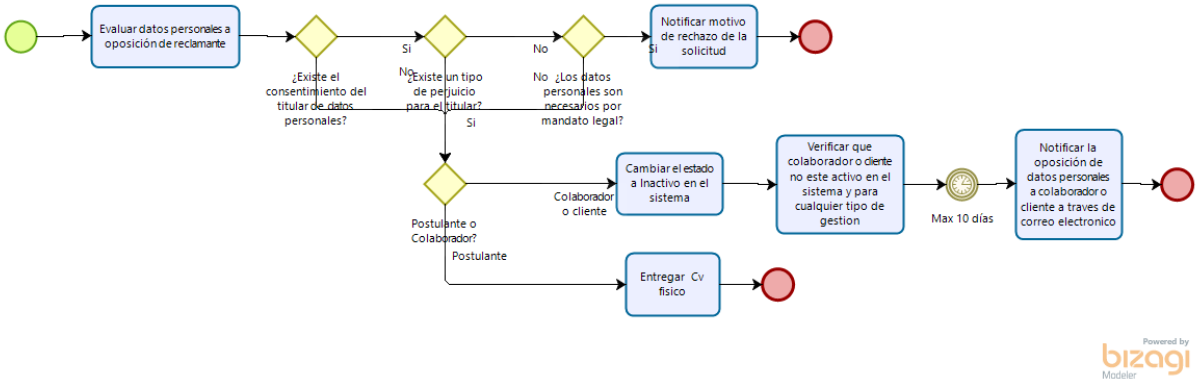


Figura 10 Oposición al Banco de Datos

Fuente: Elaboración Propia

3.3.4 Obtención de Consentimiento

Tabla 31 *Obtención del Consentimiento*

Identificar a personal recolector del consentimiento de los titulares de datos personales.	Gerente de TI, Recolector 1, Recolector 2.
Capacitación a personal recolector del consentimiento de los titulares de datos personales.	Gerente de TI, Recolector 1, Recolector 2.
Establecer nuevos procedimientos para la obtención del consentimiento de los titulares de datos personales.	Recolector 1, Recolector 2, Jefe de Proyectos de TI.

Recabar los consentimientos de los titulares de los datos personales.	Asesor Legal, Recolector 1, Recolector 2, Jefe de Proyectos de TI.
Monitoreo continuo de la metodología.	Gerente de TI, Jefe de Proyectos de TI.

Fuente: Elaboración Propia

a. Identificar a personal recolector del consentimiento de los titulares de datos personales

Para poder obtener el consentimiento de cada uno de los titulares de los datos personales, primero se debe seleccionar e identificar al personal más conveniente dependiendo de tipo de titular que sea; teniendo como principal misión el recopilar los consentimientos expresos e inequívocos de los titulares, incluyendo los que no han sido obtenidos y sin embargo la empresa ha realizado un tratamiento con esos datos personales.

A continuación, se manifiesta el personal seleccionado encargado de la obtención de los consentimientos por cada banco de datos personales.

Figura 11 Personal Encargado De La Obtención Del Consentimiento de Datos Personales

Fuente: Elaboración Propia

b. Capacitación a personal recolector del consentimiento de los titulares de datos personales

El personal seleccionado deberá ser debidamente capacitado para llevar a cabo su labor.

- Primero, se brinda una breve explicación del contenido de la presente ley de protección de datos personales, Ley N°29733, y su reglamento.
- Segundo, se da a conocer la importancia y la finalidad de la recopilación de los consentimientos.
- Finalmente, se explica el nuevo proceso que debe realizar para cumplir el objetivo.

c. Establecer nuevos procedimientos para la obtención del consentimiento de los titulares de datos personales

Obtención del consentimiento de un **Colaborador**:

El área de Recursos Humanos debe entregar al colaborador un contrato en el cual se adjunte un nuevo documento de "Consentimiento para el tratamiento de Datos Personales" en el cual se le informa el tratamiento que se realizará con sus datos personales, de esta forma el colaborador otorga su consentimiento expreso e inequívoco al titular de los bancos de datos, en este caso, la propia empresa Michell y Cía. S.A.

Así mismo, asumiendo lo que rige la Ley de Protección de Datos Personales, se evalúa si el colaborador a contratar tendrá relación con el tratamiento de datos personales.

- Si es afirmativo, tendrá que firmar un compromiso de confidencialidad.
- Caso contrario, no firma absolutamente nada y se procede a registrar sus datos en el sistema.

Obtención del consentimiento de un **Postulante**:

Debido a que se realiza un tratamiento de los datos personales de aquellas personas que postulan a una vacante de trabajo en la empresa, el área que corresponda al momento de ejecutar la entrevista personal al seleccionado le hará entrega de un formato de consentimiento el cual debe informar, expresar inequívocamente el tratamiento que se realizará con sus datos personales en el caso de no ser elegido como nuevo miembro colaborador.

Obtención del consentimiento de un **Cliente**:

Venta de Productos Finales en tienda virtual

En el caso de la tienda virtual "Sol Alpaca", los clientes deberán aceptar el Consentimiento del Tratamiento de Datos Personales haciendo clic en una casilla de aceptación antes de poder comprar el producto.

Y también existirá un apartado dentro de la página web de la empresa en el cual se informe la Política de Protección de Datos personales y el Aviso De Privacidad Para Los Bancos De Datos Personales De La Empresa Michell Y Cía. S.A.

Venta de Productos en Tiendas

Cuando un cliente se dirige a alguna tienda, el personal encargado de la venta le hace entrega de un cupón de descuento para la tienda virtual. En dicho cupón debe existir un breve mensaje informando al cliente el tratamiento de sus datos personales y que la empresa cumple con la Ley N°29733.

Dicho texto se especifica a continuación.

"Por este medio se le informa que Michell y Cía. S.A. está apegado a la Ley de Protección de Datos Personales, Ley N°29733 y a su reglamento. Por lo cual la información personal que nos proporcione es confidencial, de tal manera que no será transferida a terceros con el fin de proteger su confidencialidad. (Ver Política de Protección de Datos Personales en nuestra página web www.michell.com.pe)"

Obtención del consentimiento de un **Proveedor**:

Al momento de generar y enviar el contrato al proveedor, se debe adjuntar un formato de consentimiento el cual debe informar, expresar inequívocamente el tratamiento que se realizará con sus datos personales.

Así mismo estará publicado en la página web de la empresa el Aviso De Privacidad Para Los Bancos De Datos Personales De La Empresa Michell Y Cía. S.A.

Obtención del consentimiento de **Visitantes y Video vigilancia**:

Debido a que existe gran cantidad de visitantes en todas las sedes de la empresa, se publica un aviso fuera de todas sus sedes, el cual dé por informado a los visitantes que la empresa cumple lo establecido en la LPDP.

En el caso del banco de datos de video vigilancia debe existir una publicación en las tiendas y también plantas de la empresa, indicando a las personas que se les está filmando.

Distinguido visitante:

De acuerdo a la **Ley N° 29733 Ley de Protección de datos Personales** se le informa que Michell & Cia en cumplimiento a la normatividad que rige el Reglamento, sus datos personales seran almacenados en nuestros bancos de datos personales, asi mismo seran tratados, custodiados con las medidas de seguridad y confidencialidad pertinentes. El ejercicio de sus derechos o cualquier otra consulta sopre el tratamiento se podrá efectuar en LPDP_michell@michell.com.pe

MICHELL
Passion for Alpaca since 1931

Figura 12 Aviso Informativo de Protección de Datos Personales

Fuente: Elaboración Propia

Así mismo estará publicado en la página web de la empresa el Aviso De Privacidad Para Los Bancos De Datos Personales De La Empresa Michell Y Cía. S.A.

d. Recabar los consentimientos de los titulares de los datos personales

Obtención del consentimiento de un **Colaborador**:

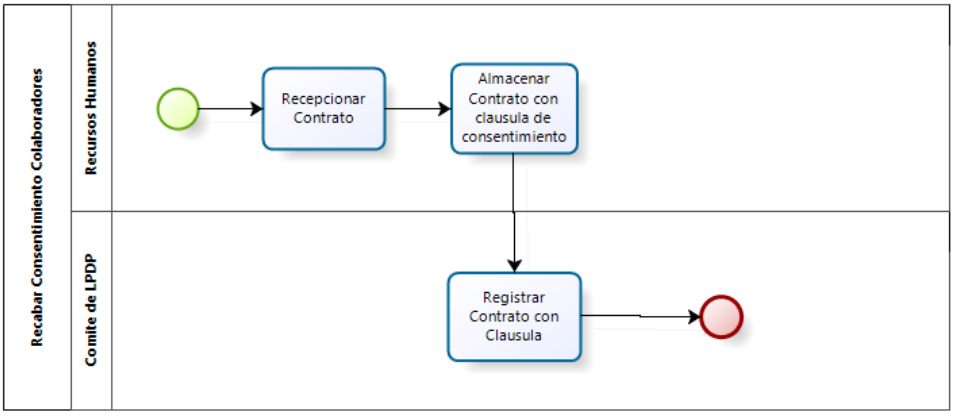


Figura 13 Obtención del Consentimiento de Colaborador

Fuente: Elaboración Propia

Obtención del consentimiento de un **Postulante**:

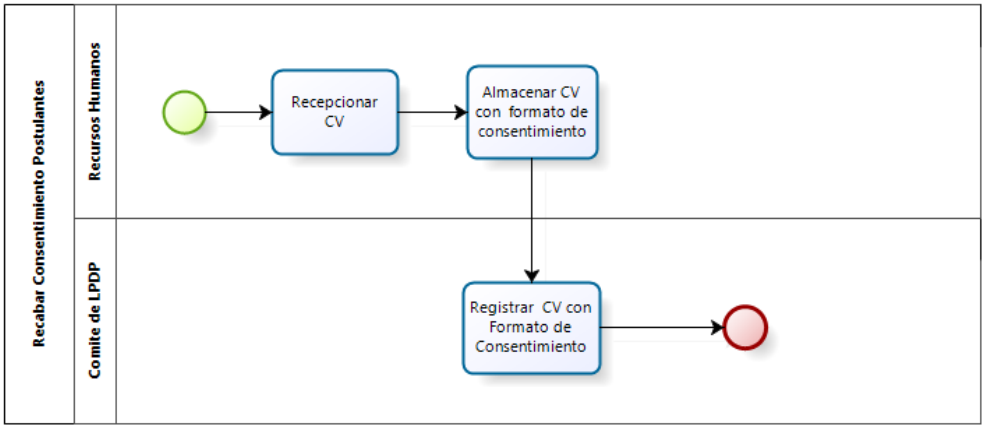


Figura 14 Obtención del Consentimiento de Postulante

Fuente: Elaboración Propia

Obtención del consentimiento de un **Cliente**:

a. Venta de Productos Finales en tienda virtual

En la tienda virtual los clientes estarán dando su consentimiento a través de una casilla de aceptación al momento de registrarse en la tienda, y que de esta forma sus datos sean almacenados y tratados por la empresa.

b. Venta de Productos en Tiendas

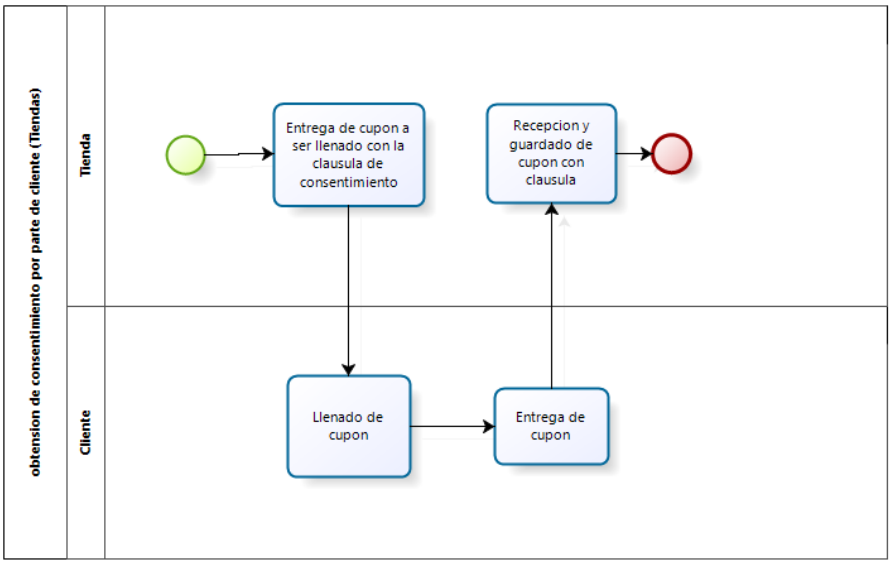


Figura 15 Obtención del Consentimiento de Cliente

Fuente: Elaboración Propia

Obtención del consentimiento de un **Proveedor**:

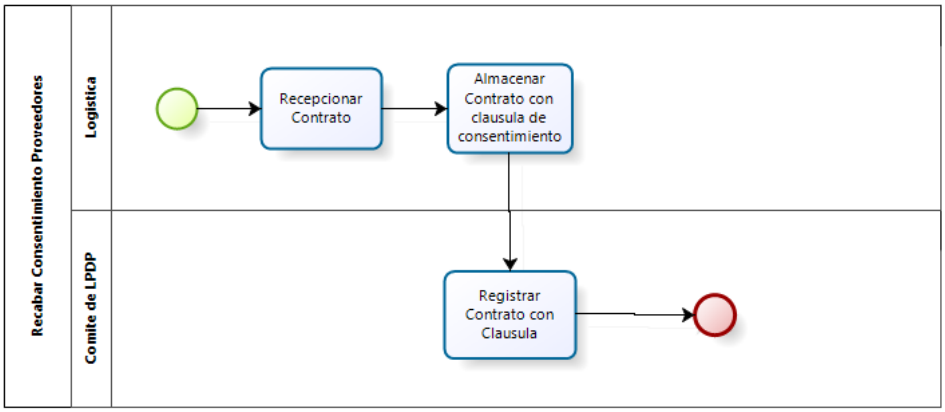


Figura 16 Obtención del Consentimiento de Proveedor

Fuente: Elaboración Propia

Obtención del consentimiento de **Visitantes y Video vigilancia**:

Al poner los anuncios fuera de cada sede y tienda de la empresa, se está aceptando el consentimiento de los visitantes como de los colaboradores para almacenar su información personal correspondiente a cada banco de datos.

e. Monitoreo continuo de la Metodología

Una de las tareas más importantes de la metodología es el monitoreo continuo porque el implementar la Ley de Protección de Datos Personales no es estática, por el contrario, debe realizarse una revisión y constante monitoreo de sus procesos y controles o medidas de seguridad adoptadas.

Por ello se recomienda realizarlo por lo menos 2 veces al año ejecutando el siguiente proceso:

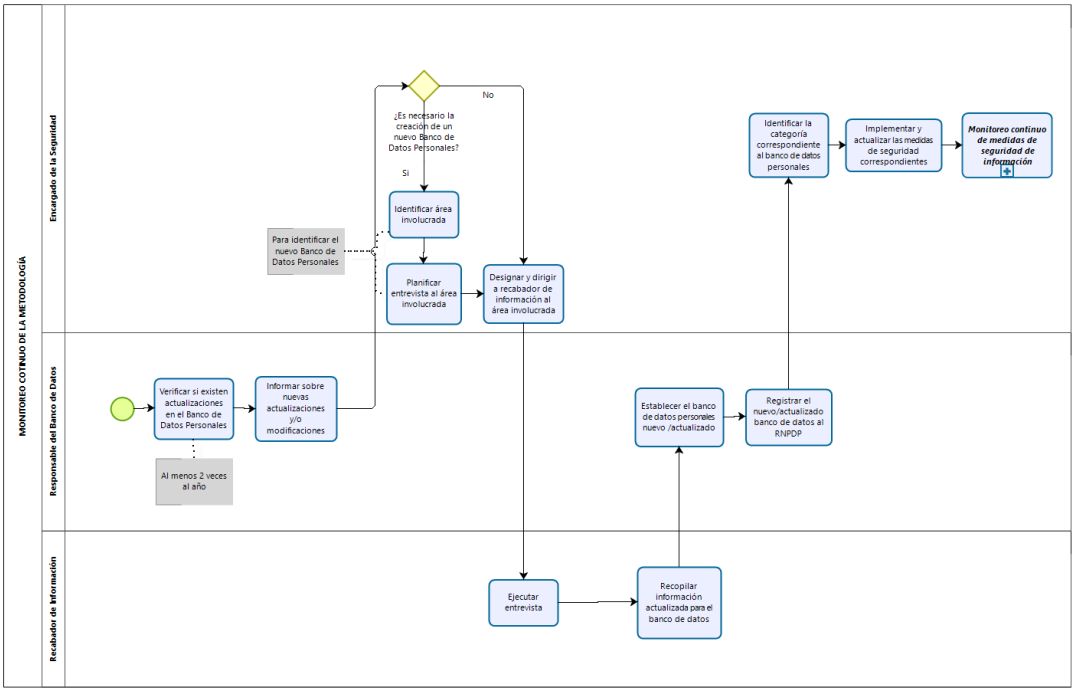


Figura 17 Monitoreo Continuo - Metodología

Fuente: Elaboración Propia

1. Primero, el Responsable del Banco de Datos debe verificar si existen actualizaciones.
2. Luego debe informar al encargado de seguridad de dichas actualizaciones o modificaciones.
3. El encargado de seguridad debe evaluar si es necesario la creación de un nuevo banco de datos personales.

   3.1 Si la respuesta es afirmativa, se tiene que identificar el nuevo banco de datos con la identificación del área involucrada y planificar una entrevista a la misma.

3.2 Caso contrario, continuar con el paso 4.

4. Designar y dirigir al recabador de información a dicha área.
5. El recabador de información ejecuta una entrevista y recopila información actualizada relevante para el banco de datos personales.
6. El responsable del banco de datos personales establece el nuevo y/o actualizado banco de datos y lo registra ante el Registro Nacional de Banco de Datos Personales.
7. El encargado de seguridad identifica la categoría correspondiente al nuevo y/o actualizado banco de datos para luego ejecutar medidas de seguridad que correspondan.
8. Continúa el proceso de Monitoreo continuo de medidas de seguridad de información

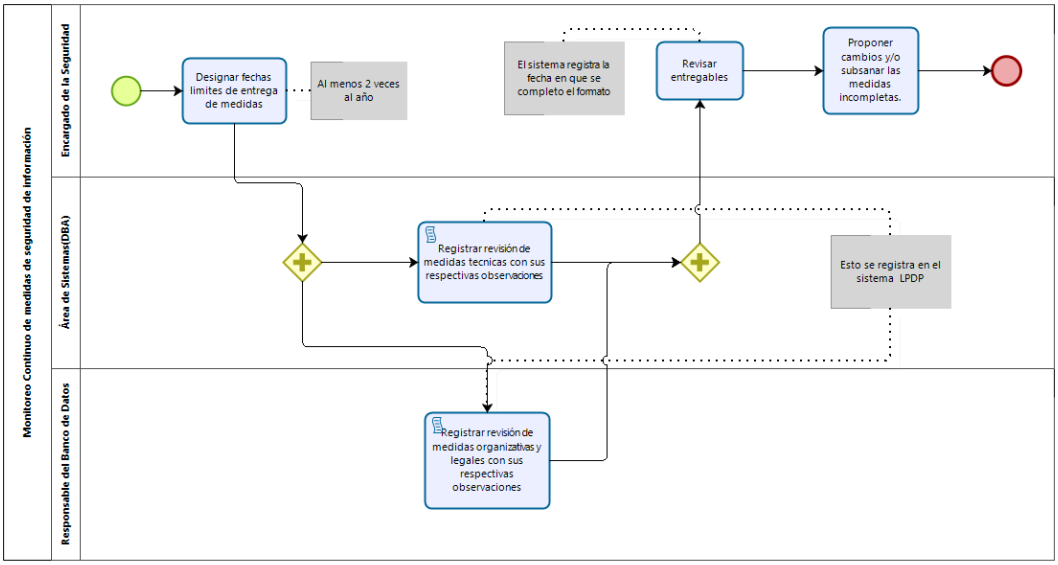


Figura 18 Monitoreo Continuo - Medidas de Seguridad de Información

Fuente: Elaboración Propia

9. El encargado de la seguridad de información debe designar fechas límites de entrega de medidas a los responsables de cada banco de datos.
10. El área de sistemas debe registrar la revisión de las medidas técnicas con sus respectivas observaciones.
11. Al mismo tiempo, los responsables de los bancos de datos también registran la revisión de sus medidas organizativas y legales con sus respectivas observaciones.

12. El encargado de la seguridad de información revisa los entregables y si corresponde propone cambios y/o solicita subsanar las medidas incompletas.

CAPITULO IV

4. RESULTADOS

En este capítulo se mostrará y explicará los resultados obtenidos en cada fase de la metodología propuesta.

Los resultados fueron los siguientes:

1. Plan General del Proyecto.
2. Resolución de Inscripción de los bancos de datos personales por parte de la Autoridad Nacional de Protección de Datos Personales.
3. Manual de Políticas y Procedimientos LPDP.
4. Formatos de Aceptación del Consentimiento.
5. Sistema web de control del cumplimiento de la LPDP.

4.1 PLAN GENERAL DEL PROYECTO

El resultado que se obtuvo de la primera fase de la metodología propuesta ha sido el Plan General del Proyecto, en el cual se especifica las tareas que se deben realizar durante todo el proceso de implementación de la metodología.

Tabla 32 *Plan General del* Proyecto

Nombre de tarea	Duración	Comienzo	Fin	Predecesor	Nombres de los recursos
Planeamiento	**28 días**	**lun 12/06/17**	**mié 19/07/17**		
Identificar el titular de los bancos de datos personales	3 días	lun 12/06/17	mié 14/06/17		
Reunión para determinar el alcance de la LPDP	3 días	jue 15/06/17	dom 18/06/17		Recolector 1; Recolector 2; Gerente de TI.
Identificar nombres de posibles bancos de datos	3 días	lun 19/06/17	mié 21/06/17	3	Recolector 1;Recolector 2
Definir responsables de áreas involucradas	2 días	jue 22/06/17	vie 23/06/17	4	Gerente de TI; Jefe Proyectos de TI[80%]
Elaborar cuadros de entrevistas	3 días	lun 26/06/17	mié 28/06/17	5	Jefe Proyectos de TI[80%];Recolector 1;Recolector 2
Listar software usado por la empresa	5 días	jue 29/06/17	mié 5/07/17	6	Recolector 1;Recolector 2
Definir plan de acción de recabadores	3 días	jue 6/07/17	lun 10/07/17	7	Recolector 1;Recolector 2
Definir y capacitar a recabadores	5 días	mar 11/07/17	lun 17/07/17	8	Gerente de TI; Jefe Proyectos de TI[80%]
Distribuir a los recabadores	2 días	mar 18/07/17	mié 19/07/17	9	Jefe Proyectos de TI[80%]
Recopilación y registro de datos	**159 días**	**jue 20/07/17**	**mar 27/02/18**	**1**	
Elaborar un listado de interrogantes a ejecutar	5 días	jue 20/07/17	mié 26/07/17	10	Recolector 1;Recolector 2
Definir el Comité de PDP	10 días	jue 27/07/17	mié 9/08/17	12	Gerente de TI; Jefe Proyectos de TI[80%];Recolector 1;Recolector 2

Definir responsabilidades de cada banco de datos	15 días	jue 10/08/17	mié 30/08/17	12	Gerente de TI; Jefe Proyectos de TI[80%];Recolector 1;Recolector 2
Recopilar listado de datos personales	60 días	jue 31/08/17	mié 22/11/17	14	Jefe Proyectos de TI[80%];Recolector 1;Recolector 2
Identificación de sistemas impactados	5 días	jue 23/11/17	mié 29/11/17	14	Jefe Proyectos de TI[80%];Recolector 1;Recolector 2
Establecimiento de la lista de banco de datos	7 días	jue 30/11/17	vie 8/12/17	16	Asesor Legal[30%];Gerente de TI; Jefe Proyectos de TI[80%];Recolector 1;Recolector 2
Registro de bancos de datos personales a la Autoridad Nacional de Protección de Datos Personales	57 días	lun 11/12/17	mar 27/02/18	17	Asesor Legal[30%];Gerente de TI
Elaboración y ejecución de procedimientos y políticas	**163 días**	**mar 12/12/17**	**jue 26/07/18**	**11**	
Identificar la categoría correspondiente de los Bancos de Datos	3 días	mar 12/12/17	jue 14/12/17	18	Jefe Proyectos de TI[80%];Recolector 1;Recolector 2
Definir medidas de seguridad a implementar por categoría	10 días	vie 15/12/17	jue 28/12/17	20	Jefe Proyectos de TI[80%];Recolector 1;Recolector 2
Establecer medidas de seguridad organizativas	30 días	vie 29/12/17	jue 8/02/18	21	Jefe Proyectos de TI[80%];Recolector 1;Recolector 2
Establecer medidas de seguridad legales	30 días	vie 9/02/18	jue 22/03/18	22	Recolector 1;Recolector 2;Asesor Legal[30%];Gerente de TI

Establecer medidas de seguridad técnicas	60 días	vie 23/03/18	jue 14/06/18	23	Gerente de TI; Jefe Proyectos TI[80%];Recolector 1;Recolector 2
Establecer el nuevo proceso para los derechos ARCO	30 días	vie 15/06/18	jue 26/07/18	24	Recolector 1;Recolector 2
Recabación de consentimiento	**70 días**	**vie 27/07/18**	**jue 1/11/18**	**19**	
Identificar al personal Recolector	3 días	vie 27/07/18	mar 31/07/18	25	Gerente de TI; Recolector 1;Recolector 2
Capacitar al personal Recolector	7 días	mié 1/08/18	jue 9/08/18	27	Gerente de TI; Recolector 1;Recolector 2
Establecer procedimientos para la obtención del consentimiento	15 días	vie 10/08/18	jue 30/08/18	28	Recolector 1;Recolector 2;Jefe Proyectos de TI[80%]
Recabar los consentimientos	15 días	vie 31/08/18	jue 20/09/18	29	Asesor Legal[30%];Gerente de TI; Jefe Proyectos de TI[80%];Recolector 1;Recolector 2
Monitoreo continuo	30 días	vie 21/09/18	jue 1/11/18		Gerente de TI; Jefe Proyectos de TI[80%];Asesor Legal[30%]

Fuente: Elaboración Propia

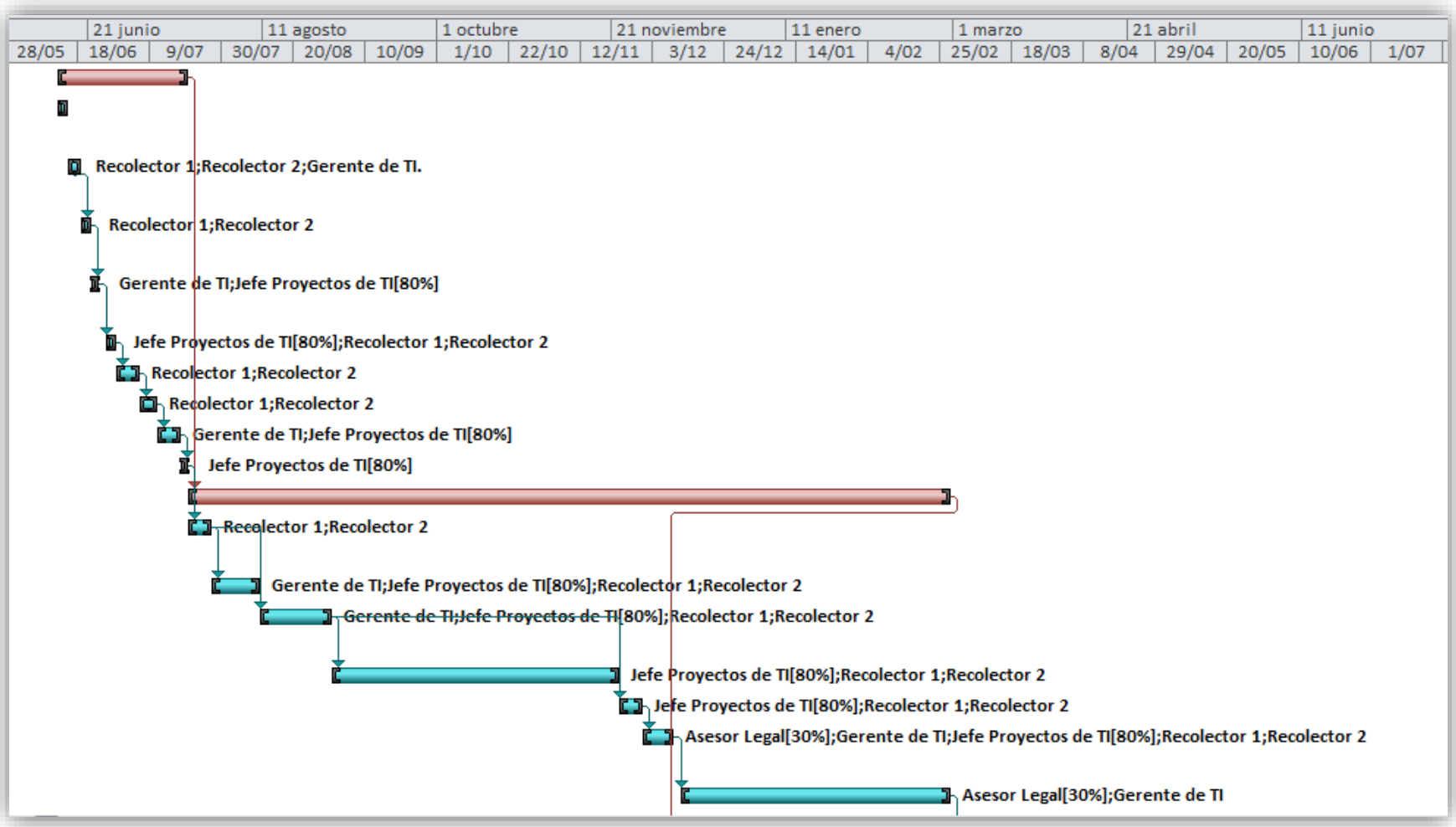


Figura 19 Diagrama de Gantt del Plan General del Proyecto 1

Fuente: Elaboración Propia

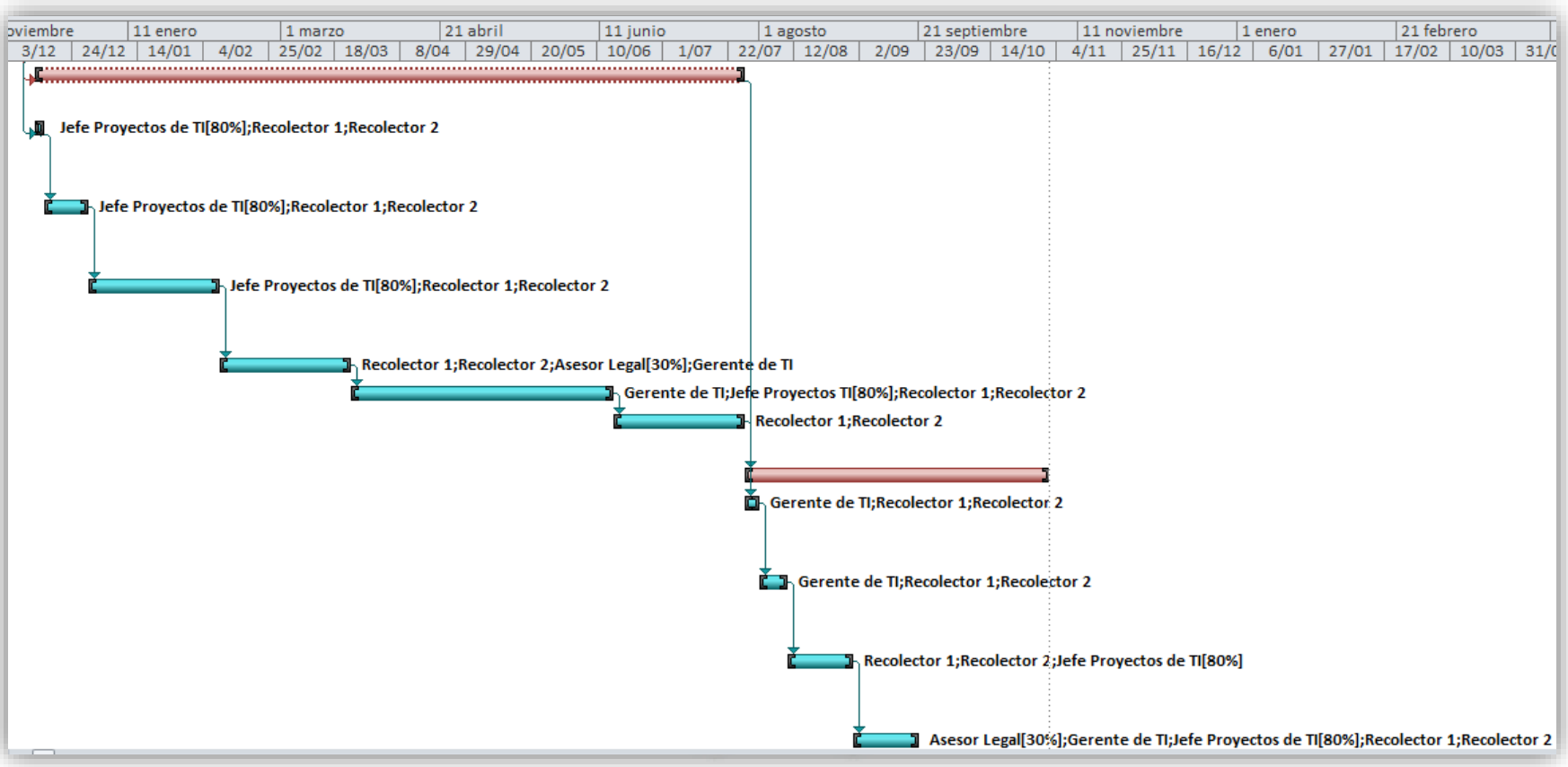


Figura 20 Diagrama de Gantt del Plan General del Proyecto 2

Fuente: Elaboración Propia

4.2 RESOLUCIÓN DE INSCRIPCIÓN DE LOS BANCOS DE DATOS PERSONALES

REPÚBLICA DEL PERÚ

Resolución Directoral

RESOLUCION N.° 3176-2018-JUS/DGTAIPD-DPDP

EXPEDIENTE N° 2001-2018-PJ

Lima, 30 de noviembre de 2018.

VISTO: El documento con registro n.° 69385 que contiene la solicitud de inscripción del banco de datos personales de administración privada presentado el 05 de noviembre de 2018 por la persona jurídica denominada **MICHELL Y CIA S.A.**

CONSIDERANDO:

Que, el artículo 34 de la Ley n.° 29733, Ley de Protección de Datos Personales, crea el Registro Nacional de Protección de Datos Personales como registro de carácter administrativo a cargo de la Autoridad Nacional de Protección de Datos Personales, con la finalidad de inscribir en forma diferenciada a nivel nacional los bancos de datos personales de administración pública o privada;

Que, el artículo 78 del Reglamento de la Ley n.° 29733, aprobado mediante el Decreto Supremo n.° 003-2013-JUS, dispone que las personas naturales o jurídicas del sector privado o entidades públicas que creen, modifiquen o cancelen bancos de datos personales están obligadas a tramitar la inscripción de éstos ante el Registro Nacional de Protección de Datos Personales;

M. GONZALEZ I.

Que, si bien se observa que no presenta el documento que acredita que la persona que solicita la inscripción cuente con facultades para representar a la sociedad ante la administración pública, conforme a lo establecido por el Decreto Legislativo n.° 1246[1], en tanto se implemente la interoperabilidad, se dará por cumplido el requisito señalado en el artículo 81 del Reglamento de la LPDP, con la declaración de la administrada en el formulario de inscripción; por consiguiente, debe procederse a la emisión del acto administrativo de inscripción;

De conformidad con lo dispuesto por la Ley n.° 29733, Ley de Protección de Datos Personales, su reglamento aprobado por el Decreto Supremo n.° 003-2013-JUS y el Texto Único de Procedimientos Administrativos – TUPA del Ministerio de Justicia y Derechos Humanos, aprobado por Decreto Supremo n.° 018-2013-JUS;

[1] Decreto Legislativo n.° 1246
Artículo 3.- Implementación progresiva de la interoperabilidad en beneficio del ciudadano.
(...)
3.2 La información de los usuarios y administrados que las entidades de la Administración Pública deben proporcionar a las entidades del Poder Ejecutivo de manera gratuita es:
Identificación y estado civil.
(...)
Vigencia de poderes y designación de representantes legales.
(...)
3.3 En tanto se implemente la interoperabilidad, la información y documentos mencionados en el numeral 3.2 precedente podrán ser sustituidos, a opción del administrado o usuario, por declaración jurada, conforme a lo establecido en la Ley n.° 27444, Ley de Procedimiento Administrativo General.

Página 1 de 3

Figura 21 Resolución de Inscripción de los Bancos de Datos Personales de MICHELL Y CIA S.A.

Fuente: Ministerio de Justicia (2019)

Artículo 1°.- Inscribir el banco de datos personales cuyos datos son los siguientes:

Nombre / Razón Social:	**MICHELL Y CIA S.A.**
Número de RUC:	20100192650
Datos del representante:	Mauricio Luis Martin Chirinos Chirinos
Código:	**RNPDP-PJP N° 15264.**
Denominación:	COLABORADORES
Dirección a efectos de notificación:	Calle Juan de la Torre n.° 101, San Lázaro, Arequipa. lpdp_michell@michell.com.pe
Finalidad:	Recopilar los datos personales de los colaboradores para evaluar el desempeño, elaborar planillas, otorgar beneficios y cumplir las obligaciones establecidos por ley.
Usos previstos:	Recursos humanos; prevención de riesgos laborales; cumplimiento/incumplimiento de obligaciones dinerarias; servicios financieros y de seguros; análisis de perfiles; fines estadísticos, históricos o científicos; gestión de listas de miembros de sindicatos; gestión de listas de asociados; actividades asociativas, culturales, recreativas y deportivas; actividades profesionales; videovigilancia; seguridad y control de acceso a edificios; gestión de comisiones del colaborador; capacitaciones e inducciones.
Sistema de tratamiento:	Automatizado y no automatizado.
Dirección para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.	Calle Juan de la Torre n.° 101, San Lázaro, Arequipa. lpdp_michell@michell.com.pe
Tipos de datos personales:	Datos de carácter identificativo: Nombres y apellidos, n. ° DNI, n. ° RUC, n. ° de Pasaporte, dirección del domicilio, teléfono, dirección de correo electrónico, imagen, firma, n.° brevete, n.° carnet de extranjería, libreta militar, n.° carnet seguro de salud, código interno del colaborador. Datos de características personales: Estado civil, fecha de nacimiento, nacionalidad, sexo, profesión, edad, datos académicos, datos de derechohabientes (nombre, edad, sexo y n.° de hijos), datos de persona de contacto, grado de instrucción. Datos económicos-financieros y de seguros: Créditos, préstamos, avales, datos bancarios, historial de créditos, información tributaria, seguros, planes de pensiones/jubilación, deudas. Datos de carácter social: Aficiones a clubes o asociaciones, características de vivienda. Datos sensibles: Características físicas (grupo sanguíneo, talla de zapato, peso, estatura), información relativa a la salud física o mental (accidente y diagnóstico), vida sexual, vida afectiva o familiar, afiliación sindical, huella digital, reconocimiento facial.
Procedimientos de obtención:	Fuente: Del titular del dato personal o su representante legal, fuentes de acceso al público, entidad privada, entidad pública. Soporte: Papel, informático/magnético, vía telemática.

M. GONZALEZ I.

Página **2** de **3**

Figura 22 Resolución de Inscripción del Banco de Datos Personales COLABORADORES

Fuente: Ministerio de Justicia (2019)

SE RESUELVE:

Artículo 1°.- Inscribir el banco de datos personales cuyos datos son los siguientes:

Nombre / Razón Social:	**MICHELL Y CIA S.A.**
Número de RUC:	20100192650
Datos del representante:	Mauricio Luis Martin Chirinos Chirinos
Código:	**RNPDP-PJP N° 15263.**
Denominación:	POSTULANTES
Dirección a efectos de notificación:	Calle Juan de la Torre n.° 101, San Lázaro, Arequipa. lpdp_michell@michell.com.pe
Finalidad:	Recopilar los datos personales de los postulantes para realizar la evaluación, verificar que cumpla con el perfil determinado y realizar el proceso de reclutamiento.
Usos previstos:	Recursos humanos; análisis de perfiles; actividades asociativas, culturales, recreativas y deportivas; actividades profesionales; educación.
Sistema de tratamiento:	Automatizado y no automatizado.
Dirección para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.	Calle Juan de la Torre n.° 101, San Lázaro, Arequipa. lpdp_michell@michell.com.pe
Tipos de datos personales:	Datos de carácter identificativo: Nombres y apellidos, n. ° DNI, n. ° RUC, n. ° de Pasaporte, dirección del domicilio, teléfono, dirección de correo electrónico, imagen, firma, carnet de extranjería. Datos de características personales: Estado civil, fecha de nacimiento, nacionalidad, sexo, profesión, edad, datos académicos. Datos de carácter social: Aficiones y hábitos personales.
Procedimientos de obtención:	Fuente: Del titular del dato personal o su representante legal, fuentes de acceso al público, entidad privada. Soporte: Papel, informático/magnético, vía telemática. Procedimiento: Formularios, transmisión electrónica, transmisión física, entrevistas personales.
Ubicación física del banco de datos:	Calle Juan de la Torre n.° 101, San Lázaro, Arequipa.
Receptores de los datos personales a nivel nacional:	Indica que no realiza transferencia de datos personales a nivel nacional.
Receptores de flujo transfronterizo:	Indica que no realiza transferencia de datos personales a nivel internacional.
Medidas de seguridad:	Sobre medidas de seguridad indica lo siguiente: No cuenta con un documento de gestión de accesos, gestión de privilegios y revisión periódica de privilegios. Existe un responsable de seguridad del banco de datos.

Dirección de Protección de Datos Personales

M. GONZALEZ I

Página **2** de **3**

Figura 23 Resolución de Inscripción del Banco de Datos Personales POSTULANTES

Fuente: Ministerio de Justicia (2019)

SE RESUELVE:

Artículo 1°.- Inscribir el banco de datos personales cuyos datos son los siguientes:

Nombre / Razón Social:	**MICHELL Y CIA S.A.**
Número de RUC:	20100192650
Datos del representante:	Mauricio Luis Martin Chirinos Chirinos
Código:	**RNPDP-PJP N° 15261.**
Denominación:	CLIENTES
Dirección a efectos de notificación:	Calle Juan de la Torre n.° 101, San Lázaro, Arequipa. lpdp_michell@michell.com.pe
Finalidad:	Recopilar los datos personales de los clientes para realizar ventas, entregar productos terminados y enviar correos electrónicos.
Usos previstos:	Gestión económica y contable de clientes; prestación de servicios de solvencia patrimonial y crédito; cumplimiento/incumplimiento de obligaciones dinerarias; servicios financieros y de seguros; gestión de listas de clientes; análisis de perfiles; publicidad y prospección comercial; fines estadísticos, históricos o científicos; comercio electrónico.
Sistema de tratamiento:	Automatizado y no automatizado.
Dirección para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.	Calle Juan de la Torre n.° 101, San Lázaro, Arequipa. lpdp_michell@michell.com.pe
Tipos de datos personales:	Datos de carácter identificativo: Nombres y apellidos, n. ° DNI, n. ° RUC, n. ° de Pasaporte, dirección del domicilio, teléfono, dirección de correo electrónico, firma, n.° Fax, código de cliente. Datos de características personales: Nacionalidad, sexo, edad, datos de persona de contacto, país de residencia, ciudad de residencia, código postal. Datos económicos-financieros y de seguros: Créditos, préstamos, avales, datos bancarios, historial de créditos, seguros, deudas.
Procedimientos de obtención:	Fuente: Del titular del dato personal o su representante legal, fuentes de acceso al público, entidad privada, entidad pública. Soporte: Papel, informático/magnético, vía telemática. Procedimiento: Formularios, transmisión electrónica, transmisión física, telemarketing, referencias comerciales, cupones de descuento.
Ubicación física del banco de datos:	Calle Juan de la Torre n.° 101, San Lázaro, Arequipa.
Receptores de los datos personales a nivel nacional:	Indica que realiza transferencia de datos personales a nivel nacional a organizaciones o personas directamente relacionadas, empresas del grupo empresarial, administración tributaria, empresas de courier.

M. GONZALEZ L.

Página **2** de **3**

Figura 24 Resolución de Inscripción del Banco de Datos Personales CLIENTES

Fuente: Ministerio de Justicia (2019)

SE RESUELVE:

Artículo 1°.- Inscribir el banco de datos personales cuyos datos son los siguientes:

Nombre / Razón Social:	**MICHELL Y CIA S.A.**
Número de RUC:	20100192650
Datos del representante:	Mauricio Luis Martin Chirinos Chirinos
Código:	**RNPDP-PJP Nº 15262.**
Denominación:	PROVEEDORES
Dirección a efectos de notificación:	Calle Juan de la Torre n.° 436, Arequipa. lpdp_michell@michell.com.pe
Finalidad:	Recopilar los datos personales de los proveedores para realizar la cotización y adquisición de los requerimientos de la empresa.
Usos previstos:	Cumplimiento/incumplimiento de obligaciones dinerarias; análisis de perfiles; fines estadísticos, históricos o científicos; gestión de listas de asociados; gestión económica y contable de proveedores; compra de materiales y maquinaria para la fabricación de los productos; gestión de listas de proveedores.
Sistema de tratamiento:	Automatizado y no automatizado.
Dirección para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.	Calle Juan de la Torre n.° 101, San Lázaro, Arequipa. lpdp_michell@michell.com.pe
Tipos de datos personales:	Datos de carácter identificativo: Nombres y apellidos, n. ° DNI, n. ° RUC, dirección del domicilio, teléfono, dirección de correo electrónico, firma, carnet de proveedor, n. ° Fax. Datos de características personales: Fecha de nacimiento, nacionalidad, sexo, datos de persona de contacto. Datos económicos-financieros y de seguros: Datos bancarios.
Procedimientos de obtención:	Fuente: Del titular del dato personal o su representante legal, fuentes de acceso al público, entidad pública. Soporte: Papel, informático/magnético, vía telemática. Procedimiento: Transmisión electrónica, transmisión física, entrevistas personales, referencias comerciales.
Ubicación física del banco de datos:	Calle Jacinto Ibañez n.° 436, Arequipa.
Receptores de los datos personales a nivel nacional:	Indica que realiza transferencia de datos personales a nivel nacional a organizaciones o personas directamente relacionadas, empresas del grupo empresarial, administración tributaria.
Receptores de flujo transfronterizo:	Indica que no realiza transferencia de datos personales a nivel internacional.

Dirección de Protección de Datos Personales

A. GONZALEZ I.

Página **2** de **3**

Figura 25 Resolución de Inscripción del Banco de Datos Personales PROVEEDORES

Fuente: Ministerio de Justicia (2019)

SE RESUELVE:

Artículo 1°.- Inscribir el banco de datos personales cuyos datos son los siguientes:

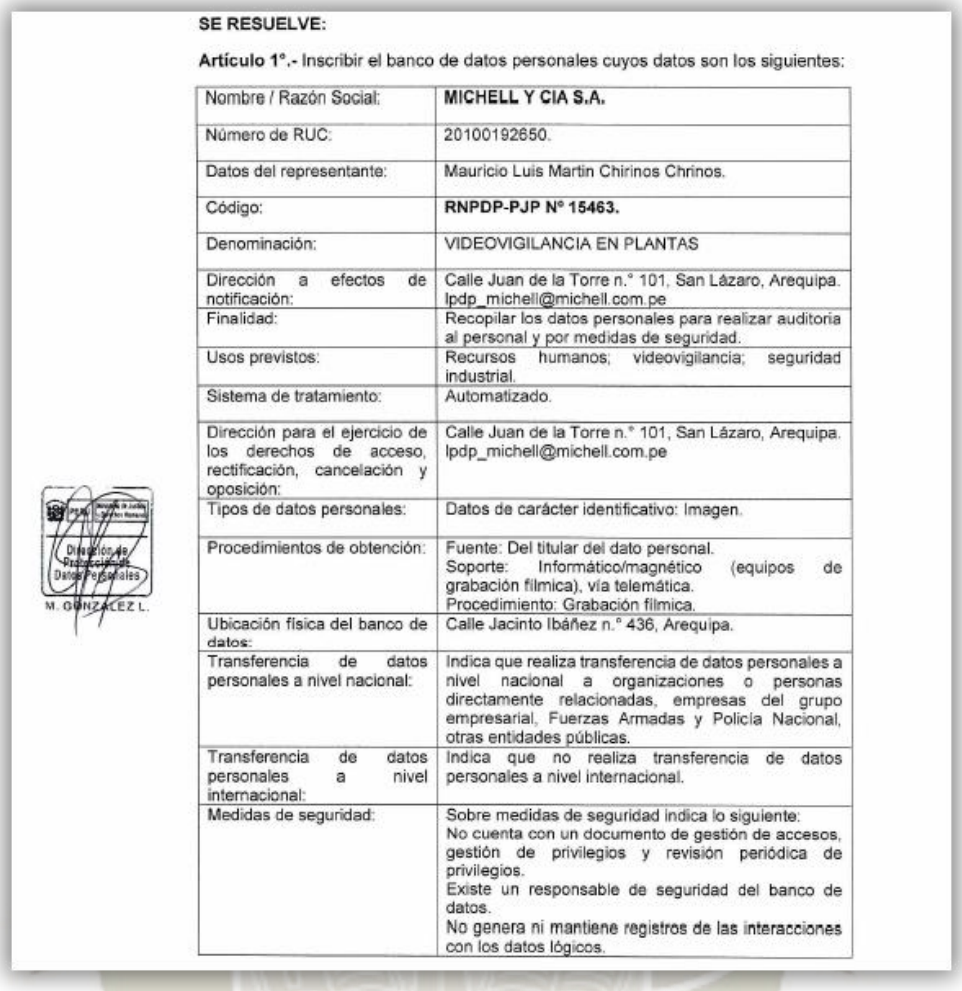
Nombre / Razón Social:	**MICHELL Y CIA S.A.**
Número de RUC:	20100192650
Datos del representante:	Mauricio Luis Martin Chirinos Chirinos
Código:	**RNPDP-PJP N° 15265.**
Denominación:	VISITANTES
Dirección a efectos de notificación:	Calle Juan de la Torre n.° 101, San Lázaro, Arequipa. lpdp_michell@michell.com.pe
Finalidad:	Recopilar los datos personales de los visitantes para controlar el acceso a las instalaciones de la empresa por motivo de seguridad.
Usos previstos:	Seguridad y control de acceso a edificios.
Sistema de tratamiento:	No automatizado.
Dirección para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.	Calle Juan de la Torre n.° 101, San Lázaro, Arequipa. lpdp_michell@michell.com.pe
Tipos de datos personales:	Datos de carácter identificativo: Nombres y apellidos, n. ° DNI, n. ° RUC, n. ° de Pasaporte, firma, carnet de extranjería.
Procedimientos de obtención:	Fuente: Del titular del dato personal. Soporte: Papel. Procedimiento: Transmisión física (Recepción de documentos de identidad).
Ubicación física del banco de datos:	Calle Juan de la Torre n.° 101, San Lázaro, Arequipa.
Receptores de los datos personales a nivel nacional:	Indica que no realiza transferencia de datos personales a nivel nacional.
Receptores de flujo transfronterizo:	Indica que no realiza transferencia de datos personales a nivel internacional.
Medidas de seguridad:	Sobre medidas de seguridad indica lo siguiente: No cuenta con un documento de gestión de accesos, gestión de privilegios y revisión periódica de privilegios. Existe un responsable de seguridad del banco de datos. No genera ni mantiene registros de las interacciones con los datos lógicos. Ha implementado medidas de seguridad en los ambientes donde realiza el tratamiento de los datos personales. Ha implementado procedimientos para impedir la generación de copias o la reproducción de documentos al personal no autorizado. No ha implementado mecanismos de respaldo de seguridad de la información del banco de datos personales.

M. GONZALEZ I.

Página **2** de **3**

Figura 26 Resolución de Inscripción del Banco de Datos Personales VISITANTES

Fuente: Ministerio de Justicia (2019)



SE RESUELVE:

Artículo 1°.- Inscribir el banco de datos personales cuyos datos son los siguientes:

Nombre / Razón Social:	**MICHELL Y CIA S.A.**
Número de RUC:	20100192650.
Datos del representante:	Mauricio Luis Martin Chirinos Chrinos.
Código:	**RNPDP-PJP N° 15463.**
Denominación:	VIDEOVIGILANCIA EN PLANTAS
Dirección a efectos de notificación:	Calle Juan de la Torre n.° 101, San Lázaro, Arequipa. lpdp_michell@michell.com.pe
Finalidad:	Recopilar los datos personales para realizar auditoria al personal y por medidas de seguridad.
Usos previstos:	Recursos humanos; videovigilancia; seguridad industrial.
Sistema de tratamiento:	Automatizado.
Dirección para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición:	Calle Juan de la Torre n.° 101, San Lázaro, Arequipa. lpdp_michell@michell.com.pe
Tipos de datos personales:	Datos de carácter identificativo: Imagen.
Procedimientos de obtención:	Fuente: Del titular del dato personal. Soporte: Informático/magnético (equipos de grabación filmica), vía telemática. Procedimiento: Grabación filmica.
Ubicación física del banco de datos:	Calle Jacinto Ibáñez n.° 436, Arequipa.
Transferencia de datos personales a nivel nacional:	Indica que realiza transferencia de datos personales a nivel nacional a organizaciones o personas directamente relacionadas, empresas del grupo empresarial, Fuerzas Armadas y Policía Nacional, otras entidades públicas.
Transferencia de datos personales a nivel internacional:	Indica que no realiza transferencia de datos personales a nivel internacional.
Medidas de seguridad:	Sobre medidas de seguridad indica lo siguiente: No cuenta con un documento de gestión de accesos, gestión de privilegios y revisión periódica de privilegios. Existe un responsable de seguridad del banco de datos. No genera ni mantiene registros de las interacciones con los datos lógicos.

Dirección de Protección de Datos Personales

M. GONZALEZ L.

Figura 27 Resolución de Inscripción del Banco de Datos Personales VIDEOVIGILANCIA EN PLANTAS

Fuente: Ministerio de Justicia (2019)

SE RESUELVE:

Artículo 1°.- Inscribir el banco de datos personales cuyos datos son los siguientes:

Nombre / Razón Social:	**MICHELL Y CIA S.A.**
Número de RUC:	20100192650.
Datos del representante:	Mauricio Luis Martin Chirinos Chrinos.
Código:	**RNPDP-PJP N° 15464.**
Denominación:	VIDEOVIGILANCIA – SOL ALPACA.
Dirección a efectos de notificación:	Calle Juan de la Torre n.° 101, San Lázaro, Arequipa. lpdp_michell@michell.com.pe
Finalidad:	Recopilar los datos personales para realizar auditoria al personal y por medidas de seguridad.
Usos previstos:	Recursos humanos; videovigilancia; prevención de robos y seguridad.
Sistema de tratamiento:	Automatizado.
Dirección para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición:	Calle Juan de la Torre n.° 101, San Lázaro, Arequipa. lpdp_michell@michell.com.pe
Tipos de datos personales:	Datos de carácter identificativo: Imagen.
Procedimientos de obtención:	Fuente: Del titular del dato personal. Soporte: Informático/magnético (equipos de grabación filmica), vía telemática. Procedimiento: Grabación filmica.
Ubicación física del banco de datos:	Calle Juan de la Torre n.° 101, Arequipa
Transferencia de datos personales a nivel nacional:	Indica que realiza transferencia de datos personales a nivel nacional a organizaciones o personas directamente relacionadas, Fuerzas Armadas y Policía Nacional, otras entidades públicas.
Transferencia de datos personales a nivel internacional:	Indica que no realiza transferencia de datos personales a nivel internacional.
Medidas de seguridad:	Sobre medidas de seguridad indica lo siguiente: No cuenta con un documento de gestión de accesos, gestión de privilegios y revisión periódica de privilegios.

Dirección de Protección de Datos Personales
M. GONZALEZ L.

Página **2** de **3**

Figura 28 Resolución de Inscripción del Banco de Datos Personales VIDEOVIGILANCIA - SOL ALPACA

Fuente: Ministerio de Justicia (2019)

4.3 MANUAL DE POLÍTICAS Y PROCEDIMIENTOS LPDP

En la fase de Elaboración y Ejecución de políticas y procedimientos se adecuaron los procedimientos y políticas de seguridad de la empresa a la normativa de la LPDP, obteniendo como resultado final el "Manual de Políticas y Procedimientos LPDP".

Este documento se llevó a cabo a través de la evaluación de tres diferentes tipos de medidas de seguridad: organizativas, legales y técnicas, y está compuesto por los resultados obtenidos de cada una de ellas, además de la elaboración del formato para ejercer los derechos ARCO y el formato de respuesta.

4.3.1 Medidas Organizativas

Como resultado de la evaluación de las medidas organizativas en la empresa tenemos los siguientes:

5. Política de Protección de Datos Personales
6. Aviso de Privacidad de los Bancos de Datos Personales para la Empresa Michell y Cía. S.A.
7. Adecuación de los procesos de negocio involucrados en el tratamiento de datos personales a la Ley N°29733.

POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

I. ALCANCE

La presente "Política de Protección de Datos Personales" se aplica a toda actividad de tratamiento de datos personales realizada por parte de ***MICHELL Y CIA S.A.*** *(en adelante "Michell").*

II. CONCEPTOS RELACIONADOS

*"**Banco de datos**" Es el conjunto de datos, de informaciones que son agrupadas y mantenidas en un mismo soporte a modo de facilitar su acceso.*

*"**Datos Personales**" Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.*

*"**Datos Sensibles**": Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones, o convicciones políticas, religiosas, filosóficas o morales, afiliación sindical e información relacionada a la salud o a la vida sexual.*

*"**Encargado**": La persona natural o jurídica, pública o privada que por sí misma realiza el Tratamiento de datos personales.*

*"**Titular**": La persona a quien corresponden los datos Personales que son objeto de Tratamiento.*

*"**Transferencia**": Es la transmisión o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta del titular de datos personales.*

*"**Tratamiento**": Cualquier operación(automatizada o no) que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.*

*"**ANPDP**": Autoridad Nacional de Protección de Datos Personales.*

La Política deberá ser revisada por lo menos cada 2 años.

Michell se reserva el derecho de actualizar el contenido de la Política sin previo aviso con el fin de reflejar cualquier cambio legislativo, técnico o de la industria.

II. OBJETIVO

Dar a conocer nuestro compromiso con la protección de datos personales, así como explicar cómo se tratan y protegen los datos personales que sean recolectados, dándote la seguridad de que tus datos serán almacenados de manera segura.

III. FINALIDAD DEL TRATAMIENTO DE LOS DATOS PERSONALES

Michell realiza tratamiento de datos personales de colaboradores, postulantes, clientes, proveedores y de todas aquellas personas que guardan relación con nuestra empresa, con la finalidad de cumplir con la legislación vigente, así como cualquier otra finalidad lícita previamente informada a los titulares de datos personales.

IV. PRINCIPIOS RECTORES

Michell tiene el compromiso de respetar los principios rectores establecidos en la Ley de Protección de Datos Personales. Estos son:

Principio de legalidad: Está prohibida la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos.

Principio de consentimiento: Se debe contar con el consentimiento del titular antes de efectuar un tratamiento con sus datos personales.

Principio de finalidad: Los datos personales serán recopilados para una finalidad determinada, explícita y lícita, y su tratamiento no debe extenderse a otra finalidad.

Principio de proporcionalidad: El tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.

Principio de calidad: Los datos personales que vayan a ser tratados deben ser veraces, exactos y, en la medida de lo posible, actualizada, necesaria, pertinente y adecuada respecto de la finalidad para la que fueron recopilados.

Principio de seguridad: El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales.

Principio de disposición de recurso: El titular de datos personales debe contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales.

Principio de nivel de protección adecuado: Para el flujo transfronterizo de datos personales, se debe garantizar un nivel suficiente de protección para los datos personales que se vayan a tratar o, por lo menos, equiparable a lo previsto por la Ley de Protección de Datos Personales o por los estándares internacionales en la materia (Ministerio de Justicia y Derechos Humanos, 2011b).

V. CONSENTIMIENTO

Michell requiere del consentimiento libre, previo, expreso, inequívoco e informado del titular de los datos personales.

Michell no requiere consentimiento para tratar sus datos personales obtenidos de fuentes accesibles al público, gratuitas o no; así mismo, podrá tratar sus datos personales o de fuentes no públicas, siempre que dichas fuentes cuenten con su consentimiento para tratar y transferir dichos datos personales.

VI. TRANSFERENCIA DE DATOS PERSONALES

Michell podrá transferir local e internacionalmente datos personales a empresas de Michell y Cía. para cualquiera de las finalidades indicadas en el punto III de la presente Política.

Michell podrá transferir datos personales a entidades públicas legalmente facultadas dentro del cumplimiento de la normativa vigente o futura o por requerimiento de éstas.

VII. DERECHOS DE LOS TITULARES

El Titular de los datos o representantes de menores de edad podrán efectuar las siguientes solicitudes:

Derecho a la Información:

La finalidad para la que sus datos son recopilados.

Qué personas son o serán sus destinatarios.

Identidad del titular del banco de datos personales.

Domicilio del titular del banco de datos personales.

Tipo de transferencia de sus datos personales.

Las consecuencias de proveer sus datos personales y de su negativa a hacerlo.

El tiempo de almacenamiento o conservación de los datos personales.

Derecho de Acceso:

Conocer la información que sobre sí mismo forma parte del tratamiento en bancos de datos.

Método o procedimiento en que sus datos fueron recopilados.

Motivo de su recopilación.

Quién solicitó su recopilación.

Transferencias de su información realizadas.

Derecho de rectificación, cancelación y oposición:

Cuando se llevó a cabo una omisión, error o falsedad.

Cuando ya no sean necesarios para ejecutar la finalidad para la cual hayan sido recopilados.

Cuando vence el plazo establecido para su tratamiento.

La solicitud de rectificación debe ser presentada junto a la documentación que lo sustente.

VIII. PROCEDIMIENTO PARA EL EJERCICIO DE LOS DERECHOS ARCO

Los Titulares podrán ejercer sus derechos ARCO o revocar el consentimiento dado, únicamente con la presentación de su DNI u otro documento oficial de identidad y llenando el Formato de Derechos ARCO.

El Titular primero deberá enviar un correo electrónico a LPDP@michell.com.pe indicando que desea realizar un reclamo.

El Comité de Protección de Datos personales reenviará un correo con un link, el cual re direccionará a un Formulario de Derechos Arco virtual.

***Nota:** Todos los Titulares deberán escanear su DNI u otro documento oficial de identidad. Y en caso que el titular del dato personal requiera ejercer sus derechos mediante un representante, éste deberá presentar carta poder legalizada por notario público escaneado que lo faculte como tal y su documento de identidad escaneado.*

Nota: *La atención de las solicitudes y reclamos, por parte de los titulares de los datos personales, debe considerar los siguientes plazos:*

Información	*10 días contados desde el día siguiente de la presentación de la solicitud.*
Acceso	*20 días contados desde el día siguiente de la presentación de la solicitud.*
Rectificación, Cancelación y Oposición.	*10 días contados desde el día siguiente de la presentación de la solicitud.*
Tutela de derechos. (APDP).	*15 días contados desde la notificación de la solicitud por parte de la APDP (Autoridad de Protección de Datos Personales).*

IX. PLAZO DEL TRATAMIENTO DE DATOS PERSONALES

Los datos personales tratados por Michell serán almacenados durante el tiempo que sea necesario y cumpliendo los fines previstos en la presente Política.

X. SEGURIDAD DE LOS DATOS PERSONALES

Michell adopta las medidas jurídicas, organizativas y técnicas adecuadas para garantizar la seguridad de los datos personales, evitando su alteración, pérdida, tratamiento indebido o acceso no autorizado.

Michell cuenta con los recursos humanos y tecnológicos necesarios para cumplir con el objetivo, aplicándolos en proporción a la naturaleza de los datos almacenados y los riesgos a los que se encuentran expuestos.

XI. ACTUALIZACIONES

La presente política puede cambiar o actualizarse periódicamente; por lo que te pedimos la revises constantemente y puedas conocer la última versión que rige el tratamiento de tus datos personales.

AVISO DE PRIVACIDAD DE LOS BANCOS DE DATOS PERSONALES PARA LA EMPRESA MICHELL Y CIA S.A.

De acuerdo a la ***Ley N° 29733, Ley de Protección de Datos Personales y su norma reglamentaria D.S. y N° 003-2013-JUS****, se genera el siguiente Aviso de Privacidad para los Colaboradores, Clientes, Postulantes, Proveedores y Visitantes de la empresa:*

I. IDENTIDAD DE LA EMPRESA

Michell & Cía. S.A (en adelante "Michell") es una empresa textil con domicilio en Calle Juan de La Torre- 101, San Lázaro, Arequipa, Perú.

Michell es responsable y encargado de la obtención, divulgación, almacenamiento y uso de los datos personales que recopile de sus Colaboradores, Postulantes, Clientes, Proveedores y Visitantes. (en adelante los "Titulares").

II. DATOS PERSONALES RECABADOS

Los datos personales que Michell recaba de los Titulares son de manera enunciativa, mas no limitativa.

Además, son recabados mediante vía telefónica, por correo electrónico, por la página web de la empresa y personalmente.

III. TRATAMIENTO DE LOS DATOS PERSONALES

Los Datos Personales proporcionados a la Empresa, son usados para cumplir con los requisitos legales y contractuales, para llevar un registro adecuado del personal, clientes, proveedores y visitantes.

IV. FINALIDAD DEL TRATAMIENTO DE LOS DATOS PERSONALES

COLABORADORES

- *Gestionar, administrar y controlar la información del personal de colaboradores para la elaboración de planillas, otorgamiento de beneficios que establece la ley, servicio social a problemas personales y familiares, cumplimiento de obligaciones del colaborador, seguridad industrial, capacitaciones, así como las condiciones necesarias para un desempeño laboral óptimo.*

POSTULANTES

- *Evaluar la información del postulante a cumplir con un perfil determinado de un puesto para el proceso de reclutamiento de personal colaborador.*

CLIENTES

- *Registro y gestión de la información de clientes para la venta de productos, análisis de riesgos crediticios, fines estadísticos, proyecciones, acciones financieras, comerciales, marketing y publicidad.*

PROVEEDORES

- *Cotizar, registrar y administrar la información de los proveedores para su evaluación y realizar la adquisición de los requerimientos que se presentan para la elaboración del producto.*

VISITANTES

- *Recopilación y almacenamiento de visitantes para controlar el acceso a las diferentes instalaciones de la empresa por motivo de seguridad.*

VIDEO VIGILANCIA – PLANTAS

- *Almacenamiento y registro de grabación fílmica a las sedes de planta y producción, para fines de auditoría al personal involucrado y cuestiones de seguridad.*

VIDEO VIGILANCIA – SOL ALPACA

- *Almacenamiento y registro de grabación fílmica a las tiendas de atención al público de Sol Alpaca, para fines de auditoría al personal involucrado y cuestiones de seguridad.*

V. EXCEPCIONES

Cabe señalar que de conformidad con la Ley existen supuestos en los cuales su consentimiento no es necesario para el tratamiento de sus datos personales, y por ello la ausencia del mismo o su negativa en su caso, no impide ni impedirá que Michell los trate (sus datos personales) en términos de la Ley y demás regulaciones que resulten aplicables.

VI. LIMITACIONES DEL USO Y DIVULGACIÓN DE LOS DATOS

Los Datos Personales que son proporcionados a Michell por medios legales son tratados de manera confidencial. Los Datos Personales podrán ser transferidos a terceras partes para (a) cumplir con obligaciones legales existentes; (b) cumplir con una orden legal o judicial; y (c) mientras que sea necesario para la operación y funcionamiento de Michell. En el caso de transferencia de los Datos Personales, esto ocurrirá a través de medios e instrumentos legales que otorguen un nivel de protección adecuado y medidas de seguridad para dicha información.

La prohibición de la divulgación de los Datos Personales forma parte de las obligaciones de confidencialidad que asume toda persona en Michell.

VII. MEDIOS PARA EJERCER LOS DERECHOS DEL TITULAR DE LOS DATOS PERSONALES

El titular tendrá en todo momento, el derecho de ejercer sus derechos de acceso, rectificación, cancelación y oposición para el tratamiento de sus Datos Personales (en lo sucesivo los "Derechos ARCO").

Para tal fin, el titular de los Datos Personales deberá completar el Formato de Derechos Arco el cual será proporcionado a los Titulares previo envío de un mensaje de correo electrónico al Comité de Protección de Datos Personales, es decir al correo electrónico LPDP@michell.com.pe, indicando que desea ejercer sus derechos ARCO y especificando el tipo de derecho, es decir, acceso, rectificación, cancelación y oposición.

Dicho Formato de Derechos Arco deberá contener como mínimo la siguiente información:

a) *El nombre del titular y domicilio, u otro medio para comunicarle la respuesta a su solicitud.*
b) *Los documentos que acrediten la identidad o, en su caso, la representación legal del titular.*
c) *La descripción clara y precisa de los Datos Personales respecto de los que se busca ejercer alguno de los derechos antes mencionados.*

d) Cualquier otro elemento o documento que facilite la localización de los Datos Personales, así como cualquier otro documento requerido por la legislación actual en el momento de presentar la solicitud.

VIII. MODIFICACIONES AL AVISO DE PRIVACIDAD

El presente aviso puede ser actualizado por nuevos requerimientos legales; cambios o nuevos productos o servicios que ofrecemos; o cambios en nuestro modelo de negocio.

Sin embargo, sobre cualquier cambio que pueda sufrir el presente aviso de privacidad, se dará a conocer en nuestra página web www.michell.com.pe.

IX. CONSULTAS

Para absolver cualquier consulta relacionada con este Aviso, usted podrá presentar una solicitud en la siguiente dirección electrónica: LPDP@michell.com.pe, u otra notificación escrita a Calle Juan de la Torre 101, San Lázaro, Arequipa, Perú; con atención al Comité de Protección de Datos Personales.

X. CONSENTIMIENTO DEL TITULAR

En caso de que el Titular no esté de acuerdo con el contenido del presente Aviso de Privacidad, puede notificar su inconformidad y desacuerdo al correo electrónico LPDP@michell.com.pe, con atención al comité de protección de datos personales.

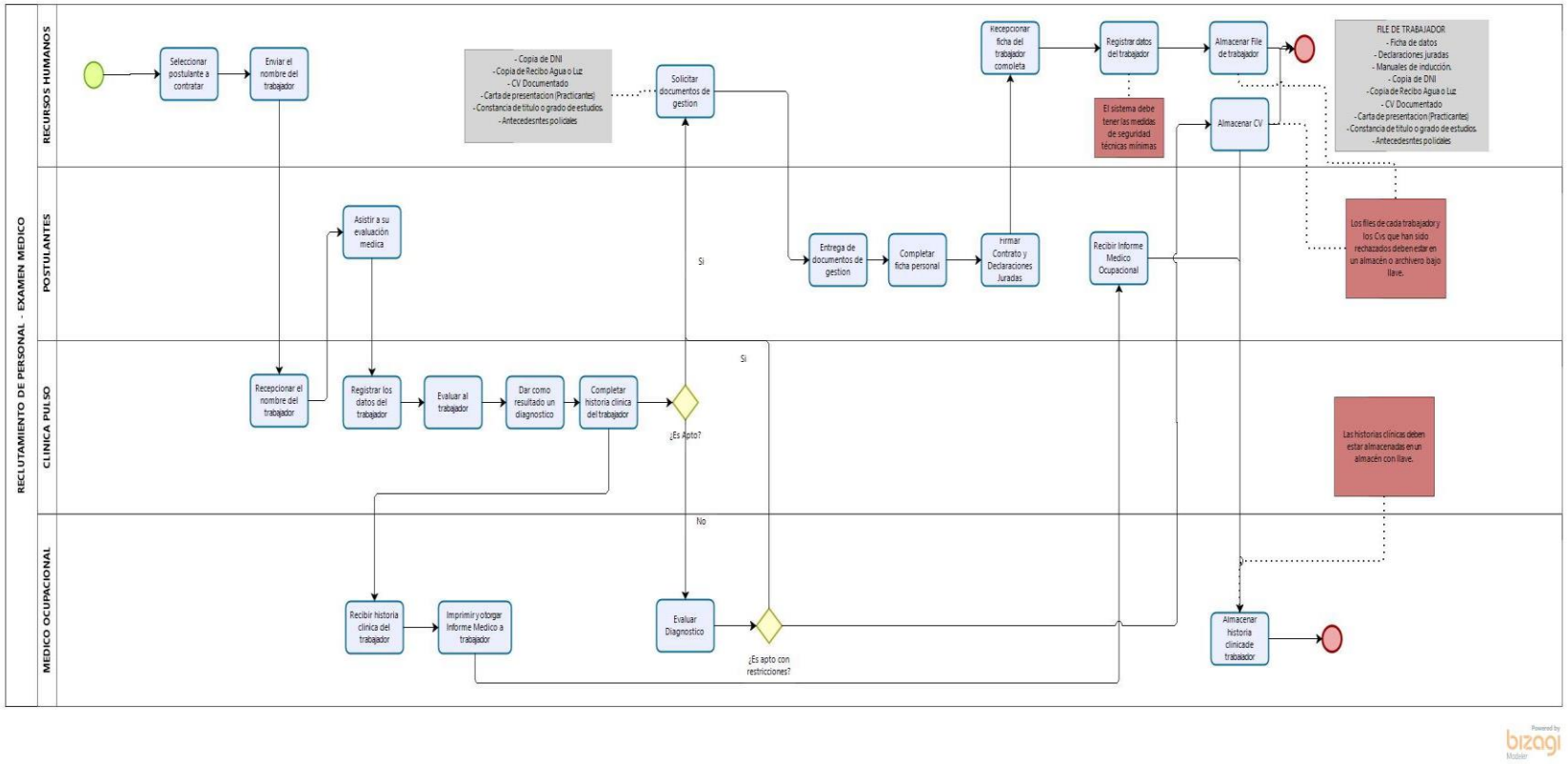


Figura 29 Proceso de Reclutamiento de Personal

Fuente: Elaboración Propia

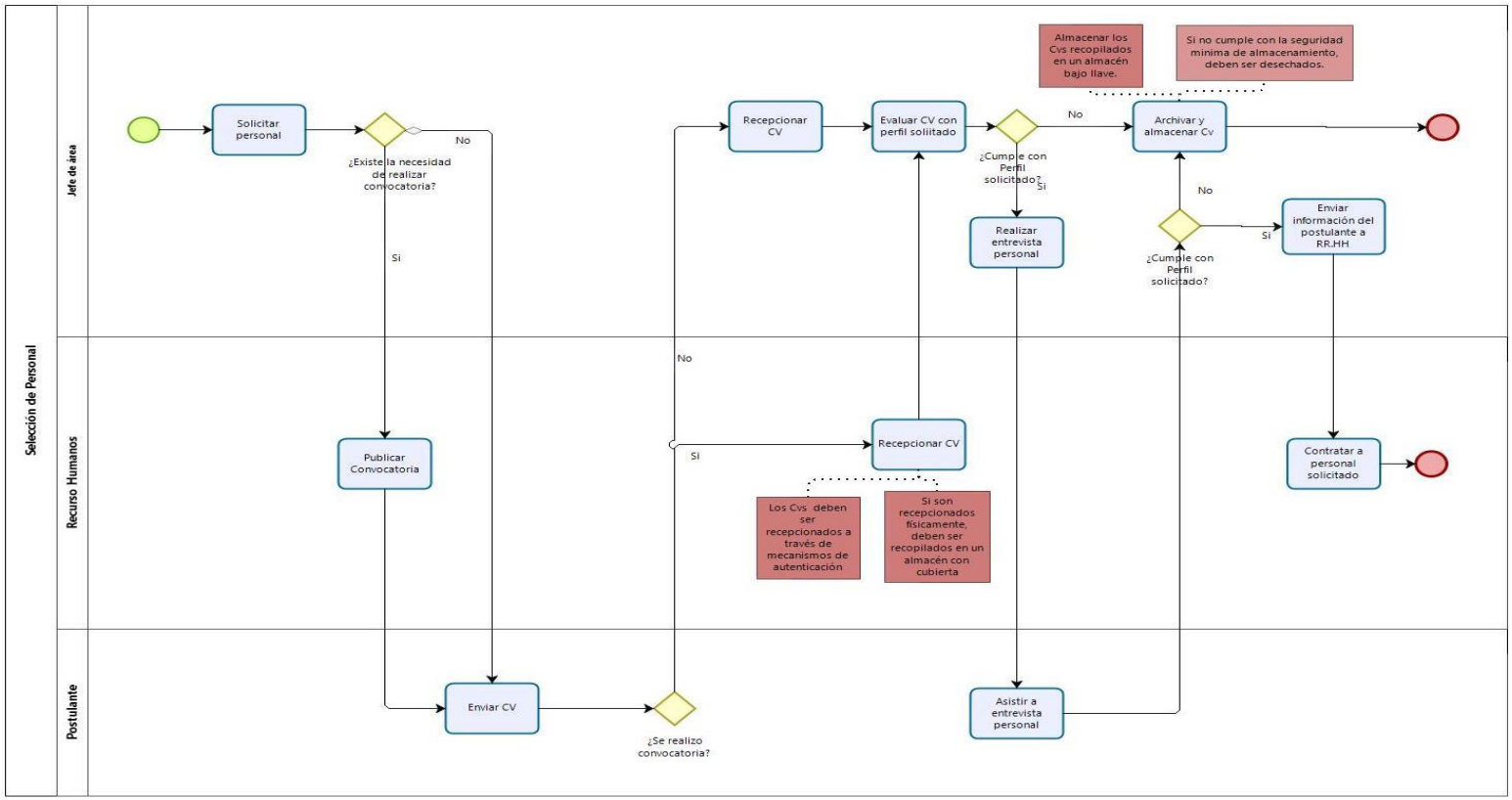


Figura 30 Proceso de Selección de Personal

Fuente: Elaboración Propia

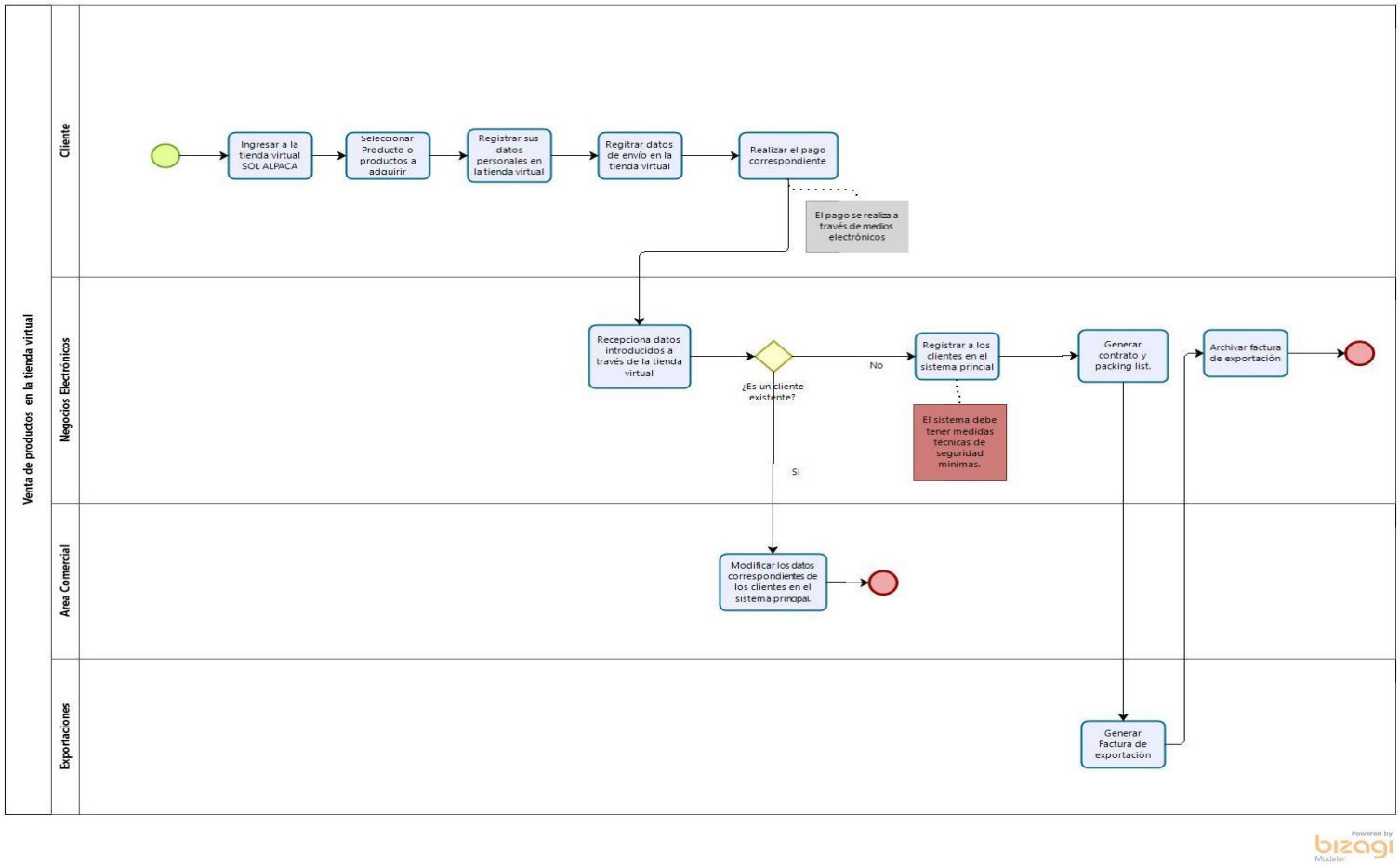


Figura 31 Proceso de Venta de Productos en Tienda Virtual

Fuente: Elaboración Propia

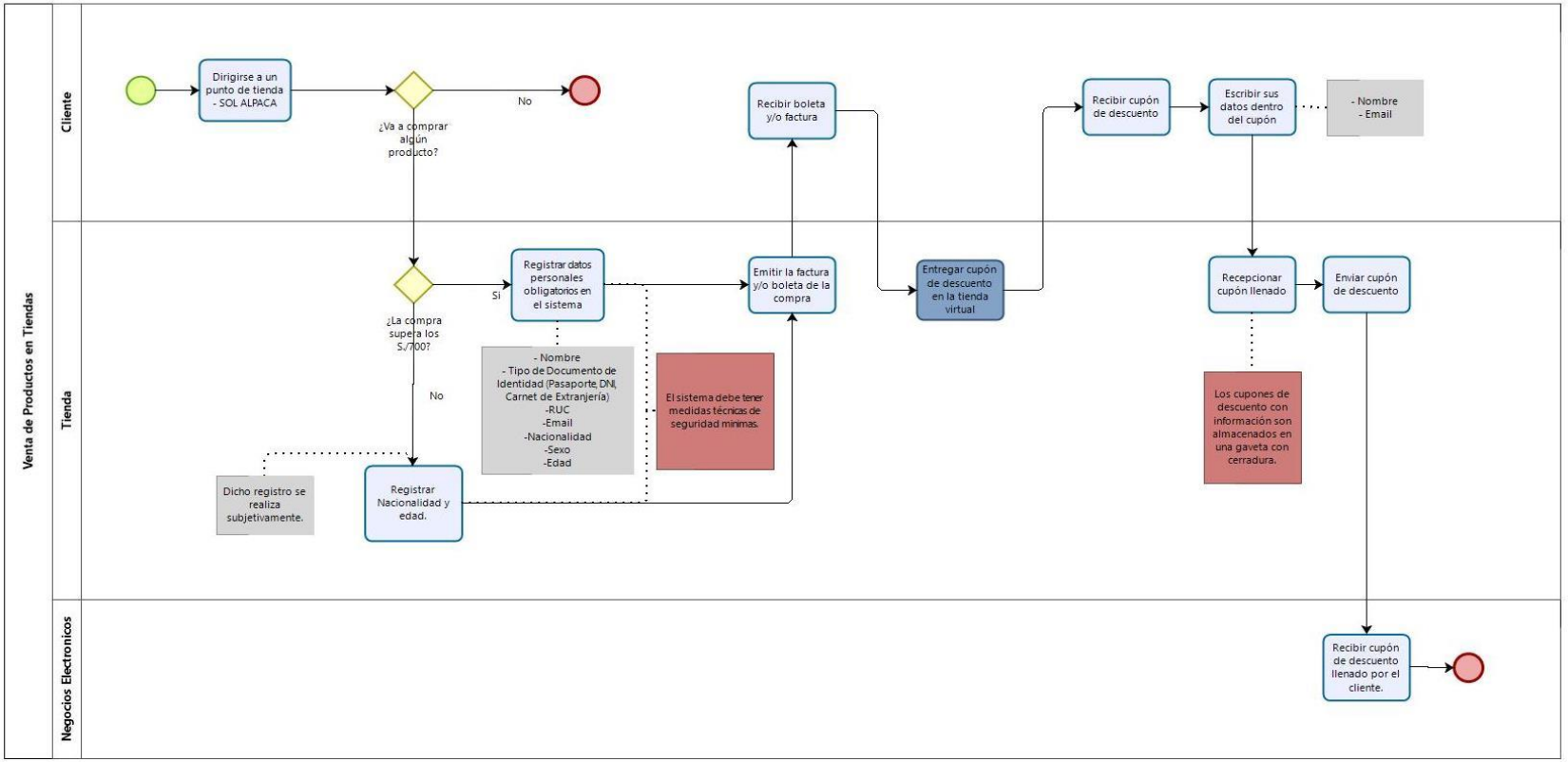


Figura 32 Proceso de Venta de Productos en Tiendas

Fuente: Elaboración Propia

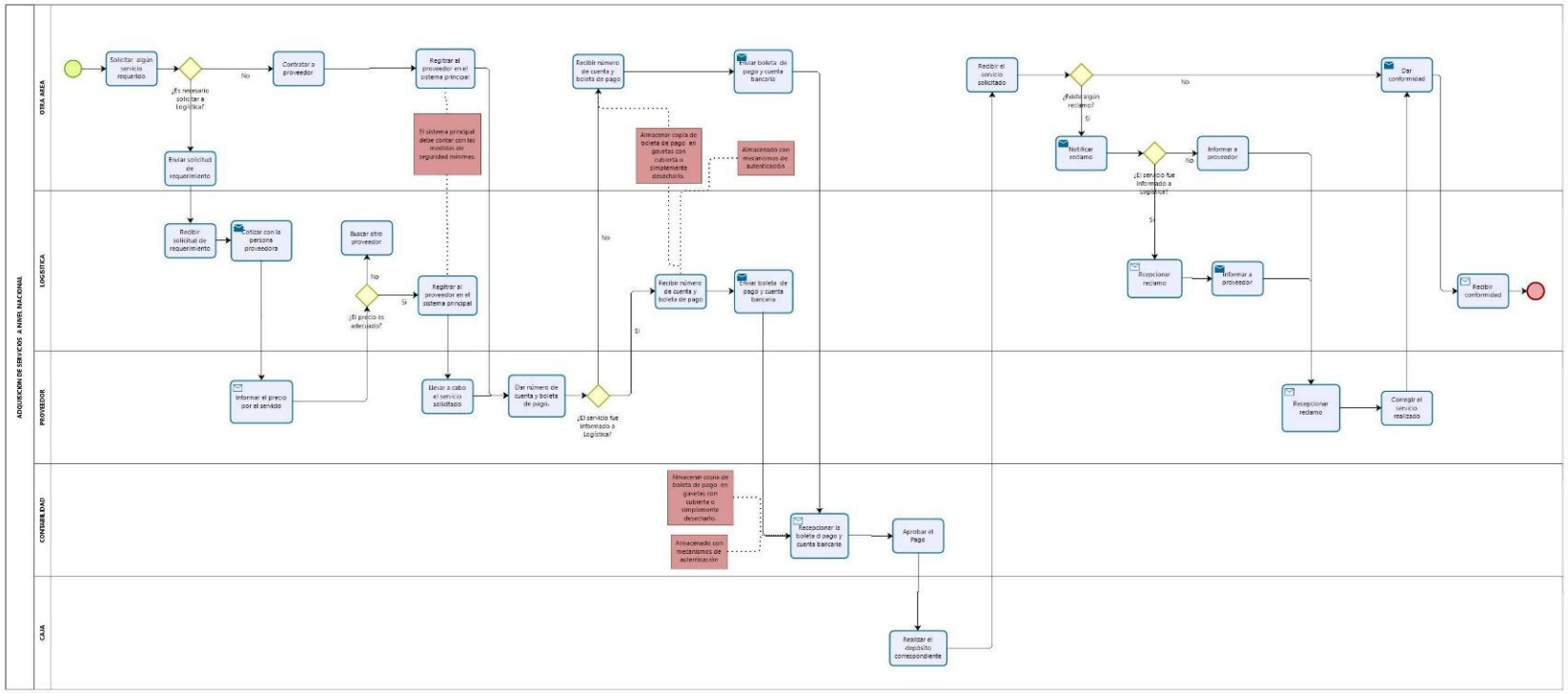


Figura 33 Proceso de Adquisicion de Servicios a Nivel Nacional

Fuente: Elaboración Propia

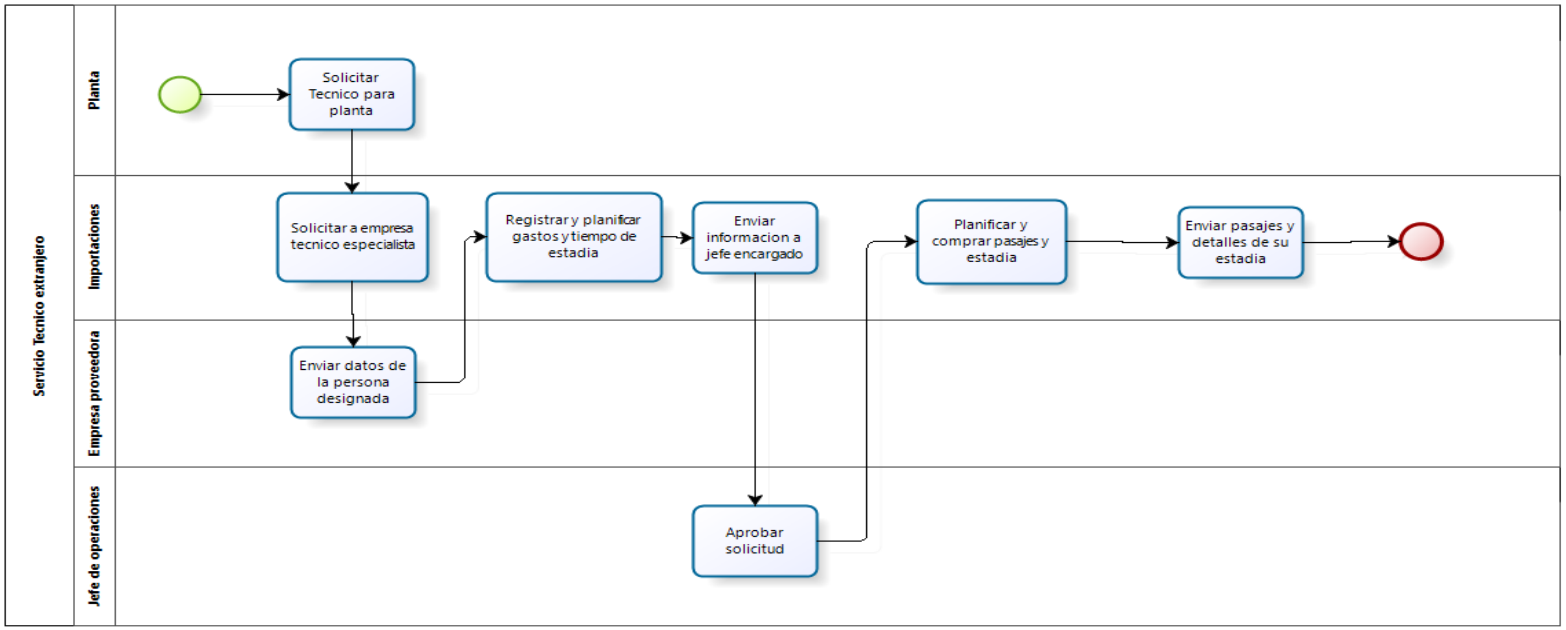


Figura 34 Proceso de Adquisicion de Servicios a Nivel Internacional

Fuente: Elaboración Propia

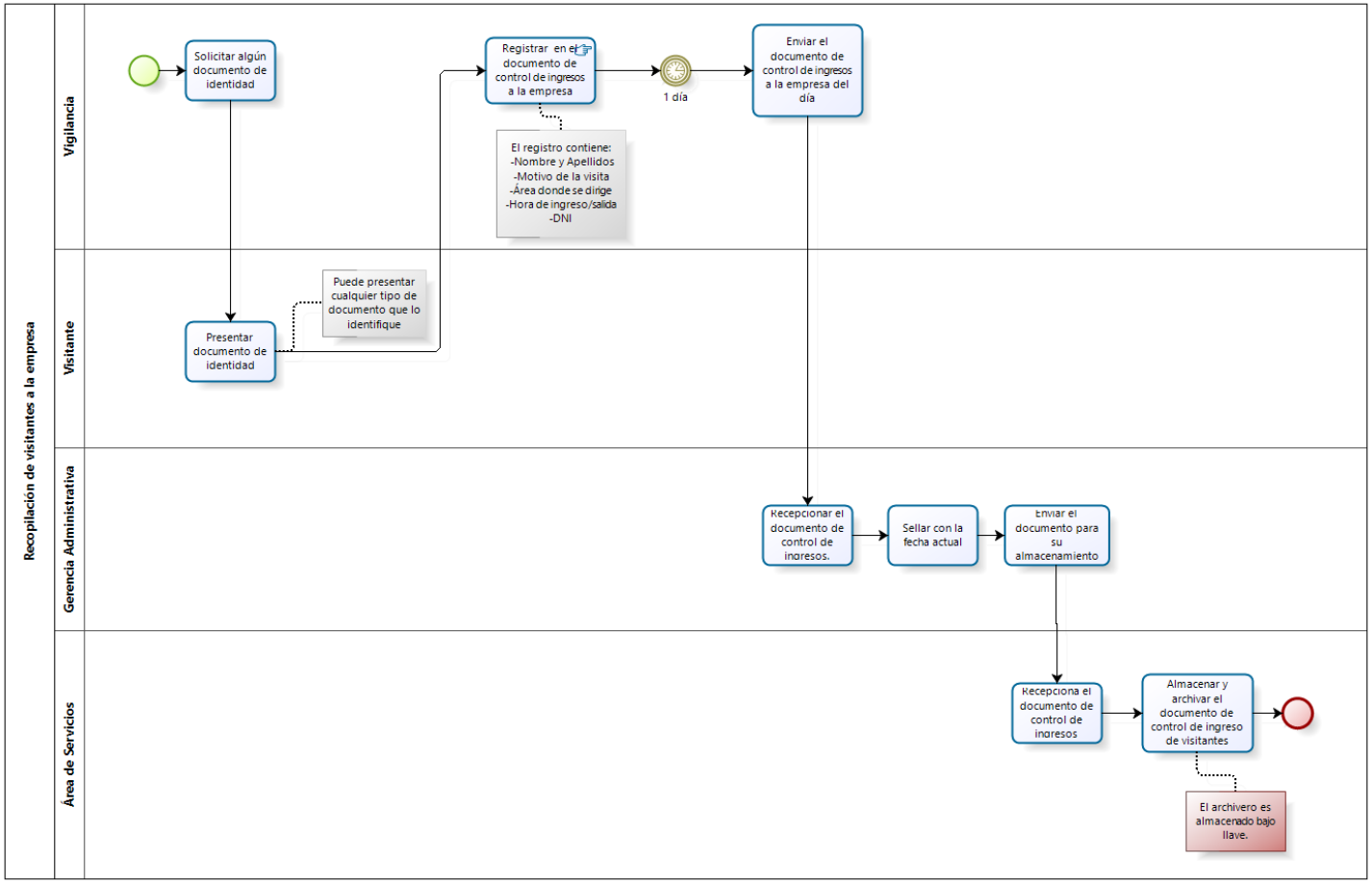


Figura 35 Proceso de Recopilacion de Visitantes a la Empresa

Fuente: Elaboración Propia

4.3.2 Medidas Legales

Como resultado de la evaluación de las medidas legales en la empresa tenemos los siguientes:

8. Modificación de contratos legales para los colaboradores, postulantes, clientes y proveedores.
9. Aviso de privacidad de datos personales para visitantes.
10. Modelo de compromiso de confidencialidad en el tratamiento de datos personales.

AVISO DE PRIVACIDAD DE DATOS PERSONALES PARA VISITANTES POR MICHELL & CÍA S.A.

El presente aviso debe estar publicado fuera de las tiendas Sol Alpaca y de cada sede de la empresa, con el objeto de informar al titular de los datos personales que la empresa cumple y se rige al Reglamento de la Ley de Protección de Datos personales, y de esta forma obtener su consentimiento.

Distinguido Visitante:

De acuerdo a la **Ley N° 29733 Ley de Protección de Datos Personales** se le informa que Michell & Cía S.A. en cumplimiento a la normatividad que rige el Reglamento, dá por concedido su consentimiento de tal manera que sus datos personales serán almacenados en nuestros bancos de datos personales, así mismo serán, custodiados con las medidas de seguridad y confidencialidad pertinentes. El ejercicio de sus derechos o cualquier otra consulta sobre el tratamiento se podrá efectuar en **LPDP_michell@michell.com.pe**

MICHELL
Passion for Alpaca since 1931

Figura 36 Aviso de Privacidad de Datos Personales para Visitantes

Fuente: Elaboración Propia

COMPROMISO DE CONFIDENCIALIDAD DE LOS COLABORADORES EN CUANTO AL TRATAMIENTO Y DIVULGACIÓN DE INFORMACIÓN

Nombre:

_____

Fecha:

_____

En mi capacidad de colaborador (ya sea fijo o temporal) y en consideración de la relación laboral que mantengo con la empresa MICHELL & CIA, así como del acceso que se me permite a sus Bases de Información, constato que:

1. *Tengo conciencia de la importancia de mis responsabilidades en cuanto a no poner en riesgo alguno la integridad, disponibilidad y confidencialidad de la información que maneja la empresa. En concreto he leído, entiendo y me comprometo a cumplir los procedimientos de Seguridad de los Sistemas de Información que corresponden en la empresa.*

2. *Estoy comprometido a cumplir, asimismo, todas las disposiciones relativas a la política de la empresa en materia de uso y divulgación de información, y a no divulgar la información que reciba a lo largo de mi relación con la empresa, subsistiendo este deber de secreto, aun después de que finalice dicha relación y tanto si esta información es de su propiedad, como si pertenece a un cliente de la misma, o a alguna otra Sociedad que nos proporcione el acceso a dicha información, cualquiera que sea la forma de acceso a tales datos o información y el soporte en el que consten, quedando absolutamente prohibido obtener copias sin previa autorización.*

3. *Comprendo que el incumplimiento de cualesquiera de las obligaciones que constan en el presente documento, intencionadamente o por negligencia, podrían implicar las sanciones disciplinarias correspondientes y el posible reclamo por parte de la empresa de los perjuicios económicos causados.*

_____

Titular de la Información o representante legal en el caso de información de hijos (as) de Empleados menores de edad

*DNI:*_____

4.3.3 Medidas Técnicas

Como resultado de la evaluación de las medidas técnicas en la empresa tenemos los siguientes:

11. Política y Procedimiento de Control de Acceso y Privilegios
12. Política y Procedimientos de Gestión de Incidencias
13. Política y Procedimiento de Gestión de los Soportes de Copias de Respaldo

POLÍTICA Y PROCEDIMIENTO DE CONTROL DE ACCESO Y PRIVILEGIOS

Cada usuario es responsable del control de acceso que le sea otorgado; es decir, de su usuario (user) y contraseña (password) necesarios para acceder a la información y a la infraestructura tecnológica de Michell y Cía. S.A., para lo cual deberá mantenerlo de forma confidencial.

El jefe de cada área de la empresa, es el único que puede otorgar la autorización para que se tenga acceso a la información que se encuentra en la infraestructura tecnológica de Michell y Cía. S.A., otorgándoles los permisos mínimos necesarios para el desempeño de sus funciones.

1. Control de acceso lógico

Todo el personal que requiera acceso en lo que respecta la infraestructura tecnológica, requieren previamente obtener un permiso de su jefe de área, y posteriormente, el mismo enviará un correo electrónico al departamento de Sistemas explicando: El motivo por el cual se les debe dar acceso a la infraestructura tecnológica y el tiempo estimado que requiera el acceso lógico.

- *Todos los usuarios de servicios de información son responsables de su identificador de usuario y contraseña que recibe para el uso y acceso de los recursos.*
- *Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de la empresa.*
- *Cada usuario que accede a la infraestructura tecnológica de la empresa debe contar con un identificador de usuario único y personalizado, por lo cual no está permitido el uso de un mismo identificador de Usuario por varios usuarios.*
- *Los usuarios tienen prohibido compartir su identificador de usuario y contraseña, ya que todo lo que ocurra con ese identificador y contraseña será responsabilidad exclusiva del usuario al que pertenezcan, salvo prueba de que le fueron usurpados esos controles.*
- *Los usuarios tienen prohibido usar el identificador de usuario y contraseña de otros, aunque ellos les insistan en usarlo.*

2. *Gestión de privilegios de usuarios*

2.1 Modificación, autorización o retiro de roles o responsabilidades de un usuario

Cualquier cambio que requiera hacerse a los roles y responsabilidades de algún empleado en la temática de privilegios de acceso a la infraestructura tecnológica de la empresa, el jefe del Área en la que pertenezca el empleado, deberá solicitarlo desde su correo oficial al área de sistemas dirigido al Gerente de Ti o el encargado de seguridad lógica de los bancos de datos personales, siendo el único encargado de registrar:

- *Usuario*
- *Día*
- *Hora de autorización, cambio o retiro*
- *Usuario que autoriza la modificación.*

2.2 Revisión y Registro de Privilegios

El encargado de seguridad lógica de los bancos de datos tiene la obligación de revisar que solo el personal autorizado pueda acceder a los datos personales, además de generar un registro de dicha revisión que lo evidencie.

Tales revisiones se hacen semestralmente, con un mínimo de dos revisiones al año.

3. *Control de acceso físico*

Se protege al banco de datos personales contra acceso físico no autorizado mediante mecanismos de bloqueo físico como:

- *Documentos aislados en una gaveta con cerradura.*
- *Documentos aislados en archiveros con cubierta.*
- *Documentos con información sensible apartados en un almacén bajo llave.*

4. *Equipo de trabajo desatendido*

4.1 Activar protector de pantalla

Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla previamente instalados y autorizados por su jefe de área como una medida de seguridad cuando el usuario necesita ausentarse de su escritorio por un tiempo.

4.2 Apagar computadoras y recursos tecnológicos cuando termina la jornada laboral

Los usuarios deben apagar sus computadoras u otros recursos tecnológicos cuando hayan terminado su jornada laboral diaria con la finalidad de proteger los equipos ante eventuales cortes de energía eléctrica.

5. *Gestión y uso de Contraseñas*

- *La asignación de la contraseña para acceso a la red y la contraseña para acceso a sistemas, debe ser realizada de forma individual, por lo que queda prohibido el uso de contraseñas compartidas.*
- *La obtención o cambio de una contraseña debe hacerse de forma segura, el usuario deberá acreditarse ante algún responsable de sistemas o su jefe de área, como empleado de la empresa.*
- *Cuando un usuario olvide, bloquee o extravíe su contraseña deberá reportarlo al área de sistemas enviando un correo electrónico, indicando si es de acceso a la red o a módulos de sistemas desarrollados por los miembros del área de sistemas, para que se le proporcione una nueva contraseña.*
- *Está prohibido que los identificadores de usuarios y contraseñas se encuentren en forma visible en cualquier medio impreso o escrito en el área de trabajo del usuario, de manera que se permita a personas no autorizadas su conocimiento.*

- *Todos los usuarios deberán observar los siguientes lineamientos para la construcción de sus contraseñas:*

  • No deben ser números consecutivos

  • Deben estar compuestos de al menos seis (8) caracteres, estos caracteres deben ser alfanuméricos, o sea, números y letras.

  • Deben ser difíciles de adivinar, esto implica que las contraseñas no deben relacionarse con el trabajo o la vida personal del usuario.

  • Deben ser diferentes a las contraseñas que se hayan usado previamente.

- *La contraseña podrá ser cambiada por requerimiento del dueño de la cuenta.*
- *Todo usuario que tenga la sospecha de que su contraseña es conocido por otra persona, tendrá la obligación de cambiarlo inmediatamente.*
- *Los cambios o desbloqueo de contraseñas solicitados por el usuario a serán solicitados mediante un correo electrónico al Gerente de TI.*

6. Control de accesos remotos

- *Se permite el acceso desde redes externa a través de cualquier dispositivo, siempre y cuando se cuenta con autorización del área de sistemas o jefe del área.*
- *Está permitida la administración remota de equipos conectados a internet, siempre que cuenten con autorización y con un mecanismo de control de acceso seguro y también autorizado por el área de sistemas.*

POLÍTICA Y PROCEDIMIENTO DE GESTIÓN DE INCIDENCIAS

En la presente política se describen los requisitos y pasos a tener en cuenta en los procedimientos de Gestión de incidentes, para cumplir con el Reglamento de Medidas de Seguridad y la normativa de la Ley de Protección de Datos Personales.

1. Clase de incidencias

Se ha clasificado de acuerdo al criterio del área que la tiene que resolver. De esta forma, la empresa dispone de una relación de incidencias que permite identificar aquellas que más suelen afectar a la seguridad de los bancos de datos.

Se lista los eventos que tienen consideración de incidencias para que se puedan dar a conocer y gestionar correctamente por la(s) áreas implicadas, en atención a las medidas de seguridad que se encuentran implementadas.

2. Incidencias relativas a usuarios

- *Requerimiento del desbloqueo de una cuenta de usuario por el olvido de la cuenta de usuario y contraseña.*
- *Fugas de información.*
- *Eliminación, voluntario o involuntario, de información.*
- *Pérdida o extravío de los soportes informáticos que contienen datos de carácter personal.*
- *Acceso a la información sin contar con autorización.*
- *Deficiencias en el control de las medidas de seguridad implementadas.*
- *Robo o pérdida de un equipo de trabajo*
- *Vigencia de los accesos al personal que ya no labora en la empresa.*
- *Continuar usando contraseñas genéricas.*

- *Permitir el ingreso de dispositivos de almacenamiento no autorizados por el usuario.*

3. Incidencias generadas en los sistemas de información

- *Fallo en el sistema de copias de respaldo de la información.*
- *Fallo en la restauración de información.*
- *Inconvenientes de software, incluidos sus parches y actualizaciones, de los equipos servidores o equipos de trabajo.*
- *Inconvenientes con el hardware de los equipos servidores o puestos de trabajo.*
- *No poder recuperar información perdida.*
- *Restaurar información.*
- *Procesos "batch" ejecutados erróneamente.*
- *Pérdida de servicio en los sistemas.*
- *Inconvenientes en los sistemas de comunicaciones.*

4. Incidencias generadas por factores externos

- *Fraudes*
- *Robos*
- *Tormentas, inundaciones, fuego, etc.*
- *Ataques cibernéticos para acceder a los sistemas de información.*
- *Extravío de soportes como consecuencia de su externalización.*
- *Propagación de virus y software malicioso.*
- *Pérdida de confidencialidad en información restringida o confidencial.*
- *Pérdida de documentación en traslados, comunicaciones, envíos o entrega de la información contenida en los ficheros.*
- *Accesos no autorizados a las instalaciones.*
- *Accesos no autorizados a información.*

5. Comunicación de incidencias

El usuario que detecta una incidencia o supone su generación, dispone de las siguientes maneras de comunicación habilitados para la notificación de incidencias:

- *Comunicación mediante e-mail al buzón de Gestión de Incidencias.*
- *Comunicación mediante la herramienta de gestión de incidencias.*
- *Comunicación telefónica al área de Sistemas.*

La información bridada para notificar una incidencia debe ser lo más completa posible con la finalidad de poder resolverla más eficazmente.

6. Registro de incidencias

El registrar cualquier incidencia que pueda afectar la seguridad de un banco de datos personales es un requerimiento obligatorio de la normativa de protección de datos personales.

La información que debe contener dicho registro, para cumplir con la norma, es la siguiente:

- *Fecha y hora en que se llevó a cabo la incidencia*
- *Tipo de incidente*
- *Fichero/os afectado/os por la incidencia.*
- *Persona que notifica la incidencia (Emisor).*
- *Persona a quien se comunica la incidencia (Receptor).*
- *Consecuencias que contrajo la incidencia: Los eventos negativos serán descritos.*

Si la incidencia afecta a bancos de datos personales de nivel complejo o crítico debe incluirse, además:

- *Detalle de los procedimientos realizados en la recuperación de los datos.*

- *Persona que ejecuta el proceso de recuperación de datos, si procede.*
- *Datos restaurados.*
- *Datos que haya sido necesario grabar manualmente en el proceso de recuperación, si procede.*
- *Persona que se ha responsabilizado por escrito para la ejecución de los procedimientos de recuperación de datos (debe estar autorizada por el responsable del banco de datos.)*
- *La información se va cumplimentando a medida que las tareas para su resolución se van realizando.*
- *El plazo mínimo de conservación de la información del Registro es de 2 años, por analogía con el Registro de accesos de usuarios.*

7. Áreas involucradas

Cualquier incidencia relacionada con la seguridad de la información y en particular con la información que contenga datos de carácter personal deberá ser comunicada al área de Sistemas.

El área de sistemas coordinará a los distintos departamentos y Áreas que estén involucrados en la incidencia o en las consecuencias de la misma.

Cada una de los áreas tienen documentados los procedimientos operativos, aplicaciones, mecanismos y herramientas utilizados para la gestión y resolución de las incidencias incluyendo los procedimientos de escalado donde se relacionan y definen la participación de los restantes departamentos de la organización que intervienen o pueden intervenir en su resolución.

8. Seguimiento de las incidencias

El responsable de cada banco de datos personales debe realizar una revisión semanal de las incidencias para ejecutar los controles pertinentes relacionados con el registro de incidencias.

POLÍTICA Y PROCEDIMIENTO DE GESTIÓN DE LOS SOPORTES DE COPIAS DE RESPALDO

1. Recuperación y gestión de copias de respaldo

Los soportes informáticos en donde se almacenen las copias de respaldo deben permitir identificar claramente la información que en ella contienen y ser debidamente inventariados.

2. Clases de soportes, ubicación y almacenamiento

Los procedimientos operativos se describen e implementan los siguientes aspectos:

1. Los mecanismos y tipos de soportes usados, por cada elemento de los Sistemas de Información, al ejecutar las copias de seguridad.

2. Identificar claramente, para cada tipo de soporte, la ubicación física donde se va a custodiar.

3. Los soportes usados para el almacenamiento de las copias de seguridad son unidades magnéticas y software sincronizado en la nube, garantizando que cumplen con las medidas de seguridad mínimas necesarias.

4. Las ubicaciones donde se custodian los soportes son:

- *Centro de Datos*
- *En la nube (Cloud)*
- *Otras unidades de almacenamiento*

Además, este lugar es de acceso restringido sólo al personal autorizado.

5. Nivel de disponibilidad asignado a los soportes.

6. La información almacenada en los soportes informáticos dispone de una copia de seguridad fuera de los locales donde se ubican los equipos informáticos para guardar backups en caso de desastre en el centro informático. En cuanto al respaldo de las computadoras de los usuarios se sitúan en discos externos y/o en la nube.

7. Como medida de seguridad se dispone no sólo de copias de seguridad de los datos sino también de los distintos elementos de los Sistemas de Información relativos al software (configuraciones, aplicaciones, etc.), puesto que constituyen parte de los procedimientos de recuperación de datos.

8. Todo los backups de la empresa están restringidos con claves de seguridad.

3. Identificación de los Backups

Los soportes de copia de seguridad son almacenados en carpetas específicas y con una nomenclatura determinada (fecha y nombre que corresponda al backup)

Entre estos tenemos:

- *Fuentes*
- *Ejecutables*
- *Usuarios*
- *Procedimientos (Documentación del área)*
- *Carpetas compartidas (identificados por el área)*

4. Inventario y registro

Alta / Modificación de un soporte (NAS)

Los nuevos soportes que se obtienen de la realización de copias de seguridad de cualquiera de los elementos de los Sistemas de Información, y soportes que modifican su contenido son inventariados y registrados.

El encargado de seguridad lógica de los bancos de datos personales es el responsable de que se mantenga un inventario actualizado con los soportes informáticos que contengan datos de carácter personal.

Los pasos que se realizan cuando para dar de alta un soporte, son:

1. Persona que decide la creación del soporte.

2. Registro del soporte en el inventario de soportes informáticos, la información mínima que se almacena es:

- *Tipo de soporte.*
- *Identificación del soporte físico.*
- *Fecha de alta.*
- *Ubicación actual.*
- *Información contenida.*

Baja de un soporte

Cuando un soporte se da de baja por cualquier motivo justificado, se actualiza el inventario de soportes informáticos.

Los pasos que se siguen cuando se da de baja un soporte, son:

1. Persona u organismo que decide la baja del soporte.

2. Actualización el inventario de soportes indicando que se produce la baja del soporte registrado.

3. Una vez localizado el soporte dentro del inventario, como mínimo, se debe completar los siguientes datos:

· Fecha de baja.

· Motivo de baja.

· Acción que se realizó con el soporte (borrado, eliminación.…).

5. *Gestión de permisos de acceso a la ubicación de los soportes*

El acceso a las salas donde se ubiquen los soportes está restringido al personal autorizado.

6. *Eliminación de soportes*

El proceso de desechado de soportes debe garantizar que no pueda volver a recuperarse la información contenida en ellos.

7. *Reutilización de soportes*

El procedimiento contempla los siguientes aspectos:

1. Se procede al borrado de la información. Verificando su completa eliminación.

13. Una vez que el soporte ha sido borrado y, por lo tanto, puede ser reutilizado nuevamente se procede a actualizar el inventario de soportes informáticos.

4.3.4 Formatos ARCO

En el Manual de Políticas y Procedimientos LPDP también se elaboró el modelo del formato para ejercer los derechos ARCO, así como también el modelo de respuesta por parte de Michell y Cía. S.A. ante esta solicitud.

FORMATO PARA EL EJERCICIO DE LOS DERECHOS ARCO

N° Solicitud: _____

Datos del Titular de Datos Personales

Nombres y Apellidos:	
Tipo de Documento de Identidad:	Número:
Dirección:	
Distrito:	Provincia:
Correo electrónico:	Teléfono:

TIPO DE SOLICITUD

☐ Acceso ☐ Rectificación

☐ Cancelación ☐ Oposición

MEDIO DE ENTREGA DE RESPUESTA

☐ Vía electrónica ☐ Personal

ESPECIFICAR LA SOLICITUD

*(*De ser necesario, adjuntar los documentos probatorios que sustenten lo solicitado.)*

En caso de Rectificación indicar:

El dato personal dice: El dato personal debe decir:

(Adjuntar los documentos probatorios que sustenten lo solicitado.)

Nota:

1. Dentro 5 días hábiles como máximo usted podrá verificar vía web o personalmente en nuestra sede Central (Av. Juan de la Torre 101, San Lázaro) si su solicitud fue observada, en caso de tener observación tendrá 5 días hábiles posteriores para subsanar su solicitud, caso contrario se dará por anulada.

2. Dentro 7 días hábiles como máximo usted podrá verificar vía web o personalmente en nuestra sede Central (Av. Juan de la Torre 101, San Lázaro) si su solicitud requiere documentación adicional para ser atendida. Usted tendrá un plazo de 10 días hábiles posteriores para presentar dicha información, caso contrario su solicitud se dará por anulada.

3. La respuesta o ampliación a su solicitud, será notificada en los siguientes plazos: Derecho de Acceso (20 días hábiles), Derecho de Rectificación (10 días hábiles), Derecho de Cancelación (10 días hábiles) y Derecho de Oposición (10 días hábiles).

4. Si en el plazo de un mes no se obtiene respuesta debe considerarse denegada la petición y se podrá interponer una reclamación ante la Autoridad Nacional de Protección de Datos Personales para iniciar el procedimiento de tutela de derechos.

_____

Firma del Solicitante

_____,_____*de*_____*del*_____

DOCUMENTACION A ADJUNTAR: *FOTOCOPIA/ESCANEO DE DOCUMENTO DE IDENTIDAD*

FORMATO DE RESPUESTA A LA SOLICITUD DE DERECHOS ARCO

N° Solicitud: _____
Sr(a): _____
Michell & Cía. S.A., en base a lo reglamentado en la Ley N°29733, Ley de Protección de Datos Personales, ha procesado y evaluado la solicitud declarándola:

☐ Procedente ☐ Improcedente

Por los siguientes motivos:

*(*De ser necesario, adjuntar los documentos probatorios que sustenten lo solicitado.)*

_____
Firma del responsable del Banco de Datos

_____,_____***de***_____***del***_____

4.4 FORMATOS DE ACEPTACIÓN DEL CONSENTIMIENTO

En la última fase de la metodología se estableció los procedimientos y mecanismos de obtención de los consentimientos de los titulares de los datos personales, teniendo como resultado la elaboración y ejecución de los siguientes formatos de aceptación de consentimientos para ser recibidos por el titular del dato personal y así autorizar o no la manipulación de su información personal.

A la actualidad, se identificó siete bancos de datos personales dentro de la empresa y para cada uno de ellos existe un procedimiento y un formato de aceptación del consentimiento distinto para obtener los consentimientos de los titulares de los datos personales.

4.4.1 Formato de Consentimiento para el Banco de Datos "Colaboradores"

El siguiente formato de consentimiento se entrega a todos los colaboradores adjuntado a su contrato de trabajo. Dicho formato informa claramente la finalidad por lo cual los datos personales son almacenados y manipulados por el titular de los bancos de datos personales (Grupo Michell, n.d.).

CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS PERSONALES PARA MICHELL Y CIA S.A

Nombre: _____ ***Fecha:*** _____

De conformidad con lo establecido a los artículos 2, 13.6 y 13.6 en la Ley N°29733 – Ley de Protección de Datos Personales, los datos personales que se obtengan por parte del Titular de la Información a través de los vínculos contractuales celebrados entre Michel y Cía. S.A., (de ahora en adelante La Empresa) y el Titular de la Información, serán compilados, almacenados, consultados, usados, compartidos, intercambiados, transmitidos, transferidos y objeto de tratamiento en bases de datos, las cuales servirán para la siguiente finalidad:
"Gestionar, administrar y controlar la información del personal de colaboradores para la elaboración de planillas, otorgamiento de beneficios que establece la ley, servicio social a problemas personales y familiares, cumplimiento de obligaciones del colaborador, seguridad industrial, capacitaciones, así como las condiciones necesarias para un desempeño laboral óptimo."

Datos sensibles. *El Empleado Titular de la Información o representante legal en el caso de información de hijos (as) de Empleados menores de edad manifiesta que conoce, acepta y autoriza de manera libre y espontánea que el tratamiento de la información relativa a pertenencia a sindicatos, organizaciones sociales, a la salud, a la vida sexual y datos biométricos, que sea necesaria para el cumplimiento de las finalidades anteriormente descritas basado en lo establecido en la presente autorización.*
De conformidad con lo dispuesto en la Ley N°29733 - Ley de Protección de Datos Personales, los datos personales que obtenga La Empresa por parte del Empleado Titular de la Información o representante legal en el caso de información de hijos(as) de Empleados menores de edad, serán recogidos y almacenados y objeto de tratamiento en bases de datos hasta la terminación del vínculo contractual entre el Empleado Titular de la Información y La Empresa y durante veinte (20) años más. Esta base de datos cuenta con las medidas de seguridad necesarias para la conservación adecuada de los datos personales.
Con la aceptación de la presente autorización, se permite el tratamiento de sus datos personales para la finalidad mencionada y reconoce que los datos suministrados a La Empresa son ciertos, dejando por sentado que no se ha omitido o adulterado ninguna información.
Así mimo, se deja constancia que usted tiene el derecho de acceder en cualquier momento a los datos suministrados, a solicitar su corrección, actualización o supresión en los términos establecidos en la Ley N°29733, mediante el envío de un correo electrónico a ***LPDP@michell.com.pe*** *indicando las razones por las cuales solicita alguno de los tramites anteriormente mencionados, con el fin que La Empresa pueda revisarlas y pronunciarse sobre las mismas.*

_____

Titular de la Información o representante legal en el caso de información de hijos (as) de Empleados menores de edad
*DNI:*_____

4.4.2 Formato de Consentimiento para el Banco de Datos “Postulantes”

El siguiente formato de consentimiento se entrega a todos los postulantes al momento de realizar una entrevista personal con el mismo indicándole la finalidad de su tratamiento (Grupo Michell, n.d.).

CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS PERSONALES (POSTULANTES)

Nombres y Apellidos:	
Tipo de Documento de Identidad:	***Número:***
Correo electrónico:	***Teléfono:***

En cumplimiento de lo establecido en la Ley N° 29733 denominada como Ley de Protección de Datos Personales, le comunicamos que los datos que usted nos facilite quedarán incorporados y serán tratados en los bancos de datos, titularidad de MICHELL & CIA con el fin de evaluar la información del postulante a cumplir con un perfil determinado de un puesto para el proceso de selección de personal colaborador.

Mediante la firma del presente documento usted otorga el consentimiento expreso para que MICHELL & CIA pueda utilizar con este fin concreto los datos facilitados por usted, comprometiéndose a tratar de forma confidencial los datos de carácter personal facilitados y a no comunicar o ceder dicha información a terceros, adoptando las medidas de seguridad que establece la normativa sobre protección de datos.

Asimismo, le informamos de la posibilidad que tiene de ejercer los derechos de acceso, rectificación, cancelación y oposición de sus datos de carácter personal mediante el envío de un correo electrónico a LPDP@michell.com.pe indicando las razones por las cuales solicita alguno de los tramites anteriormente mencionados, adjuntando una copia de su documento de identidad.

_____*de*_____*de*_____

_____

Titular de la Información
*DNI:*_____

4.4.3 Formato de Consentimiento para el Banco de Datos “Clientes”

Debido a que la empresa cuenta con proveedores como personas naturales únicamente Sol Alpaca, para obtener sus consentimientos el primer paso es leer y aceptar el siguiente formato de consentimiento haciendo clic en un recuadro de verificación antes de poder adquirir cualquier producto de la tienda virtual(Grupo Michell, n.d.).

CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS PERSONALES (CLIENTES)

De conformidad con la Ley N° 29733, Ley de Protección de Datos Personales y su norma reglamentaria D.S. y N° 003-2013-JUS en los términos vigentes de ambas, desde el momento que Ud. haya declarado la aceptación expresa del tratamiento de sus datos personales mediante la realización de cliqueo/pinchado/touch (u otro mecanismo utilizado), Ud. autoriza a Michell & Cía. S.A. domiciliada en Juan de la Torre N° 101, San Lázaro, Arequipa; que todos los datos personales suyos facilitados sean recolectados y tratados por el mismo.

Adicionalmente, se entenderá que el usuario consiente el tratamiento de sus datos personales si mediante su conducta se evidencia que ha consentido inequívocamente el tratamiento de sus datos brindados en el formulario de registro, conforme a lo permitido en el artículo 12° numeral 3 del Reglamento de la Ley de Protección de datos personales.

Los datos personales serán incorporados al banco de datos de Clientes bajo la titularidad de Michell y Cía. S.A. Sus datos serán utilizados en la gestión administrativa y comercial. Los datos se mantendrán en el banco de datos mientras se consideren útiles con el fin de emitir facturas electrónicas, enviarle por cualquier medio o soporte información y publicidad sobre las ofertas, promociones y recomendaciones de la empresa, así como para realizar encuestas, estadísticas y análisis de tendencias de mercado.

El Usuario autoriza a Michell & Cía. a conservar sus datos una vez finalizada la relación contractual, para el cumplimiento de las obligaciones legales pertinentes, y para que pueda recibir información publicitaria y ofertas comerciales, dentro de los límites legales permitidos.

El Usuario puede ejercer los derechos de acceso, rectificación, oposición y cancelación de los datos personales, los cuales podrá ejercer mediante la opción de contacto que ponemos a su disposición. El usuario responde de la veracidad de los datos facilitados por el, no imponiendo ninguna sanción o realizar las denuncias respectivas; y en caso de constatar la falsedad o inexactitud de los mismos, nuestra empresa ha adoptado los niveles de seguridad de protección de los Datos Personales legalmente requeridos.

4.4.4 Formato de Consentimiento para el Banco de Datos “Proveedores”

El siguiente formato de consentimiento se entrega únicamente a los proveedores como personas naturales antes de realizar el servicio o adquirir el producto dándole a conocer la finalidad del tratamiento de sus datos personales (Grupo Michell, n.d.).

CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS PERSONALES (PROVEEDORES)

Nombres y Apellidos:	
Tipo de Documento de Identidad:	***Número:***
Correo electrónico:	***Teléfono:***

En cumplimiento de lo establecido en la Ley N° 29733 denominada como Ley de Protección de Datos Personales, le comunicamos que los datos que usted nos facilite quedarán incorporados y serán tratados en los bancos de datos, titularidad de MICHELL & CIA con el fin de cotizar, registrar y administrar la información de los proveedores para su evaluación y realizar la adquisición de los requerimientos que se presentan para la elaboración del producto.
Mediante la firma del presente documento usted otorga el consentimiento expreso para que MICHELL & CIA pueda utilizar con este fin concreto los datos facilitados por usted, comprometiéndose a tratar de forma confidencial los datos de carácter personal facilitados y a no comunicar o ceder dicha información a terceros, adoptando las medidas de seguridad que establece la normativa sobre protección de datos.

Asimismo, le informamos de la posibilidad que tiene de ejercer los derechos de acceso, rectificación, cancelación y oposición de sus datos de carácter personal mediante el envío de un correo electrónico a LPDP@michell.com.pe indicando las razones por las cuales solicita alguno de los tramites anteriormente mencionados, adjuntando una copia de su documento de identidad.

_____*de*_____*de*_____

_____
Titular de la Información
*DNI o Documento de Identificación:*_____

4.5 SISTEMA WEB PARA EL CONTROL DEL CUMPLIMIENTO DE LA LPDP

4.5.1 Inicio

4.5.1.1 Alcance del Sistema web

El sistema web será desarrollado únicamente para poder controlar los backups, incidencias, solicitudes ARCO y medidas de seguridad de información implementadas en la empresa Michell y Cía. S.A.

4.5.1.2 Integrantes del Equipo de Trabajo

Para el presente desarrollo, se ha definido un equipo de trabajo conformado por los estudiantes: Jeanpierre Urquizo Pinto y Maryori García Tenorio, encargados de las fases de inicio, elaboración, desarrollo e implementación y transición del sistema web para el control de registros alineado a la LPDP.

4.5.1.3 Funciones de los Integrantes

Principales encargados de llevar a cabo las tareas de análisis, diseño, desarrollo e implementación del sistema web en base a los requerimientos, así como también son responsables de escoger y configurar los componentes de software a emplearse, pruebas de funcionamiento y capacitar a los usuarios que manejarán la aplicación.

4.5.1.4 Objetivo Principal del Sistema Web

Desarrollar un sistema web que permita registrar, gestionar y verificar las actividades relacionadas al cumplimiento de la Ley de Protección de Datos Personales, teniendo en cuenta las medidas de seguridad analizadas anteriormente.

4.5.1.4 Definición de Objetivos del Sistema Web

Para tener una mayor comprensión de los objetivos que cumplirá el sistema web, es necesario definirlos para poder desarrollarlos. De esta manera se tiene lo siguiente:

- Registro y gestión de backups.
- Gestión de las solicitudes recibidas de derechos ARCO.
- Registro y gestión de incidencias.
- Llevar un control de las medidas organizativas, legales y técnicas de seguridad.
- Realizar una auditoría del cumplimiento de la LPDP.

4.5.2 Elaboración (Análisis y Diseño del Sistema web)

4.5.2.1 Análisis de los requerimientos

El análisis de los requerimientos comprende el conjunto de tareas relacionadas con la determinación de las necesidades de software. El objetivo es detallar de una manera clara cada uno de los requerimientos antes de avanzar a la fase de diseño del sistema web.

La especificación de los requisitos de software es el resultado del levantamiento de información con el usuario o cliente del producto. Son un método para una comunicación más concisa y clara entre los encargados de desarrollar el software y el área de negocio o clientes que usaran el producto.

Los requerimientos identificados son los siguientes:

Registro de Incidencias: Los incidentes en cuanto a información personal (Existe 3 tipos: Información relativa a usuarios, relativa a sistemas de información y respecto a factores externos) deben ser registrados para un mejor control estos a su vez se dividen.

Información relativa a usuarios:

- Necesidad de desbloqueo de su cuenta de usuario como consecuencia del olvido de su usuario o clave de borrado involuntario/voluntario de información.
- Fugas de información
- Pérdida de los soportes que contienen datos de carácter personal de los bancos de datos personales de la empresa
- Gestión de información sin contar con la respectiva autorización
- Deficiencias en el control de las medidas de seguridad implementadas
- Realización de pruebas con datos reales sin garantizar las medidas de seguridad correspondientes
- Pérdida de un equipo de trabajo
- Vigencia de accesos para personal que haya dejado de prestar servicios
- Uso de contraseñas

Información relativa a los sistemas de información tenemos:

- Fallo en el sistema de copias de respaldo y restauración de la información
- Problemas con el software, incluidos sus parches y actualizaciones, de los equipos servidores o puestos de trabajo
- Problemas con el hardware de los equipos servidores o puestos de trabajo
- Imposibilidad de recuperación de información perdida
- Restauración de información
- Procesos “batch” ejecutados incorrectamente, erróneamente o no ejecutados
- Pérdidas de servicio en los sistemas
- Fallos en los sistemas de comunicaciones

Respecto a los factores externos:

- Robos
- Fraudes
- Factores meteorológicos tales como tormentas, inundaciones
- Ataques de acceso a los sistemas de información
- Perdidas de soporte como consecuencia de su externalización
- Difusión de virus y software malicioso
- Accesos no autorizados a información
- Pérdida de confidencialidad en información restringida o confidencial
- Pérdida de documentación en traslados, comunicaciones, envíos o entrega de la información contenida en los ficheros

Registro de backups que se realizan en la empresa: Se debe registrar los backups que se realizan por un posible incidente y revisarlos para garantizar la seguridad de la información de los involucrados.

Registrar Derechos ARCO:

Derecho de Acceso

- Se trata del derecho de una persona a solicitar información al responsable de un fichero sobre si sus datos personales están siendo tratados.
- En caso afirmativo, se deberá determinar con qué finalidad, el origen de esos datos y las comunicaciones realizadas o previstas de los mismos.
- No es necesario justificar el ejercicio de este derecho si no se ha ejercido en los últimos 12 meses.
- El plazo máximo para la resolución de la solicitud por parte del responsable del fichero es de 30 días desde la recepción de ésta.

- Tras la comunicación de resolución, el demandante dispondrá de 10 días hábiles para realizar el acceso.

Derecho de Rectificación

- Es el derecho que permite a la persona afectada solicitar la modificación de datos que sean inexactos o incompletos.
- En este caso debe justificarse qué datos son los referidos y su corrección, aportando documentación justificativa de la rectificación solicitada.
- El responsable del fichero dispone de 10 días hábiles para llevar a cabo la resolución.

Derecho de Oposición

Se trata del derecho de una persona a oponerse al tratamiento de sus datos personales o el cese de éstos en los casos:

- Que no sea necesario su consentimiento, en los que los ficheros se usen con finalidades publicitarias, o que el tratamiento tenga por finalidad la adopción de una decisión referida al afectado.
- Deberán hacerse constar los motivos fundados y legítimos, relativos a una concreta situación personal de la persona afectada, que justifiquen el ejercicio de este derecho.
- El responsable del fichero dispone de 10 días hábiles para llevar a cabo la resolución.

Derecho de Cancelación

Es por el cual el afectado puede solicitar la supresión de los datos que resulten inadecuados o excesivos, sin perjuicio del deber de bloqueo.

- Debe indicarse el dato a cancelar y el motivo, aportando documentación justificativa de la rectificación solicitada.
- El responsable del fichero dispone de 10 días hábiles para llevar a cabo la resolución.

Registrar Medidas Legales, Organizativas y Técnicas que exige el Reglamento de Protección de Datos Personales:

Se debe verificar que el sistema cumpla con las siguientes medidas de seguridad:

Medidas Organizativas

- Definir un responsable de seguridad
- Comunicar clara y oportunamente la Política de Seguridad de Información al interior de la organización.
- Llevar control de asignación y retiro de privilegios y acceso a la información contenida en el banco de datos personales y su correspondiente registro de acceso.
- Realizar un control periódico del cumplimiento de las políticas de seguridad
- Adecuación de los procesos del negocio involucrados en el tratamiento de datos personales a la Ley N°29733, Ley de Protección de Datos Personales.
- Desarrollar un procedimiento de control de acceso a datos personales
- Desarrollar un procedimiento de gestión de incidentes para la protección de datos personales

Medidas Legales

- Adecuar los contratos del personal y terceros relacionados al tratamiento de datos personales.
- Desarrollar formatos de consentimiento para el tratamiento de datos personales, adecuados y de conformidad con la finalidad para la cual son acopiadas.
- Desarrollar y mantener actualizado un documento de compromiso de confidencialidad en el tratamiento de datos personales.

Medidas Técnicas

Tabla 33 *Requerimientos - Medidas Técnicas*

Acceso No Autorizado al Banco de datos Personales	- Gestión y uso de contraseñas en medios informáticos. - Revisión y registro de los privilegios de acceso - Ubicación física segura para el banco de datos (llave, cerradura, etc.) - Mecanismos de autenticación - Autorización o Retiro de Acceso a un Usuario.
Alteración no autorizada de datos personales	- Seguridad en el traslado de información - Ubicación física que evite el acceso - Encriptación y mecanismo de verificación - Mecanismos seguros de eliminación - Mecanismos seguros de generación de copias y reproducción de documentos
A la pérdida de bancos personales	- Copias de respaldo de los datos personales - Técnicas de cifrado - Ubicación física segura de las copias de respaldo - Mecanismos de continuidad del tratamiento de los datos personales - Autorización para la recuperación de la copia de respaldo - Pruebas de verificación de integridad de los datos personales de la copia de respaldo
	- Datos personales deben ser independizados

Al tratamiento no autorizado de datos personales	- Informar el tratamiento no autorizado - Registrar los datos recuperados tras un incidente - Mantenimiento preventivo y correctivo de equipos - Poseer software de protección contra software malicioso (virus, troyanos, etc.) - Almacenamiento seguro - empleando mecanismos de control de acceso y - cifrada - Transporte de información personal mediante algún cifrado - Seguridad en el flujo transfronterizo de datos - personales. - Restringir el uso de equipos de fotografía, video, audio u otro

Fuente: Elaboración Propia

4.5.2.2 Definición de Casos de Uso

Los casos de uso representan una descripción a manera de secuencia de los pasos o actividades que deberán ser ejecutadas para desarrollar algún proceso, así como los actores que intervienen en cada una.

Para definir los casos de uso, es necesario definir primero a las personas (actores) que intervienen directamente en el sistema.

Administrador de sistemas: Es la persona encargada de realizar el mantenimiento de los usuarios, backups, incidencias, medidas de seguridad y de los derechos ARCO registrados. Además, es el encargado de otorgar y denegar permisos al sistema web.

Encargado de la seguridad lógica: Es la persona responsable de preservar la seguridad de información personal soportada en medios informáticos, como su nombre lo dice, preservar únicamente la seguridad lógica. Se encarga de registrar y gestionar las medidas de seguridad técnicas y organizativas, las incidencias y los derechos ARCO.

Responsable del Banco de Datos: Es la persona responsable de preservar la seguridad de información personal soportada en medios físicos e informáticos. Existe solo un responsable por cada banco de datos identificado, el cual se encarga del registro y gestión de las medidas organizativas y legales, de incidencias y de los derechos ARCO.

A continuación, en la siguiente figura se presenta el Resumen de Casos de Uso para el sistema web.

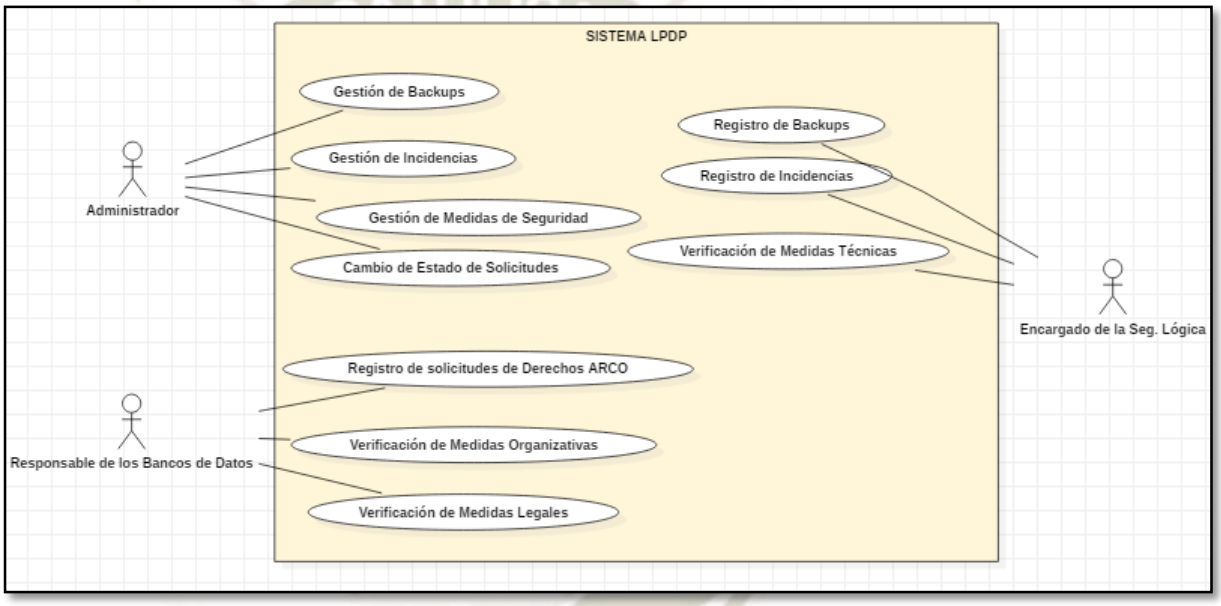


Figura 37 Diagrama de Casos de Uso

Fuente: Elaboración Propia

Tabla 34 *Especificación textual del caso de Uso*

ACCIÓN	ACTOR (ES)	OBJETIVO	PRECONDICIONES	POSTCONDICIONES	ESCENARIO BASICO
REGISTRO DE BACKUPS	Encargado de la seguridad lógica	Registrar los backups generados que contengan información de los bancos de datos personales.	Usuario registrado como encargado de seguridad lógica.	Backup registrado.	- Encargado inicia sesión. - En "Registro de Backups" el sistema solicita información para registrar el backup. - El encargado ingresa datos para el registro. - El encargado registra el backup.
GESTION DE BACKUPS	Administrador	Visualizar, editar y eliminar los backups registrados.	Usuario registrado como administrador. Registrar backups.	Backup actualizado y/o backup eliminado.	- Administrador inicia sesión. - En "Gestión de Backups" el sistema solicita la edición y/o eliminación del backup. - El administrador edita y/o elimina el backup.
REGISTRO DE INCIDENCIAS	Encargado de la seguridad lógica.	Registrar las incidencias que hayan ocasionado algún tipo de perjuicio a los bancos de datos personales.	Usuario registrado como encargado de seguridad lógica y/o	Incidencia registrada.	- Encargado y/o responsable inicia sesión. - En "Registro de Incidencias" el sistema

	Responsable del banco de datos.		responsable del banco de datos.		solicita información para registrar la incidencia. - El encargado y/o responsable ingresa datos para el registro. - El encargado registra la incidencia.
GESTION DE INCIDENCIAS	Administrador	Visualizar, editar y eliminar las incidencias registradas.	Usuario registrado como administrador. Registrar incidencias.	Incidencia actualizada y/o incidencia eliminada.	- Administrador inicia sesión. - En "Gestión de Incidencias" el sistema solicita la edición y/o eliminación de la incidencia. - El administrador edita y/o elimina la incidencia.
REGISTRO DE SOLICITUDES ARCO	Responsable del banco de datos	Registrar la solicitud de derechos ARCO recibidas por el reclamante o titular d los datos personales.	Usuario registrado como responsable del banco de datos.	Solicitud registrada.	- Responsable inicia sesión. - En "Registro de solicitudes ARCO" el sistema solicita información para registrar la solicitud - El responsable ingresa datos para el registro.

					- El responsable registra la solicitud recibida.
CAMBIO DE ESTADO	Administrador	Cambiar el estado de la solicitud recibida de "pendiente" a "atendido".	Usuario registrado como administrador. Registro de la solicitud de derechos ARCO con el adjunto correspondiente.	Solicitud registrada como atendida.	- Administrador inicia sesión. - Ir a Gestión de derechos ARCO. - Cambiar la solicitud que corresponda a "atendido".
VERIFICACIÓN DE MEDIDAS ORGANIZATIVAS	Responsable del banco de datos	Registrar las medidas de seguridad organizativas que cumpla y no cumpla la empresa.	Usuario registrado como responsable de banco de datos.	Medidas de seguridad organizativas revisadas y registradas.	- Responsable inicia sesión. - En "Medidas Organizativas" registrar las que se cumplen y las que no.
VERIFICACIÓN DE MEDIDAS LEGALES	Responsable del banco de datos	Registrar las medidas de seguridad legales que cumpla y no cumpla la empresa.	Usuario registrado como responsable de banco de datos.	Medidas de seguridad legales revisadas y registradas.	- Responsable inicia sesión. - En "Medidas Legales" registrar las que se cumplen y las que no.
VERIFICACIÓN DE MEDIDAS TÉCNICAS	Encargado de la seguridad lógica	Registrar las medidas de seguridad técnicas que cumpla y no cumpla la empresa.	Usuario registrado como responsable de banco de datos.	Medidas de seguridad técnicas revisadas y registradas.	- Responsable inicia sesión. - En "Medidas Técnicas" registrar las que se cumplen y las que no.

GESTIÓN DE MEDIDAS DE SEGURIDAD	Administrador	Verificar las medidas de seguridad que se cumplen en la empresa.	Usuario registrado como administrador. Registrar las medidas de seguridad.	Medidas de seguridad técnicas, legales y organizativas revisadas.	- Administrador inicia sesión. - En "Gestión de Medidas" el sistema solicita la visualización y eliminación de las medidas de seguridad registradas. - El administrador visualiza y/o elimina las medidas de seguridad revisadas.

Fuente: Elaboración Propia

4.5.2.3 Definición de Perfiles de acceso y privilegios

Es necesario definir los accesos y privilegios para cada usuario o actor definido anteriormente. En la siguiente tabla se podrá encontrar esta información.

Tabla 35 *Perfiles de Acceso y Privilegios*

USUARIO	DESCRIPCION	ACCESO	PRIVILEGIOS
Admin1	Administrador del sistema. (Encargado de la seguridad lógica)	Creación y gestión de backups. Creación y gestión de incidencias. Cambio de estado a solicitud de derechos ARCO. Medidas técnicas. Medidas organizativas. Medidas Legales.	Visualizar. Registrar. Editar Eliminar.
Sistemas1	Encargado de la seguridad lógica 2.	Creación y gestión de backups. Creación y gestión de incidencias. Medidas técnicas.	Visualizar. Registrar.
Responsable1	Responsable del banco de datos colaboradores y postulantes.	Creación y gestión de incidencias. Creación de solicitud de derechos ARCO. Medidas organizativas y medidas legales.	Visualizar. Registrar.
Responsable2	Responsable del banco de datos clientes.	Creación y gestión de incidencias. Creación de solicitud de derechos ARCO. Medidas organizativas y medidas legales.	Visualizar. Registrar.

Responsable3	Responsable del banco de datos proveedores.	Creación y gestión de incidencias. Creación de solicitud de derechos ARCO. Medidas organizativas y medidas legales.	Visualizar. Registrar.
Responsable4	Responsable del banco de datos visitantes y video vigilancia.	Creación y gestión de incidencias. Creación de solicitud de derechos ARCO. Medidas organizativas y medidas legales.	Visualizar. Registrar.

Fuente: Elaboración Propia

4.5.2.4 Diccionario de datos

Es necesario especificar el alojamiento de los datos que representan los casos de uso. De esta manera, se ha definido un diccionario de datos, el cual presenta la forma de almacenamiento.

Un diccionario de datos no es más que el conjunto de metadatos, el cual posee las características lógicas de los datos que serán usados.

Para este procedimiento se ha definido un estándar, en el cual se cita:

- Columna
- Tipo
- Nulo
- Predeterminado
- Comentarios

Tabla 36 *Diccionario de Datos – Tabla ARCO*

Columna	Tipo	Nulo	Predeterminado	Comentarios
id *(Primaria)*	int(255)	No		Clave primaria de reclamo ARCO
tipo	varchar(20)	No		Tipo de incidencia: Acceso Rectificación Cancelación Oposición
nombre	varchar(100)	No		Nombre de la persona que realiza el reclamo
fecha	date	Sí	*NULL*	Fecha del registro
estado	varchar(100)	No		Estado del reclamo: Pendiente, En Proceso, Solucionado
observaciones	text	Sí	*NULL*	Observaciones adicionales al reclamo
docreq	tinyint(1)	No		Indica si se ha adjuntado la documentación requerida.
archivo	string	No		Archivo adjunto de la solicitud ARCO
usuario_id	int(255)	No		Usuario que registra el reclamo

Fuente: Elaboración Propia

Tabla 37 *Índices - Tabla ARCO*

Nombre de la clave	Tipo	Único	Empaquetado	Columna	Cardinalidad	Cotejamiento	Nulo	Comentario
PRIMARY	BTREE	Sí	No	id	3	A	No	
fk_arco_usuario	BTREE	No	No	usuario_id	3	A	No	

Fuente: Elaboración Propia

Tabla 38 *Diccionario de Datos - Tabla Backup*

Columna	Tipo	Nulo	Predeterminado	Comentarios
id *(Primaria)*	int(255)	No		Clave primaria y única de Registro de Backup
nombre	varchar(100)	No		**Nombre del archivo o paquete de backups**
fecha	date	Sí	*NULL*	Fecha de registro de backup
verificado	tinyint(1)	No		Registra si el Backup ha sido verificado (Se puede restaurar o no)
comentarios	text	Sí	*NULL*	Comentarios adicionales a registro del backup
usuario_id	int(255)	No		Usuario que registra el backup

Fuente: Elaboración Propia

Tabla 39 *Índices - Tabla Backup*

Nombre de la clave	Tipo	Único	Empaquetado	Columna	Cardinalidad	Cotejamiento	Nulo	Comentario
PRIMARY	BTREE	Sí	No	id	3	A	No	
fk_backup_usuario	BTREE	No	No	usuario_id	3	A	No	

Fuente: Elaboración Propia

Tabla 40 *Diccionario de Datos - Tabla Incidencias*

Columna	Tipo	Nulo	Predeterminado	Comentarios
id *(Primaria)*	int(255)	No		Clave primaria de la incidencia
tipo	int(11)	No		Tipo de la incidencia: Usuarios, Sistemas o factores Externos
incidencia	varchar(100)	No		Nombre de la incidencia relacionada al tipo
fecha	date	No		Fecha de registro de la incidencia
efectos	text	Sí	*NULL*	Efectos negativos de la incidencia
usuario_id	int(255)	No		Usuario que registra la incidencia
crit	tinyint(1)	No		¿Afecta a un banco de datos critico?

Fuente: Elaboración Propia

Tabla 41 *Índices - Tabla* Incidencias

Nombre de la clave	Tipo	Único	Empaquetado	Columna	Cardinalidad	Cotejamiento	Nulo	Comentario
PRIMARY	BTREE	Sí	No	id	3	A	No	
fk_incidencia_usuario	BTREE	No	No	usuario_id	3	A	No	

Fuente: Elaboración Propia

Tabla 42 *Diccionario de Datos - Tabla Medidas*

Columna	Tipo	Nulo	Predeterminado	Comentarios
id *(Primaria)*	int(255)	No		Clave primaria de la medida de seguridad
medida	text	No		Descripción de la medida de seguridad

Fuente: Elaboración Propia

Tabla 43 *Índices - Tabla Medidas*

Nombre de la clave	Tipo	Único	Empaquetado	Columna	Cardinalidad	Cotejamiento	Nulo	Comentario
PRIMARY	BTREE	Sí	No	id	33	A	No	

Fuente: Elaboración Propia

Tabla 44 *Diccionario de Datos - Tabla Medidas_usuario*

Columna	Tipo	Nulo	Predeterminado	Comentarios
id *(Primaria)*	int(255)	No		Clave primaria de la relación de las medidas de seguridad y los usuarios
usuario_id	int(255)	No		Clave Usuario que registra la medida
medida_id	int(255)	No		Clave de Medida de Seguridad a evaluar
valor	tinyint(1)	No		Valor de la medida 0: No 1: Si
obs	text	Sí	*NULL*	Observaciones adicionales

Fuente: Elaboración Propia

Tabla 45 *Índices - Tabla Medidas_usuario*

Nombre de la clave	Tipo	Único	Empaquetado	Columna	Cardinalidad	Cotejamiento	Nulo	Comentario
PRIMARY	BTREE	Sí	No	id	0	A	No	
fk_mu_usuario	BTREE	No	No	usuario_id	0	A	No	Clave foránea Usuario
fk_mu_medida	BTREE	No	No	medida_id	0	A	No	Clave foránea Medida

Fuente: Elaboración Propia

Tabla 46 *Diccionario de Datos - Tabla Usuarios*

Columna	Tipo	Nulo	Predeterminado	Comentarios
id *(Primaria)*	int(255)	No		Clave primaria de usuario
nombre	varchar(100)	No		Nombre de Usuario
apellidos	varchar(100)	Sí	*NULL*	Apellidos de Usuario
usuario	varchar(255)	No		Nickname de usuario
password	varchar(255)	No		Password de usuario (Codificado BCRYPT)
rol	varchar(20)	No		Rol de Usuario: Admin, Sistemas o Responsable

imagen	varchar(255)	Sí	*NULL*	Imagen del usuario
empresa	varchar(100)	No		Empresa de Usuario

Fuente: Elaboración Propia

Tabla 47 *Índices - Tabla Usuarios*

Nombre de la clave	Tipo	Único	Empaquetado	Columna	Cardinalidad	Cotejamiento	Nulo	Comentario
PRIMARY	BTREE	Sí	No	id	13	A	No	
uq_usuario	BTREE	Sí	No	usuario	13	A	No	

Fuente: Elaboración Propia

En base al Diccionario de Datos definido y a los requerimientos Funcionales planteados, se tiene la información necesaria para representar la base de datos mediante un Diagrama de Clases, Diagrama Entidad-Relación y un Diagrama de Secuencias.

- **Diagrama de Clases**

  En este diagrama vemos las clases más relevantes del sistema web. Para proporcionar mayor claridad se han omitido los métodos get y set de cada atributo de cada clase.

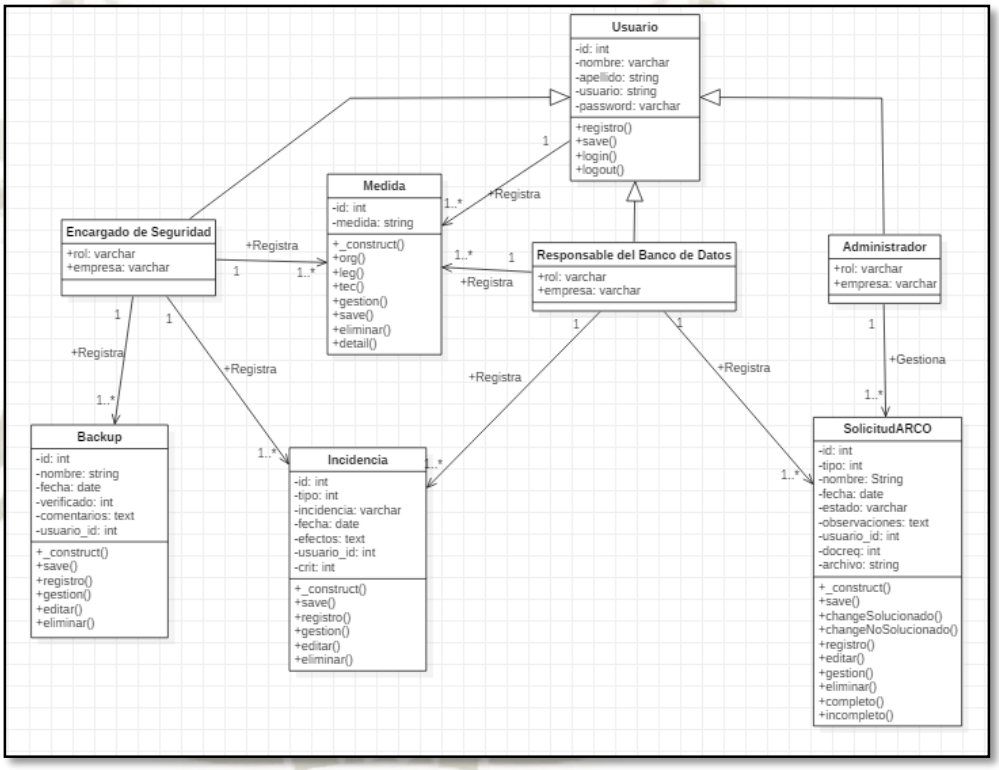


Figura 38 Diagrama de Clases

Fuente: Elaboración Propia

- **Diagrama Entidad-Relación**

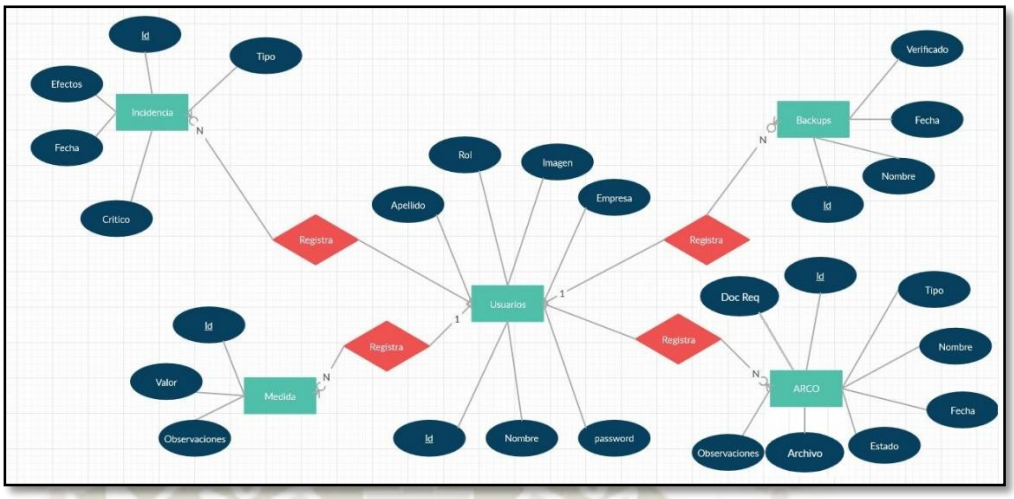


Figura 39 Diagrama Entidad-Relación

Fuente: Elaboración Propia

- **Diagrama de Secuencia**

  - **Registro de backups**

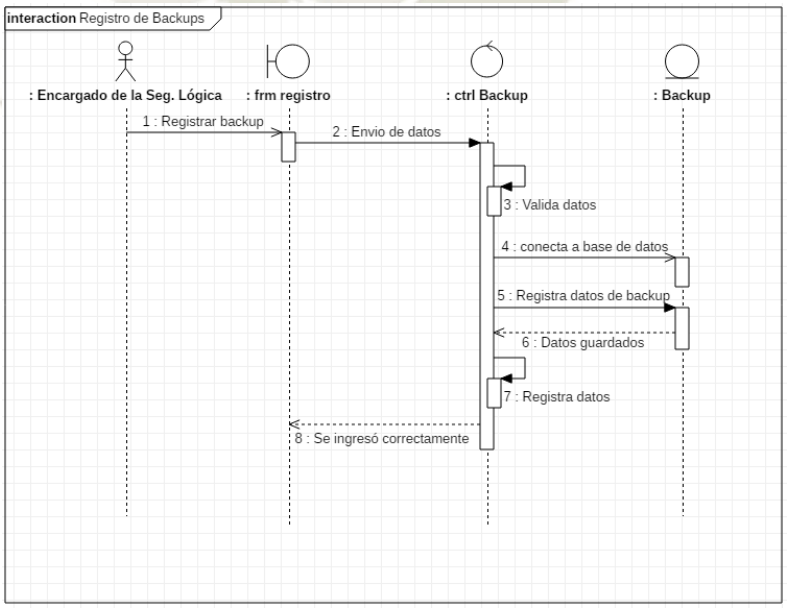


Figura 40 Diagrama de Secuencia – Registro de Backups

Fuente: Elaboración Propia

- **Registro de incidencias**

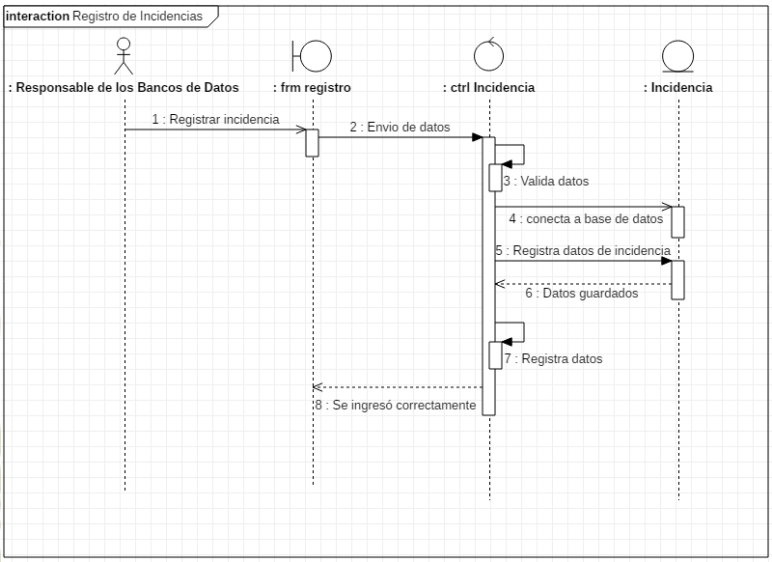


Figura 41 Diagrama de Secuencia – Registro de Incidencias

Fuente: Elaboración Propia

- **Gestión de backups**

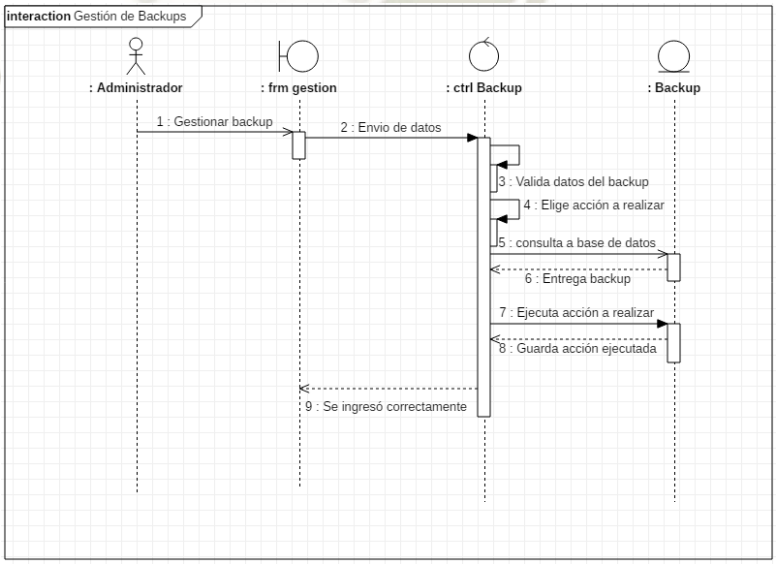


Figura 42 Diagrama de Secuencia - Gestión de Backups

Fuente: Elaboración Propia

- **Gestión de incidencias**

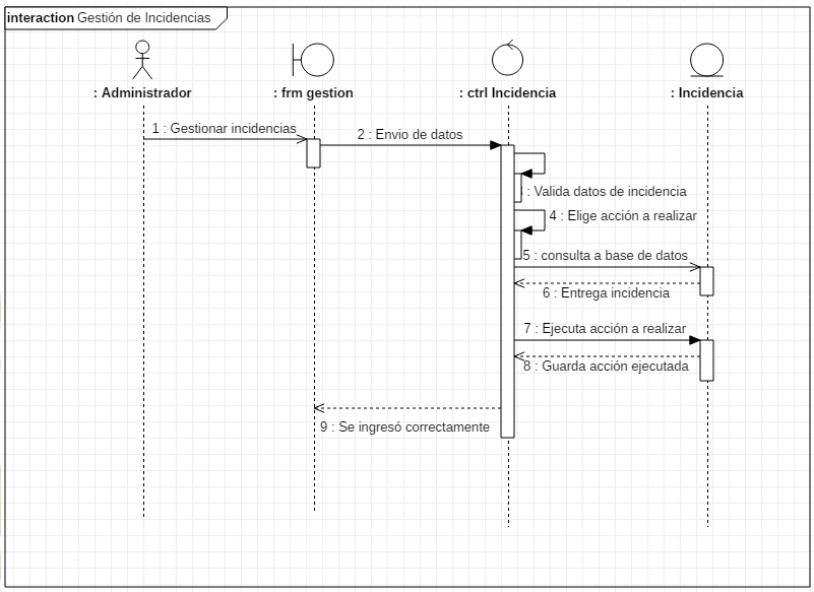


Figura 43 Diagrama de Secuencia - Gestión de incidencias

Fuente: Elaboración Propia

- **Registro de solicitudes ARCO**

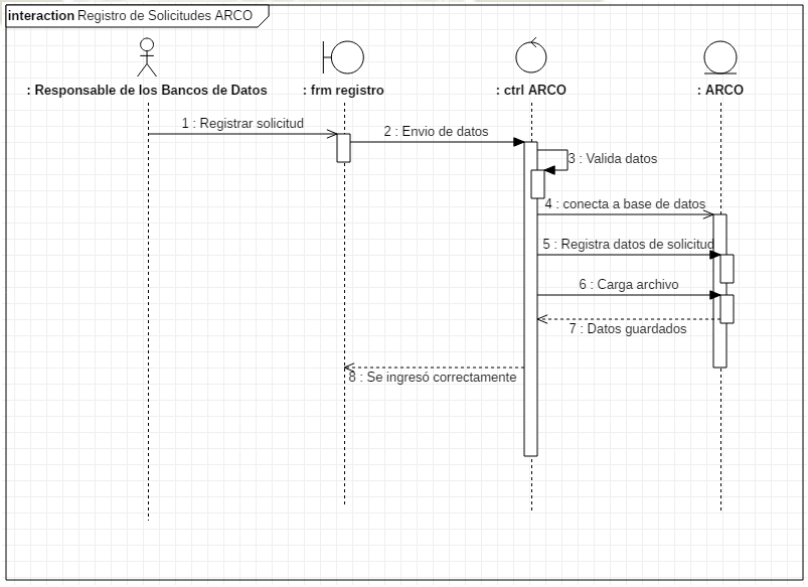


Figura 44 Diagrama de Secuencia - Registro de Solicitudes ARCO

Fuente: Elaboración Propia

- **Gestión de solicitudes ARCO**

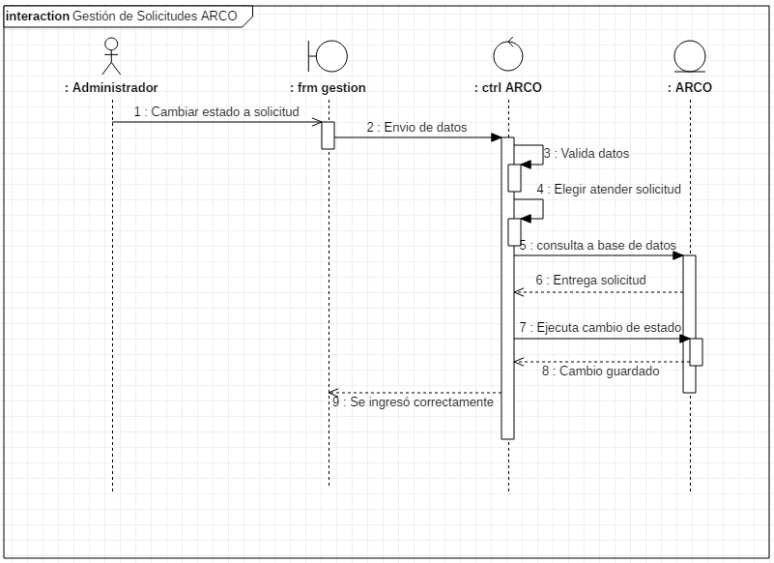


Figura 45 Diagrama de Secuencia - Gestión de solicitudes ARCO

Fuente: Elaboración Propia

- **Verificación de medidas organizativas**

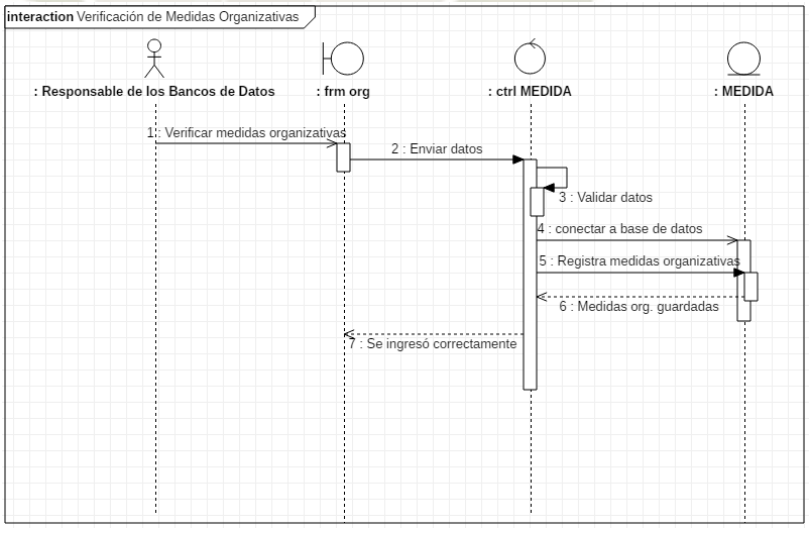


Figura 46 Diagrama de Secuencia - Verificación de medidas organizativas

Fuente: Elaboración Propia

- **Verificación de medidas legales**

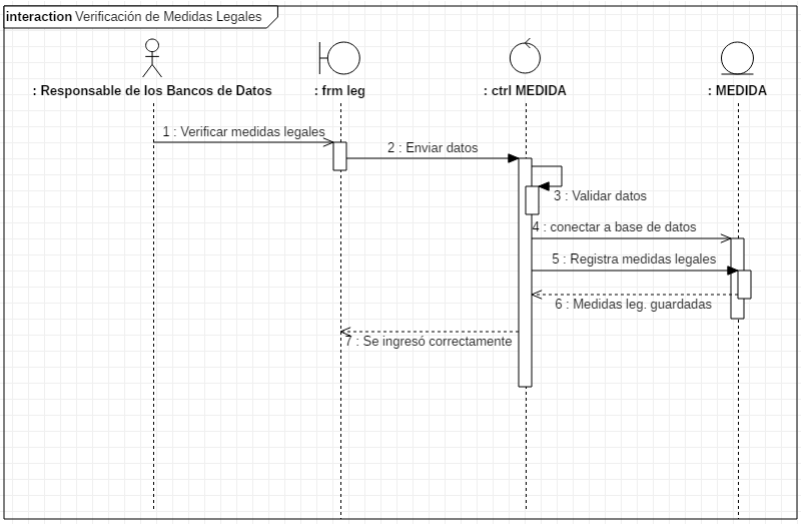


Figura 47 Diagrama de Secuencia - Verificación de medidas legales

Fuente: Elaboración Propia

- **Verificación de medidas técnicas**

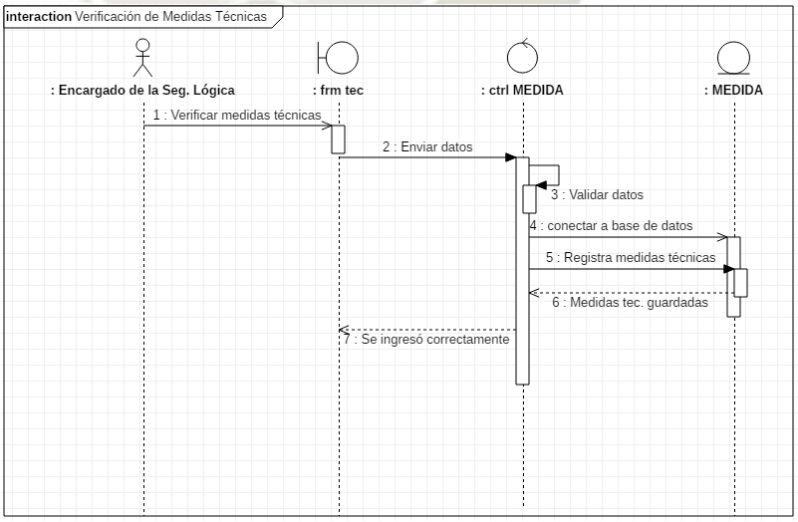


Figura 48 Diagrama de Secuencia - Verificación de medidas técnicas

Fuente: Elaboración Propia

- **Gestión de medidas de seguridad**

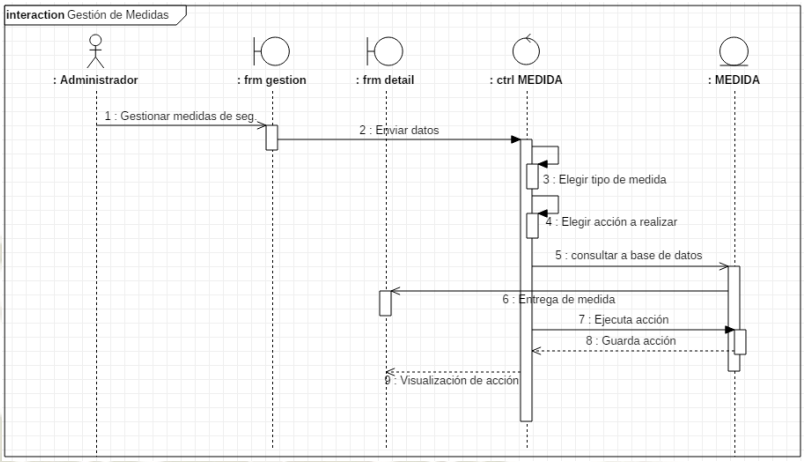


Figura 49 Diagrama de Secuencia - Gestión de medidas de seguridad

Fuente: Elaboración Propia

4.5.2.5 Diseño de Interfaces

Se muestran a continuación las interfaces que se emplearán para el sistema web, tomando en cuenta los requerimientos citados anteriormente, considerando aspectos de facilidad de uso y eficacia.

- ***Inicio del sistema***

La página de inicio al sistema web es la siguiente.

Figura 50 Inicio del Sistema de Control LPDP

Fuente: Elaboración Propia

Para que un usuario pueda acceder al sistema tendrá que hacerlo desde el menú “Entrar al sistema”.

Figura 51 Inicio de Sesión

Fuente: Elaboración Propia

En la figura anterior se presentan los datos requeridos para el inicio de sesión como son: Usuario y Contraseña.

Previamente se trató sobre los requerimientos que debe cumplir el sistema, lo cual se resume en las interfaces presentadas en la figura 52. Esto aplica para el Administrador del sistema, quien tiene un control sobre todas las interfaces.

Ahora se citarán los módulos que manejará el Administrador y posteriormente se detallará cada uno.

Figura 52 Módulos que controla el Administrador

Fuente: Elaboración Propia

- ***Registrar Backups***

Dentro de la interfaz “Registrar Backups” se podrá crear un nuevo registro de una copia de respaldo que se haya realizado. Estas copias de respaldo abarcan todo aquel medio informático que almacene información personal, por ejemplo: el sistema, la base de datos, computadoras del personal, discos duros, entre otros.

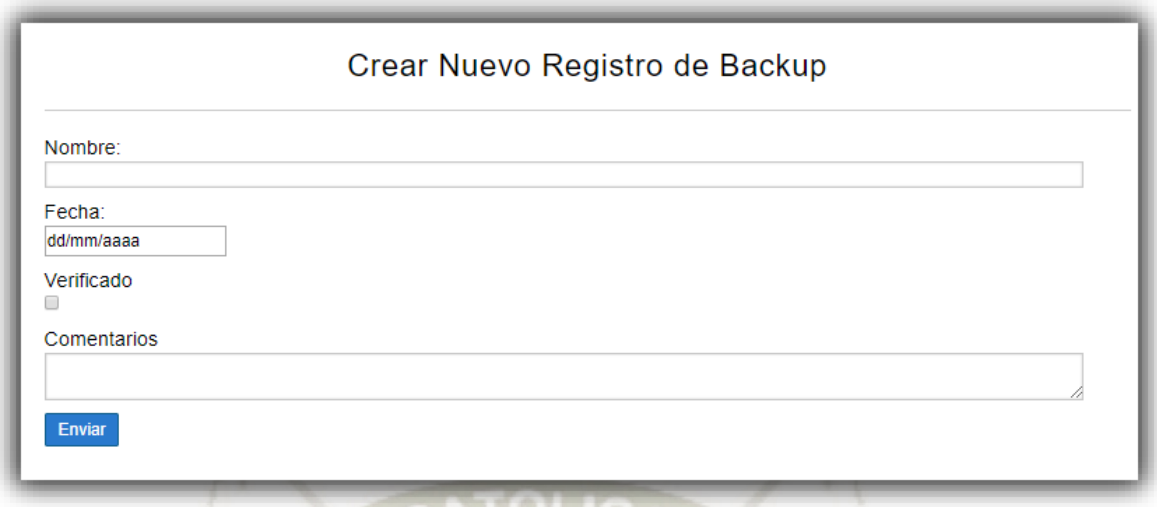


Figura 53 Interfaz para crear registro de Backup

Fuente: Elaboración Propia

En la figura anterior se puede apreciar un formulario en el cual se ingresará:

Nombre: Nombre de la persona que ha realizado el backup.

Fecha: Fecha en que se realizó el backup.

Verificado: Permite validar que la copia de respaldo se haya generado correctamente, es decir, que se pueda recuperar información íntegra de la copia de respaldo.

Comentario: Permite ingresar algún tipo de comentario u observación respecto a la copia de respaldo. Aquí se podrá especificar el medio informático al cual se genera la copia de respaldo.

Al presionar ***"Enviar"*** automáticamente se almacenará el registro del backup.

- ***Gestión de Backups***

A continuación, se presenta la interfaz para gestionar los backups:

Figura 54 Gestión de Backups

Fuente: Elaboración Propia

En la figura anterior, se puede apreciar claramente cómo se debe mostrar un registro generado en la interfaz anterior.

A través de esta interfaz se podrá dar mantenimiento a dicho registro.

Crear Backup: Permite crear un nuevo registro de Backup.

Editar: Permite modificar o actualizar un registro de backup ya existente.

Eliminar: Permite borrar un registro de backup generado por equivocación o que no fue verificado correctamente.

- ***Registro de Incidencias***

Dentro de la interfaz "Registro de Incidencias" se podrá crear un registro de una incidencia ocasionada dentro de la empresa. De acuerdo a los requerimientos para la gestión de incidencias citadas previamente en la sección de *Análisis de Requerimientos* las incidencias podrán ser diversas de acuerdo al tipo de incidencia seleccionado.

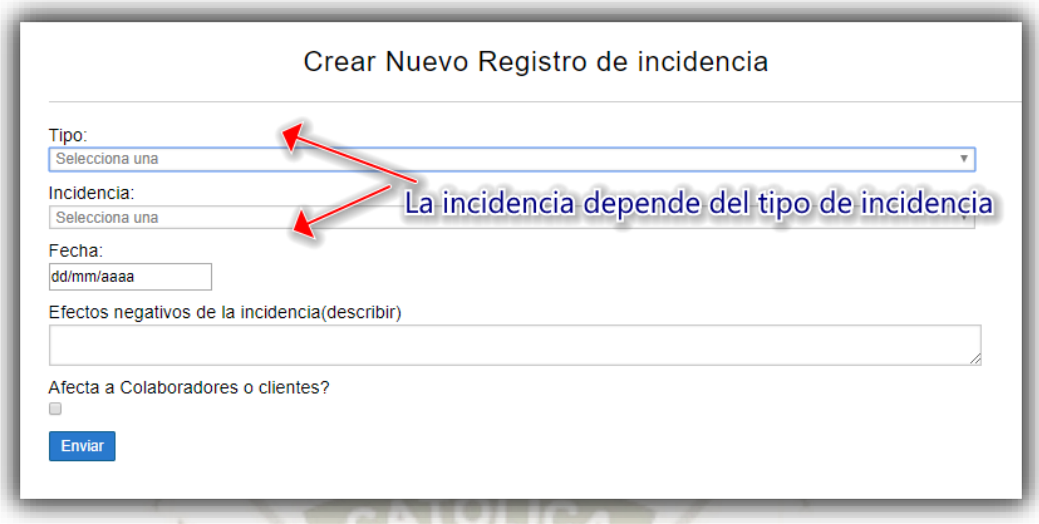


Figura 55 Interfaz para crear registro de incidencias

Fuente: Elaboración Propia

En la figura anterior se puede apreciar un formulario en el cual se ingresará:

Tipo: Es el tipo de incidencia que se requiere registrar. Los tipos están especificados en la sección de *Análisis de requerimientos.*

Incidencia: Es la incidencia ocasionada propiamente dicha. Las incidencias mostradas dependen del tipo. Las incidencias están especificadas en la sección de *Análisis de Requerimientos.*

Fecha: Es la fecha en que ha ocurrido el incidente.

Efectos negativos: Permite describir las consecuencias negativas que provocó el incidente.

Afecta a algún Banco Crítico: Permite validar si la incidencia ocurrida es crítica. Esto sirve para tener un control de aquellos incidentes críticos y verificar que la información personal no haya sido sometida a un tratamiento inadecuado.

Al presionar ***"Enviar"*** automáticamente se almacenará el registro de la incidencia.

- ***Gestión de Incidencias***

A continuación, se presenta la interfaz para gestionar incidencias ocurridas en la empresa:

Figura 56 Gestión de Incidencias

Fuente: Elaboración Propia

En la figura anterior, se puede apreciar claramente cómo se debe mostrar un registro generado en la interfaz anterior.

A través de esta interfaz se podrá dar mantenimiento a dicho registro.

Crear Incidencia: Permite crear un nuevo registro de incidencias.

Editar: Permite modificar o actualizar un registro de incidencias ya existente.

Eliminar: Permite borrar un registro de incidencias generado erróneamente o por equivocación.

- ***Registro de Derechos ARCO***

Dentro de la interfaz "Registro de Derechos ARCO" se podrá crear un registro de un ejercicio de derecho ARCO solicitado por el titular de datos personales dirigido a la empresa. De acuerdo a los requerimientos para el registro de derechos ARCO citados previamente en la sección de *Análisis de Requerimientos* los tipos de derechos ARCO serán de Acceso, Rectificación, Cancelación u Oposición.

Figura 57 Interfaz para crear Derecho ARCO

Fuente: Elaboración Propia

En la figura anterior se puede apreciar un formulario en el cual se ingresará:

Tipo: Es el tipo de derecho ARCO que se requiere registrar. Los tipos están especificados en la sección de *Análisis de requerimientos.*

Nombre de Persona Solicitante: Es el titular de los datos personales que desea ejercer sus derechos ARCO.

Fecha: Es la fecha en que se recibe la solicitud de derecho ARCO por parte del reclamante.

Observaciones y/o anotaciones: Permite describir alguna observación que sea necesaria e importante en la solicitud de derecho ARCO.

¿Adjunta Doc. Requerida? : Permite validar si el reclamante ha adjuntado la documentación que acredite lo solicitado.

Documentación: *Permite adjuntar todos los documentos que sean convenientes para proceder con la solicitud.*

Al presionar ***"Enviar"*** automáticamente se almacenará el registro de la solicitud del derecho ARCO.

- ***Gestión de Solicitudes de Derechos ARCO***

A continuación, se presenta la interfaz para gestionar los derechos ARCO solicitados y dirigidos a la empresa ***(mostrada únicamente para el usuario de Administrador)***:

Figura 58 Cambio de estado de las Solicitudes de Derechos ARCO - Administrador

Fuente: Elaboración Propia

A través de esta interfaz se podrá cambiar de estado a la solicitud de "pendiente" a "atendido". En donde:

Crear Solicitud de Derechos ARCO: Permite crear un nuevo registro de solicitud de derechos ARCO.

Días Transcurridos: Permite conocer los días transcurrido después de registrar la solicitud del reclamante.

Doc: Permite visualizar y descargar el archivo .zip o .rar adjuntado a la solicitud.

Atendido: Permite cambiar el estado de la solicitud a "atendido".

- ***Medidas Organizativas***

Dentro de la interfaz "Medidas Organizativas" se podrá verificar que hayan cumplido dichas medidas según los requerimientos en *Registrar Medidas Legales, Organizativas y Técnicas que exige la Ley de Protección de Datos Personales* citados previamente en la sección de *Análisis de Requerimientos.*

El sistema además permitirá guardar un registro del avance de la implementación de las medidas organizativas.

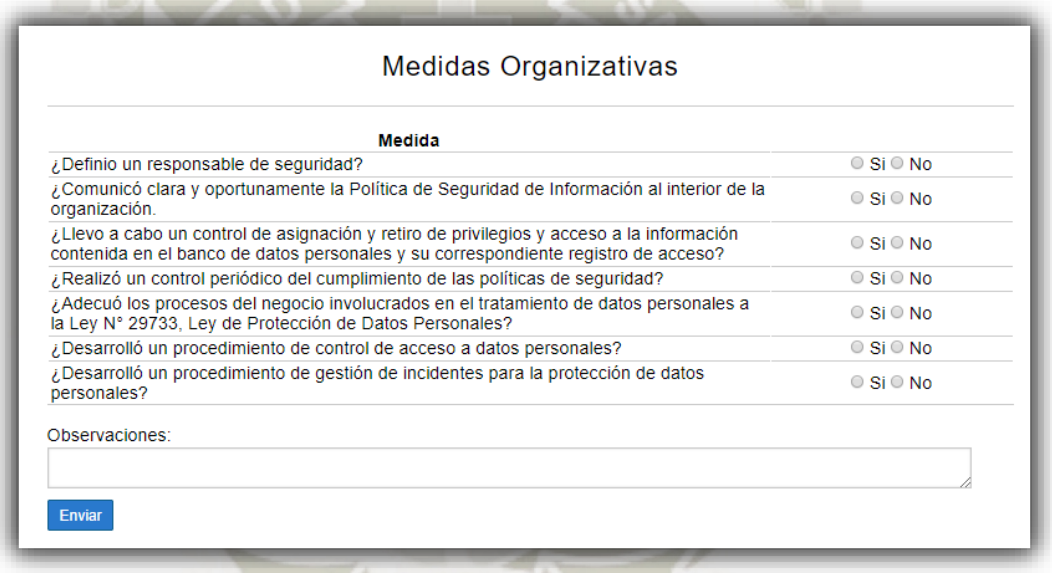


Figura 59 Medidas Organizativas

Fuente: Elaboración Propia

En la figura anterior se puede apreciar un formulario en el cual se verificará el cumplimiento de cada una de las medidas organizativas requeridas para cumplir con el reglamento de la Ley de Protección de Datos Personales.

En la parte inferior se podrá ingresar alguna observación necesaria a la validación de estas medidas.

Al presionar “Enviar” automáticamente se almacenará un registro de avance del cumplimiento de las medidas organizativas.

- ***Medidas Legales***

Dentro de la interfaz “Medidas Legales” se podrá verificar que hayan cumplido dichas medidas según los requerimientos en Registrar Medidas Legales, Organizativas y Técnicas que exige la Ley de Protección de Datos Personales citados previamente en la sección de Análisis de Requerimientos.

El sistema además permitirá guardar un registro del avance de la implementación de las medidas legales.

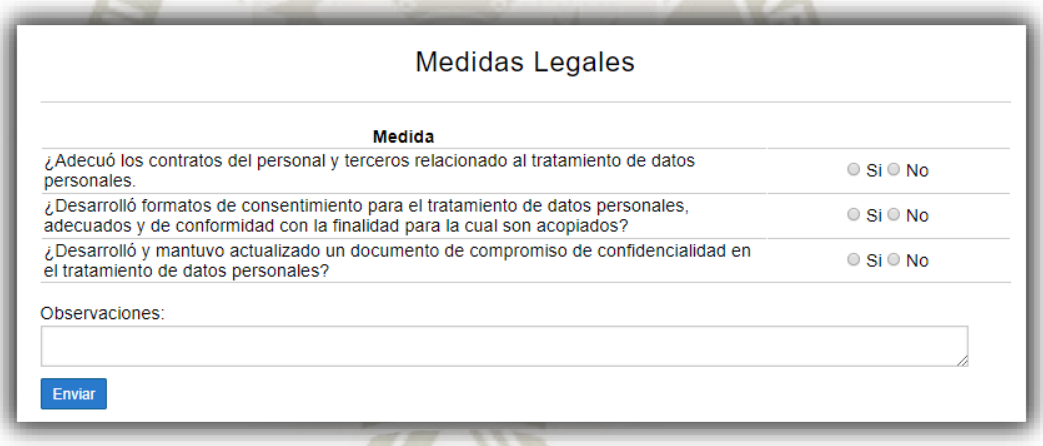


Figura 60 Medidas Legales

Fuente: Elaboración Propia

En la figura anterior se puede apreciar un formulario en el cual se verificará el cumplimiento de cada una de las medidas legales requeridas para cumplir con el reglamento de la Ley de Protección de Datos Personales.

En la parte inferior se podrá ingresar alguna observación necesaria a la validación de estas medidas.

Al presionar **"Enviar"** automáticamente se almacenará un registro de avance del cumplimiento de las medidas legales.

- ***Medidas Técnicas***

Dentro de la interfaz "Medidas Técnicas" se podrá verificar que hayan cumplido dichas medidas.

Según los requerimientos en Registrar Medidas Legales, Organizativas y Técnicas que exige la Ley de Protección de Datos Personales citados previamente en la sección de Análisis de Requerimientos las medidas técnicas son evaluadas en cuatro categorías.

- Acceso no autorizado
- Alteración no autorizada
- A la pérdida del Banco de Datos
- Al tratamiento no autorizado

El sistema además permitirá guardar un registro del avance de la implementación de las medidas técnicas.

La siguiente imagen hace referencia a aquellas medidas técnicas que deben ser implementadas para evitar el acceso no autorizado al sistema que gestiona y almacena información personal.

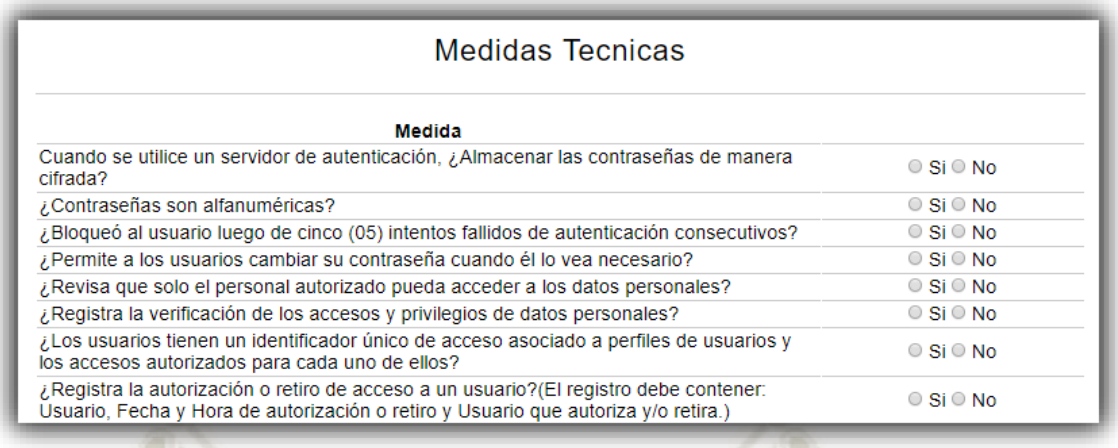


Figura 61 Medidas Técnicas – Acceso No Autorizado

Fuente: Elaboración Propia

La siguiente imagen hace referencia a aquellas medidas técnicas que deben ser implementadas para evitar la alteración no autorizada de la información personal que almacena el sistema.

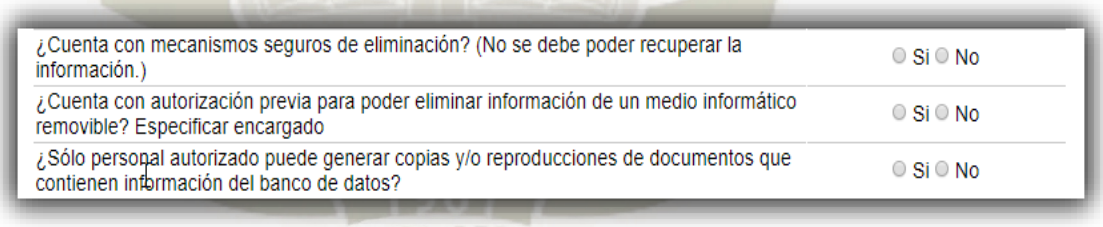


Figura 62 Medidas Técnicas – Alteración No Autorizada

Fuente: Elaboración Propia

La siguiente imagen hace referencia a aquellas medidas técnicas que deben ser implementadas para evitar la pérdida de información de un banco de datos.

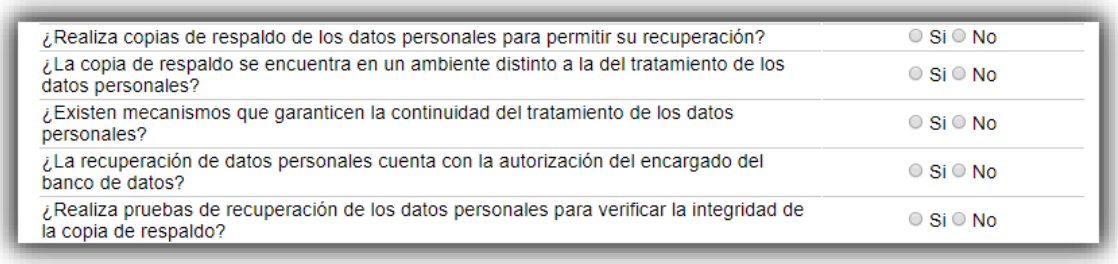


Figura 63 Medidas Técnicas – A la pérdida del Banco de Datos

Fuente: Elaboración Propia

La siguiente imagen hace referencia a aquellas medidas técnicas que deben ser implementadas para evitar el tratamiento no autorizado de la información personal que almacena el sistema.

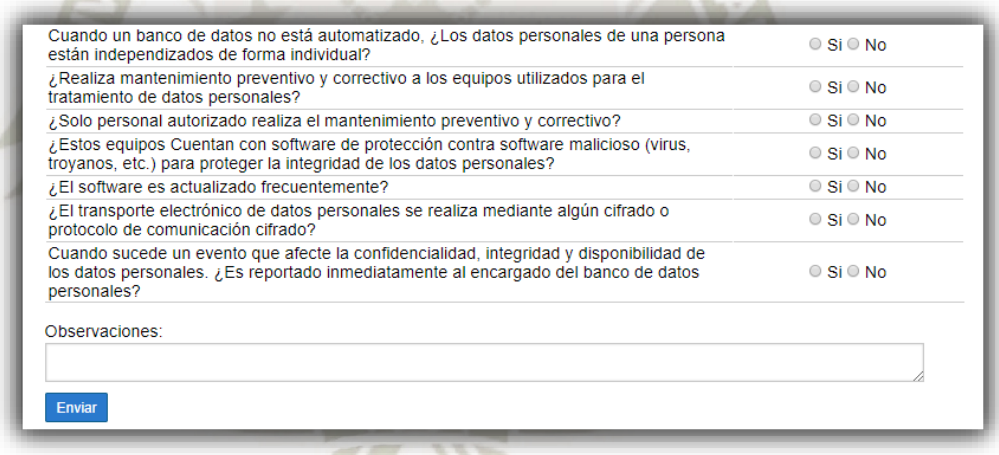


Figura 64 Medidas Técnicas – Al Tratamiento No Autorizado

Fuente: Elaboración Propia

En las figuras anteriores se puede apreciar un formulario en el cual se verificará el cumplimiento de cada una de las medidas técnicas requeridas para cumplir con el reglamento de la Ley de Protección de Datos Personales.

En la parte inferior se podrá ingresar alguna observación necesaria a la validación de estas medidas.

Al presionar **"Enviar"** automáticamente se almacenará un registro de avance del cumplimiento de las medidas técnicas.

4.5.3 Desarrollo del sistema web

Se expondrá la manera en la cual ha sido desarrollado el sistema web, basando el trabajo en el contexto tecnológico previamente definido, empezando por la configuración de las herramientas empleadas, continuando con la aplicación de estándares, y finalmente presentando la estructura desarrollada de cada uno de las interfaces del sistema web.

Para el proyecto utilizaremos el IDE NetBeans con el servidor APACHE y base de datos Mysql (WAMP)

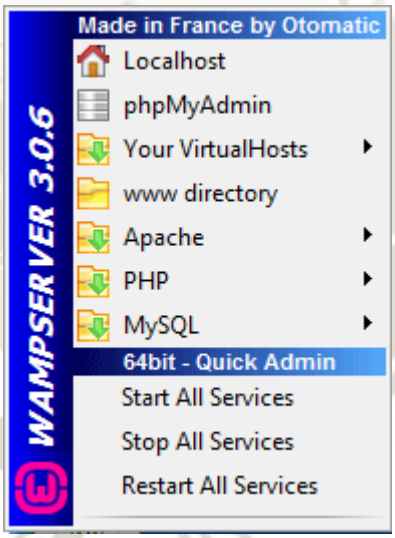


Figura 65 Wamp Server

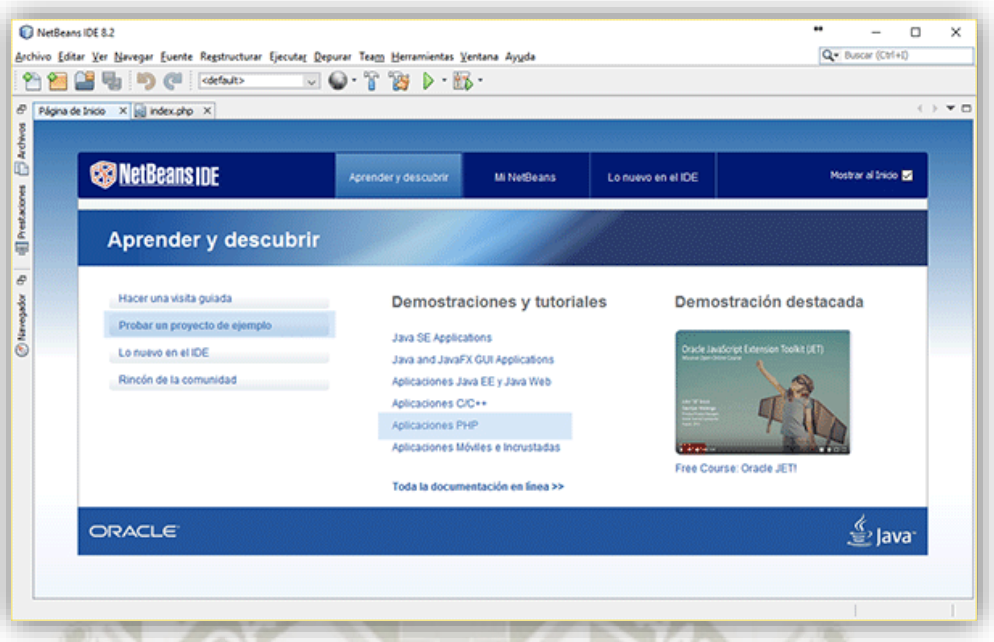


Figura 66 IDE Netbeans

Se iniciará con la creación del proyecto en PHP.

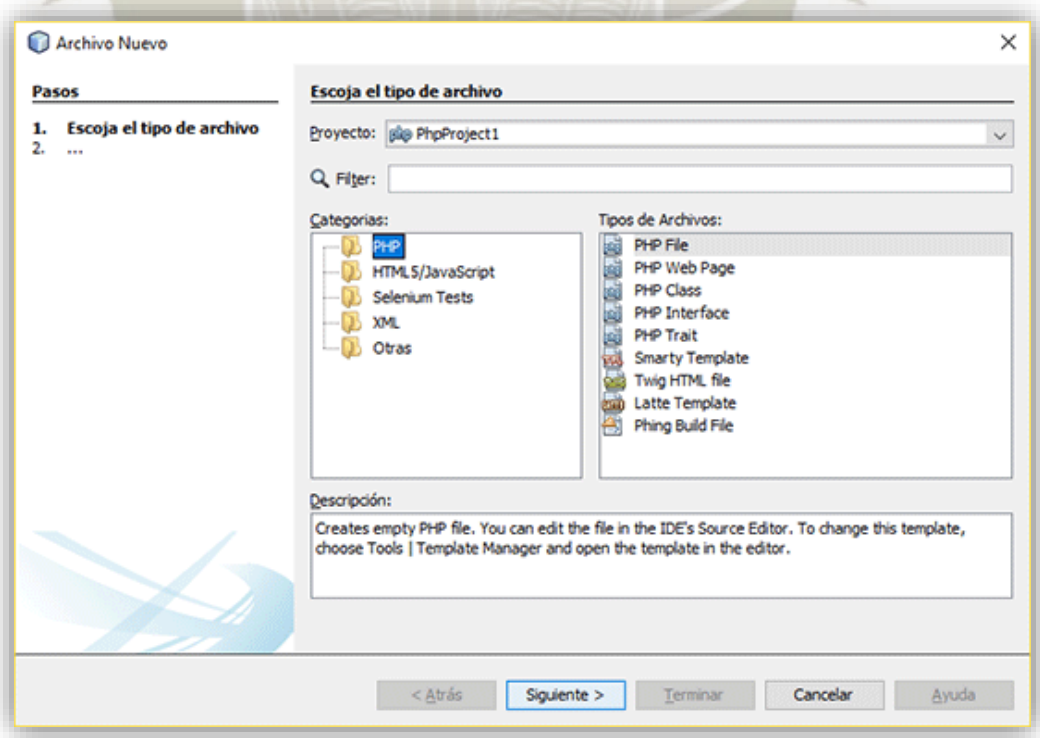


Figura 67 Crear nuevo proyecto en PHP

4.5.3.1 Desarrollo

Es primordial que se defina el esquema de la base de datos dentro de la aplicación, esto se lo hace a través de la herramienta de mapeo de bases de datos que brinda Mysql, para lo cual usaremos el gestor phpmyadmin para su gestión.

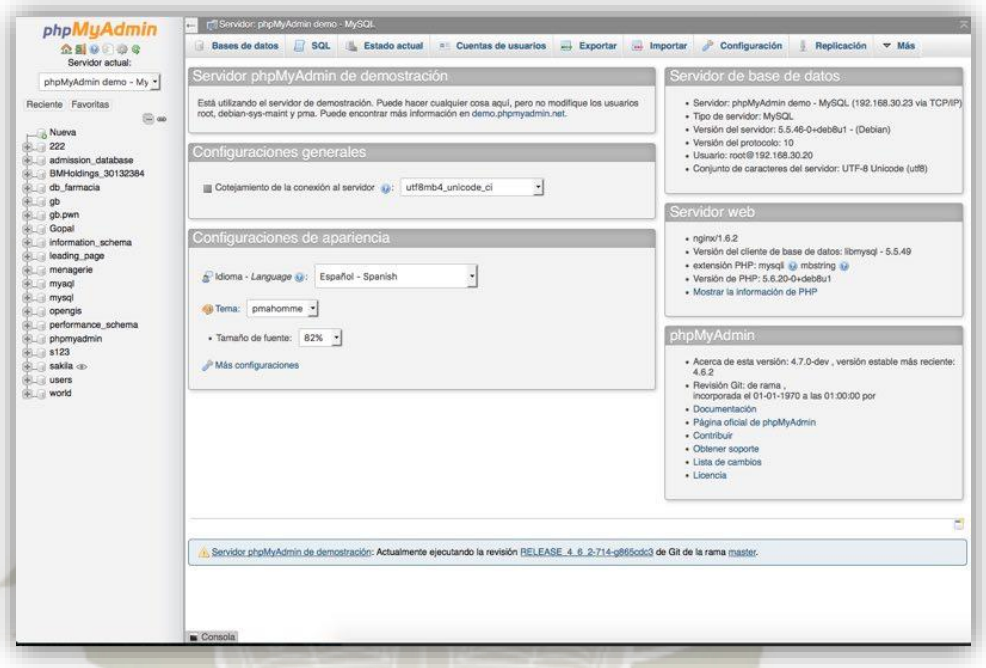


Figura 68 Phpmyadmin

Para poder trabajar se insertará las tablas ya diseñadas con sus respectivas claves (PKS y FKS)

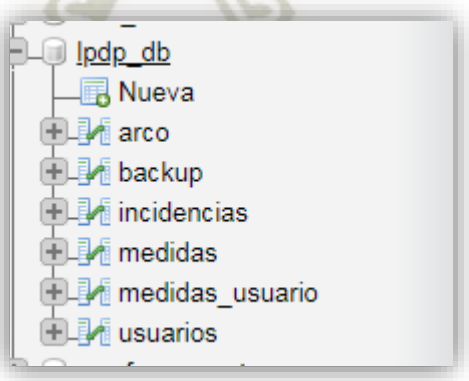


Figura 69 Tablas de la Base de Datos

En el IDE se creará las carpetas en donde estarán los archivos.

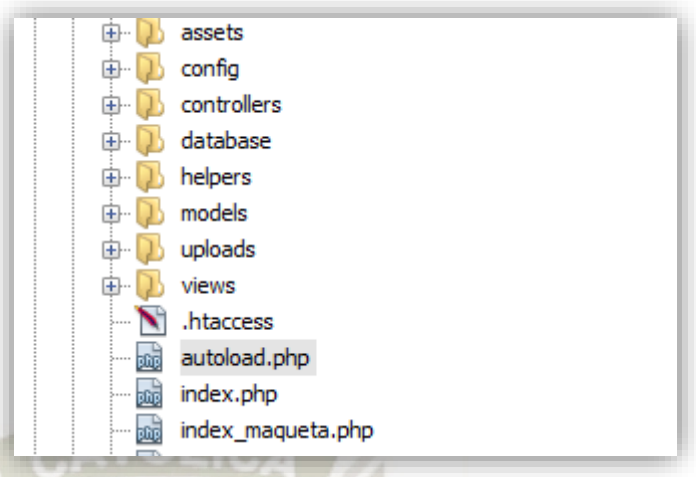


Figura 70 Carpetas del Proyecto

Assets: Están ubicados los archivos css y js que tendrá nuestro proyecto

Config: Conexiones a la base de datos y asignación de variables estáticas

Controllers: Controladores de la aplicación con la siguiente sintaxis (nombre)+Controller.php

Database: Esta incluido el script total de la base de datos para una migración.

Uploads: Se colocan los archivos subidos al sistema (imágenes de usuarios, etc.).

Views: Se encuentran las vistas que usaremos en el proyecto

Añadimos el archivo **htaccess** para crear rutas amigables al usuario al momento de la redirección.

<IfModule mod_rewrite.c>

Activar rewrite

RewriteEngine on

ErrorDocument 404 http://localhost/lpdp/error/

```
RewriteCond %{SCRIPT_FILENAME} !-d

RewriteCond %{SCRIPT_FILENAME} !-f

Rewriterule ^(.*)/(.*) index.php?controller=$1&action=$2

</IfModule>
```

4.5.4 Ejecución de Pruebas al sistema web

Tiene como finalidad presentar la ejecución de la aplicación web desarrollada, haciendo uso de las interfaces implementadas, con el objeto de analizar los resultados obtenidos y compararlos con los requerimientos.

4.5.4.1 Inicio de Sesión

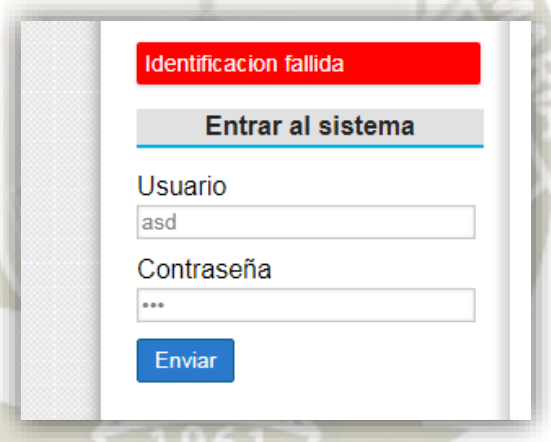


Figura 71 Pruebas - Inicio de Sesión

Fuente: Elaboración Propia

4.5.4.2 Crear Registro de Incidencia

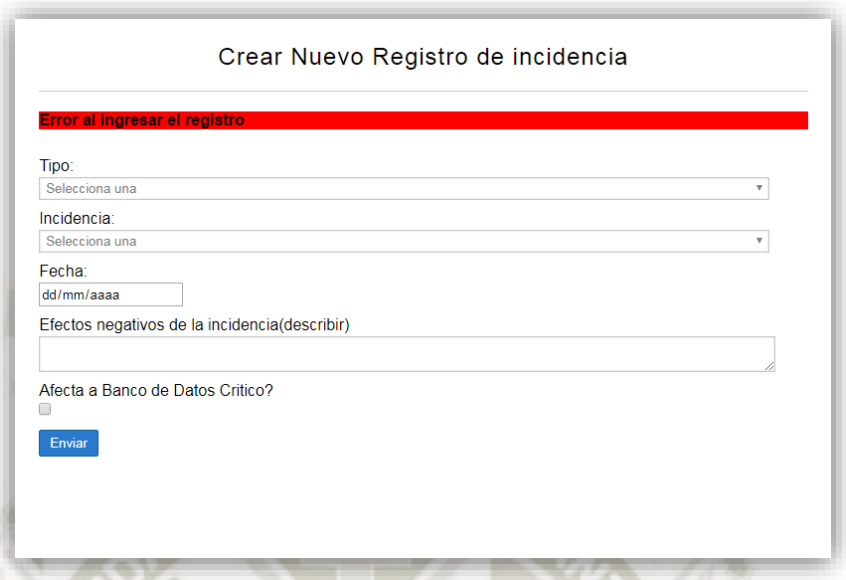


Figura 72 Pruebas - Crear Registro de Incidencia

Fuente: Elaboración Propia

4.5.4.3 Medidas de Seguridad

Figura 73 Pruebas - Medidas de Seguridad

Fuente: Elaboración Propia

4.5.4.4 Gestión de Backups

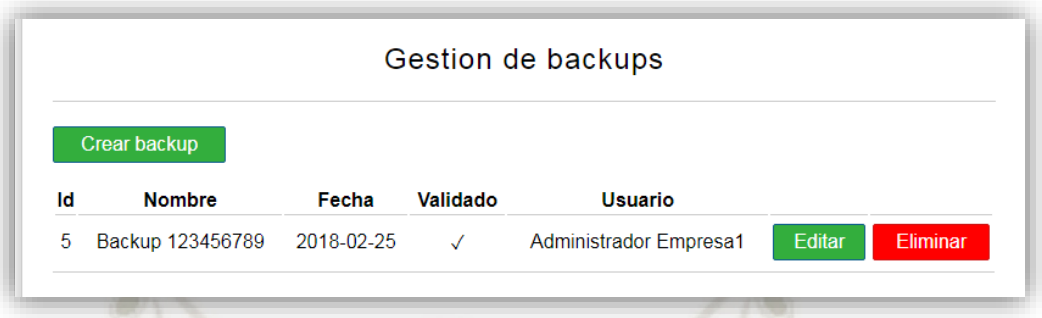


Figura 74 Pruebas - Gestión de Backups

Fuente: Elaboración Propia

4.5.4.5 Gestión de Incidencias

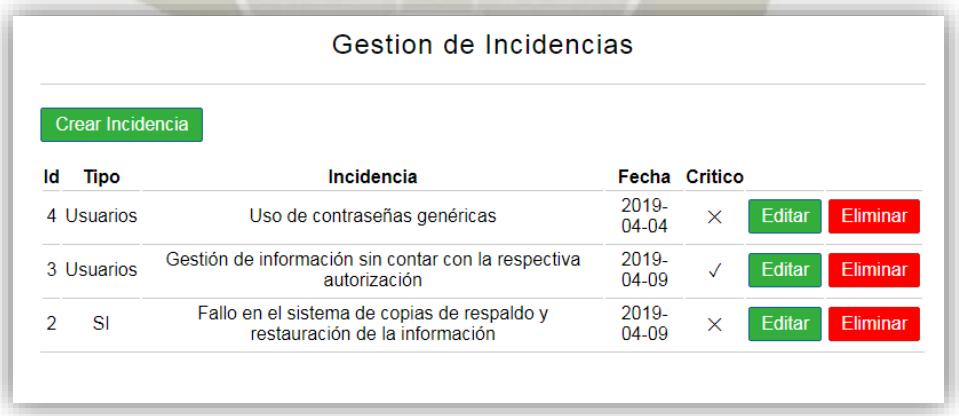


Figura 75 Pruebas - Gestión de Incidencias

Fuente: Elaboración Propia

4.5.4.6 Registro de Solicitudes de derechos ARCO

Figura 76 Prueba – Carga de archivo adjunto de derechos ARCO

Fuente: Elaboración Propia

Figura 77 Prueba - Visualización de archivo adjunto

Fuente: Elaboración Propia

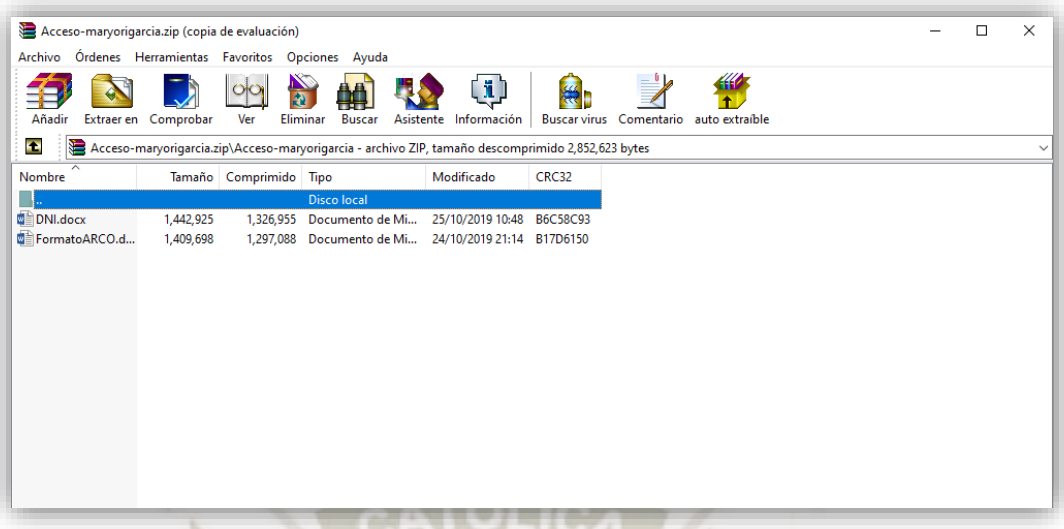


Figura 78 Prueba - Descarga del archivo adjunto

Fuente: Elaboración Propia

4.5.4.7 Gestión de Solicitudes de derechos ARCO

La siguiente figura muestra la alerta que es lanzada cada vez que se quiere ingresar a la interfaz de gestión de solicitudes de Derechos ARCO.

Figura 79 Alerta de vencimiento de Solicitud de Derechos ARCO

Fuente: Elaboración Propia

La alerta permitirá conocer cuántas solicitudes ya han sido vencidas y las que estarán por vencer. Es decir:

- **ACCESO:** La solicitud de acceso será vencida después de 20 días de recibida la solicitud por parte del reclamante.
- **RECTIFICACIÓN:** La solicitud de acceso será vencida después de 10 días de recibida la solicitud por parte del reclamante.
- **CANCELACIÓN:** La solicitud de acceso será vencida después de 10 días de recibida la solicitud por parte del reclamante.
- **OPOSICIÓN:** La solicitud de acceso será vencida después de 10 días de recibida la solicitud por parte del reclamante.

A continuación, se presenta la interfaz para gestionar los derechos ARCO solicitados y dirigidos a la empresa ***(mostrada únicamente para el usuario de Responsable del Banco de Datos)***:

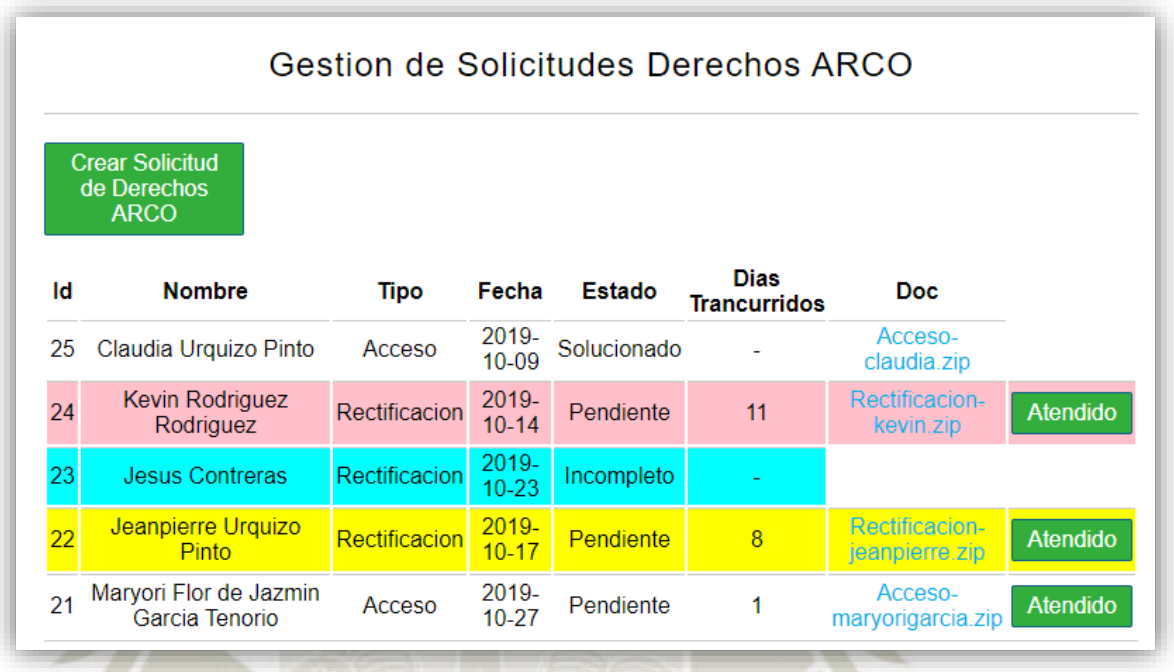


Figura 80 Cambio de estado de las Solicitudes de Derechos ARCO – Responsable del Banco de Datos

Fuente: Elaboración Propia

En donde, se puede visualizar cuál es el estado de la solicitud registrada, si se ha adjuntado los documentos requeridos y los días transcurridos.

A continuación, detallaremos el significado de cada estado y el color asociado:

- **Pendiente (Blanco):** Cuando la solicitud ha sido registrada en el sistema pero aún no se ha atendido ni respondido al reclamante.
- **Pendiente (Amarillo):** Cuando la solicitud registrada está a 2 días de vencer el plazo de respuesta.

- **Pendiente (Rojo):** Cuando la solicitud no ha sido atendida porque se venció el plazo de respuesta a dicha solicitud.
- **Solucionado (Blanco):** Cuando la solicitud ha sido atendida y respondida al reclamante.
- **Incompleto (Celeste):** Cuando la solicitud ha sido recepcionada pero no se ha adjuntado documentación requerida para que la solicitud sea atendida.

4.5.4.8 Gestión de medidas de seguridad

Figura 81 Pruebas - Gestión de Medidas de Seguridad

Fuente: Elaboración Propia

CAPITULO V

5. ANÁLISIS Y DISCUSIÓN

El propósito fundamental de esta investigación fue proponer una metodología para implementar la Ley N°29733, Ley de Protección de Datos Personales con sus respectivos controles y medidas de seguridad en el tratamiento de los datos personales.

Para dar respuesta a este objetivo se ha aplicado un cuestionario a los empleados de Michell y Cía. a través de un **muestreo no probabilístico por cuotas.**

La población o universo son todos los empleados administrativos de la empresa porque son los que realizan un tratamiento con los datos personales, y las variables clave empleadas para dividir la población en grupos fueron:

1. *Participación en el Comité de Ley de Protección de Datos Personales.*
2. *Nivel de responsabilidad del área.*
3. *Alto nivel de tratamiento físico de datos personales.*
4. *Alto nivel de tratamiento lógico de datos personales.*

Tabla 48 *Criterios para dividir la población en grupos*

GRUPO	DESCRIPCION DEL GRUPO
Participación en el comité de LPDP	Miembros del comité de LPDP.
Nivel de responsabilidad del área	Empleados que sean gerentes y jefes de área y que no pertenezcan al comité de LPDP.
Alto nivel de tratamiento físico de datos personales.	Empleados que realizan un frecuente uso o tratamiento físico de datos personales.

Alto nivel de tratamiento lógico de datos personales.	Empleados que realizan un frecuente uso o tratamiento lógico de datos personales.

Fuente: Elaboración Propia

Tabla 49 *Miembros que conforman la muestra*

GRUPO	MIEMBROS DEL GRUPO
Participación en el comité de LPDP	Responsables de los bancos de datos: - Jefe de RRH - Gerente Comercial - Gerente Administrativo - Jefe de Retail en Sol Alpaca - Jefe de Logística Encargado de la seguridad lógica de los bancos de datos. - Gerente de TI Encargado de gestionar el correo lpdp@michell.com.pe - Jefe de Proyectos de TI
Nivel de responsabilidad de área	- Gerente Financiero - Gerente de Contabilidad - Gerente de Producción - Gerente de Proyectos - Gerente de Marketing - Gerente de Operaciones - Jefa de Negocios Electrónicos - Jefa de Exportaciones e Importaciones - Jefe de Logística – Sol Alpaca - Jefe de Vigilancia - Jefa de Bienestar Social

Alto nivel de tratamiento físico de datos personales.	- Médico Ocupacional - Asistentes de Recursos Humanos - Secretaria de Gerencia Comercial - Asistente de Exportaciones e Importaciones - Asistente de Logística – Sol Alpaca - Asistente de Caja - Vigilante - Asistenta Social
Alto nivel de tratamiento lógico de datos personales.	- Administrador de Base de Datos - Jefes de sistemas (Sede Acabados y Topería) - Asistente de Negocios Electrónicos

Fuente: Elaboración Propia

5.1 EVALUACION DE USUARIOS

5.1.1 Cuestionario

Para la elaboración del cuestionario se tomaron en cuenta 4 criterios de evaluación que fueron: Documentación, obtención del consentimiento, derechos ARCO y medidas de seguridad de información.

El tamaño de la muestra fue de 30 personas, dicha muestra fue seleccionada por muestreo no probabilístico.

Además, se utilizó una herramienta de encuesta como *Google Forms.*

Las preguntas que forman parte del cuestionario fueron las siguientes:

- **Documentación**

Pregunta 1. ¿Se ha realizado y documentado una política de seguridad de datos personales en la empresa?

Si	No

Pregunta 2. Si la respuesta anterior ha sido afirmativa ¿La política ha sido comunicada al interior de la organización?

Si	No

Pregunta 3. ¿Se ha realizado y documentado un manual de políticas y procedimientos para proteger los datos personales en la empresa?

Si	No

Pregunta 4. Si la respuesta anterior ha sido afirmativa ¿Considera que el manual es completo para preservar la seguridad de los bancos de datos personales?

Completamente	En su mayor parte	Regularmente	Poco o nada

Pregunta 5. ¿Se ha adecuado los contratos correspondientes de la empresa al reglamento de la Ley N°29733, Ley de Protección de Datos Personales?

Si	No

Pregunta 6. ¿Se ha desarrollado un compromiso de confidencialidad en el tratamiento de datos personales?

Si	No

- **Obtención del Consentimiento**

Pregunta 7. ¿Existe un consentimiento previo expreso, informado y lícito del titular de los datos personales antes de realizar un tratamiento con sus datos personales?

Si	No

Pregunta 8. ¿Se ha establecido un procedimiento para la obtención del consentimiento del titular de los datos personales?

Si	No

Pregunta 9. ¿Se ha desarrollado formatos de consentimiento para el tratamiento de los datos personales de cada banco de datos personales?

Si	No

Pregunta 10. Si la respuesta anterior ha sido afirmativa ¿En qué medida considera que dichos formatos son entregados oportunamente a los titulares de los datos personales?

Muy bueno	Bueno	Regular	Malo

- **Derechos ARCO**

Pregunta 11. ¿Se puede ejercer los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) dentro de la empresa?

Muy bueno	Bueno	Regular	Malo

Pregunta 12. ¿Se ha desarrollado un procedimiento de atención de los derechos ARCO?

Si	No

Pregunta 13. Si la respuesta es afirmativa, ¿Considera que el procedimiento es correcto de acuerdo a lo que rige la Ley de Protección de Datos Personales?

Muy bueno	Bueno	Regular	Malo

Pregunta 14. ¿Se ha desarrollado formatos para el ejercicio de los derechos ARCO?

Si	No

Pregunta 15. Si la respuesta es afirmativa, ¿Considera que el formato ha sido bien diseñado de acuerdo a lo que rige la Ley de Protección de Datos Personales?

Muy bueno	Bueno	Regular	Malo

- **Medidas de Seguridad**

Pregunta 16. ¿Cómo califica el resultado de las medidas de seguridad físicas?

Muy bueno	Bueno	Regular	Malo

Pregunta 17. ¿Cómo califica el resultado de las medidas seguridad adoptadas para el control de acceso y privilegios en el tratamiento de los bancos de datos personales?

Muy bueno	Bueno	Regular	Malo

Pregunta 18. ¿Cómo califica el resultado de las medidas seguridad adoptadas para la gestión de incidencias en el tratamiento de los bancos de datos personales?

Muy bueno	Bueno	Regular	Malo

Pregunta 19. ¿Existe una adecuada gestión y uso de contraseñas en medios informáticos?

Si	No

Pregunta 20. ¿Existen mecanismos seguros de eliminación de información?

Si	No

Pregunta 21. ¿Cómo califica las medidas de seguridad adoptadas en la gestión de copias de respaldo?

Muy bueno	Bueno	Regular	Malo

Pregunta 22. ¿Existen mecanismos de seguridad para la transferencia de información a nivel nacional e internacional?

Si	No

Pregunta 23. ¿En qué medida la metodología propuesta garantiza los tres principios de la seguridad de la información (confidencialidad, integridad y disponibilidad)?

Completamente	En su mayor parte	Regularmente	Poco o nada

Pregunta 24. ¿En qué medida una guía metodológica garantiza la protección de los bancos de datos personales de la empresa?

Completamente	En su mayor parte	Regularmente	Poco o nada

Pregunta 25. ¿En qué medida la propuesta metodológica ayuda a implementar la Ley N°29733, Ley de Protección de Datos Personales en la empresa? (amplitud)

Completamente	En su mayor parte	Regularmente	Poco o nada

La encuesta podrá ser accedida desde cualquier dispositivo con acceso a internet por medio del siguiente enlace: ***https://forms.gle/WointyNR1DqeqfZR6***

5.1.2 Resultado del Cuestionario

Dadas las respuestas obtenidas en la encuesta:

- **Documentación**

Pregunta 1:

Del total de encuestados y dentro de las opciones de respuestas sí o no, podemos ver en el siguiente diagrama circular que de un total de 30 encuestados:

• El 87.0% de los encuestados afirma que "Si" respecto a la pregunta.

• El 13.0% de los encuestados afirma que "No" respecto a la pregunta.

Lo que nos dice, que si se tiene documentado una política de seguridad de datos personales.

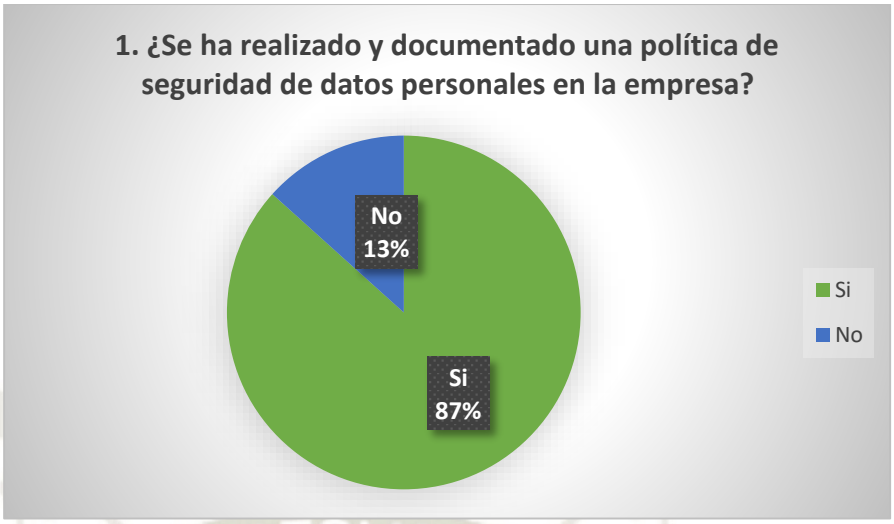


Figura 82 Gráfico Circular - Resultado de la pregunta 1

Fuente: Elaboración propia – Google Forms

Pregunta 2:

Del total de encuestados y dentro de las opciones de respuestas sí o no, podemos ver en el siguiente diagrama circular que de un total de 30 encuestados:

• El 100.0% de los encuestados afirma que "Si" respecto a la pregunta.

Lo que nos dice, que la política de seguridad de los datos personales sí ha sido comunicada al interior de la organización.

Figura 83 Gráfico Circular - Resultado de la pregunta 2

Fuente: Elaboración propia – Google Forms

Pregunta 3:

Del total de encuestados y dentro de las opciones de respuestas sí o no, podemos ver en el siguiente diagrama circular que de un total de 30 encuestados:

• El 73.0% de los encuestados afirma que "Si" respecto a la pregunta.

• El 27.0% de los encuestados afirma que "No" respecto a la pregunta.

Lo que nos dice, que sí se ha documentado el manual de políticas y procedimientos para proteger los datos personales en la empresa.

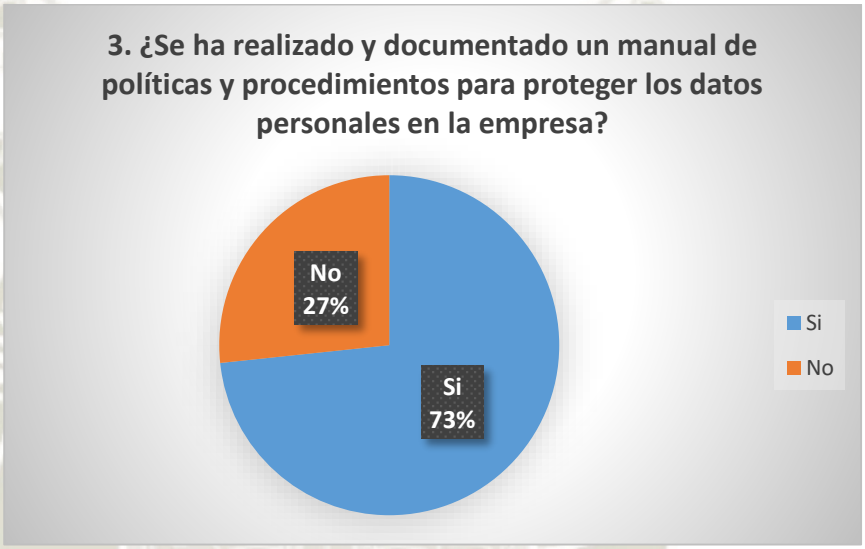


Figura 84 Gráfico Circular - Resultado de la pregunta 3

Fuente: Elaboración propia – Google Forms

Pregunta 4:

Del total de encuestados y dentro del rango de respuestas de 1 al 4, donde 1 es “Poco o nada” y 4 es “Completamente”; podemos ver en el siguiente diagrama circular que de un total de 30 encuestados:

• El 40.0% de los encuestados afirma que “Completamente” respecto a la pregunta.

• El 33.0% de los encuestados afirma que “En su mayor parte” respecto a la pregunta.

• El 27.0% de los encuestados afirma que “Regularmente” respecto a la pregunta.

Lo que nos dice, que la mayoría de los encuestados consideran que el manual es completo para preservar la seguridad de los bancos de datos personales.

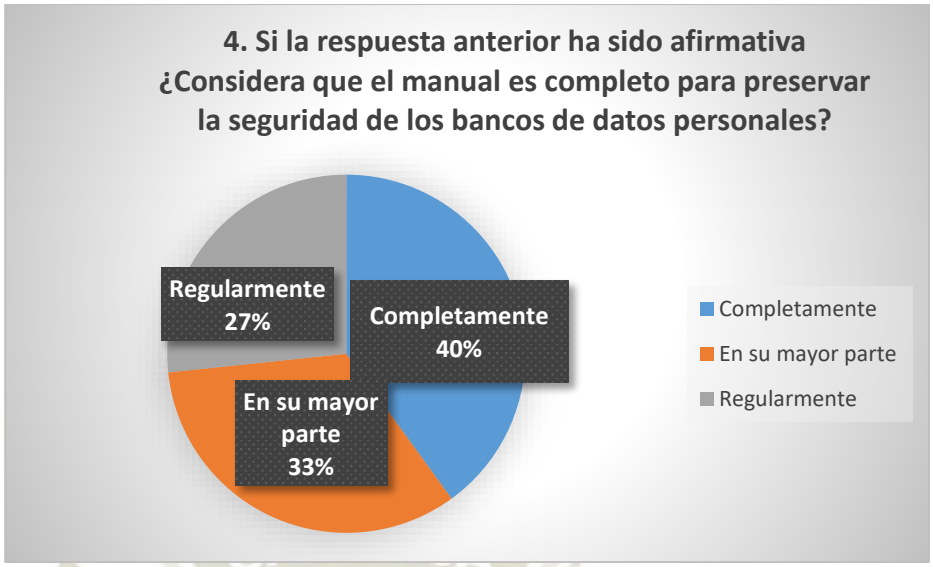


Figura 85 Gráfico Circular - Resultado de la pregunta 4

Fuente: Elaboración propia – Google Forms

Pregunta 5:

Del total de encuestados y dentro de las opciones de respuestas sí o no, podemos ver en el siguiente diagrama circular que de un total de 30 encuestados:

• El 100.0% de los encuestados afirma que "Si" respecto a la pregunta.

Lo que nos dice, que los contratos de la empresa si han ido adecuados a lo que rige la Ley de Protección de Datos Personales.

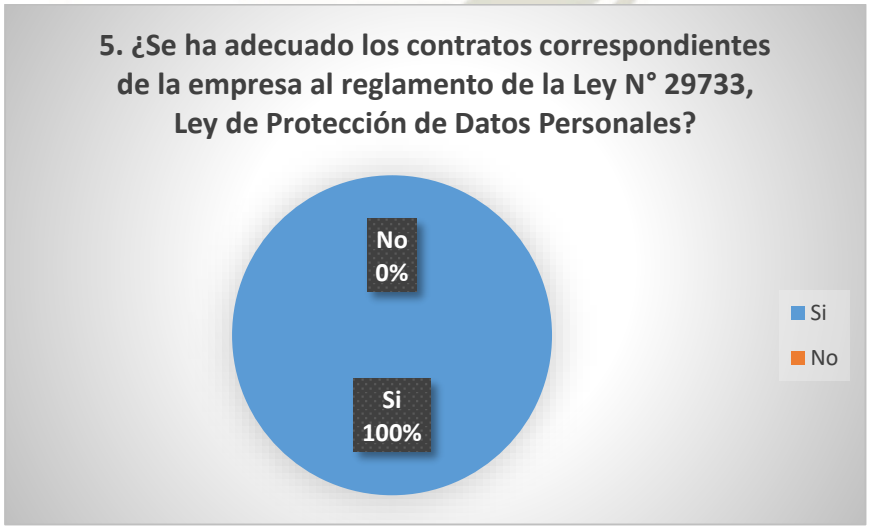


Figura 86 Gráfico Circular - Resultado de la pregunta 5

Fuente: Elaboración propia – Google Forms

Pregunta 6:

Del total de encuestados y dentro de las opciones de respuestas sí o no, podemos ver en el siguiente diagrama circular que de un total de 30 encuestados:

• El 80.0% de los encuestados afirma que "Si" respecto a la pregunta.

• El 20.0% de los encuestados afirma que "No" respecto a la pregunta.

Lo que nos dice, que sí se ha desarrollado un compromiso de confidencialidad para el tratamiento de datos personales.

Figura 87 Gráfico Circular - Resultado de la pregunta 6

Fuente: Elaboración propia – Google Forms

- **Obtención del consentimiento**

  Pregunta 7:

  Del total de encuestados y dentro de las opciones de respuestas sí o no, podemos ver en el siguiente diagrama circular que de un total de 30 encuestados:

  • El 73.0% de los encuestados afirma que "Si" respecto a la pregunta.

  • El 27.0% de los encuestados afirma que "No" respecto a la pregunta.

  Lo que nos dice, que sí se ejecuta un consentimiento previo expreso, informado y lícito del titular de los datos personales antes de realizar un tratamiento con sus datos.

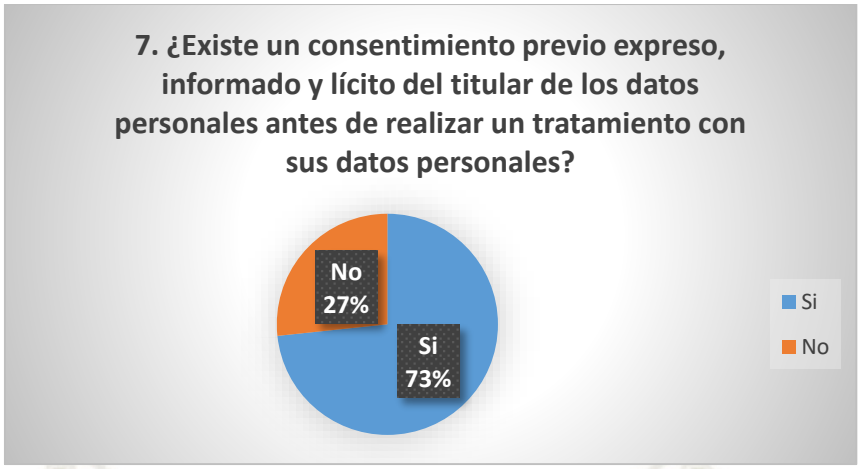


Figura 88 Gráfico Circular - Resultado de la pregunta 7

Fuente: Elaboración propia – Google Forms

Pregunta 8:

Del total de encuestados y dentro de las opciones de respuestas sí o no, podemos ver en el siguiente diagrama circular que de un total de 30 encuestados:

• El 80.0% de los encuestados afirma que "Si" respecto a la pregunta.

• El 20.0% de los encuestados afirma que "No" respecto a la pregunta.

Lo que nos dice, que sí se ha establecido un procedimiento para la obtención del consentimiento del titular de los datos personales.

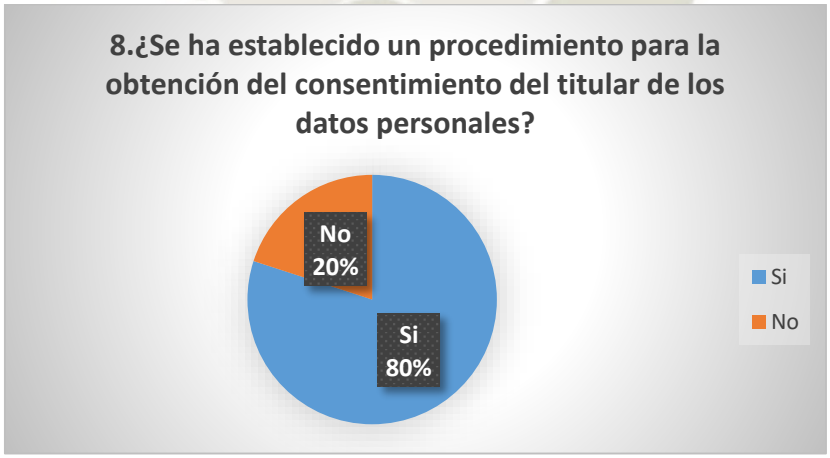


Figura 89 Gráfico Circular - Resultado de la pregunta 8

Fuente: Elaboración propia – Google Forms

Pregunta 9:

Del total de encuestados y dentro de las opciones de respuestas sí o no, podemos ver en el siguiente diagrama circular que de un total de 30 encuestados:

• El 100.0% de los encuestados afirma que "Si" respecto a la pregunta.

Pregunta 10:

Del total de encuestados y dentro del rango de respuestas de 1 al 4, donde 1 es "Malo" y 4 es "Muy Bueno"; podemos ver en el siguiente diagrama circular que de un total de 30 encuestados:

• El 13.0% de los encuestados afirma que "Muy Bueno" respecto a la pregunta.

• El 54.0% de los encuestados afirma que "Bueno" respecto a la pregunta.

• El 33.0% de los encuestados afirma que "Regular" respecto a la pregunta.

Lo que nos dice, que la mayoría de los encuestados consideran que los formatos son entregados oportunamente a los titulares de los datos personales.

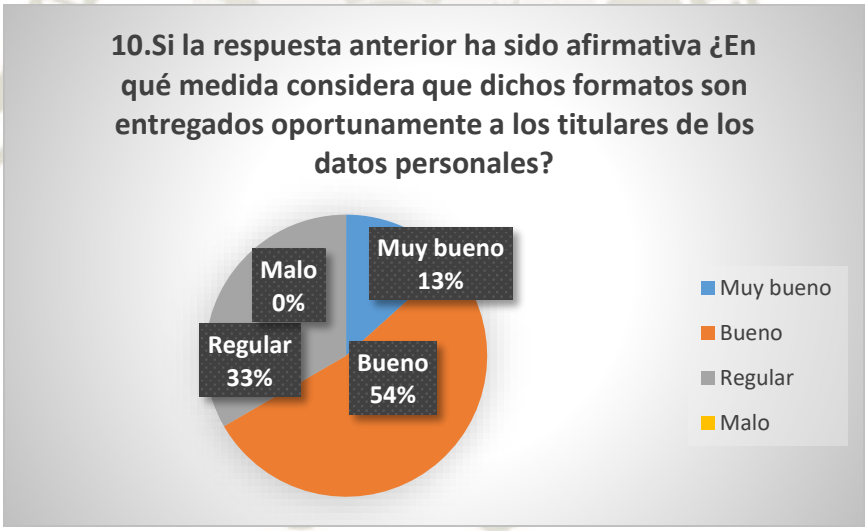


Figura 90 Gráfico Circular - Resultado de la pregunta 10

Fuente: Elaboración propia – Google Forms

- **Derechos ARCO**

  Pregunta 11:

  Del total de encuestados y dentro de las opciones de respuestas sí o no, podemos ver en el siguiente diagrama circular que de un total de 30 encuestados:

  • El 100.0% de los encuestados afirma que "Si" respecto a la pregunta.

  Lo que nos dice, que sí se puede ejercer los derechos ARCO dentro de la empresa.

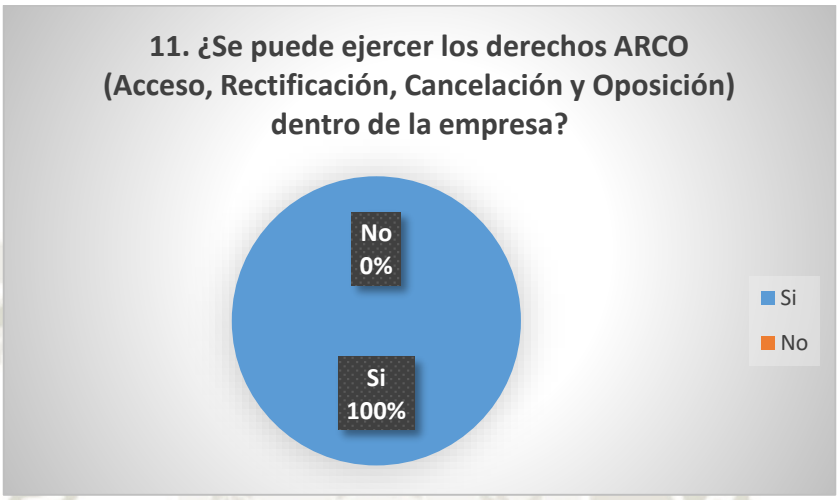


Figura 91 Gráfico Circular - Resultado de la pregunta 11

Fuente: Elaboración propia – Google Forms

Pregunta 12:

Del total de encuestados y dentro de las opciones de respuestas sí o no, podemos ver en el siguiente diagrama circular que de un total de 30 encuestados:

• El 100.0% de los encuestados afirma que "Si" respecto a la pregunta.

Figura 92 Gráfico Circular - Resultado de la pregunta 12

Fuente: Elaboración propia – Google Forms

Pregunta 13:

Del total de encuestados y dentro del rango de respuestas de 1 al 4, donde 1 es "Malo" y 4 es "Muy Bueno"; podemos ver en el siguiente diagrama circular que de un total de 30 encuestados:

• El 33.0% de los encuestados afirma que "Muy Bueno" respecto a la pregunta.

• El 53.0% de los encuestados afirma que "Bueno" respecto a la pregunta.

• El 13.0% de los encuestados afirma que "Regular" respecto a la pregunta.

Lo que nos dice, que la mayoría de los encuestados consideran que el procedimiento establecido para ejercer los derechos ARCO es correcto y alineado a lo que rige la Ley de Protección de Datos Personales.

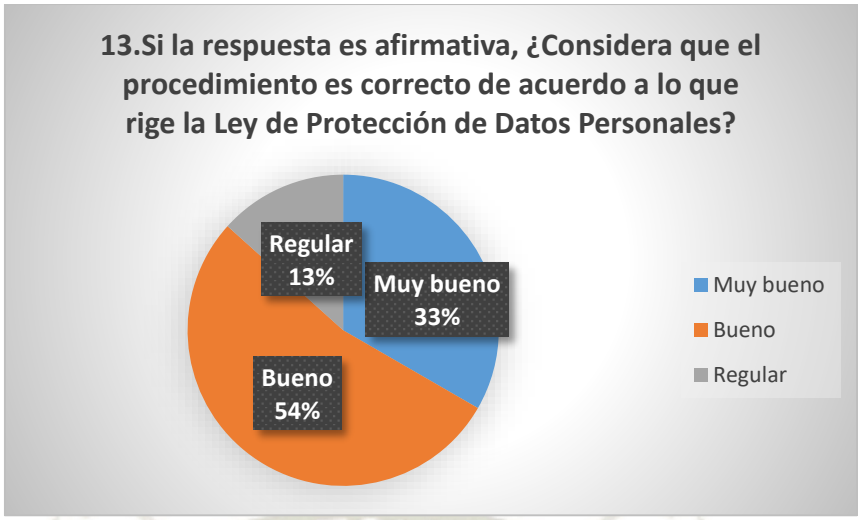


Figura 93 Gráfico Circular - Resultado de la pregunta 13

Fuente: Elaboración propia – Google Forms

Pregunta 14:

Del total de encuestados y dentro de las opciones de respuestas sí o no, podemos ver en el siguiente diagrama circular que de un total de 30 encuestados:

• El 87.0% de los encuestados afirma que "Si" respecto a la pregunta.

• El 13.0% de los encuestados afirma que "No" respecto a la pregunta.

Lo que nos dice, que la mayoría de los encuestados consideran que si se ha desarrollado formatos para ejercer los derechos ARCO.

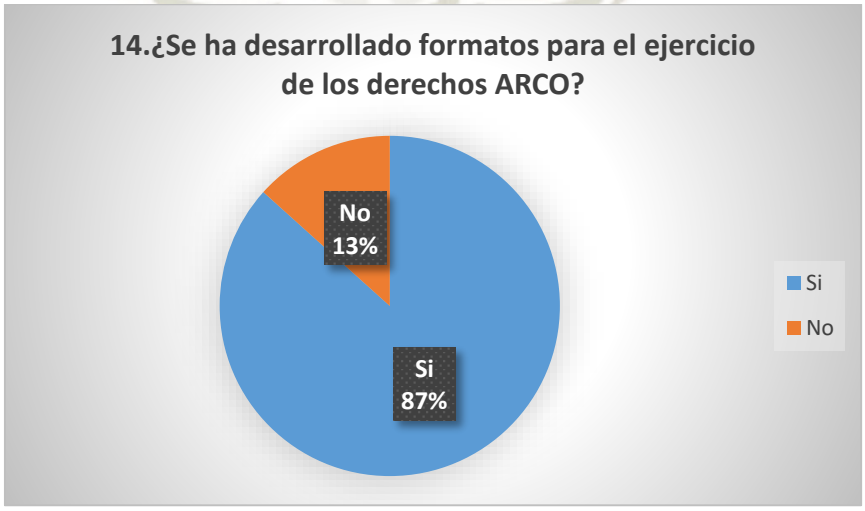


Figura 94 Gráfico Circular - Resultado de la pregunta 14

Fuente: Elaboración propia – Google Forms

Pregunta 15:

Del total de encuestados y dentro del rango de respuestas de 1 al 4, donde 1 es "Malo" y 4 es "Muy Bueno"; podemos ver en el siguiente diagrama circular que de un total de 30 encuestados:

• El 13.0% de los encuestados afirma que "Muy Bueno" respecto a la pregunta.

• El 60.0% de los encuestados afirma que "Bueno" respecto a la pregunta.

• El 27.0% de los encuestados afirma que "Regular" respecto a la pregunta.

Lo que nos dice, que la mayoría de los encuestados consideran que el formato está bien diseñado de acuerdo a lo que rige la Ley de Protección de Datos Personales.

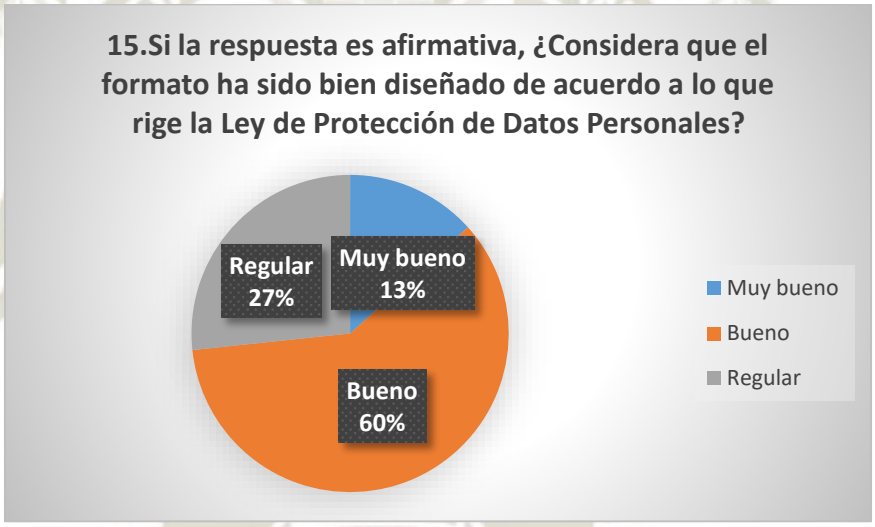


Figura 95 Gráfico Circular - Resultado de la pregunta 15

Fuente: Elaboración propia – Google Forms

- **Medidas de Seguridad**

Pregunta 16:

Del total de encuestados y dentro del rango de respuestas de 1 al 4, donde 1 es "Malo" y 4 es "Muy Bueno"; podemos ver en el siguiente diagrama circular que de un total de 30 encuestados:

• El 33.0% de los encuestados afirma que "Muy Bueno" respecto a la pregunta.

• El 53.0% de los encuestados afirma que "Bueno" respecto a la pregunta.

• El 13.0% de los encuestados afirma que “Regular” respecto a la pregunta.

Lo que nos dice, que la mayoría de los encuestados consideran que es “Bueno” el resultado de las medidas de seguridad físicas.

Figura 96 Gráfico Circular - Resultado de la pregunta 16

Fuente: Elaboración propia – Google Forms

Pregunta 17:

Del total de encuestados y dentro del rango de respuestas de 1 al 4, donde 1 es “Malo” y 4 es “Muy Bueno”; podemos ver en el siguiente diagrama circular que de un total de 30 encuestados:

• El 27.0% de los encuestados afirma que “Muy Bueno” respecto a la pregunta.

• El 60.0% de los encuestados afirma que “Bueno” respecto a la pregunta.

• El 13.0% de los encuestados afirma que “Regular” respecto a la pregunta.

Lo que nos dice, que la mayoría de los encuestados consideran que es “Bueno” el resultado de las medidas de seguridad físicas.

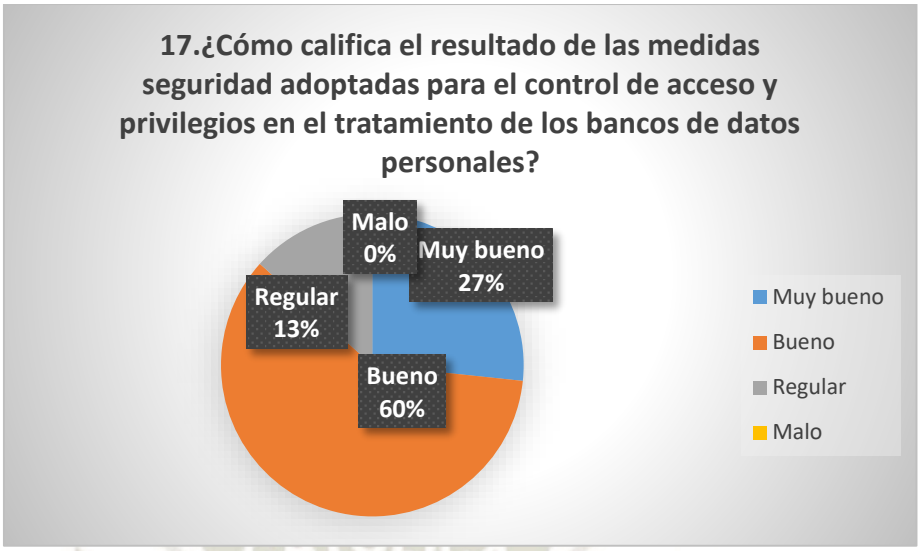


Figura 97 Gráfico Circular - Resultado de la pregunta 17

Fuente: Elaboración propia – Google Forms

Pregunta 18:

Del total de encuestados y dentro del rango de respuestas de 1 al 4, donde 1 es "Malo" y 4 es "Muy Bueno"; podemos ver en el siguiente diagrama circular que de un total de 30 encuestados:

• El 40.0% de los encuestados afirma que "Muy Bueno" respecto a la pregunta.

• El 33.0% de los encuestados afirma que "Bueno" respecto a la pregunta.

• El 27.0% de los encuestados afirma que "Regular" respecto a la pregunta.

Lo que nos dice, que la mayoría de los encuestados consideran que es "Bueno" el resultado de las medidas de seguridad físicas.

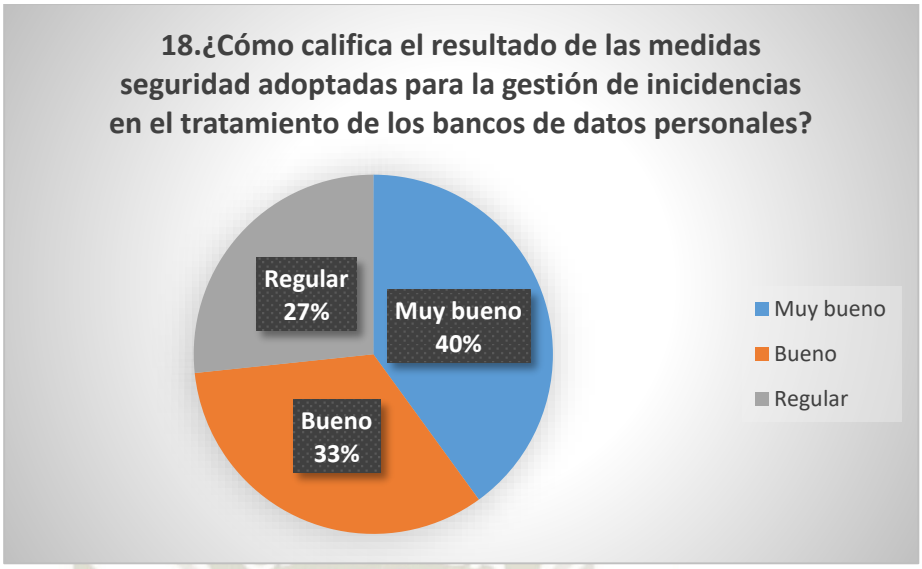


Figura 98 Gráfico Circular - Resultado de la pregunta 18

Fuente: Elaboración propia – Google Forms

Pregunta 19:

Del total de encuestados y dentro de las opciones de respuestas sí o no, podemos ver en el siguiente diagrama circular que de un total de 30 encuestados:

• El 67.0% de los encuestados afirma que "Si" respecto a la pregunta.

• El 33.0% de los encuestados afirma que "No" respecto a la pregunta.

Lo que nos dice, que la mayoría de los encuestados consideran que si se ha desarrollado formatos para ejercer los derechos ARCO.

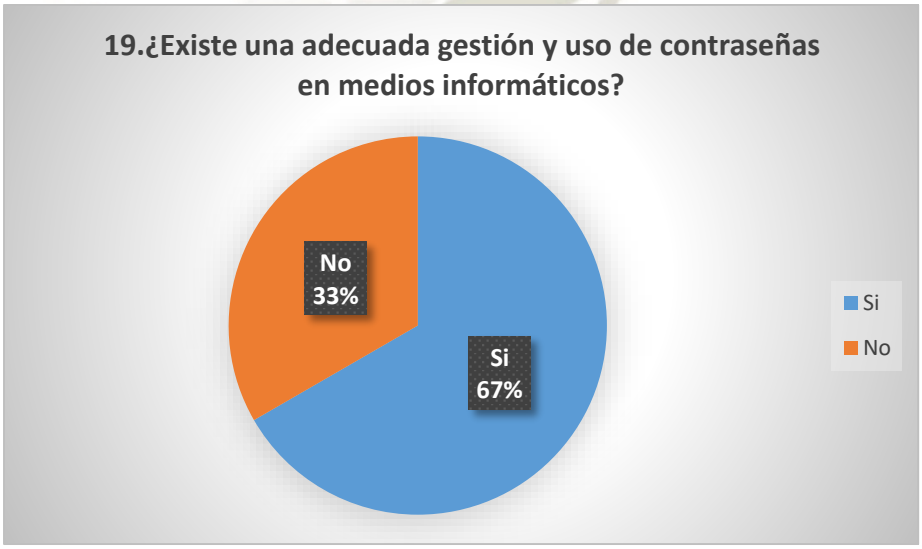


Figura 99 Gráfico Circular - Resultado de la pregunta 19

Fuente: Elaboración propia – Google Forms

Pregunta 20:

Del total de encuestados y dentro de las opciones de respuestas sí o no, podemos ver en el siguiente diagrama circular que de un total de 30 encuestados:

• El 73.0% de los encuestados afirma que "Si" respecto a la pregunta.

• El 27.0% de los encuestados afirma que "No" respecto a la pregunta.

Lo que nos dice, que la mayoría de los encuestados consideran que si se ha desarrollado formatos para ejercer los derechos ARCO.

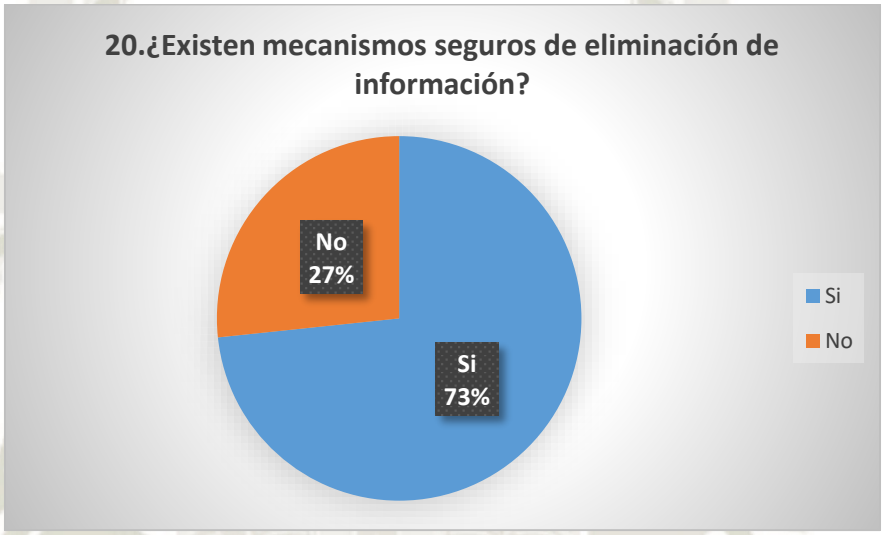


Figura 100 Gráfico Circular - Resultado de la pregunta 20

Fuente: Elaboración propia – Google Forms

Pregunta 21:

Del total de encuestados y dentro del rango de respuestas de 1 al 4, donde 1 es "Malo" y 4 es "Muy Bueno"; podemos ver en el siguiente diagrama circular que de un total de 30 encuestados:

• El 20.0% de los encuestados afirma que "Muy Bueno" respecto a la pregunta.

• El 47.0% de los encuestados afirma que "Bueno" respecto a la pregunta.

• El 33.0% de los encuestados afirma que "Regular" respecto a la pregunta.

Lo que nos dice, que la mayoría de los encuestados consideran que es "Bueno" el resultado de las medidas de seguridad físicas.

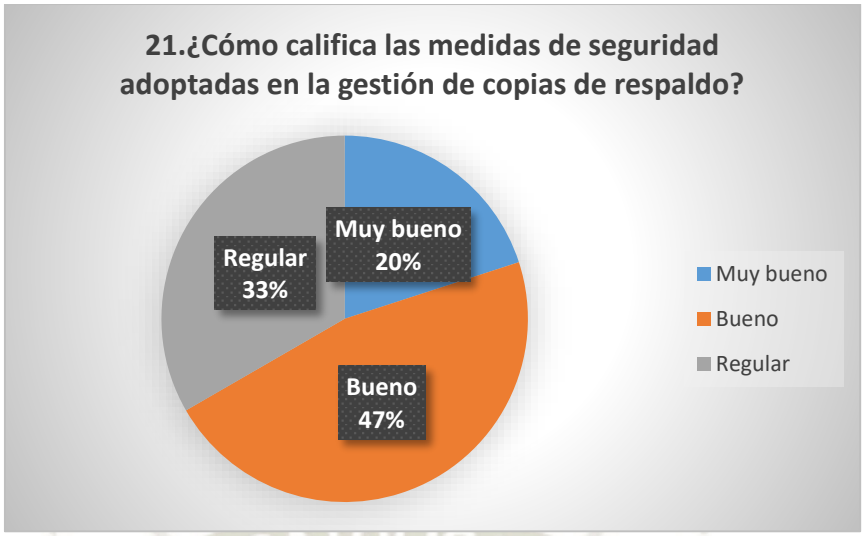


Figura 101 Gráfico Circular - Resultado de la pregunta 21

Fuente: Elaboración propia – Google Forms

Pregunta 22:

Del total de encuestados y dentro de las opciones de respuestas sí o no, podemos ver en el siguiente diagrama circular que de un total de 30 encuestados:

• El 60.0% de los encuestados afirma que "Si" respecto a la pregunta.

• El 40.0% de los encuestados afirma que "No" respecto a la pregunta.

Lo que nos dice, que la mayoría de los encuestados consideran que si se ha desarrollado formatos para ejercer los derechos ARCO.

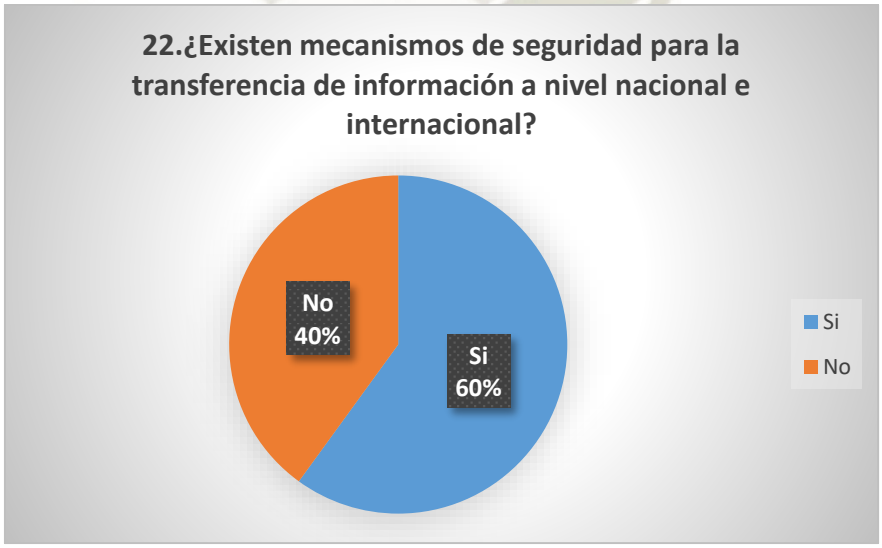


Figura 102 Gráfico Circular - Resultado de la pregunta 22

Fuente: Elaboración propia – Google Forms

Pregunta 23:

Del total de encuestados y dentro del rango de respuestas de 1 al 4, donde 1 es "Malo" y 4 es "Muy Bueno"; podemos ver en el siguiente diagrama circular que de un total de 30 encuestados:

• El 13.0% de los encuestados afirma que "Muy Bueno" respecto a la pregunta.

• El 54.0% de los encuestados afirma que "Bueno" respecto a la pregunta.

• El 33.0% de los encuestados afirma que "Regular" respecto a la pregunta.

Lo que nos dice, que la mayoría de los encuestados consideran que es "Bueno" el resultado de las medidas de seguridad físicas.

Figura 103 Gráfico Circular - Resultado de la pregunta 23

Fuente: Elaboración propia – Google Forms

Pregunta 24:

Del total de encuestados y dentro del rango de respuestas de 1 al 4, donde 1 es "Malo" y 4 es "Muy Bueno"; podemos ver en el siguiente diagrama circular que de un total de 30 encuestados:

• El 53.0% de los encuestados afirma que "Muy Bueno" respecto a la pregunta.

• El 27.0% de los encuestados afirma que "Bueno" respecto a la pregunta.

• El 20.0% de los encuestados afirma que "Regular" respecto a la pregunta.

Lo que nos dice, que la mayoría de los encuestados consideran que es "Bueno" el resultado de las medidas de seguridad físicas.

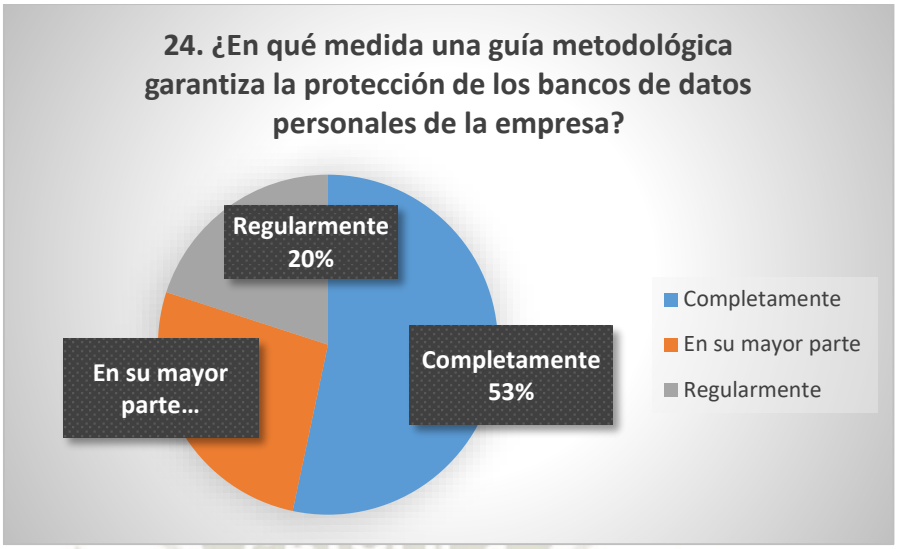


Figura 104 Gráfico Circular - Resultado de la pregunta 24

Fuente: Elaboración propia – Google Forms

Pregunta 25:

Del total de encuestados y dentro del rango de respuestas de 1 al 4, donde 1 es "Malo" y 4 es "Muy Bueno"; podemos ver en el siguiente diagrama circular que de un total de 30 encuestados:

• El 40.0% de los encuestados afirma que "Muy Bueno" respecto a la pregunta.

• El 33.0% de los encuestados afirma que "Bueno" respecto a la pregunta.

• El 27.0% de los encuestados afirma que "Regular" respecto a la pregunta.

Lo que nos dice, que la mayoría de los encuestados consideran que es "Bueno" el resultado de las medidas de seguridad físicas.

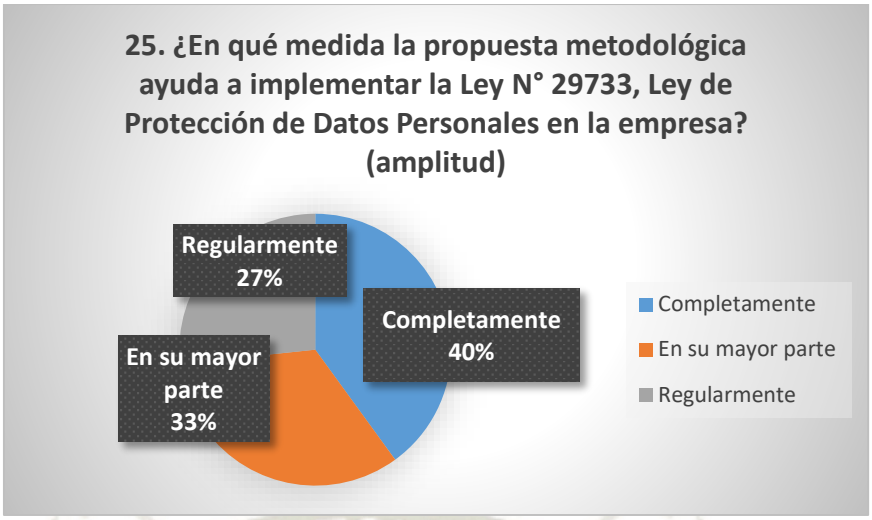


Figura 105 Gráfico Circular - Resultado de la pregunta 25

Fuente: Elaboración propia – Google Forms

6. CONCLUSIONES

1. Mediante la presente tesis se propuso una metodología que logre garantizar la seguridad de los datos personales a través de la adopción de controles que permitan preservar la confidencialidad, disponibilidad e integridad durante el tratamiento de datos personales.

2. Se establecieron cuatro fases: Planeamiento, Recopilación y Registro, Elaboración y Ejecución y Obtención del consentimiento; en donde se desarrollan las actividades necesarias para obtener los resultados previstos.

3. En la fase de Planeamiento se identifica los bancos de datos personales usados por la empresa. Los primeros bancos de datos son identificados con el apoyo de los gerentes y directivos de la empresa, y los bancos de datos complementarios son identificados a través de las entrevistas llevadas a cabo en cada área.

4. Una vez registrado a cada banco de datos personales ante el Registro Nacional de Datos Personales con su respectivo formato de inscripción llenado, se obtiene la resolución de inscripción de los Bancos de Datos Personales.

5. Con el apoyo del Gerente de TI, la información obtenida y basándonos en la Directiva de Seguridad de Información, se logra establecer e implementar aquellas medidas de seguridad que son necesarias para garantizar un nivel de protección adecuado y salvaguardar la información contenida en cada banco de datos personales.

6. Se elabora un procedimiento para el ejercicio de los derechos arco, porque de acuerdo al reglamento de la Ley N° 29733, Ley de Protección de Datos Personales, es una obligación que las personas puedan ejercer sus derechos ARCO, acrónimo de, acceso, rectificación, cancelación y oposición a sus datos personales ante cualquier empresa.

7. En la última fase de la metodología se elaboraron procedimientos para recabar el consentimiento del titular de los datos personales de acuerdo a la necesidad de cada banco de datos personales.

8. Como aporte adicional a la metodología propuesta se lleva a cabo el desarrollo de un sistema web que permita ayudar a las empresas a gestionar y validar las solicitudes ARCO, incidencias relacionadas al tratamiento de datos personales y backups que contengan datos personales.

Además, permite identificar qué medidas de seguridad están y cuáles faltan implementar en la empresa.

9. El éxito de la implementación de la propuesta metodológica y/o mejora permanente es el apoyo y el compromiso de los funcionarios y la gerencia de una empresa privada.

7. RECOMENDACIONES Y TRABAJOS FUTUROS

1. Desarrollar un aplicativo móvil que contenga todas las fases de la metodología propuesta y así verificar el cumplimiento de la Ley de Protección de datos personales.

3. Desarrollar un marco de trabajo estandarizado que permita un cumplimiento más amplio de la Ley de Protección de Datos personales.

4. Revisar y mantener actualizada todos los procedimientos y políticas para que la empresa no pueda ser multada por no cumplir con la seguridad mínima en los bancos de datos personales.

5. La empresa debe formar un Comité de Protección de Datos Personales que se encargue de velar por la seguridad de los bancos de datos personales y realizar el seguimiento a los procedimientos y políticas de seguridad.

6. Mejorar y formalizar sus procesos de negocio que incluyan tratamiento de datos personales para que pueda seguir ofreciendo a sus clientes el servicio que ellos esperan.

7. Realizar investigaciones sobre los beneficios de tener una correcta implementación de medidas de seguridad en cuanto a la Ley de Protección de Datos Personales para tener una ventaja competitiva sólida respecto a otras empresas del sector textil.

8. Investigar periódicamente posibles actualizaciones en el reglamento de la Ley de Protección de datos personales y en la Directiva de Seguridad de Información para mantenerse actualizados y adecuarse a los cambios.

9. Se recomienda que la empresa aproveche las condiciones que le favorecen actualmente para implementar nuevos procesos estratégicos que le permitan tomar mejores decisiones en un futuro.

8. REFERENCIAS

Arce Janáriz, A. (1996). El derecho a la intimidad: De Samuel D. Warren y louis D. Brandeis. *Revista Española de Derecho Constitucional*, *16*(47), 367–373.

Autoridad Nacional de Protección de Datos Personales APDP. (2013). *Directiva-de-Seguridad-DGPDP.pdf*.

Carrión., J. (2016). Diferencia Entre Dato, Información Y Conocimiento. *Http://Iibi.Unam.Mx*.

Cerda Silva, A. (2011). El "nivel adecuado de protección" para las transferencias internacionales de datos personales desde la Unión Europea. *Revista de Derecho (Valparaíso)*, (36), 327–356. https://doi.org/10.4067/s0718-68512011000100009

Comite Tecnico de Normalizacion de Codificacion e Intercambio Electronico de Datos. (2007). NTP-ISO / IEC 17799 EDI . Tecnología de la información . Código de buenas. *El Peruano*, *2a. Edició*(Lima 41), 179. Retrieved from http://www.iso.org/iso/catalogue_detail?csnumber=39612

Congreso. (1993). Constitución política del Perú. *Археология*, *1*(August), 117–125.

Cordero Torres, G. (2015). *Estudio comparativo entre las metodologías MAGERIT y CRAMM, utilizadas para Análisis y Gestión de Riesgos de Seguridad de la Información*. 97. Retrieved from http://dspace.uazuay.edu.ec/bitstream/datos/5051/1/11490.pdf

Enrique, L., Crespo, S., Parra, A. S., Fernández-medina, E., Od, G. H., Od, H. Q., … Sxhghq, T. X. H. (2011). *Cumplimiento de la LOPD y los requerimientos legales de la ISO27001 en la citación de pacientes en Hospitales*. (November).

Fernández Vargas, A. J., & Mayta Aguilar, J. R. (2017). *DISEÑO DE UN MODELO SISTÉMICO DE GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN, INTEGRANDO LA METODOLOGÍ A MAGERIT Y LA NORMA ISO 27002:2013 EN EMPRESAS FINANCIERAS*.

Gómez, R., Pérez, D., Donoso, Y., & Herrera, A. (2010). Metodología y gobierno de la gestión de riesgos de tecnologías de la información Methodology and Governance of the IT Risk Management. *Revista de Ingeniería*, *31*, 109–118.

Gregorio, C. G., & Ornelas, L. (2011). *Protección De Datos Personales En Las Redes Sociales Digitales : En Particular De Niños Y Adolescentes* .

Grupo Michell. (n.d.). Portal del Grupo Michell. Retrieved May 11, 2019, from http://www.michell.com.pe/

ISOTools Excellence. (2003). La norma ISO 27001. Retrieved May 10, 2019, from https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

Ministerio de Justicia y Derechos Humanos. (2011a). *Ley de Proteccion de Datos Personales*. 1–17.

Ministerio de Justicia y Derechos Humanos. (2011b). *Ley de Protección de Datos Personales*.

Ministerio de Justicia y Derechos Humanos. (2013a). El derecho fundamental a la protección de datos personales. *La Unión Europea, Conclusion*. Retrieved from http://www.minjus.gob.pe/wp-content/uploads/2014/02/Cartilla-Derecho-Fundamentalok.pdf

Ministerio de Justicia y Derechos Humanos. (2013b). *El Derecho Fundamental a la Protección de Datos Personales "Tú también tienes derechos y deberes."* Retrieved from www.minjus.gob.pe

Ministerio de Justicia y Derechos Humanos. (2014). *Autoridad Nacional de Protección de Datos Personales APDP*. Retrieved from https://www.minjus.gob.pe/wp-content/uploads/2014/02/Informate-DGPDP.pdf

Ministerio de Justicia y Derechos Humanos. (2019). Organización | Ministerio de Justicia y Derechos Humanos del Perú. Retrieved May 19, 2019, from https://www.minjus.gob.pe/dgpdp-organizacion/

Provided, S., No, I. S. O., & Licensee, I. H. S. (2013). *International Standard ISO/IEC 13335-1. 2004*.

Ramírez, A., & Ortiz, Z. (2011). *Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios and ISO 27005 , and its contribution to business operation continuity*. *16*(2), 56–66.

Report, T. (2008). TECHNICAL REPORT ISO / IEC TR Systems engineering —. *Systems Engineering, 2008*.

Rodríguez, F., Jesús, C., Ferrando, G., Alvira, F., Enrique, L., Escobar, M., … Alonso, L. E. (2016). El análisis de la realidad social: métodos y técnicas de investigación (4ª edición). Manuel García Ferrando, Francisco Alvira, Luis Enrique Alonso y Modesto Escobar

(comps.). (Madrid, Alianza Editorial, 2015). *Reis. Revista Española de Investigaciones Sociológicas*, (154), 165–169.

Sánchez, L. E., Santos-Olmo, A., Álvarez, E., Fernandez-Medina, E., & Piattini, M. (2011). *Cumplimiento de la LOPD y los requerimientos legales de la ISO27001 en la citación de pacientes en Hospitales*. (November).

Sosa, J. (2012). *Análisis de Riesgos: Estándares para la administración de riesgos*. 51.

Suca Ancachi, J. T. (2014). *Propuesta metodológica para implementar la Norma Técnica Peruana ISO/IEC 27001:2008 de Seguridad de la Información en entidades públicas del Estado*.

Vilca, J. (2015). *Propuesta desarrollo de un nuevo marco de trabajo para la gestión de centrales telefónica IP en base de los marcos de gestión específicos como ITIL, ISO 27001 y COBIT*. 208.

9. ANEXOS

ANEXO A

RESUMEN DE LOS FORMULARIOS DE INSCRIPCIÓN

Las siguientes tablas muestran el detalle de cada formulario de inscripción llenado para cada banco de datos personales identificado en la empresa Michell y Cía. S.A., y así proceder a la inscripción ante el Registro Nacional de Protección de Datos Personales.

Tabla A. 1 *Banco de datos colaboradores*

BANCO DE DATOS	
COLABORADORES	
REPRESENTANTE	Jefe de División de Personal y Recursos Humanos
TIPO DE TRATAMIENTO	Automatizado y No automatizado
FINALIDAD	Gestionar, administrar y controlar la información del personal de colaboradores para la elaboración de planillas, otorgamiento de beneficios que establece la ley, servicio social a problemas personales y familiares, cumplimiento de obligaciones del colaborador, seguridad industrial, capacitaciones, así como las condiciones necesarias para un desempeño laboral óptimo.
PROCEDIMIENTO DE OBTENCIÓN DE LOS DATOS PERSONALES	
FUENTE	Titular del dato personal
	Fuentes de acceso al público
	Entidad privada
	Entidad pública
SOPORTE	Papel
	Soporte informático
	Vía telemática
PROCEDIMIENTO	Formularios
	Transmisión física
	Transmisión electrónica

	Entrevistas personales
	Telemarketing
TRANSFERENCIA DE DATOS PERSONALES	
Transferencia Nacional	Si
Transferencia Internacional	No

Fuente: Elaboración propia

Tabla A. 2 *Banco de datos postulantes*

BANCO DE DATOS	
POSTULANTES	
REPRESENTANTE	Jefe de División de Personal y Recursos Humanos
TIPO DE TRATAMIENTO	Automatizado y No automatizado
FINALIDAD	Evaluar la información del postulante a cumplir con un perfil determinado de un puesto para el proceso de reclutamiento de personal colaborador.
PROCEDIMIENTO DE OBTENCIÓN DE LOS DATOS PERSONALES	
FUENTE	Titular del dato personal
	Fuentes de acceso al público
	Entidad Privada
SOPORTE	Papel
	Soporte informático
	Vía telemática
PROCEDIMIENTO	Formularios
	Transmisión física
	Transmisión electrónica
	Entrevistas personales
TRANSFERENCIA DE DATOS PERSONALES	
Transferencia Nacional	No
Transferencia Internacional	No

Fuente: Elaboración propia

Tabla A. 3 *Banco de datos clientes*

BANCO DE DATOS	
CLIENTES	
REPRESENTANTE	Gerente Comercial
TIPO DE TRATAMIENTO	Automatizado y No automatizado
FINALIDAD	Recopilar información de los clientes como personas naturales para ventas y entrega de los productos terminados y envío de correos electrónicos por parte del área comercial.
PROCEDIMIENTO DE OBTENCIÓN DE LOS DATOS PERSONALES	
FUENTE	Titular del dato personal
	Fuentes de acceso al público
	Entidad privada
	Entidad pública
SOPORTE	Papel
	Soporte informático
	Vía telemática
PROCEDIMIENTO	Formularios
	Transmisión física
	Transmisión electrónica
	Referencias comerciales
	Telemarketing
	Cupones de Descuento
TRANSFERENCIA DE DATOS PERSONALES	
Transferencia Nacional	Si
Transferencia Internacional	No

Fuente: Elaboración propia

Tabla A. 4 *Banco de datos proveedores*

BANCO DE DATOS	
PROVEEDORES	
REPRESENTANTE	Jefa de Logística
TIPO DE TRATAMIENTO	Automatizado y No automatizado
FINALIDAD	Cotizar, registrar y administrar la información de los proveedores para su evaluación y realizar la adquisición de los requerimientos que se presentan para la elaboración del producto.
PROCEDIMIENTO DE OBTENCIÓN DE LOS DATOS PERSONALES	
FUENTE	Titular del dato personal
	Fuentes de acceso al público
	Entidad pública
	Tarjetas de Presentación
	Llamadas telefónicas
SOPORTE	Papel
	Soporte informático
	Vía telemática
PROCEDIMIENTO	Transmisión física
	Transmisión electrónica
	Entrevistas personales
	Referencias comerciales
TRANSFERENCIA DE DATOS PERSONALES	
Transferencia Nacional	Si
Transferencia Internacional	No

Fuente: Elaboración propia

Tabla A. 5 *Banco de datos video vigilancia*

BANCO DE DATOS	
VIDEO VIGILANCIA	
REPRESENTANTE	Gerente Administrativo
TIPO DE TRATAMIENTO	Automatizado
FINALIDAD	Almacenamiento y registro de grabación fílmica a las sedes de planta y producción, para fines de auditoría al personal involucrado y cuestiones de seguridad.
PROCEDIMIENTO DE OBTENCIÓN DE LOS DATOS PERSONALES	
FUENTE	Equipos electrónicos de filmación
SOPORTE	Soporte informático
PROCEDIMIENTO	Grabación Fílmica
TRANSFERENCIA DE DATOS PERSONALES	
Transferencia Nacional	Si
Transferencia Internacional	No

Fuente: Elaboración propia

Tabla A. 6 *Banco de datos video vigilancia-Sol Alpaca*

BANCO DE DATOS	
VIDEO VIGILANCIA	
REPRESENTANTE	Jefe de Retail Sol Alpaca
TIPO DE TRATAMIENTO	Automatizado
FINALIDAD	Almacenamiento y registro de grabación fílmica a las tiendas de atención al público de Sol Alpaca, para fines de auditoría al personal involucrado y cuestiones de seguridad.
PROCEDIMIENTO DE OBTENCIÓN DE LOS DATOS PERSONALES	
FUENTE	Equipos electrónicos de filmación
SOPORTE	Soporte informático
	Vía Telemática
PROCEDIMIENTO	Grabación Fílmica
TRANSFERENCIA DE DATOS PERSONALES	
Transferencia Nacional	Si
Transferencia Internacional	No

Fuente: Elaboración propia

Tabla A. 7 *Banco de datos visitantes*

BANCO DE DATOS	
VISITANTES	
REPRESENTANTE	Gerente Administrativo
TIPO DE TRATAMIENTO	No automatizado
FINALIDAD	Recopilación y almacenamiento de visitantes para controlar el acceso a las diferentes instalaciones de la empresa por motivo de seguridad.
PROCEDIMIENTO DE OBTENCIÓN DE LOS DATOS PERSONALES	
FUENTE	Titular del dato personal
SOPORTE	Papel

PROCEDIMIENTO	Recepción y recopilación de documentos de identidad.
TRANSFERENCIA DE DATOS PERSONALES	
Transferencia Nacional	No
Transferencia Internacional	No

Fuente: Elaboración propia

ANEXO B

CRITERIOS DE CATEGORIZACIÓN DE LOS BANCOS DE DATOS PERSONALES

a) **Volumen de registros**: Es importante considerar que existe una diferencia importante entre realizar el tratamiento manual de los datos personales de veinte (20) personas que, de un millón, toda vez que se requiere mecanismos, procesos y herramientas diferentes.

El tratamiento de altos volúmenes de datos personales requiere, actualmente, el uso de tecnologías de la información, lo cual, incorpora mejoras fundamentales en los tiempos de procesamiento, pero también incorpora un conjunto de vulnerabilidades asociadas a la tecnología utilizada, por lo que los niveles de protección deben ser adecuados y comúnmente son mayores a los de un tratamiento sin tecnologías de la información.

b) **Número de datos**: El número de datos personales de cada titular de datos personales que se procesa es un criterio a considerar porque incluye un mayor nivel de detalle sobre el titular de los datos personales con o sin la inclusión de datos sensibles.

c) **Periodo de tiempo para la finalidad del tratamiento de datos personales**: El tener un periodo de tiempo indeterminado o muy largo, para cumplir la finalidad del tratamiento, implica un aumento en el nivel de seguridad que debe observarse en el almacenamiento que se dé a los datos personales durante el periodo del tratamiento, así como en el nivel de impacto sobre el titular de los datos personales en caso de pérdida a la implementación de mecanismos de recuperación ante desastres o no.

d) **La titularidad del banco de datos personales**: Proporciona un criterio de selección que principalmente separa los extremos de las categorías. Es decir, no se le puede asignar a una persona natural una categoría de altísimo nivel porque no dispone de los recursos necesarios, ni será necesario –como regla general- que implemente las medidas más complejas.

   En el caso de las entidades públicas, se cuenta con la Resolución Ministerial 129-2012-PCM, que las obliga a implementar un sistema de gestión de seguridad de la información. Con lo cual, no se les puede asignar una categoría de menor nivel, debido a que la información que manejan impacta directamente en los titulares de datos personales. Sin embargo, para las categorías simple, intermedio y complejo se pueden tener combinaciones más acordes al tipo de tratamiento que se realice.

e) **Finalidad del tratamiento de datos personales respaldada por norma legal**: Tiene especial impacto por ser obligatorio, esto determina el tipo crítico.

f) **Múltiples localizaciones**: El acceso o tratamiento distribuido incorpora un nivel de atención especial porque incluye la transferencia de datos entre múltiples locales de tratamiento (ubicaciones diferentes, pueden ser inmuebles diferentes en la misma ciudad o ciudades diferentes), lo que genera complejidad y puede hacerlo crítico.

g) **Tratamiento de datos sensible**: Al incluir estos datos se debe tomar medidas de protección como mínimo de categoría intermedio.

De esta manera se muestra algunos gráficos para un mejor entendimiento.

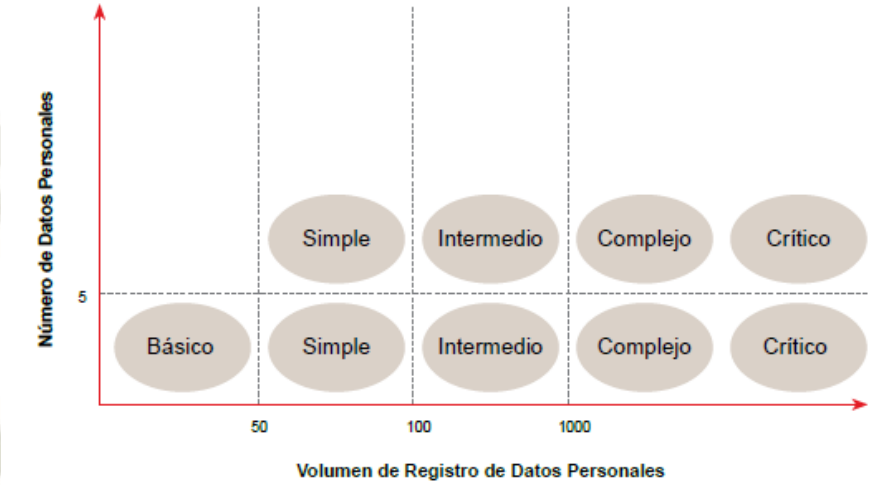


Figura B 1 Volumen de datos / Número de datos

Fuente: Directiva de Seguridad

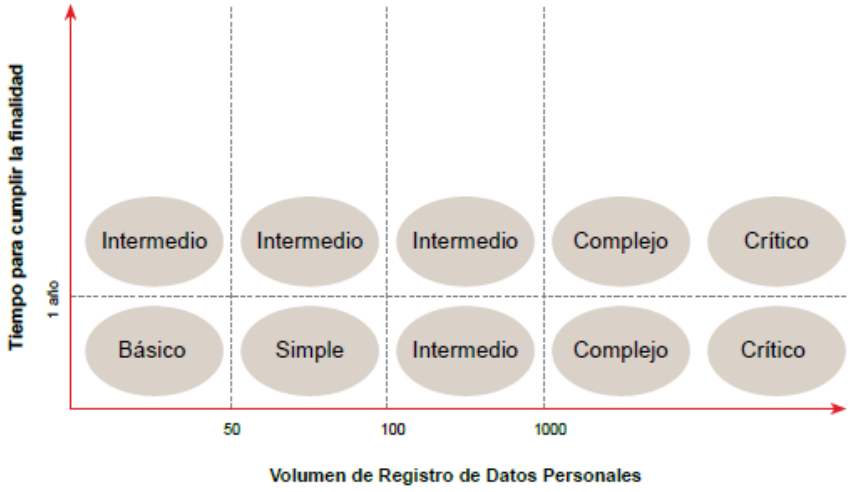


Figura B 2 Volumen de datos / Tiempo para cumplir la finalidad

Fuente: Directiva de seguridad

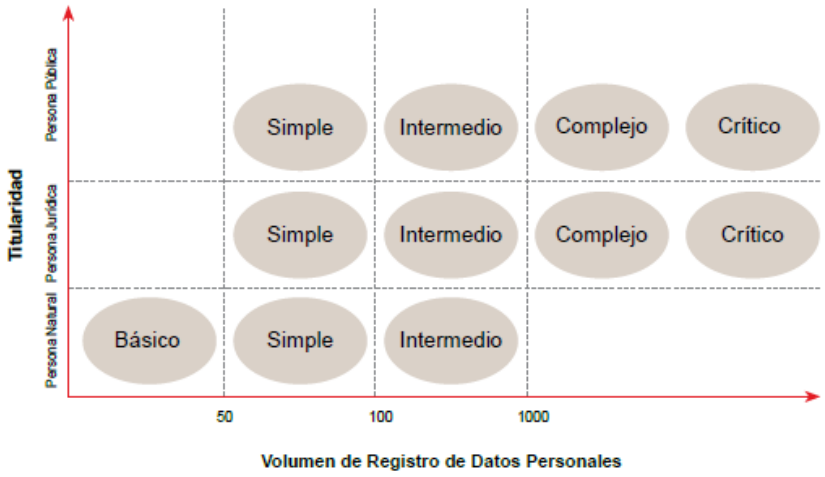


Figura B 3 Volumen de datos / Titularidad del banco de datos personales

Fuente: Directiva de Seguridad

A continuación, la siguiente figura muestra una matriz de apoyo para la Identificación de la categoría de los bancos de datos.

ÍTEM	CRITERIO	BÁSICO	SIMPLE	INTERMEDIO	COMPLEJO	CRÍTICO
1	Volumen de registros, número de titulares de datos personales que consienten el tratamiento de sus datos. (Criterio utilizado para determinar las categorías).	Hasta 50	Hasta 100	Hasta 1000	Indeterminado	Indeterminado
2	Número de datos personales en banco de datos personales que no contienen datos sensibles. (Criterio utilizado para determinar el tipo básico).	Hasta 5	Más de 5	Más de 5	Más de 5	Más de 5
3	Finalidad del tratamiento de datos personales respaldada por ley o similar. (Criterio utilizado para determinar el tipo crítico).	No aplica	No aplica	No aplica	No aplica	Aplica
4	Periodo mayor a un (01) año o indeterminado para cumplir la finalidad (tiempo de tratamiento de los datos personales).	No aplica	No aplica	Aplica	Aplica	Aplica
5	Tipo de Titular del banco de datos personales: persona natural. (Criterio utilizado para determinar el tipo entre básico a intermedio).	Aplica	Aplica	Aplica	No aplica	No aplica
6	Tipo de Titular del banco de datos personales: persona jurídica. (Criterio utilizado para determinar la categoría entre simple a complejo).	No Aplica	Aplica	Aplica	Aplica	Aplica
7	Titular del banco de datos personales del tipo persona jurídica o entidad pública con múltiples localizaciones desde las cuales se tiene acceso al banco de datos personales o se realiza tratamiento de los datos personales. (Criterio utilizado para determinar la categoría complejo o crítico).	No Aplica	No aplica	No aplica	Aplica	Aplica
8	El banco de datos personales puede incluir datos sensibles. (Criterio utilizado para determinar la categoría entre intermedio a crítico).	No Aplica	No aplica	Aplica	Aplica	Aplica

Figura B 4 Matriz de apoyo para la categorización

Fuente: Directiva de Seguridad

ANEXO C

GLOSARIO DE TÉRMINOS

Autoridad Nacional de Protección de Datos Personales (APDP). Nace con la dación de la Ley N° 29733, Ley de Protección de Datos Personales. La cual establece los términos en que se garantiza el derecho fundamental a la protección de los datos personales a través de un adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales.

Banco de Datos. Cuando se habla de un banco de datos estamos señalando que esa información está clasificada y ordenada de acuerdo a diferentes parámetros ya que la misma puede ser solicitada muy a menudo con diversos fines.

Banco de datos personales. Conjunto de datos personales.

Consentimiento del titular de los datos personales. Es la aceptación de una persona de realizar un tratamiento con sus datos personales.

Dato Personal. Información sobre una persona natural que la identifica o la hace identificable.

Dato Sensible. Datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual.

Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición). Son el conjunto de derechos a través de los cuales la Ley N°29733 – Ley de Protección de Datos Personales, garantiza a las personas el poder de control sobre sus datos personales.

Registro Nacional de Protección de Datos Personales. Es un registro de carácter administrativo a cargo de la Autoridad Nacional de Protección de Datos Personales, que tiene como finalidad de inscribir en forma diferenciada, a nivel nacional, lo siguiente:

1. Los bancos de datos personales de administración pública o privada.
2. Las comunicaciones de flujo transfronterizo de datos personales.
3. Las sanciones, medidas cautelares o correctivas.

Directiva de Seguridad de Información. Es un documento que se usa como instrumento para que facilite el cumplimiento de la Ley.

Flujo transfronterizo de datos personales. Transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban.

ISO 27001. Es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

Medidas de seguridad físicas. Consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas, ante amenazas a los recursos e informaciones confidenciales. Desastres naturales, sabotajes internos o externos, etc, forman parte de este tipo de seguridad.

Medidas de seguridad lógicas. Es el conjunto de operaciones y técnicas orientadas a la protección de la información contra la destrucción, la modificación, la divulgación indebida o el retraso en su gestación.

Medidas Legales. Son aquellas medidas que se deben adoptar en una empresa con el apoyo del área legal. Estos pueden ser: modificación de contratos y creación de nuevas cláusulas, entre otros.

Medidas Organizativas. Son aquellas medidas que se deben adoptar en una empresa con el apoyo de todas las áreas. Estos pueden ser: creación de nuevas políticas, entre otros.

Medidas Técnicas. Son aquellas medidas que se deben adoptar en una empresa con el apoyo del área de tecnologías de la información. Estos pueden ser: generación de copias de respaldo, control de acceso al sistema, entre otros.

Políticas de seguridad de información. Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Principio de calidad. El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.

Principio de consentimiento. Para el tratamiento de los datos personales debe mediar el consentimiento de su titular.

Principio de disposición de recurso. Todo titular de datos personales debe contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales.

Principio de finalidad. Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización.

Principio de legalidad. El tratamiento de los datos personales se hace conforme a lo establecido en la ley. Se prohíbe la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos.

Principio de proporcionalidad. Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.

Principio de seguridad. El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.

Titular de los datos personales. Persona natural o jurídica a la cual pertenecen los datos personales.

Titular del banco de datos personales. Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad.

Transferencia de Datos personales. Toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta del titular de datos personales.

Tratamiento de datos personales. Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.