MODELO PARA LA IMPLEMENTACIÓN DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES BASADO EN EL SGSI DE LA NORMA ISO 27001

JOHN JAIRO RUIZ CONCHA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIAS E INGENIERIAS
ESPECIALIZACION EN SEGURIDAD INFORMATICA
CALI
2018

MODELO PARA LA IMPLEMENTACIÓN DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES BASADO EN EL SGSI DE LA NORMA ISO 27001

JOHN JAIRO RUIZ CONCHA

Monografía para optar al título de
Especialista en Seguridad Informática

Esp. Ing. Freddy Enrique Acosta
Director del Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIAS E INGENIERIAS
ESPECIALIZACION EN SEGURIDAD INFORMATICA
CALI
2018

Nota de aceptación:

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Santiago de Cali, mayo de 2018

Este proyecto está dedicado a Dios por darme la fuerza, ayudarme con la perseverancia, constancia y brindarme la salud para seguir adelante y no desfallecer.

A mi esposa por su amor, ayuda incondicional y comprensión en los momentos de mayor exigencia y dificultad con el tiempo.

A mis hijos por ser el motor de impulso y decisión de seguir adelante con mis proyectos y carrera.

A mis padres y abuela que dieron origen a mi existencia y marcaron la persona que soy actualmente.

John Jairo Ruiz Concha

AGRADECIMIENTOS

John Jairo expresa su agradecimiento a:

Al ingeniero Luis Enrique Escobar Tafur Docente CEAD Palmira, por su tiempo, atención y diligencia para aclarar dudas relacionados con el proceso realizado en la carrera y trámites para lograr la especialización.

A nuestro director de curso, Ingeniero Salomón González García, por su acompañamiento y oportunas orientaciones para el desarrollo de este proyecto.

Al director de proyecto, Ingeniero Esp. Freddy Enrique Acosta, por su seguimiento y observaciones en la elaboración de esta monografía.

A la Universidad Nacional Abierta y a Distancia UNAD, por darme la oportunidad de mejorar mis competencias y perfil profesional en el área de Ingeniería de sistemas y la seguridad informática.

A todas aquellas personas, tutores y docentes que me ayudaron en el desarrollo de este proyecto y me brindaron sus conocimientos.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

GLOSARIO

ACTIVO: En seguridad de la información se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, personas etc) que tenga valor para la organización[1].

AMENAZA: Causa potencial de un incidente no deseado o planeado, que representa un riesgo o que puede provocar daños a un sistema o a la organización[2].

ANÁLISIS DE RIESGO: Proceso por el cual se busca comprender la naturaleza del riesgo y determinar su nivel o impacto[3].

AUDITORÍA: Proceso sistemático, independiente y documentado para obtener evidencias y poder determinar el grado de cumplimiento de los criterios de una auditoria[4].

ATAQUE: Acción de vulnerar la seguridad de un software, hardware o persona explotando algún tipo de debilidad, vulnerabilidad, bug o problema[5].

DATO PERSONAL: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables[6].

DISPONIBILIDAD: Disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio[7].

HABEAS DATA: Es el derecho que tiene toda persona o institución a solicitar la información que sobre sí mismo se encuentre almacenada en cualquier base de datos y el derecho de ser actualizada o eliminada si así se requiere[8].

---

[1] Glosario Sistemas de Gestión de Seguridad de la Información. {En línea}. {citado 14 de noviembre de 2017} disponible en: https://glosarios.servidor-alicante.com/sistemas-gestion-seguridad-informacion_es-en/activo
[2] Guía para realizar el Análisis de Impacto de Negocios BIA. {En línea}. {citado 14 de noviembre de 2017} disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G11_Analisis_Impacto.pdf. p. 6.
[3] Ibid., p. 6.
[4] Ibid., p. 6.
[5] MIERES, Jorge. Fundamentos sobre Seguridad de la Información. {En línea}. {citado 14 de noviembre de 2017} disponible en: http://www.seguinfo.com.ar/terceros. p. 5.
[6] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1581. Bogotá. (octubre 17 de 2012). Diario Oficial 48587 de octubre 18 de 2012.
[7] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método. Madrid, España octubre de 2012 p. 9.
[8] REMOLINA, Nestor. El habeas data en Colombia. {En línea}. {citado 14 de noviembre de 2017} disponible en: https://habeasdatacolombia.uniandes.edu.co/

HARDWARE: Conjunto de elementos materiales o físicos que componen una computadora[9].

INCIDENTE: Evento con consecuencias en detrimento de la seguridad del sistema de información[10].

INFORMACIÓN: Conjunto de datos que al ser unidos tienen un significado especifico más allá de cada uno de estos[11].

IMPACTO: Costo asociado a un incidente, que puede o no ser medido en términos estrictamente financieros, pérdida de reputación, implicaciones legales, etc.[12].

INTEGRIDAD: Propiedad de la información relativa a su exactitud y completitud[13].

OFIMÁTICA: Es el conjunto de métodos, aplicaciones y herramientas informáticas que se usan en labores de oficina con el fin de perfeccionar, optimizar, mejorar el trabajo y operaciones relacionados[14].

RIESGO: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias[15].

SOFTWARE: Conjunto de programas que pueden ser ejecutados por el hardware para realizar tares solicitadas por los usuarios[16].

SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, integridad y disponibilidad de la información[17].

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI: Conjunto de elementos interrelacionados que se utilizan para establecer una política, unos objetivos de seguridad y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua[18].

---

[9] MIERES. Op. cit., p. 5.
[10] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. Op. cit., p. 101.
[11] MIERES. Op. cit., p. 5.
[12] Glosario. El portal de ISO 27001 en español. {En línea}. {citado 14 de noviembre de 2017} disponible en: http://www.iso27000.es/glosario.html#section10i
[13] Ibid.
[14] Significados. Significado de Ofimática. {En línea}. {citado 14 de noviembre de 2017} disponible en: https://www.significados.com/ofimatica/
[15] Ibid.
[16] Ibid.
[17] Guía para realizar el Análisis de Impacto de Negocios BIA. {En línea}. {citado 14 de noviembre de 2017} disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G11_Analisis_Impacto.pdf. p. 6.
[18] Ibid., p. 7.

VULNERABILIDAD: Debilidad de un activo o control que puede ser explotada por una o más amenazas[19].

[19] Glosario. El portal de ISO 27001 en español. {En línea}. {citado 14 de noviembre de 2017} disponible en: http://www.iso27000.es/glosario.html#section10i

RESUMEN

Con la nueva ley 1581 o régimen general de protección de datos personales que estableció el gobierno desde 2012 y dadas las sanciones que se han generado a muchas empresas en Colombia a la fecha, por el desconocimiento de la norma, mal tratamiento de los datos personales y problemas de seguridad asociados en su tratamiento y almacenamiento, se propone el desarrollo del presente trabajo, para que sirva como guía y modelo para la implementación y adopción de la ley 1581 al interior de las organizaciones.

Este modelo se basa en lineamientos de la norma ISO 27001, la metodología de análisis de riesgos que propone MAGERIT y el sistema de gestión de protección de datos SGDP que adopto la unión europea, para tratar de lograr que este mandato cumpla su cometido, que es la concientización de las empresas por la protección de nuestros datos personales y el derecho que tienen todas las personas a la intimidad, privacidad y correcto tratamiento de sus datos personales que permita actualizar, rectificar, consultar y oponerse a su tratamiento en el momento que sea requerido.

Además de ayudar al cumplimiento de la Ley 1581 de protección de datos personales, el uso de este modelo permitirá a las empresas PYMES de Colombia identificar y analizar amenazas, riesgos y vulnerabilidades asociadas a los activos tecnológicos vinculados en el manejo de la información, permitiendo de esta manera establecer políticas, controles y buenas prácticas para proteger y mejorar la seguridad de la información y los datos, los cuales son uno de los activos más valioso que tienen las organizaciones para ayudarles a cumplir sus objetivos misionales y mantener la confianza y credibilidad de sus clientes.

Palabras claves:

Datos personales, Ley, Seguridad de la información, Seguridad informática, Protección, Riesgos, Amenazas, Vulnerabilidades, Metodología, Políticas, Sanciones

ABSTRACT

With the new law 1581 or the general regime of protection of personal data established by the government since 2012 and the laws that have been generated in many companies in Colombia to date, due to ignorance of the norm, poor treatment of personal data and security problems associated with its treatment, it is proposed the development of the present work, for those who serve as a guide and model for the implementation and adoption of law 1581 within organizations.

This model is based on the guidelines of the ISO 27001 standard, the Risk Analysis Methodology offered by MAGPRIT and the SGDP data protection management system adopted by the European Union, in order to ensure that this mandate fulfills its purpose, which is the awareness of the companies for the protection of our personal data and the right that all people have to the privacy, privacy and right to the processing of their personal data that allow updating, rectifying, consulting and opposing their treatment at the time it is required .

In addition to helping to comply with Law 1581 on the protection of personal data, the use of this model allows SMEs in Colombia to identify and analyze threats, risks and vulnerabilities associated with technological assets linked to the handling of information, which allows the use of this information, modes of operation, controls and good practices to protect and improve the security of information and data, which are the most appropriate for the security and credibility of its customers.

Keywords:

Personal data, Law, Information security, Computer security, Protection, Risks, Threats, Vulnerabilities, Methodology, Policies, Sanctions

INTRODUCCIÓN

El valor que tiene la información y los datos es cada vez mayor para las empresas, ya que su importancia radica en la forma como se usa y procesa para la toma de decisiones, acciones que se dan por su calidad de secreto industrial y como activo relevante en las operaciones que se hacen diariamente. Estos datos no siempre son propiedad de las empresas, ya que la mayoría de veces son datos que pertenecen a los clientes, usuarios o titulares. La diversidad de datos que puede ser asociada a una persona es bastante amplia y puede encontrarse en distintas formas, ya sea física o digital. Es por esto que los cibercriminales vean con mayor interés este activo, ya que se utilizan los medios tecnológicos para cometer delitos que ponen en riesgo la integridad de las personas y la continuidad de las organizaciones.

Cada vez se ven más incidentes de seguridad en las empresas, relacionados con fuga de información, donde ciberdelincuentes utilizan distintos vectores de ataque para lograr el cometido, de esta manera en 2014 se conocieron casos de fuga de información relacionados con malware en Punto de venta (POS), en compañías como Target, Home Depot o UPS, donde los atacantes lograron obtener más de 40 millones de números de tarjetas de crédito y débito de usuarios. Empresas como eBay o Yahoo! también se vieron en la necesidad de notificar a miles de usuarios que sus cuentas y contraseñas habían sido filtradas a través de un ataque cibernético y el caso de Comunity Health System (CHS) en los Estados Unidos en 2015, que fue víctima de la fuga de 4.5 millones de registros médicos. De acuerdo con el comunicado de la entidad, sus sistemas fueron víctimas de una APT (Amenaza avanzada persistente).[20]

Brasil, México y Colombia son los países de América Latina más afectados en el último año por ataques informáticos, que dejaron pérdidas en la región por unos

[20] MENDOZA, Miguel Ángel. Importancia de la protección de los datos {En línea}. {citado 26 de mayo de 2017} disponible en: http://www.welivesecurity.com/la-es/2015/10/16/importancia-datos-personales-proteccion/

184.000 millones de dólares, según estudio presentado por el proveedor de seguridad informática Digiware en 2016. En Colombia se reportaron pérdidas por 5.700 millones de dólares, que significan un aumento del 4 % con respecto al año pasado.[21]

En Colombia la Ley 1581 de Protección de Datos Personales de 2012 reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar los datos que se hayan recogido sobre ellas en archivos físicos o bases de datos digitales que sean aptos de tratamiento por entidades de naturaleza pública o privada, ya sean fundaciones, colegios, conjuntos residenciales o empresas.

Como dice el Abogado Miguel Ángel Ramírez, la Ley 1581 de protección de datos personales: “Es también una herramienta legal para proteger a los ciudadanos de fraudes por el uso indebido de su información. En internet abundan programas que recolectan datos específicos de los usuarios, los cuales pueden ser usados por delincuentes para cometer fechorías”.[22]

Es claro que se están dando pasos lentos pero progresivos en materia de protección de datos personales, sin embargo, falta aún mucho camino por recorrer para lograr conciencia en las organizaciones por tener programas con la suficiente madurez y consolidación que permitan una efectiva protección de los datos personales[23] (Balanta Heidy, 2017), y se le dé el valor que debe tener el activo más importante como es la información.

[21] EFE FUTURO. Ciberataques en América Latina dejan pérdidas por 184.000 millones de dólares. {En línea}. {citado 26 de mayo de 2017} disponible en: http://america.efefuturo.com/noticia/ciberataques-america-latina-dejan-perdidas-184-000-millones-dolares/

[22] RAMIREZ, Miguel Ángel. Ley de Protección de datos en Colombia. {En línea}. {citado 14 de noviembre de 2017} disponible en: http://www.colombialegalcorp.com/especialistas/bogota/miguel-ramirez/

[23] BALANTA, Heidy. Retos de los programas de protección de datos personales en Colombia. {En línea}. {citado 14 de noviembre de 2017} disponible en: https://colombiadigital.net/opinion/columnistas/derecho-y-economia-digital/item/9578-retos-de-los-programas-de-proteccion-de-datos-personales-en-colombia.html

De acuerdo a este nuevo régimen general de protección de datos personales establecido por el gobierno y con las sanciones y multas que se han generado a muchas empresas en Colombia a la fecha, por el desconocimiento de la norma y mal tratamiento de los datos personales, este documento sirve como guía y modelo para la adopción e implementación de la Ley 1581 en las PYMES de Colombia.

Este modelo se basa en el estándar internacional para la seguridad de la información ISO 27001, la metodología de análisis de riesgos que propone MAGERIT y el sistema de gestión de protección de datos personales (SGPDP) que adopto la unión europea.

Con esta guía se busca ayudar al cumplimiento de este mandato y su cometido, que es la concientización de las empresas por la protección de los datos personales y el derecho que tienen todas las personas a la intimidad, privacidad y correcto tratamiento de sus datos personales que permita actualizar, rectificar, consultar y oponerse a su tratamiento en el momento que sea requerido, además de dar pautas necesarias para mejorar la seguridad de la información y de los datos personales en las empresas.

1. DEFINICION DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

Con la firma y entrada en vigor de la ley 1581 en 2012 se creó un régimen que busca que todas las empresas y personas naturales que manejan datos personales en sus relaciones comerciales tengan políticas, controles, procedimientos y medidas tecnológicas que garanticen el correcto tratamiento de los datos y seguridad de los mismo, además se estableció que los responsables y encargados de las bases de datos realicen el reporte de las misma ante la Superintendencia de Industria y Comercio SIC, al Registro Nacional de Bases de Datos (RNBD).

En Colombia la Superintendencia de Industria y Comercio (SIC) es el ente de control escogido por el gobierno central y bajo la Ley 1581 para hacer cumplir esta norma que al 2016 había sancionado a más de 600 empresas y personas naturales por violar la ley de protección de datos personales generando alrededor de $19.000 millones en sanciones[24] y que a junio de 2017 subió a $21.000 millones de acuerdo a notificación oficial[25], donde se destacan:

- La falta de la autorización para el manejo de datos personales
- No informar la finalidad para el tratamiento de los datos recogidos
- No atender oportunamente las consultas y reclamos de los titulares dueños de los datos personales
- Falta de medidas técnicas y fallas en la seguridad de la información

[24] COLPRENSA. Hay 602 empresas sancionadas por violar la ley de protección de datos. {En línea}. {citado 26 de mayo de 2017} disponible en: http://www.laopinion.com.co/economia/hay-602-empresas-sancionadas-por-violar-la-ley-de-proteccion-de-datos-127060

[25] SIC. Sanciones {En línea}. {citado 2 de octubre de 2017} disponible en: http://www.sic.gov.co/noticias/por-violaciones-de-datos-personales-superindustria-ha-impuesto-sanciones-por-mas-de-21-mil-millones-de-pesos

Con respecto a las fallas de seguridad y de acuerdo con el estudio “Impacto de los incidentes de seguridad digital en Colombia 2017”, realizado por la Organización de los Estados Americanos (OEA), el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (Min TIC) y el Banco Interamericano de Desarrollo (BID), se revela que el 51% de las medianas empresas y el 63% de las grandes empresas en Colombia sufrieron incidentes digitales en 2016.[26]

A la fecha solo un 27%[27] de las empresas en Colombia han cumplido con el registro RNBD y para el cumplimiento de la norma se debe implementar las disposiciones legales y las recomendaciones dadas por la SIC antes de su vencimiento o plazo final el 30 de enero de 2018.

El desconocimiento de la ley y los puntos a realizar es uno de los factores que ha impedido que las empresas en Colombia cumplan con este requisito que puede generar sanciones hasta por 2000 SMMV o cierre parcial o definitivo del establecimiento.

Otro factor de incumplimiento es la falta de compromiso y tiempo que se le debe dedicar por parte de directivos de la empresa y colaboradores para entender y cumplir con los puntos que establece la SIC en la guía de responsabilidad demostrada, la cual da las pautas necesarias para el cumplimiento de la Ley y correcto registro de las bases de datos personales.

[26] EL TIEMPO. El 63 % de las grandes empresas identificaron incidentes digitales. {En línea}. {citado 14 de noviembre de 2017} disponible en: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/resultados-del-estudio-impacto-de-los-incidentes-de-seguridad-digital-en-colombia-2017-137222
[27] SIC. Sanciones {En línea}. {citado 12 de noviembre de 2017} disponible en: http://www.sic.gov.co/registro-nacional-de-bases-de-datos

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo ayudar a las PYMES en Colombia a cumplir con el registro RNBD y la Ley 1581 de 2012 de protección de datos personales de forma completa y evitar ser sancionado?

1.3 OBJETIVOS

1.3.1 Objetivo General

Proponer un modelo para la implementación de la Ley 1581 de protección de datos personales que permita de forma adecuada el cumplimiento de la norma por parte de las PYMES en Colombia.

1.3.2 Objetivo Específicos

- Reconocer el estado de la organización frente al cumplimiento de la ley 1581 de protección de datos personales.
- Definir pautas para la identificación y clasificación de los datos personales que maneja la empresa.
- Presentar un modelo de documentación básica que requiere la empresa para la implementación de la Ley 1581.
- Proponer mecanismos para identificar riesgos, amenazas y el estado actual de seguridad de la información en la empresa.
- Establecer medidas, procedimientos y buenas prácticas para prevenir incidentes relacionados con el tratamiento de datos personales.
- Preparar a la organización para el proceso de registro de bases de datos ante la SIC.

1.4 JUSTIFICACION

El derecho a la protección de los datos personales y la intimidad es un derecho de tipo fundamental consagrado en la constitución colombiana que tienen todas las personas a conocer, actualizar y rectificar los datos que se hayan recogido sobre ellas en archivos físicos o bases de datos digitales, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma, pero a pesar de esto, hoy en día se enfrentan constantes irregularidades tanto en la captura de los datos, como en los procedimientos de tratamiento y conservación de los datos de las personas naturales y jurídicas.

Es normal que todas las empresas utilicen información personal en distintos procesos para el desarrollo de su actividad, en su día a día se recogen datos personales, de forma verbal y escrita, a través de página web, correo electrónico, formularios físicos o digitales etc.; desconociendo en muchas ocasiones que dichos datos y su posterior tratamiento debe cumplir con las disposiciones legales en materia de manejo, procesamiento, almacenamiento, uso de las bases de datos, tecnología y seguridad, so pena de incurrir en sanciones importantes de hasta 2000 Salarios Mínimos Legales Mensuales Vigentes.[28]

De acuerdo a datos presentados por la Súper intendencia de Industria y Comercio SIC, a la fecha se han presentado más de 5.000 quejas y alrededor de 600 multas impuestas por más de $19.000 Millones de Pesos en materia de protección de datos personales. Estas sanciones se han presentado por incumplir los términos legales a nivel de procedimientos, pero también se deben a deficiencias en la seguridad de

[28] TABARES, Ands, Ensayo de protección de datos. {En línea}. {citado 26 de mayo de 2017} disponible en: http://ensayosands.blogspot.com.co/2016/05/ensayo.html”

la información que presentan las empresas como falta de protocolos, controles y medidas técnicas que se derivan en fuga de información o robo de datos.[29]

Es necesario y obligatorio en términos de la Ley 1581 de 2012 adoptar medidas legales, procedimentales y técnicas necesarias para cubrir posibles contingencias y cumplir con los 10 puntos del principio de responsabilidad demostrada, además del decreto 886 de 2014 donde se reglamentó el registro nacional de bases de datos (RNBD) ante la SIC y se estableció un plazo para que las empresas hagan el registro de forma organizada por rangos de acuerdo a su NIT el cual vencen en enero 30 de 2018.

Por tal razón, la siguiente monografía incluye elementos importantes para el reconocimiento de la norma que permita la adopción e implementación de la ley 1581 en la organización y ayude en el proceso de crear un sistema de gestión de protección de datos personales alineado a buenas prácticas internacionales de seguridad de la información como ISO 27001.

Además, este trabajo, busca que las PYMES en Colombia tengan una guía o modelo base, que les permita desarrollar de forma clara y correcta los puntos requeridos para el cumplimiento de la ley y de esta manera, se eviten sanciones o multas que puedan generar dificultades al desarrollo y crecimientos de las mismas, pero que también ayude a prevenir incidentes de seguridad que afecten el activo más valioso que tienen las empresas que es la información y de esta manera se logre mantener la confianza de sus clientes y titulares.

[29] CARACOL RADIO. Multas por violación a ley de datos ascienden a 19.000 millones de pesos. {En línea}. {citado 26 de mayo de 2017} disponible en: http://caracol.com.co/radio/2017/01/27/economia/1485540887_417956.html

1.5 ALCANCE Y LIMITACIONES

1.5.1 Alcance

La presente monografía se encuentra entre los proyectos de gestión de seguridad y lo que pretende es proponer un modelo teórico para la implementación de la Ley 1581 de protección de datos personales en las PYMES de Colombia, reuniendo de manera organizada las actividades básicas necesarias para llevar a cabo el cumplimiento de los términos legales impuestos por la Ley.

Este modelo se basa en el sistema de gestión de seguridad la información SGSI de la norma ISO 27001, toma como referencia la metodología de análisis de riesgos que propone MAGERIT y el sistema de gestión de protección de datos personales SGPDP que adopto España como referente de la norma a nivel internacional.

También tendrá como alcance proponer acciones y recomendaciones de seguridad informática para que las empresas mejoren sus niveles de protección para evitar la fuga de información o robo de datos.

1.5.2. Limitaciones

Es conveniente resaltar que el desarrollo de la presente monografía no abarcara temas como los que se definen a continuación:

- Diseño y desarrollo de todos los procedimientos y documentación relacionada con el tratamiento de datos personales en la empresa.
- Implementación del sistema de gestión de protección de datos personales SGPDP en la empresa.
- Implementación del sistema de gestión de seguridad de la información SGSI en la empresa.

1.6 DISEÑO METODOLÓGICO

1.6.1 Unidad de Análisis

Pequeñas y medianas empresas (PYMES) de Colombia que desarrollan actividades comerciales y que tratan datos personales.

1.6.2 Población y Muestra

1.6.2.1 Población

Empresas PYMES ubicadas en la ciudad de Cali, Colombia.

1.6.2.2 Muestra

Empresas PYMES comerciales registradas en cámara de comercio.

1.6.3 Estudio metodológico

Este proyecto es una investigación de tipo proyectiva.

Este tipo de investigación, consiste en la elaboración de un modelo, como solución a un problema o necesidad de tipo práctico, ya sea de un grupo social, o de una institución, o de una región geográfica, en un área particular del conocimiento, a partir de un diagnóstico preciso de las necesidades del momento, los procesos explicativos o generadores involucrados y de las tendencias futuras, es decir, con base en los resultados de un proceso investigativo.[30]

[30] Hurtado de Barrera, Jacqueline. La investigación proyectiva. {En línea}. {citado 12 de noviembre de 2017} disponible en: http://investigacionholistica.blogspot.com.co/2008/02/la-investigacin-proyectiva.html

El modelo para la implementación de la ley de protección de datos personales está basado en el SGSI de la norma ISO 27001 y toma como referencia la Guía de responsabilidad demostrada que presento la SIC, donde se deben desarrollar unas fases o pasos para su correcta implementación, además de usar la metodología MAGERIT para el análisis y valoración de los riesgos, se realizaran encuestas y se recolectaran pruebas con software de seguridad informática especial para hacer auditorias de seguridad o hacking ético, para identificar vulnerabilidades que pueden afectar los activos informáticos de la empresa y que generen riesgos para el total cumplimiento de la norma de protección de datos personales.

2. MARCO DE REFERENCIA

2.1 MARCO TEÓRICO:

2.1.1 Ley orgánica de protección de datos de España

España ha sido un país referente en el desarrollo normativo en materia de protección de datos. La Constitución Española1 incluyó como derecho fundamental, el Derecho a la intimidad y la Ley Orgánica 15/1999, de 13 de diciembre, transpuso la Directiva Europea 95/46/CE.

En la actualidad, la ley orgánica de protección de datos (LOPD) se aplica a empresas y organismos públicos que manejan datos de clientes y/o usuarios, esto es, datos de personas físicas. A nivel de sanciones es una de las legislaciones más estrictas, con cuantías muy altas, con rangos que van desde 900€ hasta 600.000€ y los tipos penales varían en función de la gravedad de los hechos, pudiendo ir de 1 a 7 años de prisión.

La Agencia Española de Protección de Datos (AEPD) es la autoridad estatal de control independiente encargada de velar por el cumplimiento de la normativa sobre protección de datos. Garantiza y tutela el derecho fundamental a la protección de datos de carácter personal de los ciudadanos. La Agencia es un Ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones. Se relaciona con el Gobierno a través del Ministerio de Justicia.[31]

[31]AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía del responsable de ficheros. {En línea}. {citado 26 de mayo de 2017} disponible en: http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/conoce/index-ides-idphp.php

En Latinoamérica, el derecho de protección de datos ha sido consagrado expresamente, en algunos países, en su constitución política; mientras que, en otros, se ha desarrollado a través de la institución del hábeas data.

Argentina destaca por ser el primer país en expedir una normativa de protección de datos y es el único reconocido actualmente por la Unión Europea con un nivel adecuado de protección. Países como Perú, Chile, Paraguay, Uruguay, México (centro-américa) y Colombia, tienen actualmente una ley vigente de hábeas data. Teniendo en cuenta que estos países afrontan una "reciente" generación normativa en materia de protección de datos, el reto actual de los gobiernos es lograr que dicha normativa sea acogida e implementada por las empresas. Así, la recomendación hacia el sector empresarial, es la de actuar con carácter preventivo y prepararse con una estructura empresarial que garantice la protección de las bases de datos, incluyendo protocolos internos de actuación y una cultura organizacional hacia el respeto y la protección de los datos de clientes y terceros data.[32]

2.1.2 Ley 1581 de protección de datos en Colombia

Los primeros lineamientos sobre la protección de datos personales en Colombia aparecen con la Constitución política de 1991 con el artículo 15, donde se consagra el derecho de cualquier persona de conocer, actualizar y rectificar los datos personales que existan sobre ella en bancos de datos o archivos de entidades públicas o privadas. Igualmente, ordena a quienes tienen datos personales de terceros respetar los derechos y garantía previstos en la Constitución cuando se recolecta, trata y circula esa clase de información.

[32] VEGA SUÁREZ, Ana Maritza. El cumplimiento de la normativa de protección de datos en Iberoamérica. {En línea}. {citado 26 de mayo de 2017} disponible en: http://www.abogacia.es/2013/11/11/el-cumplimiento-de-la-normativa-de-proteccion-de-datos-en-iberoamerica/

Veamos la evolución cronológica de la normativa:

Ley 1266 de 2008: Se dictan las disposiciones generales del Habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones (Habeas Data).

Decreto 1727 de 2009: Se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información.

Decreto 235 de 2010: Se reglamenta el intercambio de información entre entidades para el cumplimiento de funciones públicas.

Decreto 2280 de 2010: Se modifica el artículo 3° del Decreto 235 de 2010.

Decreto 2952 de 2010: Se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008.

Ley 1581 de 2012: Se dictan disposiciones generales para la protección de datos personales.

Decreto 1377 de 2013: Se reglamenta parcialmente la Ley 1581 de 2012.

Ley 1712 de 2014: Se crea la ley de transparencia y del derecho de acceso a la información pública nacional.

Decreto 886 de 2014: Se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.[33]

[33] ROZO, Catalina. Que debes conocer de la ley 1581. {En línea}. {citado 26 de mayo de 2017} disponible en: https://www.securityartwork.es/2015/06/10/que-debes-conocer-de-la-ley-1581-de-proteccion-de-datos-personales-colombiana/

Guía del Principio de Responsabilidad Demostrada, dada por la SIC para indicar que debe hacer una empresa para implementar un programa integral de gestión de datos personales.[34]

Decreto 1759 del 8 de noviembre de 2016 con el cual se amplía el plazo para llevar a cabo el registro de las bases de datos los Responsables del Tratamiento, personas jurídicas de naturaleza privada y sociedades de economía mixta inscritas en las cámaras de comercio del país hasta junio 30 de 2017 y personas naturales, entidades de naturaleza pública distintas de las sociedades de economía mixta y personas jurídicas de naturaleza privada que no están inscritas en las cámaras de comercio hasta junio 30 de 2018[35], pero dado el bajo registro de las empresas, mediante el Decreto 1115 del 29 de junio de 2017 se modificó el artículo 2.2.2.26.3.1 del Decreto 1074 de 2015 y amplio el plazo final al 31 de enero de 2018 para las personas jurídicas de naturaleza privada y sociedades de economía mixta y 31 de enero de 2019 para las personas naturales y entidades públicas.

2.1.3 Seguridad de la Información

La seguridad de la información tiene como fin preservar los principios básicos como son: confidencialidad, integridad y disponibilidad de la misma y de los sistemas implicados en su tratamiento. Estos tres pilares se definen[36] como:

- Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados.
- Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

[34]ITECH SAS. Responsabilidad Demostrada. {En línea}. {citado 26 de mayo de 2017} disponible en: http://www.itechsas.com/blog/ley-1581-protecion-de-datos/responsabilidad/
[35] SIC. Registro nacional de bases de datos. {En línea}. {citado 26 de mayo de 2017} disponible en: http://www.sic.gov.co/registro-nacional-de-bases-de-datos
[36] ISO27000. Preguntas más frecuentes. {En línea}. {citado 26 de mayo de 2017} disponible en: “Preguntas más Frecuentes, doc_faq_all.pdf pág. 9”, www.iso27000.es.

- Disponibilidad: Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.

En la seguridad de la información se deben tener en cuenta los aspectos tecnológicos, los procesos, los ambientes o espacios de trabajo (centro de cómputo, ubicación de oficinas) y principalmente las personas.

2.1.4 Norma ISO27001

Es un estándar ISO que proporciona un modelo para establecer, implementar, utilizar, monitorizar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Se basa en el ciclo de vida PDCA (Planear-Hacer-Verificar-Actuar; o ciclo de Deming) de mejora continua, al igual que otras normas de sistemas de gestión (ISO 9001 para calidad, ISO 14001 para medio ambiente, etc.).

Este estándar es certificable, es decir, cualquier organización que tenga implantado un SGSI según este modelo, puede solicitar una auditoria externa por parte de una entidad acreditada y, tras superar con éxito la misma, recibir la certificación en ISO 27001.

El origen de la Norma ISO27001 está en el estándar británico BSI (British Standards Institution) BS7799Parte 2, estándar que fue publicado en 1998 y era certificable desde entonces. Tras la adaptación pertinente, ISO 27001 fue publicada el 15 de octubre de 2005[37].

La norma ISO 27001 está creada para ser aplicable a cualquier tipo de organización y no solo se concentra en la infraestructura tecnología, sino también en otros activos

[37] MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA ESTRATEGIA DE GOBIERNO EN LÍNEA. {En línea}. {citado 26 de mayo de 2017} disponible en: http://programa.gobiernoenlinea.gov.co/apc-aa-files/da4567033d075590cd3050598756222c/Modelo_Seguridad_Informacion_2_0.pdf

como los servicios, la documentación, las personas, proveedores, los clientes, socios, etc., además de buscar controles que apliquen para disminuir los riesgos que existen en la organización.

Según la norma ISO 27001, para implementar un Sistema de Gestión de la Seguridad de la Información (SGSI), se debe profundizar en la Evaluación de Riesgos. Esto permitirá a la dirección organizacional tener la visión necesaria para definir el alcance y aplicación de la norma, así como el diseño de políticas y medidas a implantar, teniendo en cuenta siempre la mejora continua.[38]

2.1.5 Sistema de Gestión de la Seguridad de la Información -SGSI

Un Sistema de Gestión de la Seguridad de la Información SGSI, es un sistema que consta de un conjunto de actividades o acciones de gestión que deben realizarse por medio de procesos organizados, documentados y que son conocidos por una organización o entidad.[39]

La figura 1 muestra de forma resumida las fases de un Sistema de Gestión de la Seguridad de la Información que propone el estándar ISO 27001:

[38] Normas ISO. Implantando la Norma ISO 27001. {En línea}. {citado 14 de Noviembre de 2017} disponible en: http://www.normas-iso.com/2012/implantando-iso-27001
[39] ISO27000. SGSI. {En línea}. {citado 26 de mayo de 2017} disponible en: http://www.iso27000.es/sgsi.html

Figura 1. Fases del SGSI de la norma ISO 27001

Fuente: http://www.normas-iso.com/iso-27001

La norma busca que se haga un análisis y evaluación de riesgos y de esta forma se seleccionen los controles correctos para mitigarlos. El anexo A de la norma ISO 27001:2013, es un compendio de 114 controles de seguridad. A continuación, se listan los controles del anexo A en sus 14 secciones que posee:

A.5 Políticas de seguridad, relacionados con la definición y revisión de las políticas.
A.6 Organización de la seguridad de la información, los aplicados a definición de responsabilidades, contacto con autoridades, teletrabajo y dispositivos móviles.

A.7 Seguridad en los recursos humanos, definen los requisitos para la contratación de nuevos empleados, su permanencia y luego de su retiro.

A.8 Gestión de activos, inventario de activos, uso aceptable de los mismos, clasificación de la información y manejo de medios extraíbles.

A.9 Control de acceso, relacionados con el acceso y responsabilidades de los usuarios, control de acceso a aplicaciones y sistemas.

A.10 Criptografía, cifrado de información y administración de claves.

A.11 Seguridad física y del entorno, definición de áreas seguras, salvaguardas contra amenazas, seguridad de equipos, políticas de pantalla limpia, entre otros.

A.12 Seguridad en las operaciones, controles relacionados con la gestión de la infraestructura tecnológica, copias de seguridad, supervisión, etc.

A.13 Seguridad en las comunicaciones, relacionados con seguridad de redes, transferencia de información, mensajería, etc.

A.14 Adquisición, desarrollo y mantenimiento de sistemas, definen requisitos de seguridad en los procesos de desarrollo, mantenimiento y soporte de sistemas.

A.15 Relaciones con proveedores, cómo definir y supervisar los acuerdos con proveedores.

A.16 Gestión de incidentes de seguridad de la información, controles para informar sobre eventos, asignación de responsabilidades, recopilación de evidencias y procedimientos de respuesta.

A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio, controles garanticen la continuidad del negocio y la recuperación ante incidentes.

A.18 Cumplimiento, controles para el cumplimiento de requisitos legales, contractuales y normatividad aplicable.

2.1.6 Fases del análisis de riesgos

Sin importar que metodología usemos, por lo general todas tienen estas 3 fases básicas:

- Identificación de activos: Es el conjunto de elementos que sostienen las actividades de la organización y que requieren un nivel de protección de acuerdo a su importancia. Es preciso identificar la información que se requiere proteger, su valor, y los elementos como: hardware, software, redes, procesos y personas que soportan el almacenamiento, procesamiento y transmisión de información.
- Evaluación de amenazas y vulnerabilidades: Es el proceso para identificar las amenazas, los activos que pueden ser afectados y el cálculo de la probabilidad de que ocurra, junto con la identificación de vulnerabilidades de los activos valorados.
- Tratamiento del riesgo: Se establecen los controles que permitan mitigar el riesgo, pero que a su vez sean acordes al tipo de empresa y sus necesidades. La base de seleccionar medidas o controles de protección optimas es la de que el costo de controlar cualquier riesgo no exceda la máxima pérdida asociada al riesgo. El objetivo final es minimizar el riesgo al nivel que para la empresa sea aceptable.

El riesgo residual es el nivel de riesgo que queda después de la formulación de los controles, vulnerabilidad y amenazas relacionadas entre sí. Una vez identificado este riesgo residual el paso siguiente es identificar la manera más eficiente de reducirlo a un nivel aceptable.

Teniendo en cuenta el proceso de evaluación de riesgos, estos pueden ser aceptados o mitigados. Para mitigar un riesgo se tenemos 3 opciones:

- Eliminar la causa del riesgo, eliminando la vulnerabilidad o la posibilidad de la amenaza.
- Reducir el riesgo un nivel aceptable, por ejemplo, mediante la implementación de controles para reducir el impacto o la frecuencia esperada.
- Transferir el riesgo, cuando asignamos el riesgo a otra parte o tercero.

2.1.7 MAGERIT

Es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno. MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

Esta metodología persigue los siguientes objetivos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso[40]

[40] PAE, Portal de administración electrónica. MAGERIT. {En línea}. {citado 26 de mayo de 2017} disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WSJBdWg1_IU

2.1.8 Ciclo de Deming[41]

Conocido como modelo PHVA (Planear, Hacer, Verificar, Actuar). Es un método de gestión de cuatro fases que busca la mejora continua por medio de la revaluación constante de controles y políticas adoptadas para garantizar la seguridad de la información y sistemas informáticos.

Planear: En esta fase se define el problema a resolver, se obtienen datos y se reconocen las causas del problema.

Hacer: Aquí se desarrolla e implementa una solución, además de seleccionar medidas para evaluar su eficacia. En esta etapa se da la transición entre el diseño y las actividades reales.

Verificar: Esta fase se enfoca en evaluar los resultados de la solución adoptada, buscando mantener el rendimiento óptimo para asegurar el éxito de cualquier proceso.

Actuar: En esta fase se documentan los resultados, se informa sobre cambios en el proceso, y se hacen recomendaciones para los problemas que se abordarán en el próximo ciclo. Este paso es la mejora del ciclo, los resultados de la auditoría son las referencias fundamentales para realizar las actividades de mejora.

La figura 2 muestra las fases que se presentan en el modelo PHVA:

[41] El ciclo de Deming. {En línea}. {citado 26 de noviembre de 2017} disponible en: https://www.sbqconsultores.es/el-ciclo-de-deming-o-circulo-pdca/

Figura 2. Fases del ciclo de Deming

Fuente: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I-Método

2.1.8 OSSTMM

El Manual de la Metodología Abierta de Testeo de Seguridad (OSSTMM, Open Source Security Testing Methodology Manual) es una metodología que reúne las diversas pruebas y métricas de seguridad, utilizadas por los profesionales durante las Auditorías de Seguridad.

Este documento ha sido desarrollado gracias a un consenso de más de 150 expertos de seguridad de todo el mundo, y se encuentra en constante evolución. El OSSTMM se centra en los detalles técnicos de los elementos que deben ser probados. ¿Qué hacer antes, durante y después de una prueba de seguridad?, y ¿cómo medir los resultados?

Los casos de prueba se dividen en las siguientes secciones:

- Seguridad de la Información
- Seguridad de los Procesos
- Seguridad en las tecnologías de Internet
- Seguridad en las Comunicaciones
- Seguridad Inalámbrica
- Seguridad Física[42]

2.2 MARCO CONCEPTUAL

Seguridad de la información[43]: La información es un activo muy valioso para la organización y tiene que ser protegido de forma adecuada. Esta puede tener diferentes tipos, formas y puede ser almacenada en distintos medios. La seguridad de la información debe velar por la confidencialidad, integridad y disponibilidad de la información en todas las formas en las que se encuentre, tales como físicos, impresos y digitales.

Además, se debe tener en cuenta la seguridad de los recursos tecnológicos, la seguridad física, la gestión del recurso humano, la protección legal, organización, procesos, etc. El objetivo final de la seguridad de la información es tener un sistema de gestión que identifique los riesgos, los analice, evalué e implementa controles que reduzcan o mitiguen cualquier tipo de riesgo.

Protección de datos personales: Es el derecho que tiene toda personas a conocer, actualizar, rectificar y oponerse al tratamiento o manejo de la información que se haya recogido sobre ella en bases de datos o archivos por entidades de naturaleza pública o privada.

[42] GARCIA, Laura. Metodología OSSTMM. {En línea}. {citado 26 de mayo de 2017} disponible en: http://www.securitybydefault.com/2010/03/metodologia-osstmm.html
[43] Glosario Sistemas de Gestión de Seguridad de la Información. {En línea}. {citado 14 de noviembre de 2017} disponible en: https://glosarios.servidor-alicante.com/sistemas-gestion-seguridad-informacion_es-en/activo

Los datos personales son toda aquella información asociada a una persona y que permite su identificación. Por ejemplo, su documento de identidad, el lugar de nacimiento, estado civil, edad, lugar de residencia, trayectoria académica, laboral, o profesional. Existe también información más sensible como su estado de salud, sus características físicas, ideología política, vida sexual, entre otros aspectos.[44]

Norma ISO 27001: Es la norma internacional publicada por la Organización Internacional de Normalización (ISO), que describe cómo administrar la seguridad de información en una organización. La última versión es la 2013, y se conoce como la norma ISO/IEC 27001:2013. La primera revisión de la norma se publicó en 2005, y fue desarrollada teniendo como base a la norma británica BS7799.

La norma ISO 27001 tiene como fin que se garantice la confidencialidad, integridad y disponibilidad, de forma sistemática en organizaciones de cualquier tipo, a través de un Sistema de Gestión de la Seguridad de la Información (SGSI), que permita el equilibrio entre el uso de las tecnologías de la información y la gestión administrativa de la empresa, además de la participación de la alta dirección de forma que sea alinee con los objetivos estratégicos de la organización.

Gestión del riesgo: Los riesgos son posibles eventos no deseados que pueden afectar la seguridad de la información y los activos de la empresa. La gestión de riesgos es la base fundamental de la norma ISO 27001, la cual describe cómo desarrollar un SGSI que contiene un conjunto de políticas, procedimientos y elementos de control que permitan tener reglas de seguridad de la información en una organización.

La gestión y evaluación del riesgo son elementos esenciales del Sistema de Gestión de la Seguridad de la Información. Esta gestión debe incluir la identificación del riesgo, su evaluación y las medidas para mitigarlos a niveles aceptables para la organización.

[44] SIC. Sobre la protección de datos personales. {En línea}. {citado 16 de noviembre de 2017} disponible en: http://www.sic.gov.co/sobre-la-proteccion-de-datos-personales

2.3 ANTECEDENTES

Con el documento “El habeas data como derecho fundamental y la ley 1581 de 2012 y su decreto 1377 de 2013” presentado por Eliseo Cuartas Rodríguez y Juan David Jaller Escudero de la Universidad EAFIT, Escuela de derecho de Medellín. Su desarrollo aporta conocimientos importantes sobre la ley 1581 de protección de datos personales que sirven como referencia para el proyecto planteado en el presente documento.

El “Diseño de un sistema de gestión de seguridad de la información - SGSI bajo la norma ISO/IEC 27001:2013 para la empresa “En Línea Financiera” de la ciudad de Cali - Colombia”, presentado por Juan Carlos Oidor González de la Universidad Nacional Abierta y a Distancia en la ciudad de Popayán (Colombia). Aporta conocimientos y puntos importantes para el diseño del SGSI en empresas privadas.

La “Metodología para el diagnóstico continuo de la seguridad informática de la red de datos de la Universidad Militar Nueva Granada”, presentado por Juan Sebastian Echeverry Parada de la Universidad Militar Nueva Granada Facultad de Ingeniería en la ciudad de Bogotá. Aporta conceptos importantes para realizar pruebas de seguridad e identificación de vulnerabilidades.

2.4 MARCO LEGAL

2.4.1 La Constitución política de Colombia

“La constitución política, también llamada Carta magna o Carta Fundamental, es la ley máxima y suprema de un país o estado. En ella se especifican los principales derechos y deberes de sus participantes, y define la estructura y organización del

Estado. En Colombia esta constitución se modificó drásticamente por última vez en 1991, luego de durar más de 100 años con la constitución de 1886."[45]

Para el desarrollo del presente trabajo tomaremos como referencia los artículos:

"ARTÍCULO 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

ARTICULO 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación.

Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura."[46]

2.4.2 Ley Estatutaria 1266 de 2008[47]

"Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones".

"La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan

[45] CONSTITUCIÓN POLÍTICA DE COLOMBIA. ¿Qué es la Constitución Política? {En línea}. {citado 26 de mayo de 2017} disponible en: http://www.constitucioncolombia.com/historia.php
[46] SECRETARIA SENADO. Constitución política de 1991. {En línea}. {citado 26 de mayo de 2017} disponible en: http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html#15
[47] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1266. Bogotá. (diciembre 31 de 2008). Diario Oficial 47.219 de diciembre 31 de 2008. p. 1-15.

recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política."[48]

2.4.3 Ley 1273 de Delitos informáticos de 2009

"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones."[49]

2.4.4 Ley 1581 de protección de datos de 2012

"La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada."[50]

[48] SECRETARIA SENADO. Ley Estatutaria 1266 de 2008. {En línea}. {citado 26 de mayo de 2017} disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html
[49] SECRETARIA SENADO. Ley Estatutaria 1273 de 2012. {En línea}. {citado 26 de mayo de 2017} disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html
[50] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley estatutaria 1581 de 2012. Bogotá. (octubre 17 de 2012). Diario Oficial 48587 de octubre 18 de 2012. {En línea}. {25 de mayo de 2017} disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

2.4.5 Decreto 1377 de 2013

“Por el cual se reglamenta parcialmente la Ley1581de 2012. El presente Decreto tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.”[51]

2.4.6 Decreto 886 de 2014

“Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos, el cual se define como el directorio público de las bases de datos personales sujetas a Tratamiento que operan en el país, administrado por la Superintendencia de Industria y Comercio y de libre consulta para los ciudadanos.”[52]

2.4.7 Decreto 1074 de 2015

“Artículo 2.2.2.26.3.1. Plazo de inscripción: Los Responsables del Tratamiento deberán inscribir sus bases de datos en el Registro Nacional de Bases de Datos dentro del año siguiente a la fecha en que la Superintendencia de Industria y Comercio habilite dicho registro, de acuerdo con las instrucciones que para el efecto imparta esa entidad. Las bases de Datos que se creen con posterioridad a ese plazo, deberán inscribirse dentro de los dos (2) meses siguientes, contados a partir de su creación.”[53]

---

[51] EL CONGRESO DE LA REPÚBLICA, “DECRETO 1377 DE 2013,” *Repositorio Digital de documentación en materia de Gestión Documental*, revisado 22 de mayo de 2017. {En línea}. {citado 26 de mayo de 2017} disponible en: http://www.archivogeneral.gov.co/normatividad/items/show/288.

[52] PRESIDENCIA. Decreto 886 de 2014. {En línea}. {citado 26 de mayo de 2017} disponible en: http://wsp.presidencia.gov.co/Normativa/Decretos/2014/Documents/MAYO/13/DECRETO%20886%20DEL%2013%20DE%20MAYO%20DE%202014.pdf

[53] ALCALDÍA DE BOGOTÁ. Decreto 1074 de 2015. {En línea}. {citado 26 de mayo de 2017} disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=62508

2.4.8 Decreto 1759 del 8 de noviembre de 2016

"Por el cual se modifica el artículo 2.2.2.26.3.1 del Decreto 1074 de 2015 y amplió el plazo para registrar las bases de datos en el Registro Nacional de Bases de Datos RNBD al 30 de junio del 2017."[54]

2.4.9 Decreto 1115 del 29 de junio de 2017

"Se informa que mediante el Decreto 1115 del 29 de junio de 2017 se modificó el artículo 2.2.2.26.3.1 del Decreto 1074 de 2015 - Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, relacionado con el plazo para llevar a cabo el registro de las bases de datos. En particular, el decreto señaló lo siguiente:

Artículo 2.2.2.26.3.1. Plazo de inscripción. La inscripción de las bases de datos en el Registro Nacional de Bases de Datos se llevará a cabo en los siguientes plazos:

Los responsables del Tratamiento, personas jurídicas de naturaleza privada y sociedades de economía mixta inscritas en las cámaras de comercio del país, deberán realizar la referida inscripción a más tardar el **treinta y uno (31) de enero de 2018**, de acuerdo con las instrucciones que para el efecto imparta la Superintendencia de Industria y Comercio.

Los responsables del Tratamiento, personas naturales, entidades de naturaleza pública distintas de las sociedades de economía mixta y personas jurídicas de naturaleza privada que no están inscritas en las cámaras de comercio, deberán inscribir sus bases de datos en el Registro Nacional de Bases de Datos a más tardar

[54] PRESIDENCIA. Decreto 1759 de 2016 {En línea}. {citado 26 de mayo de 2017} disponible en: http://es.presidencia.gov.co/normativa/normativa/DECRETO%201759%20DEL%2008%20DE%20NOVIEMBRE%20DE%202016.pdf

el **treinta y uno (31) de enero de 2019**, conforme con las instrucciones impartidas para tales efectos por la Superintendencia de Industria y Comercio.”[55]

[55] SIC. Registro nacional de bases de datos. {En línea}. {citado 2 de octubre de 2017} disponible en: http://www.sic.gov.co/registro-nacional-de-bases-de-datos

3. ESTADO DE LA ORGANIZACIÓN FRENTE AL CUMPLIMIENTO DE LA LEY

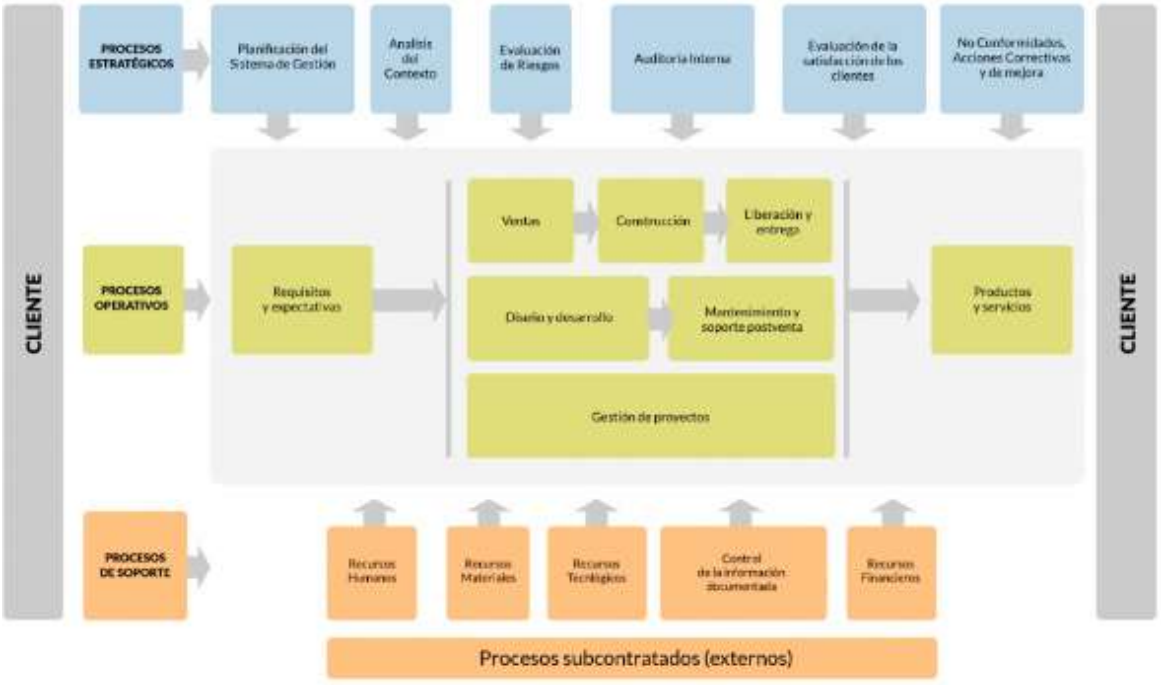
Antes de iniciar con el proceso de implementación de la ley 1581 en la organización, es necesario reconocer el estado actual de la empresa, identificando aspectos importantes como son:

3.1 INFORMACIÓN DE LA ORGANIZACIÓN

Es necesario tener información de la organización e identificar cuál es su actividad económica, como está conformada internamente, si cuenta con un organigrama y número de áreas administrativas, distribución geográfica o sedes, si cuentan con un sistema de gestión, si se ha definido un mapa de procesos y datos referente a servicios contratados con terceros. Esto con el fin de tener una idea del tamaño de la empresa, nivel de organización, procesos y recurso humano involucrado en el desarrollo de sus actividades.

Como muestra la figura 3, un mapa de proceso ayuda a reconocer como se comunica internamente la empresa y que relación existe entre áreas frente al tratamiento de los datos que hacen los colaboradores en la realización de sus actividades.

Figura 3. Mapa de procesos según ISO 9001-2015



Fuente: https://www.isotools.org/2016/05/11/mapa-procesos-nueva-iso-9001-2015/

3.2 INFORMACIÓN TECNOLÓGICA

Es claro que la tecnología juega un papel importante en las empresas para el desarrollo, productividad y gestión de sus procesos, por eso se debe conocer información de su infraestructura tecnológica como son:

- Equipos de cómputo, portátiles o tablets
- Servidores
- Sistemas de información y aplicaciones del negocio
- Página web
- Cámaras de seguridad

Adicionalmente, identificar el número de usuarios, acceso a servicios locales o en la nube donde se almacene información o datos personales.

Es importante reconocer un número aproximado de bases de datos con información personal que maneja la empresa, que tienen los colaboradores en el desarrollo de sus actividades propias de sus funciones y si se comparte con terceros en sus procesos de tratamiento, además, es fundamental identificar si la empresa actualmente ha realizado actividades frente al cumplimiento de la ley 1581 de protección de datos personales como la inscripción a la página de registro RNBD, si cuenta con la cuenta de acceso a dicha página o si ha registrado alguna base de datos, como también, si cuenta con alguna política de privacidad y tratamiento de datos personales, formatos de autorización y avisos de privacidad que usen para el tratamiento y recolección de datos personales etc.

Para recolectar esta información inicial, se puede hacer por medio de entrevistas, usando un formato de chequeo o check list, el cual debe ser diligenciado por una persona directiva o administrativa que conozca muy bien la organización o que tenga comunicación con personal que pueda responder a dichas preguntas, por ejemplo, el encargado del área de sistemas, con el fin de tener la mayor cantidad de información posible de la organización.

Este check list, como se muestra en la tabla 1, contiene preguntas relacionadas con los contactos de la empresa, equipos informáticos y tecnología, preguntas sobre la relación de los datos en la empresa, con terceros y gestión, además de indagar sobre actividades que haya realizado la organización en materia de protección de datos o si cuenta con un sistema de gestión de calidad o sistema de seguridad de la información. Ver tabla 1.

Tabla 1. Formato de chequeo o check list

Formato captura de datos de la empresa

Fecha	DD/MM/AAAA								
Empresa									
Dirección									
1. Información de Contacto	Nit		Ciudad		Nº Sedes		Ubicación sedes		
	Nombre de Sistemas				Teléfono		Correo		
	Nombre Administrativo				Teléfono		Correo		
	Nombre Financiero				Teléfono		Correo		
	Actividad Empresa		Tel. Fijo		Celular		Skype		
	Pagina Web			Proveedor de Hosting			Correo en Hosting(Nº buzones)		
4. Equipos		Computador	Portatiles	Tabletas	Smartphone	Camaras - DVRs	Servidores	Softconta / Admin	Total Activos
	Cantidad#								0
	Que Sistema Operativo								
	Cual Antivirus								
5. Información relacionada con el tratamiento de datos personales	Nº de bases que contengan datos personales. Ejm: clientes, proveedores, rrhh, correos etc	Nº de areas organizativas (Comercial, Sistemas, Contabilidad etc)	Nº de clientes y/o titulares de datos personales con los que cuentan	Cuenta con procedimientos claros y documentados para el acceso y manejo de la información	Maneja datos personales en la nube	Nº de usuarios que acceden a Bases de Datos en la empresa	Cuenta su organización con un organigrama	Nº de Empleados Directos e Indirectos	Existe relacion con empresas que tengan acceso a sus datos personales (S/N-No se)
								D- I-	
	Nº Servidos contratados con terceros. Ejm: Asesorias, abogado, mensajeria etc	Las sedes realizan tratamiento de datos personales	Cuentan con un Sistemas de Gestión de Seguridad de la Información	Cuenta su organización con Procesos de Certificación ISO9000	La organización cuenta con un mapa de procesos	Han capacitado y concientizado al personal sobre seguridad de Información	Tiene clasificados y categorizados los datos	Cuenta con procedimientos para la atención de solicitudes y reclamos	Cual es el principal mecanismo utilizado para la recolección de datos personales
6. formatos y medidas solicitadas	Aviso de privacidad y proteccion de datos	Formatos De autorizacion y reclamos	Manual de procedimientos	Politica de protección de datos personales	Politica de seguridad	Analisis de Riesgos de activos de TI	Clasificacion de Riesgos	Controles de seguridad Información	Clasificacion de tipos de datos
Cuenta con usuario de acceso al RNBD			Que medidas tecnicas o tecnologicas tiene para evitar la fuga de Información						
Observaciones									

Diligenciando este formulario nos autoriza para tratar sus datos personales con la finalidad de ofrecerle productos, servicios, noticias y eventos, de acuerdo a los términos de tratamiento de datos personales Ley 1581 publicado en nuestra página web. Usted se encuentra facultado en todo momento para ejercer su derecho de acceso, rectificación, cancelación y oposición ante nuestras oficinas en Cali. Esta información esta respaldada bajo Acuerdo de Confidencialidad.

Firma o Nombre del Diligenciador

Recibido

Fuente: Propiedad del autor

También es relevante tener el inventario de los equipos informáticos que tiene la empresa, para lo cual se puede usar la tabla 2, donde se identifica: el nombre del equipo como se conoce en la organización, el tipo (computador, servidor, servicio, software), la ubicación o área de la empresa, descripción y responsable del uso o manejo:

Tabla 2. Listado de equipos

Nombre del equipo	Tipo	Ubicación	Descripción	Responsable

Fuente: Propiedad del autor

4. IDENTIFICACIÓN Y CLASIFICACIÓN DE BASE DE DATOS PERSONALES

La organización como un ente conformado por áreas y procesos organizacionales cuenta con mucha información en la cual se tratan datos de carácter personal por cada una de las personas o colaboradores. Para poder identificar y clasificar las bases de datos personales de acuerdo a lo que dice la ley 1581, se debe reconocer primero, que son los datos personales y cuales los tipos:

4.1 DATO PERSONAL

Es toda información que permite asociar una persona o identificarla. Por ejemplo, su edad, documento de identidad, lugar de nacimiento, estado civil, dirección, formación académica, experiencia laboral, salario, información financiera, crediticia, estado de salud, características físicas, partido político, hijos, conyugue etc. En la tabla 3 se identifican los tipos de datos reconocidos en la ley 1581:

Tabla 3. Tipos de datos personales

DATOS PERSONALES			
Público	**Semiprivado**	**Privado**	**Sensible**
• La norma y la Constitución los han definido públicos. • Para la recolección y tratamiento no se requiere autorización del titular. • Ejm: Nombre, dirección,	• Datos que no tienen una naturaleza íntima, reservada, ni pública. • Su conocimiento o divulgación puede interesar al titular o a un grupo de personas en general.	• Dato de carácter íntimo o reservado • Solo le interesa a su titular • Para su tratamiento se requiere de su autorización expresa. • Ejm: Nivel de escolaridad, fotografía, correo	• Dato personal de especial protección • Relacionado con la intimidad del titular • Su tratamiento puede generar discriminación por lo tanto requiere autorización expresa.

teléfono, fecha de nacimiento, estado civil, profesión u oficio, calidad de comerciante o de servidor público, datos contenidos en sentencias judiciales ejecutoriadas, documentos públicos, etc.	• Para su tratamiento se requiere la autorización expresa del titular de la información. • Ejm: Dato financiero, historia crediticia.	electrónico personal, teléfono privado	• Ejm: estado de salud, origen racial o étnico, orientación política, creencia religiosa, datos biométricos, huella etc.

Fuente: PRESIDENCIA DE LA REPUBLICA. GUÍA PARA LA CALIFICACIÓN DE LA INFORMACIÓN DE ACUERDO CON SUS NIVELES DE SEGURIDAD. Versión 6. Bogotá marzo de 2017

Según el el artículo 7° de la Ley 1581, “El Tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública y cuando dicho Tratamiento cumpla con los siguientes aspectos:

1. Que responda y respete el interés superior de los niños, niñas y adolescentes.
2. Que se asegure el respeto de sus derechos fundamentales.

Cumplidos los anteriores requerimientos, el representante o apoderado del niño, niña o adolescente otorgará la autorización previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.”[56]

[56] CONGRESO DE LA REPÚBLICA, “DECRETO 1377 DE 2013,” *Repositorio Digital de documentación en materia de Gestión Documental*, revisado 22 de mayo de 2017. {En línea}. {citado 26 de mayo de 2017} disponible en: http://www.archivogeneral.gov.co/normatividad/items/show/288.

4.2 IDENTIFICAR Y CLASIFICAR LOS DATOS

Para identificar y poder clasificar las bases de datos personales se debe indagar a los colaboradores líderes de área sobre las siguientes preguntas:

- Que datos personales maneja el funcionario, identificando el nombre de la base y que tipo de datos contiene: publico, semiprivado, privado y sensible
- Cantidad de registros que maneja la base datos
- Como capta esos datos personales
- Con quien los comparte hacia el interior y exterior de la empresa
- Donde los guarda o como almacena los datos personales
- Como se cuidan esos datos personales
- Si manejan dispositivos móviles o de almacenamiento externo en el manejo de los datos personales.

Adicionalmente, se debe identificar que conocimientos básicos de seguridad se tienen al interior de la empresa, como son:

- El uso y manejo de contraseñas
- La realización de copias de seguridad
- El manejo de controles para evitar la fuga y robo de datos
- El uso de una política de seguridad informática.

Es de mucha importancia tratar de medir el conocimiento que tiene cada colaborador frente a la norma 1581 y leyes referentes o relacionadas, ya que eso permite tener una idea más clara del tipo de organización que se está analizando y de acuerdo al grado de conocimiento reflejado, se debe solicitar documentación que tenga relación como: formatos de captación de datos, autorizaciones, procedimientos o políticas.

4.3 INFORME DE RECONOCIMIENTO Y FLUJO DE DATOS

Con la información y datos recogidos hasta el momento, se puede hacer un análisis donde se ve más claro como fluye la información relacionada con datos personales y su tratamiento de dentro de la empresa, alineándose a las áreas que conforman la empresa y su mapa de procesos.

Este flujo transaccional de datos personales que viaja entre las áreas internas y hacia el exterior de la empresa, permite identificar riesgos en el tratamiento de dichos datos y da el insumo para la construcción de controles asociados a formatos de tratamiento y captación de datos que deben alinearse a la norma de protección de datos personales.

Con el resultado del flujo transaccional se debe generar una tabla que resuma los datos que se tratan en la empresa como aparece en la tabla 4:

Tabla 4. Flujo transaccional de datos

ORIGEN			**TIPO DATO**				**DESTINO**	
Colaborador	Área	Base datos	Publico	Semi privado	Privado	Sensible	Interno	Externo
Juan Pérez	Admintrativa	Proveedores	x	X			Contabilidad	
Juan Pérez	Admintrativa	Empleados	x	X	x	x	RRHH	
Leidy Diaz	Comercial	Clientes	x	X	x		Facturación	
María Perea	Operaciones	Proyectos	x	X		x		Abogado

Ruby Cano	RRHH	HV Físicas	x	X	X	x		ADICO

Fuente: Propiedad del autor

Posterior a este análisis se debe segmentar y clasificar los datos identificados para etiquetarlos como: confidenciales, sensibles, privados y públicos, y de esta manera socializar a los funcionarios de la empresa la forma de tratamiento que se tendrá y políticas de manejo de estos tipos de datos, a partir del momento en que se haga efectiva y oficial la política de privacidad y protección de datos personales en la organización.

Con el análisis anterior y la tabla de flujo de datos personales, se pueden tomar como base los criterios que da ISO 27001 para su clasificación, de acuerdo al carácter confidencial que tenga la información. ISO 27001 no plantea los niveles de clasificación a seguir, sino que da flexibilidad para que cada organización adopte el más indicado en función de la industria. Así, por ejemplo, para una organización de mediano tamaño, podríamos definir los siguientes 4 niveles para clasificar el carácter confidencial de su información:

- Confidencial: cuando presenta un nivel mayor de confidencialidad.
- Restringida: nivel medio de confidencialidad.
- De uso interno: nivel más bajo de confidencialidad
- Público: cuando la información es accesible a todo el público[57]

De acuerdo a esto, en la tabla 5 se pueden referenciar las bases de datos que servirán como inventario para más adelante hacer el registro RNBD ante la SIC.

[57] ISOTOOLS. Cómo clasificar la información según ISO 27001. {En línea}. {citado 12 de Noviembre de 2017} disponible en: http://www.isotools.com.co/clasificar-la-informacion-segun-iso-27001/

Tabla 5. Inventario de bases de datos

RESPONSABLE	BASE DATOS	# REG	TIPO DE DATO				CLASIFICA	FINALIDAD	ENCARGADO
Nombre Colaborador	Nombre de base datos		Publico	Semiprivado	Privado	Sensible	Tipo de carácter	Tratamiento del dato	Nombre del tercero
Carlos Solis	Prospectos	500	x				Publico	Mercadeo	
Juan Pérez	Proveedores	50	x	x			Uso interno	Contabilidad	
Juan Pérez	Empleados	35	x	x	x	x	Confidencial	RRHH	
Leidy Diaz	Clientes	250	x	x	x		Restringida	Facturación	
María Perea	Proyectos	15	x	x		x	Confidencial	Contratos	Abogado
Ruby Cano	HV Físicas	45	x	x	x	x	Confidencial	RRHH	ADECO

Fuente: Propiedad del autor

5. MODELO DE DOCUMENTACIÓN BÁSICA REQUERIDA POR LA LEY 1581

Teniendo claro que el régimen general de protección de datos personales 1581 no aplica a las bases de datos mantenidas en un ámbito exclusivamente personal o doméstico, es importante indicar que todas las empresas privadas, públicas o personas naturales que realicen tratamiento de datos personales con fines comerciales o con propósitos relacionados a su razón de ser, deberán cumplir esta ley de manera obligatoria, de tal manera, es importante que se genere una documentación para dicho cumplimiento.

Con el resultado de las entrevistas, encuestas y flujo transaccional de datos personales asociado al tratamiento interno, se realiza la construcción de los documentos, políticas y formatos que se deben ajustar a la empresa para su adopción, socialización e implementación, y de esta forma, prepararse para el cumplimiento operativo de la ley 1581, así como para los análisis que posiblemente se tengan que hacer en materia de contratos con terceros para blindar la empresa en término del tratamiento de datos personales que sean responsabilidad de la misma.

De acuerdo a lo que establece la ley 1581 de 2012, se deben tener en cuenta varios aspectos y definiciones que deben estar relacionados en los documentos a desarrollar, entre ellos encontramos:

- Aspectos relacionados con la autorización del Titular de información para el tratamiento de sus datos personales
- El ejercicio de los derechos de los titulares de información
- Las políticas de tratamiento de los Responsables y Encargados
- Las transferencias de datos personales
- La responsabilidad demostrada frente al Tratamiento de datos personales

5.1 DEFINICIONES

Las definiciones que establece la ley 1581 de 2012, conforme al Artículo 3° son las siguientes:

- **"Autorización:** La autorización es el consentimiento que se debe tomar previamente y de forma expresa e informado del Titular para llevar a cabo el Tratamiento de datos personales.
- **Base de Datos:** Las bases de datos, son el conjunto organizado de datos personales que son tratados por el responsable.
- **Dato personal**: Es cualquier información o dato que pueda vincular o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Encargado del Tratamiento**: Es la persona natural o jurídica, pública o privada, que por su propia voluntad o en asocio con otros, realice el proceso de tratamiento de datos personales designado por cuenta del responsable del Tratamiento.
- **Responsable del Tratamiento**: Es la persona natural o jurídica, pública o privada, que decide que hacer sobre la base de datos y/o el Tratamiento de los datos personales.
- **Titular**: Es la persona natural que le son tratados sus datos personales.
- **Tratamiento**: El tratamiento corresponde a cualquier actividad, operación o conjunto de operaciones que se realicen sobre los datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión."[58]

[58] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley estatutaria 1581 de 2012. Bogotá. (octubre 17 de 2012). Diario Oficial 48587 de octubre 18 de 2012. {En línea}. {25 de mayo de 2017} disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

5.1.1 Recolección de los datos personales

“En desarrollo de los principios de finalidad y libertad, la recolección de datos deberá limitarse a aquellos datos personales que son pertinentes y adecuados para la finalidad para la cual son recolectados o requeridos conforme a la normatividad vigente. Salvo en los casos expresamente previstos en la ley, no se podrán recolectar datos personales sin autorización del Titular”. Artículo 4° ley 1581.

5.1.2 Autorización

“La empresa como responsable del Tratamiento deberá adoptar procedimientos para solicitar, a más tardar en el momento de la recolección de sus datos, la autorización del Titular para el Tratamiento de los mismos e informarle los datos personales que serán recolectados, así como todas las finalidades específicas del Tratamiento para las cuales se obtiene el consentimiento”. Artículo 5° ley 1581.

De acuerdo con el Artículo 10, la autorización del Titular no será necesaria cuando se trate de:

- “Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial
- Datos de naturaleza pública
- Casos de urgencia médica o sanitaria
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos
- Datos relacionados con el Registro Civil de las Personas.”

De igual forma, si los datos personales tratados no requieren previa autorización, se deberá cumplir con las disposiciones contenidas en la presente ley.

5.1.3 Aviso de privacidad

"Es la comunicación verbal o escrita generada por el responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.

De acuerdo con el artículo 15 del decreto 1377 de 2013, el contenido mínimo del Aviso de Privacidad, deberá contener la siguiente información:

- Nombre o razón social y datos de contacto del responsable del tratamiento.
- El Tratamiento al cual serán sometidos los datos y la finalidad del mismo.
- Los derechos que le asisten al titular.
- Los mecanismos dispuestos por el responsable para que el titular conozca la política de Tratamiento de la información y los cambios sustanciales que se produzcan en ella o en el Aviso de Privacidad correspondiente. En todos los casos, debe informar al Titular cómo acceder o consultar la política de Tratamiento de información."[59]

Con base en las definiciones anteriores se adjunta un formato de autorización de tratamiento de datos personales. Ver Anexo B: Formato de autorización

5.1.4 Derechos de los Titulares

De acuerdo con el Artículo 8°, el Titular de los datos personales tendrá los siguientes derechos:

[59] EL CONGRESO DE LA REPÚBLICA, "DECRETO 1377 DE 2013," *Repositorio Digital de documentación en materia de Gestión Documental*, revisado 22 de mayo de 2017. {En línea}. {citado 26 de mayo de 2017} disponible en: http://www.archivogeneral.gov.co/normatividad/items/show/288.

- “Conocer, actualizar y rectificar sus datos personales frente a los responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.
- Solicitar prueba de la autorización otorgada al responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley.
- Ser informado por el responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales.
- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen.
- Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución.
- Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento."[60]

5.1.5 Políticas de Tratamiento de la información

De acuerdo al Artículo 13 del decreto 1377 de 2013 “Los responsables del tratamiento deberán desarrollar sus políticas para el tratamiento de los datos

[60] Ibid., p.4.

personales y velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas.

Las políticas de Tratamiento de la información deberán constar en medio físico o electrónico, en un lenguaje claro y sencillo y ser puestas en conocimiento de los Titulares. Dichas políticas deberán incluir, por lo menos, la siguiente información:

1. Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del responsable.
2. Tratamiento al cual serán sometidos los datos y finalidad del mismo cuando esta no se haya informado mediante el aviso de privacidad.
3. Derechos que le asisten como Titular.
4. Persona o área responsable de la atención de peticiones, consultas y reclamos ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.
5. Procedimiento para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización.
6. Fecha de entrada en vigencia de la política de tratamiento de la información y período de vigencia de la base de datos.

Cualquier cambio sustancial en las políticas de tratamiento, deberá ser comunicado oportunamente a los titulares de los datos personales de una manera eficiente, antes de implementar las nuevas políticas."[61]

Con base en las definiciones anteriores, se adjunta un formato de política de tratamiento de información, el cual sirve como referencia para la creación de la política que tendrá la empresa. Es importante tener claro que la política debe estar

[61] Ibid., p.6.

alineada al tipo de organización, tamaño y actividad comercial, además, dejar claro que la autorización para el tratamiento de los datos este ajustada a las finalidades por las cuales serán captados los datos personales de los titulares, junto con los demás puntos requeridos para su correcta creación. Ver Anexo C: Formato de política de tratamiento de información.

6. IDENTIFICAR RIESGOS, AMENAZAS Y EL ESTADO DE SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA

Para conocer el estado de seguridad de la información que tiene la empresa es necesario realizar un diagnóstico de seguridad informática a los activos tecnológicos con los que cuenta la empresa. Utilizando el estándar ISO 27001 como buena práctica para el análisis de los activos y herramientas de seguridad informática, poder identificar vulnerabilidades que generen riesgos a la seguridad y protección de los datos personales que custodia la empresa.

6.1 POLITICAS DE SEGURIDAD EXISTENTES

Partiendo de la información recolectada en los capítulos anteriores y especialmente en la identificación de la información de la organización, se debe revisar que documentos existen de políticas de seguridad. Este diagnóstico se puede realizar por medio de una serie de entrevistas y encuestas a los responsables del área, las cuales pueden ser complementadas con una revisión documental de los procedimientos y políticas asociadas a la seguridad de la información. Para realizar dicha entrevista se puede usar la tabla 6.

Tabla 6. Formato de encuesta para identificar Políticas seguridad

Empresa:		**Nº**		
Proceso	Seguridad de la Información			
Objetivo de Control	Seguridad de la Información a nivel general			
Cuestionario				
Pregunta		**SI**	**NO**	**N/A**

¿Existe algún archivo de tipo Log donde guarde información referida a las operaciones que realiza la Base de datos?			
¿Se lleva a cabo una comprobación, para verificar que los cambios efectuados son los solicitados por el interesado?			
¿Se documentan los cambios efectuados?			
¿Hay algún procedimiento para dar de alta a un usuario?			
¿Hay algún procedimiento para dar de baja a un usuario?			
¿Existe algún plan de contingencia ante alguna situación no deseada en la Base de Datos?			
¿Se cuenta con un inventario de todos los equipos que integran el centro de cómputo?			
¿Con cuanta frecuencia se revisa el inventario?			
Pregunta	**SI**	**NO**	**N/A**
¿Se posee de bitácoras de fallas detectadas en los equipos?			
¿Se cuenta con procedimientos definidos para la adquisición de nuevos equipos?			
¿Se cuenta con procedimientos definidos para el respaldo de la información?			
¿Existen metodologías de clasificación de información?			
¿Se realizan respaldos de información periódicamente?			
¿Cuenta con una política de seguridad?			
¿Cuenta con una política de privacidad y tratamiento de datos?			
Documentos probatorios presentados:			
TOTAL			

Fuente: Propiedad del autor

6.2 ACTIVOS INFORMÁTICOS DE LA ORGANIZACIÓN

Partiendo del concepto que activo es cualquier elemento que tenga valor para la organización y que puede estar expuesto a ataques accidentales o intencionales que puede afectar el desempeño de la organización, debemos tener claro que los activos esenciales son la información que se maneja y administra y los servicios prestados de manera interna, restringida o al público, de los cuales se derivan los demás elementos de la organización, como son:

- Datos que son procesados para generar la información.
- Aplicaciones o Software que manejan los datos.
- Equipos o Hardware que alojan tanto datos, aplicaciones y servicios.
- Soportes que almacenan datos de respaldo.
- Equipamiento auxiliar que ayuda a minimizar la carga de los otros activos.
- Instalaciones donde se encuentran todos los activos físicos.
- Personas encargadas de manipular e interactuar con los activos.

De acuerdo a esto y usando el inventario de activos inicialmente recolectado, se debe generar una tabla de acuerdo a los parámetros que maneja la metodología MAGERIT.

6.2.1 Tipos de Activos:

Existen 2 elementos esenciales en un sistema de información: la información que se manipula y los servicios que se suministran.

“Activos esenciales: Los activos esenciales definen los parametros de seguridad para todos los demás elementos del sistema.

Dentro de la información que se maneja, se debe considerar algunas características como si son de tipo personal, legal, normativos, si están sometidos a alguna clasificación de seguridad, como se muestra en la tabla 7"[62]

Tabla 7. Activos esenciales

[essential] Activos esenciales
[info] información [adm] datos de interés para la administración pública [vr] datos vitales (registros de la organización) (1) [per] datos de carácter personal (2) [A] nivel alto [M] nivel medio [B] nivel bajo [classified] datos clasificados (3) [C] nivel confidencial [R] difusión limitada [UC] sin clasificar [pub] de carácter público [service] servicio
(1) Aquellos que son esenciales para la supervivencia de la Organización; es decir que su carencia o daño afectaría directamente a la existencia de la Organización. (2) Cualquier información concerniente a personas físicas identificadas o identificables. Los datos de carácter personal están regulados por leyes y reglamentos en cuanto afectan a las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal y familiar. (3) Aquellos sometidos a normativa específica de control de acceso y distribución; es decir aquellos cuya confidencialidad es especialmente relevante.

Fuente: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II

[62] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método. Madrid, España octubre de 2012 p. 8.

“Datos / Información: Los datos son el corazón que permite a una organización prestar sus servicios. La información es un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos de acuerdo a la tabla 8”.[63]

Tabla 8. Datos / Información

[D] Datos / Información
[files] ficheros [backup] copias de respaldo [conf] datos de configuración (1) [int] datos de gestión interna [password] credenciales (ej. contraseñas) [auth] datos de validación de credenciales [acl] datos de control de acceso [log] registro de actividad (2) [source] código fuente [exe] código ejecutable [test] datos de prueba
(1) Los datos de configuración son críticos para mantener la funcionalidad de las partes y del conjunto del sistema de información. (2) Los registros de actividad sustancian los requisitos de trazabilidad.

Fuente: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II

En la tabla 9 se presenta como ejemplo para realizar el inventario, esta deberá contener los tipos de activos que se identifique en la organización, si hay algún tipo

[63] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método. Madrid, España octubre de 2012 p. 4.

que no se encuentre en la empresa, no se tendrá en cuenta. Ejm: si en la empresa no existe una UPS.

Tabla 9. Inventario de activos según MAGERIT

Activos Esenciales			
Código grupo Magerit	**Nombre grupo Magerit**	**Código Activo Entidad**	**Nombre activo Entidad**
[info]			
[adm]	Datos de interés para la administración pública	DO_LE	Documentos legales de constitución y cumplimiento
[vr]	Datos vitales	DO_PE	Procedimientos, instructivos, planes estratégicos
[per]	Datos de Carácter Personal	BD_CL	Bases de Datos Clientes
		BD_PI	Base de Datos Personal interno de la organización
[classified]	Datos clasificados	AR_HL	Archivo físico de Historia laboral
		AR_MOC	Archivo físico y digital de material oficial de cursos
Datos Información			
Código grupo Magerit	**Nombre grupo Magerit**	**Código Activo Entidad**	**Nombre activo Entidad**
[files]	Ficheros	D_BD	Base de Datos
[backup]	Copias de Respaldo	D_BK	Respaldo de Bases de Datos
[conf]	Datos de configuración	D_CONF	Configuración de aplicaciones almacenada en Base de datos
[password]	Credenciales	D_PWD	Credenciales de acceso de usuario a Software, Windows, Bases de Datos, Contable.
		D_FRM	Firmas Digitales
Inventario de servicios			
Código grupo Magerit	**Nombre grupo Magerit**	**Código Activo Entidad**	**Nombre activo Entidad**
[www]	World wide web	S_INT	Internet

[email]	Correo electrónico	S_EMAIL	Gestor de correo
[file]	Almacenamiento de archivos	S_NUBE	Gestor de almacenamiento
Software			
Código grupo Magerit	**Nombre grupo Magerit**	**Código Activo Entidad**	**Nombre activo Entidad**
[app]	Servidor de aplicaciones	SW_MD	Software Moodle
		SW_CB	Software contable
[dbms]	Sistema de gestión de bases de datos	SW_DBMS	Manejado de BD
[Office]	Ofimática	SW_OFI	Software de ofimática
[av]	Antivirus	SW_AV	Software antivirus
[os]	Sistema operativo	SW_OS	Sistema operativo pc
			Sistema operativo Server
Equipos Informáticos			
Código grupo Magerit	**Nombre grupo Magerit**	**Código Activo Entidad**	**Nombre activo Entidad**
[mid]	Equipos medios	HW_SRV	Servidor de aplicación y datos
[pc]	Informática personal	HW_PE	Pc de escritorio
[print]	Medios de impresión	HW_IMP	Impresora
[router]	Enrutadores	HW_RT	Router de internet
[switch]	Switch	HW_SW	Switch de red
Redes de comunicaciones			
Código grupo Magerit	**Nombre grupo Magerit**	**Código Activo Entidad**	**Nombre activo Entidad**
[wifi]	Red inalámbrica	COM_WIFI	Red Inalámbrica
[LAN]	Red local	COM_LOCAL	Red local
[Internet]	Internet	COM_INTERNET	Internet
Soporte información electrónica			
Código grupo Magerit	**Nombre grupo Magerit**	**Código Activo Entidad**	**Nombre activo Entidad**
[disk]	Discos Duros	M_MR_DE	Medio de respaldo Disco externo
[dvd]	DVR		
Soporte información no electrónica			
Código grupo Magerit	**Nombre grupo Magerit**	**Código Activo Entidad**	**Nombre activo Entidad**
[printed]	Material impreso	M_DO_PY	Respaldo documentación de cada proyecto en ejecución

		M_DO_FV	Respaldo de facturas impresos
		M_DO_FN	Respaldo Carpetas de obligación financiera.
Equipamiento auxiliar			
Código grupo Magerit	**Nombre grupo Magerit**	**Código Activo Entidad**	**Nombre activo Entidad**
[ups]	Sistema ininterrumpido de potencia	AUX_UPS	Ups
Personal			
Código grupo Magerit	**Nombre grupo Magerit**	**Código Activo Entidad**	**Nombre activo Entidad**
[ui]	Usuarios internos	P_JTI	Jefe de TI
		P_ST	Soporte técnico
[adm]	Administradores de sistemas	P_WM	Web Master

Fuente: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II

6.3 VALORACION DE LOS ACTIVOS

En un sistema de información se aprovechan los datos para generar servicios para la empresa o para terceros. El conjunto de estos elementos esenciales permite definir funcionalmente una organización. Las subordinaciones entre los activos permiten corresponder los demás activos con datos y servicios.

De un activo se puede validar diferentes dimensiones:

- “Su confidencialidad: ¿qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos.
- Su integridad: ¿qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falsos o, incluso, faltar datos.

- Su disponibilidad: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios"[64]

En los sistemas de información, el reconocimiento de los actores es indispensable para poder ofrecer el servicio correctamente e identificar los fallos (accidentales o premeditados) que pudieran darse. De esta manera, en los activos esenciales, se debe valorar:

- "La autenticidad: ¿qué perjuicio causaría no saber quién hace o ha hecho cada cosa?
  Esta valoración es típica de servicios (autenticidad del usuario) y de los datos (autenticidad de quien accede a los datos para escribir o, simplemente, consultar)
- La trazabilidad del uso del servicio: ¿qué daño causaría no saber a quién se le presta el servicio? O sea, ¿quién hace qué y cuándo?
- La trazabilidad del acceso a los datos: ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?"[65]

Las Dimensiones de Seguridad a usar son:
D: Disponibilidad, I: Integridad, C: Confidencialidad, A: Autenticidad, T: Trazabilidad.

Ahora se identifica el grado de daño que representaría su afectación al activo. En la tabla 10 se muestra la escala de valoración usada:

[64] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método. Madrid, España octubre de 2012 p. 24.
[65] Ibid., p.6.

Tabla 10. Escala de Valoración de Activos

VALOR			CRITERIO
10	Extremo	E	Daño extremadamente grave
9	Muy alto	MA	Daño muy grave
6-8	Alto	A	Daño grave
3-5	Medio	M	Daño importante
1-2	Bajo	B	Daño menor
0	Despreciable	D	Irrelevante a efectos prácticos

Fuente: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I

De acuerdo a estos conceptos, se debe valor los activos de acuerdo a las diferentes dimensiones de seguridad y tomando como criterio el grado de daño que representaría su afectación.

Por ejemplo, que pasaría si el activo base de datos de clientes (BD CL) de la empresa se daña, cuál sería el valor que le daría a cada una de estas variables:

D: Disponibilidad, I: Integridad, C: Confidencialidad, A: Autenticidad, T: Trazabilidad.

La tabla 11 se puede usar para valorar este activo:

Tabla 11: Valoración de Activos

Activo	Dimensiones de seguridad				
	D	I	C	A	T
BD CL	10	10	10	9	9

Fuente: Propiedad del autor

Esta tabla se debe completar con los valores por activo de acuerdo a las dimensiones de seguridad y grado de daño que representa.

6.4 VALORACION DE AMENAZAS

Para realizar el análisis y valoración de amenazas, es necesario tener claro dos conceptos fundamentales:

- Amenazas: Situaciones que podrían ocurrir causando un perjuicio a un determinado activo. Este tipo de escenarios causan potenciales incidentes ocasionando como principal consecuencia daños a sistemas de información o a la organización en general.
- Salvaguardas: Conocidas también como controles, son aquellos procedimientos o medidas tecnológicas que reducen el riesgo de que ocurra para determinada amenaza.

En esta fase se busca valorar el daño que puede causar una amenaza sobre los tipos de activos si ésta se materializa. La valoración de la amenaza está asociada con el daño que puede causar a una o varias de las dimensiones de un activo identificado, también se mide su factor de probabilidad, es decir, que probable seria que la amenaza se materialice. Cuando un activo es afectado por una amenaza, no necesariamente se manifiesta en todas sus dimensiones, ni en la misma cantidad.

La tabla 12 presenta los valores para la medir el daño o nivel de degradación que puede presentar el activo si se ve afectado por las amenazas que lo ataca:

Tabla 12. Valores para medir degradación

Valor	**Descripción**	
100%	MA	Muy alta
80%	A	Alta
50%	M	Media
20%	B	Baja
10%	MB	Muy baja

Fuente: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I

En la tabla 13 se presenta la escala de los valores que se usarán para medir la probabilidad de que una amenaza se materialice sobre un activo determinado:

Tabla 13. Valores para medir probabilidad de ocurrencia

Valor	**Probabilidad**		
100	MF	Muy frecuente	A diario
10	F	Frecuente	Mensualmente
1	N	Normal	Una vez al año
1/10	P	Poco	Cada varios años
1/100	MP	Muy poco frecuente	Siglos

Fuente: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I

Asimismo, se expresan las notaciones utilizadas:

- Dimensiones de Seguridad:

D: Disponibilidad, I: Integridad, C: Confidencialidad, A: Autenticidad, T: Trazabilidad.

Para cumplir con este objetivo se toma el listado de amenazas que se presentan en el catálogo de elementos libro II Versión 3.0 de la metodología MAGERIT, las cuales están clasificadas en 4 categorías:

- [N] Desastres naturales
- [I] De origen industrial
- [E] Errores y fallos no intencionados
- [A] Ataques intencionados

Las amenazas en las cuales se enfocará el análisis están asociadas a los datos, información o hardware donde se almacenan dichos datos, ya que el propósito del ejercicio es identificar el riesgo asociado en el tratamiento de los datos como lo muestra la tabla 14.

Tabla 14. Catálogo de amenazas

[N] Desastres naturales Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta. **Origen:** Natural (accidental)
[N.1] Fuego

Tipos de activos:	Dimensiones:
• [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	1. [D] disponibilidad
Descripción: Incendios: posibilidad de que el fuego acabe con recursos del sistema. **Ver:** EBIOS: 01- INCENDIO	
[N.2] Daños por agua	
Tipos de activos:	**Dimensiones:**
• [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	1. [D] disponibilidad
Descripción: inundaciones: posibilidad de que el agua acabe con recursos del sistema. **Ver:** EBIOS: 02 - PERJUICIOS OCASIONADOS POR EL AGUA	
[N.*] Desastres naturales	
Tipos de activos:	**Dimensiones:**
• [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	1. [D] disponibilidad
Descripción: Otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, etc.	
[I] De origen industrial Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.	
[I.1] Fuego	

Tipos de activos:	Dimensiones:
• [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	1. [D] disponibilidad
Descripción: incendio: posibilidad de que el fuego acabe con los recursos del sistema. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 01- INCENDIO	
[I.2] Daños por agua	
Tipos de activos:	**Dimensiones:**
• [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	1. [D] disponibilidad
Descripción: escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 02 - PERJUICIOS OCASIONADOS POR EL AGUA	
[I.*] Desastres industriales	
Tipos de activos:	**Dimensiones:**
• [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	1. [D] disponibilidad

Descripción:

otros desastres debidos a la actividad humana: explosiones, derrumbes, ... contaminación química, ...

sobrecarga eléctrica, fluctuaciones eléctricas,

... accidentes de tráfico, ...

Origen:

Entorno (accidental) Humano (accidental o deliberado)

Ver: EBIOS: 04 - SINIESTRO MAYOR

[I.3] Contaminación mecánica

Tipos de activos:	**Dimensiones:**
• [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	1. [D] disponibilidad

Descripción:

vibraciones, polvo, suciedad, ...

Origen:

Entorno (accidental)

Humano (accidental o deliberado)

Ver: EBIOS: 03 – CONTAMINACIÓN

[I.4] Contaminación electromagnética

Tipos de activos:	**Dimensiones:**
• [HW] equipos informáticos (hardware) • [Media] soportes de información (electrónicos) • [AUX] equipamiento auxiliar	1. [D] disponibilidad

Descripción:

interferencias de radio, campos magnéticos, luz ultravioleta, ...

Origen:

Entorno (accidental) Humano (accidental o deliberado)

Ver:

EBIOS:

14 - EMISIONES ELECTROMAGNÉTICAS

15- RADIACIONES TÉRMICAS

16 - IMPULSOS ELECTROMAGNÉTICOS

[I.5] Avería de origen físico o lógico

Tipos de activos:	**Dimensiones:**
• [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	1. [D] disponibilidad

Descripción: fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.

Origen:

Entorno (accidental) Humano (accidental o deliberado)

Ver:

EBIOS:

28 - AVERÍA DEL HARDWARE

29 - FALLA DE FUNCIONAMIENTO DEL HARDWARE

[I.6] Corte del suministro eléctrico

Tipos de activos:	**Dimensiones:**
• [HW] equipos informáticos (hardware) • [Media] soportes de información (electrónicos) • [AUX] equipamiento auxiliar	1. [D] disponibilidad

Descripción: cese de la alimentación de potencia **Origen:**

Entorno (accidental) Humano (accidental o deliberado)

Ver:

EBIOS: 12 - PÉRDIDA DE SUMINISTRO DE ENERGÍA

[I.7] Condiciones inadecuadas de temperatura y/o humedad

Tipos de activos:	Dimensiones:
• [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	1. [D] disponibilidad

Descripción: deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, ...

Origen:

Entorno (accidental) Humano (accidental o deliberado)

Ver:

EBIOS: 11- FALLAS EN LA CLIMATIZACIÓN

[I.10] Degradación de los soportes de almacenamiento de la información

Tipos de activos:	Dimensiones:
• [Media] soportes de información	1. [D] disponibilidad

Descripción: como consecuencia del paso del tiempo

Origen:

Entorno (accidental) Humano (accidental o deliberado)

Ver:

EBIOS:

28 - AVERÍA DEL HARDWARE

29 - FALLA DE FUNCIONAMIENTO DEL HARDWARE

[I.11] Emanaciones electromagnéticas

Tipos de activos:	Dimensiones:
• [HW] equipos informáticos (hardware) • [Media] media • [AUX] equipamiento auxiliar • [L] instalaciones	1. [C] confidencialidad

Descripción: hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque.

Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información.

Origen:

Entorno (accidental) Humano (accidental o deliberado)

Ver:

EBIOS: 17 - INTERCEPTACIÓN DE SEÑALES PARÁSITAS COMPROMETEDORAS

[E] Errores y fallos no intencionados

Fallos no intencionales causados por las personas.

Origen:

Humano (accidental)

[E.1] Errores de los usuarios

Tipos de activos:	**Dimensiones:**
• [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [Media] soportes de información	1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad

Descripción:

equivocaciones de las personas cuando usan los servicios, datos, etc.

Ver:

EBIOS: 38 - ERROR DE USO

[E.2] Errores del administrador

Tipos de activos:	**Dimensiones:**
• [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software)	1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad

• [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [Media] soportes de información	
Descripción: equivocaciones de personas con responsabilidades de instalación y operación **Ver:** EBIOS: 38 - ERROR DE USO	
[E.3] Errores de monitorización *(log)*	
Tipos de activos: • [D.log] registros de actividad	**Dimensiones:** 1. [I] integridad (trazabilidad)
Descripción: inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, ... **Ver:** EBIOS: no disponible	
[E.4] Errores de configuración	
Tipos de activos: • [D.conf] datos de configuración	**Dimensiones:** 1. [I] integridad
Descripción: Introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. **Ver:** EBIOS: no disponible	
[E.15] Alteración accidental de la información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información	**Dimensiones:** 1. [I] integridad

• [L] instalaciones	

Descripción:

alteración accidental de la información.

Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

Ver: EBIOS: no disponible

[E.18] Destrucción de información

Tipos de activos:	**Dimensiones:**
• [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	1. [D] disponibilidad

Descripción:

pérdida accidental de información.

Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

Ver: EBIOS: no disponible

[E.19] Fugas de información

Tipos de activos:	**Dimensiones:**
• [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones • [P] personal (revelación)	1. [C] confidencialidad

Descripción:

revelación por indiscreción.

Incontinencia verbal, medios electrónicos, soporte papel, etc.

Ver: EBIOS: no disponible

[E.23] Errores de mantenimiento / actualización de equipos (hardware)

Tipos de activos:	**Dimensiones:**
• [HW] equipos informáticos (hardware) • [Media] soportes electrónicos • [AUX] equipamiento auxiliar	1. [D] disponibilidad

Descripción: defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.

Ver: EBIOS: 32 - PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACIÓN

[E.24] Caída del sistema por agotamiento de recursos

Tipos de activos:	**Dimensiones:**
• [S] servicios • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	1. [D] disponibilidad

Descripción: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

Ver: EBIOS: 30 - SATURACIÓN DEL SISTEMA INFORMÁTICO

[E.25] Robo

Tipos de activos:	**Dimensiones:**
• [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	1. [D] disponibilidad 2. [C] confidencialidad

Descripción:

la pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.

Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales.

En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.

Ver: EBIOS: 22 - RECUPERACIÓN DE SOPORTES RECICLADOS O DESECHADOS

[A] Ataques intencionados

Fallos deliberados causados por las personas.

Origen:

Humano (deliberado)

[A.4] Manipulación de los registros de actividad (log)

Tipos de activos:	**Dimensiones:**
• [D.log] registros de actividad	1. [I] integridad (trazabilidad)

Descripción:

Ver: EBIOS: no disponible

[A.4] Manipulación de la configuración

Tipos de activos:	**Dimensiones:**
• [D.log] registros de actividad	1. [I] integridad 2. [C] confidencialidad 3. [A] disponibilidad

Descripción: prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.

Ver: EBIOS: no disponible

[A.5] Suplantación de la identidad del usuario

Tipos de activos:	Dimensiones:
• [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	1. [C] confidencialidad 2. [A] autenticidad 3. [I] integridad

Descripción:

Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios.

Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.

Ver: EBIOS: 40 - USURPACIÓN DE DERECHO

[A.6] Abuso de privilegios de acceso

Tipos de activos:	Dimensiones:
• [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad

Descripción: cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

Ver: EBIOS: 39 - ABUSO DE DERECHO

[A.11] Acceso no autorizado

Tipos de activos:	Dim1nsiones:
• [D] datos / información	1. [C] confidencialidad

• [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	2. [I] integridad

Descripción:

El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

Ver: EBIOS: 33 - USO ILÍCITO DEL HARDWARE

[A.13] Repudio

Tipos de activos:	**Dimensiones:**
• [S] servicios • [D.log] registros de actividad	1. [I] integridad (trazabilidad)

Descripción: negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación.

Repudio de recepción: negación de haber recibido un mensaje o comunicación.

Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.

Ver: EBIOS: 41 - NEGACIÓN DE ACCIONES

[A.15] Modificación deliberada de la información

Tipos de activos:	**Dimensiones:**
• [D] datos / información • [keys] claves criptográficas • [S] servicios (acceso) • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	1. [I] integridad

Descripción:

Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.

Ver: EBIOS: no disponible

[A.18] Destrucción de información

Tipos de activos:	**Dimensiones:**
• [D] datos / información • [keys] claves criptográficas • [S] servicios (acceso) • [SW] aplicaciones (SW) • [Media] soportes de información • [L] instalaciones	1. [D] disponibilidad

Descripción:

Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.

Ver: EBIOS: no disponible

[A.19] Revelación de información

Tipos de activos:	**Dimensiones:**
• [D] datos / información • [keys] claves criptográficas • [S] servicios (acceso) • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	1. [C] confidencialidad

Descripción:

revelación de información.

Ver: EBIOS:

23 – DIVULGACIÓN

27 – GEOLOCALIZACIÓN

34 - COPIA ILEGAL DE SOFTWARE

[A.22] Manipulación de los equipos

Tipos de activos:	Dimensiones:
• [HW] equipos • [Media] soportes de información • [AUX] equipamiento auxiliar	1. [C] confidencialidad 2. [D] disponibilidad

Descripción:

alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.

Ver: EBIOS: 25 - SABOTAJE DEL HARDWARE

[A.24] Denegación de servicio

Tipos de activos:	Dimensiones:
• [S] servicios • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	1. [D] disponibilidad

Descripción: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

Ver: EBIOS: 30 - SATURACIÓN DEL SISTEMA INFORMÁTICO

[A.25] Robo

Tipos de activos:	Dimensiones:
• [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	3. [D] disponibilidad 4. [C] confidencialidad

Descripción: la sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.

El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales.

El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias.

En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.

Ver: EBIOS:

20 - ROBO DE SOPORTES O DOCUMENTOS

21 - ROBO DE HARDWARE	
[A.26] Ataque destructivo	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: vandalismo, terrorismo, acción militar, ... Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal. **Ver:** EBIOS: 05 - DESTRUCCIÓN DE HARDWARE O DE SOPORTES	

Fuente: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I

De acuerdo al anterior listado de amenazas, se debe crear una tabla con cada activo donde se muestren las amenazas de dicho activo y la valoración de cada una de las dimensiones de los activos. Para tal ejercicio se puede usar la tabla 15 como referencia, para llenar esta tabla se debe tener en cuenta las escalas usadas en las tablas 12 y 13 anteriormente.

Tabla 15. Identificación y Valoración de Amenazas

Activo: [BD CL] Base de clientes						
Amenaza	**Frecuencia**	**Dimensiones**				
		D	**I**	**C**	**A**	**T**
[E.1] Errores de los usuarios	N	M	A	M		
[E.2] Errores del administrador	P	M	A	A	M	

[E.4] Errores de configuración	P	A		A		
[E.19] Fugas de información	P			A		
[E.25] Pérdida de equipos	P	A		A		
[A.5] Suplantación de la identidad del usuario	P	A	A	A		

Fuente: Propiedad del autor

6.5 VALORACION DEL RIESGO

La valoración del riesgo es una parte muy importante en este punto, ya que hace parte del proceso de gestión que más adelante se debe desarrollar a nivel de todos los activos. Una vez que los riesgos se han identificado, analizados y evaluados, los pasos siguientes son prevenir que estos ocurran, minimizarlos y protegerse contra ellos para mitigar sus consecuencias.

Con la metodología MAGERIT podemos calcular el riesgo al combinar el impacto con la probabilidad de que ocurra. La tabla 16 presenta los valores de escala para medir el impacto, la probabilidad y el riesgo:

Tabla 16. Descripción de escalas de valoración

Escalas		
Impacto	**Probabilidad**	**Riesgo**
MA: muy alto	**MA:** prácticamente seguro	**MA:** crítico
A: alto	**A:** probable	**A:** importante
M: medio	**M:** posible	**M:** apreciable
B: bajo	**B:** poco probable	**B:** bajo

MB: muy bajo	**MB:** muy raro	**MB:** despreciable

Fuente: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III

La tabla 17 presenta los valores que se usan para medir el riesgo de acuerdo al factor o probabilidad de ocurrencia y el impacto que puede causar una amenaza en el activo afectado, teniendo como base el uso de la tabla 16 de descripción de escalas de valoración. De esta manera, la intersección de los valores dados para el impacto y los valores de probabilidad darán el valor del riesgo, el cual se identifica con un color de acuerdo a su criticidad, siendo el color rojo el de mayor criticidad, el color naranja con grado importante, el color amarillo de grado apreciable, el color verde de bajo riesgo y el color gris en grado despreciable o más bajo.

Tabla 17. Valores del riesgo de acuerdo al impacto vs probabilidad

Riesgo		**Probabilidad**				
		MB	**B**	**M**	**A**	**MA**
Impacto	**MA**	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III – Guía de técnicas. Madrid, España

Los riesgos que tengan valores A o MA requieren de atención inmediata.

En la tabla 18 se debe ingresar el valor de la probabilidad, el valor del impacto y se calcula el valor del riesgo de acuerdo a la tabla 12 de los riesgos sobre los activos de la empresa.

Tabla 18. Valoración de riesgos por activo

Activo: [BD CL] Base de clientes			
Amenaza	**Probabilidad**	**Impacto**	**Riesgo**
[E.1] Errores de los usuarios	M	M	M
[E.2] Errores del administrador	M	M	M
[E.4] Errores de configuración	B	B	B
[E.19] Fugas de información	A	A	MA
[E.25] Pérdida de equipos	A	A	MA
[A.5] Suplantación de la identidad del usuario	M	A	A

Fuente: Propiedad del Autor

6.6 SELECCIÓN DE CONTROLES

Después de evaluados los riesgos se continua con la selección de los controles que permitirán mitigar o eliminar dichos riesgos. La declaración de aplicabilidad es un documento que trae la norma ISO 27001-2013 que sirve para relacionar la evaluación de riesgos, el tratamiento y la puesta en práctica de la seguridad de la información, la cual posee un listado de los controles que la empresa debería tener en cuenta para cumplir con el estándar.

La tabla 19 representa los controles que se deben implementar y en las últimas cuatro columnas se muestran las razones para tomar el control, la descripción de estas razones es:

- RL: REQUERIMIENTO LEGAL
- OC: OBLIGACIONES CONTRACTUALES
- RN: REQUERIMIENTOS DEL NEGOCIO
- AR: ANALISIS DE RIESGOS

Tabla 19. Declaración de aplicabilidad

A 5. POLITICA DE SEGURIDAD								
A 5.1 Política de Seguridad de la Información								
CONTROL ISO	**CONTROLES**	**CUMPLE**		**CONTROL / DESCRIPCIÓN**	**Razones para seleccionar control**			
		SI	NO		**RL**	**OC**	**RN**	**AR**
A 5.1.1	Políticas de seguridad de la información	**X**		Un documento de política de seguridad de la información ha sido aprobado por la administración.			**X**	**X**
A 5.1.2	Revisión de las políticas para seguridad de la información		**X**	Aún se encuentra en implementación.			**X**	**X**
A 6. ORGANIZACION DE LA SEGURIDAD DE LA INFORMACIÓN								
A 6.1 Organización Interna								
CONTROL ISO	**CONTROLES**	**CUMPLE**		**CONTROL / DESCRIPCIÓN**	**Razones para seleccionar control**			
		SI	NO		**RL**	**OC**	**RN**	**AR**
A 6.1.1	Roles y responsabilidades para la seguridad de la información		**X**	No todas las responsabilidades de seguridad de la información están definidas y asignadas.				**X**

A 6.1.2	Separación de deberes	**X**		No existen funciones en conflicto y las áreas de responsabilidad están separadas para reducir las posibilidades de modificación o mal uso de los activos de la empresa.				**X**
A 6.1.3	Contacto con las autoridades	**X**		Se mantienen contactos con las autoridades pertinentes.				**X**
A.6.2. Dispositivos móviles y Teletrabajo.								
A 6.2.1	Política para dispositivos móviles		**X**	Controles de seguridad serán adoptadas para gestionar los riesgos debidos al uso de dispositivos móviles.				**X**
A 6.2.2	Teletrabajo			La empresa no ha implementado el Teletrabajo.				
A 7. SEGURIDAD DE LOS RECURSOS HUMANOS								
A 7.1 Antes de asumir el empleo								
A 7.1.1	Selección	**X**		Se realiza verificación de datos sobre los candidatos para el empleo.		**X**		**X**
A 7.1.2	Términos y condiciones del empleo	**X**		Existen acuerdos contractuales con los empleados y contratistas.		**X**		**X**
A 7.2 Durante la ejecución del empleo								
A 7.2.1	Responsabilidades de la dirección	**X**		La administración exige a empleados y contratistas la aplicación de controles para la seguridad de la información.		**X**		**X**
A 7.2.2	Toma de conciencia, educación y formación en la seguridad de la información		**X**	Aún se encuentra en implementación.		**X**		**X**

A 7.2.3	Proceso disciplinario		**X**	Falta documentar un proceso disciplinario formal.		**X**		**X**
A 7.3 Terminación y Cambio de Empleo								
A 7.3.1	Terminación o cambio de responsabilidades de empleo	**X**		Se comunican las responsabilidades de seguridad de la información y de los derechos que permanezcan válidos después de la terminación o el cambio de puesto de trabajo.		**X**		**X**
A 8. GESTIÓN DE ACTIVOS								
A 8.1 Responsabilidad por los Activos								
CONTROL ISO	**CONTROLES**	**CUMPLE**		**CONTROL / DESCRIPCIÓN**	**Razones para seleccionar control**			
		SI	NO		**RL**	**OC**	**RN**	**AR**
A 8.1.1	Inventario de Activos	**X**		Se identifican los activos asociados a las instalaciones de procesamiento de la información y la información.				**X**
A 8.1.2	Propiedad de los activos	**X**		Cada activo tendrá un responsable de su seguridad y funcionamiento correcto.				**X**
A 8.1.3	Uso aceptable de los activos	**X**		Se identifican, documentan e implementan las reglas para el uso aceptable de la información y de los activos asociados.				**X**
A 8.1.4	Devolución de activos	**X**		Los empleados y usuarios externos deben devolver los activos de la empresa que se encuentren en su posesión a la terminación de				**X**

				su empleo, contrato o acuerdo.				
A 8.2 Clasificación de la Información								
A 8.2.1	Clasificación de la información		**X**	La información se clasificará en términos de requisitos legales, valor, la criticidad y sensibilidad a la divulgación o modificación no autorizada.				**X**
A 8.2.2	Etiquetado de la información		**X**	Se elaborará un conjunto de procedimientos para el etiquetado de información y éstos se aplicarán de acuerdo con el esquema de clasificación de la información adoptado por la empresa				**X**
A 8.2.3	Manejo de activos		**X**	Se elaborarán procedimientos para el manejo de los activos de acuerdo con el esquema de clasificación de la información adoptado por la empresa.				**X**
A 8.3 Manejo de Medios								
A 8.3.1	Gestión de los medios removibles		**X**	Aún se encuentra en implementación.				**X**
A 8.3.2	Disposición de los medios		**X**	Aún se encuentra en implementación.				**X**
A 8.3.3	Transferencia de medios físicos		**X**	Aún se encuentra en implementación.				**X**
A 9. CONTROL DE ACCESO								
A 9.1 Requisitos del Negocio para el Control de Acceso								
CONTROL ISO	**CONTROLES**	**CUMPLE**		**CONTROL / DESCRIPCIÓN**	**Razones para seleccionar control**			

		SI	NO		RL	OC	RN	AR
A 9.1.1	Política de control de acceso	**X**		Existe una política de control de acceso, documentada y revisada.				**X**
A 9.1.2	Acceso a redes y a servicios de red	**X**		Los usuarios sólo tienen acceso a los servicios y la red que le han sido autorizados.				**X**
A 9.2 Gestión del Acceso de Usuarios								
A 9.2.1	Registro y cancelación del registro de usuarios	**X**		Existe un proceso para el registro de usuarios y la cancelación de estos.				**X**
A 9.2.2	Suministro de acceso a usuarios	**X**		Hay un proceso para asignar y revocar derechos de acceso.				**X**
A 9.2.3	Gestión de derechos de acceso privilegiado	**X**		Se restringe la asignación de los derechos de acceso.				**X**
A 9.2.4	Gestión de información de autenticación secreta de usuarios	**X**		Existe un proceso para la asignación de la información secreta de autenticación.				**X**
A 9.2.5	Revisión de los derechos de acceso de usuarios		**X**	Los propietarios de activos deberán revisar cada cierto tiempo los derechos de acceso de los usuarios.				**X**
A 9.2.6	Retiro o ajuste de los derechos de acceso	**X**		Los derechos de acceso de empleados y usuarios externos deben ser retirados a la terminación de su empleo, contrato o acuerdo.				**X**
A 9.3 Responsabilidades de los Usuarios								
A 9.3.1	Uso de información de autenticación secreta	**X**		Los usuarios deben seguir las prácticas de la empresa en el uso de la información de autenticación secreta.				**X**

A 9.4 Control de Acceso a Sistemas y Aplicaciones								
A 9.4.1	Restricción del acceso a la información	**X**		Existen límites de acuerdo con la política de control de acceso.				**X**
A 9.4.2	Procedimiento de ingreso seguro	**X**		Existen métodos de conexión segura.				**X**
A 9.4.3	Sistema de gestión de contraseñas		**X**	No existe.				**X**
A 9.4.4	Uso de programas utilitarios privilegiados	**X**		Se restringe el uso de programas que puedan anular los controles del sistema.				**X**
9.4.5	Control de acceso al código fuente de los programas	**X**		El acceso al código fuente de los programas está restringido	**X**			**X**
A 10. CRIPTOGRAFIA								
A 10.1 Controles Criptográficos								
CONTROL ISO	**CONTROLES**	**CUMPLE**		**CONTROL / DESCRIPCIÓN**	**Razones para seleccionar control**			
		SI	NO		**RL**	**OC**	**RN**	**AR**
A 10.1.1	Política sobre el uso de controles criptográficos		**X**	Se implementará una política sobre el uso de controles criptográficos para la protección de la información.				**X**
A 10.1.2	Gestión de llaves		**X**	Se implementará una política sobre el uso y protección de las claves criptográficas.				**X**
A 11. SEGURIDAD FÍSICA Y DEL ENTORNO								
A 11.1 Áreas Seguras								
A 11.1.1	Perímetro de seguridad física	**X**		Existen perímetros de seguridad para proteger las áreas que contienen información y procesamiento de la información.			**X**	**X**

A 11.1.2	Controles de acceso físicos	**X**		Existen controles de entrada.			**X**	**X**
A 11.1.3	Seguridad de oficinas, recintos e instalaciones	**X**		Existen elementos de seguridad física.			**X**	**X**
A 11.1.4	Protección contra amenazas externas y ambientales	**X**		Existen elementos de protección física.			**X**	**X**
A 11.2 Equipos								
A 11.2.1	Ubicación y protección de los equipos	**X**		Los equipos están protegidos para reducir los riesgos de las amenazas ambientales y de acceso no autorizado.				**X**
A 11.2.2	Servicios de suministro	**X**		El equipo está protegido contra fallos del suministro eléctrico y otros trastornos causados por fallas en los servicios públicos.				**X**
A 11.2.3	Seguridad del cableado	**X**		Existen elementos para proteger contra interceptación, interferencia o daños.				**X**
A 11.2.4	Mantenimiento de los equipos	**X**		Existen planes de mantenimiento de equipos para asegurar su disponibilidad e integridad.				**X**
A 11.2.5	Retiro de activos		**X**	No se ha implementado.				**X**
A 11.2.6	Seguridad de los equipos fuera de las instalaciones		**X**	No se ha implementado.				**X**
11.2.7	Disposición segura o reutilización de equipos		**X**	No se ha implementado.	**X**			**X**
11.2.8	Equipo de usuario desatendido	**X**		Existe una política para bloquear el equipo ante la ausencia de su operador.				**X**

11.2.9	Política de escritorio despejado y de pantalla despejada		**X**	No se ha implementado.				**X**
A 12. SEGURIDAD DE LAS OPERACIONES								
A 12.1 Procedimientos Operacionales y Responsabilidades								
CONTROL ISO	**CONTROLES**	**CUMPLE**		**CONTROL / DESCRIPCIÓN**	**Razones para seleccionar control**			
		SI	NO		**RL**	**OC**	**RN**	**AR**
A 12.1.1	Procedimientos de operación documentados		**X**	No se ha implementado.			**X**	**X**
A 12.1.2	Gestión de cambios		**X**	No se ha implementado.			**X**	**X**
A 12.1.3	Gestión de la capacidad		**X**	No se ha implementado.			**X**	**X**
A 12.2 Protección contra Códigos Maliciosos								
A 12.2.1	Controles contra códigos maliciosos	**X**		Existen herramientas antivirus.				**X**
A 12.3 Copias de Respaldo								
A 12.3.1	Respaldo de la información	**X**		Las copias de seguridad de la información, software y del sistema son realizadas y analizadas periódicamente de acuerdo con una política de copia de seguridad establecida.				**X**
A 12.4 Registro y Seguimiento								
A 12.4.1	Registro de eventos	**X**		Se almacenan y revisan periódicamente los registros de actividades de usuarios, excepciones, errores y eventos sobre la seguridad de la información.				**X**
A 12.4.2	Registros del administrador y del operador	**X**		Las actividades del administrador y el operador del sistema deberán ser				**X**

				registrados y sus registros protegidos y revisados con regularidad.				
A 12.4.3	Sincronización de relojes	**X**		Los relojes de todos los sistemas de procesamiento de información deben estar sincronizados a una sola fuente de tiempo.				**X**
A 12.5 Control de Software Operacional								
A 12.5.1	Instalación de software en sistemas operativos		**X**	No se ha implementado.				**X**
A 12.6 Gestión de la Vulnerabilidad Técnica								
A 12.6.1	Gestión de las vulnerabilidades técnicas		**X**	No se ha implementado.				**X**
A 12.6.2	Restricción sobre la instalación de software		**X**	No se ha implementado.				**X**
A 12.7 Consideraciones sobre Auditorias de Sistemas de Información								
A 12.7.1	Controles de auditorías de sistemas de información	**X**		Las auditorías de las actividades relacionadas con los sistemas están planificadas y acordadas para minimizar las interrupciones a los procesos de negocio.				**X**
A 13 SEGURIDAD DE LAS COMUNICACIONES								
A 13.1 Gestión de la Seguridad de las Redes								
CONTROL ISO	**CONTROLES**	**CUMPLE**		**CONTROL / DESCRIPCIÓN**	**Razones para seleccionar control**			
		SI	NO		**RL**	**OC**	**RN**	**AR**
A 13.1.1	Controles de las redes	**X**		Las redes están gestionadas y controladas.				**X**

A 13.1.2	Seguridad de los servicios de red	**X**		Se identifican los mecanismos de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de red.				**X**
A 13.1.3	Separación en las redes	**X**		Grupos de servicios de información, los usuarios y los sistemas de información estarán separados en las redes.				**X**
A 13.2 Transferencia de Información								
A 13.2.1	Políticas y procedimientos para el intercambio de información		**X**	No se ha implementado.				**X**
A 13.2.2	Acuerdos sobre transferencia de información		**X**	No se ha implementado.				**X**
A 13.2.3	Mensajería electrónica		**X**	No se ha implementado.				**X**
A 13.2.4	Acuerdos de confidencialidad o de no divulgación	**X**		Se identifican y documentan los requisitos para los acuerdos de confidencialidad o de no divulgación que reflejan las necesidades de la empresa para la protección de la información.				**X**
A 14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN								
A 14.1 Requisitos de Seguridad de los Sistemas de Información								
CONTROL ISO	**CONTROLES**	**CUMPLE**		**CONTROL / DESCRIPCIÓN**	**Razones para seleccionar control**			
		SI	NO		**RL**	**OC**	**RN**	**AR**

A 14.1.1	Análisis y especificación de los requisitos de seguridad de la información		**X**	No se ha implementado.				**X**
A 14.1.2	Seguridad de servicios de las aplicaciones en redes públicas		**X**	No se ha implementado.				**X**
A 14.1.3	Protección de transacciones de los servicios de las aplicaciones		**X**	No se ha implementado.				**X**
A 14.2 Seguridad en los Procesos de Desarrollo y Soporte								
A 14.2.1	Política de desarrollo seguro	**X**		Se establecen y aplican reglas para el desarrollo de software y sistemas dentro de la empresa.	**X**			**X**
A 14.2.2	Procedimientos de control de cambios en sistemas	**X**		Los cambios en los sistemas deben realizarse mediante el uso de procedimientos de control de cambios.	**X**			**X**
A 14.2.3	Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación	**X**		Cuando se cambian las plataformas en funcionamiento, las aplicaciones deben revisarse para asegurar que no hay impacto adverso sobre las operaciones de la empresa.				**X**
A 14.2.4	Restricciones en los cambios a los paquetes de software	**X**		Las modificaciones necesarias a los paquetes de software se deben controlar de forma estricta				**X**

A 14.2.5	Principios de construcción de los sistemas seguros	**X**		Se establecerán principios de ingeniería para sistemas seguros documentados.	**X**			**X**
A 14.2.6	Ambiente de desarrollo seguro	**X**		Se establecen y protegen los entornos de desarrollo.				**X**
A 14.2.7	Desarrollo contratado externamente		**X**	No se ha implementado.				**X**
A 14.2.8	Pruebas de seguridad de sistemas	**X**		Se llevan a cabo pruebas de la funcionalidad de seguridad durante el desarrollo.				**X**
A 14.2.9	Prueba de aceptación del sistema	**X**		Se establecen pruebas de aceptación para los nuevos sistemas de información.				**X**
A 14.3 Datos de prueba								
A 14.3.1	Protección de los datos de prueba del sistema	**X**		Los datos de prueba son cuidadosamente seleccionados, protegidos y controlados.				**X**
A 15. RELACIONES CON LOS PROVEEDORES								
A 15.1 Seguridad de la Información en las Relaciones con los Proveedores								
CONTROL ISO	**CONTROLES**	**CUMPLE**		**CONTROL / DESCRIPCIÓN**	**Razones para seleccionar control**			
		SI	NO		**RL**	**OC**	**RN**	**AR**
A 15.1.1	Política de seguridad de la información para las relaciones con proveedores		**X**	No se ha implementado.		**X**		**X**
A 15.1.2	Cadena de suministro de tecnología de información y comunicación		**X**	No se ha implementado.		**X**		**X**
A 15.2 Gestión de la Prestación del Servicios de Proveedores								

A 15.2.1	Seguimiento y revisión de los servicios de los proveedores		**X**	No se ha implementado.		**X**		**X**
A 15.2.2	Gestión cambios en los servicios de los proveedores		**X**	No se ha implementado.		**X**		**X**
A 16. GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN								
A 16.1 Gestión de los Incidentes y las mejoras en la Seguridad de la Información								
A 16.1.1	Responsabilidades y procedimientos	**X**		Se establecen las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.				**X**
A 16.1.2	Reporte sobre las debilidades en la seguridad	**X**		Se requiere que los empleados y contratistas reporten cualquier deficiencia de seguridad de información detectada o sobre sospecha.				**X**
A 16.1.3	Respuesta a incidentes de seguridad de la información	**X**		Los incidentes de seguridad de la información deberán recibir una respuesta de acuerdo con los procedimientos documentados.				**X**
A 16.1.4	Recolección de evidencias	**X**		Se definen procedimientos para la identificación, recolección y conservación de la información, que pueda servir como prueba.				**X**
A 16.1.5	Evaluación de eventos de seguridad de la	**X**		Los eventos de seguridad de la información deben ser evaluados.				**X**

	información y decisiones sobre ellos							
A 16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	**X**		El conocimiento adquirido a partir del análisis y solución de los incidentes de seguridad de la información se utilizará para reducir la probabilidad o el impacto de los incidentes en el futuro.				**X**
A 17. ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO								
A **17. Continuidad de Seguridad de la Información**								
CONTROL ISO	**CONTROLES**	**CUMPLE**		**CONTROL / DESCRIPCIÓN**	**Razones para seleccionar control**			
		SI	NO		**RL**	**OC**	**RN**	**AR**
A 17.1.1	Planificación de la continuidad de la seguridad de la información	**X**		Se determina los requisitos de seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas.			**X**	**X**
A 17.1.2	Implementación de la continuidad de la seguridad de la información	**X**		Se establece, documenta, implementa y mantienen procedimientos y controles para garantizar el nivel necesario de continuidad de la seguridad durante una situación adversa.			**X**	**X**
A.17.2 Redundancias								
A 17.2.1	Disponibilidad de instalaciones de procesamiento de información	**X**		Las instalaciones de procesamiento de información tendrán la redundancia suficiente para garantizar la disponibilidad.				**X**

18. CUMPLIMIENTO								
A 18.1 Cumplimiento de los Requisitos Legales y Contractuales								
A 18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	**X**		Todo lo pertinente al marco legal, los requisitos contractuales, y el enfoque de la empresa para cumplir con estos deben ser identificados, documentados y actualizados.	**X**	**X**		**X**
A 18.1.2	Derechos de propiedad intelectual (DPI)	**X**		Se aplican procedimientos para garantizar el cumplimiento de los derechos de propiedad intelectual.	**X**			**X**
A 18.1.3	Protección de registros	**X**		Se debe evitar pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada.				**X**
A 18.1.4	Privacidad y protección de información de datos personales	**X**		Los datos personales deben asegurarse según la legislación.	**X**	**X**		**X**
A 18.2 Revisiones de Seguridad de la Información								
A 18.2.1	Revisión independiente de la seguridad de la información		**X**	No se ha implementado.				**X**
A 18.2.2	Cumplimiento con las políticas y las normas de seguridad	**X**		Se comprobará periódicamente el cumplimiento de las políticas de seguridad.				**X**
A 18.2.3	Revisión del cumplimiento técnico	**X**		Los sistemas de información deben revisarse regularmente para verificar el cumplimiento de las políticas y normas de				**X**

				seguridad de la información de la empresa.				

Fuente: Norma NTC-ISO-IEC 27001:2013

Las salvaguardas o controles de seguridad son aquellos procedimientos o medidas tecnológicas que hacen que se reduzca el riesgo, haciendo que se disminuyan las amenazas de cada activo. Hay amenazas que son solucionadas simplemente con un proceso de organización, otras requieren componentes técnicos como: programas, software, hardware o dispositivos de seguridad, hay otras que requieren implementar seguridad física y finalmente otras requieren políticas orientada a las personas.

Es importante identificar las salvaguardas existentes que tengan los activos y sistemas de información, para determinar su nivel de eficacia y de esta manera proponer nuevas salvaguardas, eliminarlas o simplemente mantener las que están cumpliendo con los respectivos criterios de seguridad.

Una vez realizado el inventario de activos, e identificado las amenazas y vulnerabilidades, se definen las salvaguardas que son procedimiento tecnológico que reduce el riesgo, de acuerdo a los activos que se van proteger, en la tabla 20 se tienen en cuenta las salvaguardas definidas en MAGERIT.

Tabla 20. Tipos de salvaguardas de seguridad

Tipo de protección	**Descripción**
[PR] prevención	Una salvaguarda es preventiva cuando reduce las oportunidades de que un incidente ocurra.
[DR] disuasión	Una salvaguarda es disuasoria cuando tiene un efecto tal sobre los atacantes que estos no se atreven o lo piensan dos veces antes de atacar.

[EL] eliminación	Una salvaguarda elimina un incidente cuando impide que éste tenga lugar. Son salvaguardas que actúan antes de que el incidente se haya producido
[IM] minimización del impacto / limitación del impacto	una salvaguarda minimiza o limita el impacto cuando acota las consecuencias de un incidente.
[CR] corrección	Una salvaguarda es correctiva cuando, habiéndose producido un daño, lo repara. Son salvaguardas que actúan después de que el incidente se haya producido y por tanto reducen los daños.
[RC] recuperación	una salvaguarda ofrece recuperación cuando permite regresar al estado anterior al incidente. Son salvaguardas que no reducen las probabilidades del incidente, pero acotan los daños a un periodo de tiempo.
[MN] monitorización	Son las salvaguardas que trabajan monitorizando lo que está ocurriendo o lo que ha ocurrido. Si se detectan cosas en tiempo real, podemos reaccionar atajando el incidente para limitar el impacto; si se detectan cosas a posteriori, podemos aprender del incidente y mejorar el sistema de salvaguardas de cara al futuro.
[DC] detección	Una salvaguarda funciona detectando un ataque cuando informa de que el ataque está ocurriendo. Aunque no impide el ataque, sí permite que entren en operación otras medidas que atajen la progresión del ataque, minimizando daños.
[AW] concienciación	Son las actividades de formación de las personas anexas al sistema que pueden tener una influencia sobre él. La formación reduce los errores de los usuarios, lo cual tiene un efecto preventivo.
[AD] administración	Se refiere a las salvaguardas relacionadas con los componentes de seguridad del sistema. Una buena administración evita el desconocimiento de lo que hay y por tanto impide que haya

	puertas desconocidas por las que pudiera tener éxito un ataque. En general pueden considerarse medidas de tipo preventivo.[66]

Fuente: PILAR. Análisis y Gestión de Riesgos. Glosario de Términos

6.7 PRUEBAS DE SEGURIDAD Y ANALISIS DE VULNERABILIDADES

En esta fase se deben identificar las vulnerabilidades que se presentan por la falta de controles de seguridad, que mitiguen los riesgos. Estas pruebas están pensadas para evaluar la estructura de seguridad en la organización.

Las pruebas de vulnerabilidad son técnicas empleadas para comprobar la seguridad de una empresa. Las pruebas a realizar son esencialmente a servidores, equipos, redes y aplicaciones.

6.7.1 Herramientas de trabajo

Se proponen unas herramientas de software para realizar el diagnóstico de la seguridad. El uso de otra herramienta se deja a elección, mientras está no comprometa o afecte el desempeño de la red a testear:

- WIRESHARK: Esta herramienta permite analizar protocolos de red, capturando los paquetes que pasen por la red. De esta forma se puede verificar si por medio de la red viajan datos sin cifrar, enviando información confidencial que puede ser fácilmente interceptada por cualquier persona dentro de la red.[67]
- ETTERCAP: Este software permite realizar ataques de "*man in the middle*" o "hombre en el medio" sobre las redes LAN, especialmente las basadas en

[66] A.L.H. J. Mañas. PILAR Análisis y Gestión de Riesgos. Glosario de Términos [en línea]. Disponible en Internet: http://www.ar-tools.com/es/glossary/index.html
[67] Sharpe, Richard y Warnicke, Ed. Wireshark User's Guide [en línea]. Disponible en Internet: http://www.wireshark.org

switches. Algunas características que trae son: *sniffer*, ARP *Spoofing* y otras para el análisis de redes y equipos.[68]

- NETSTUMBLER: Esta herramienta corre bajo Windows y permite detectar redes inalámbricas usando los protocolos 802.11a, 802.11b y 802.11g. Se puede identificar la presencia de redes inalámbricas inseguras, su cobertura y detectar interferencias con otras redes.[69]
- NESSUS: Permite escanear equipos de la red con el fin de encontrar posibles vulnerabilidades. Puede ayudar a identificar si al equipo le falta algún parche o está desactualizado.[70]
- METASPLOIT FRAMEWORK: Con esta herramienta se puede escribir, probar y usar código exploit, utilizado para aprovechar las vulnerabilidades de los equipos en la red. Este software es una sólida plataforma para las pruebas de penetración e investigación de vulnerabilidades.[71]
- NMAP: Software open source para escáner la red y hacer auditorias de seguridad. Con esta herramienta se puede hacer escaneo de puertos, enumerar los de equipos activos en la red y ayudar a identificar los sistemas operativos en cada equipo.[72]
- YERSINIA: Esta herramienta se enfoca en aprovechar debilidades en diferentes protocolos de la capa de enlace como: STP, DTP, CDP, IEEE 802.1Q, IEEE 802.1X, VTP y otros. Se pueden hacer ataques de negación de servicio a dichos protocolos, ganar privilegios dentro de las redes segmentadas en VLAN's y así capturar el tráfico de otras VLAN's.[73]

---

[68] Manual Reference Pages – ETTERCAP [en línea]. Disponible en Internet: http://www.irongeek.com/i.php?page=backtrack-3man/ettercap
[69] Milner, Marius. NetStumbler v0.4.0 Release Notes [en línea]. Disponible en Internet: http://www.stumbler.net/readme/readme_0_4_0.html
[70] Getting Started with Tenable.io [en línea]. Disponible en Internet: https://docs.tenable.com/cloud/Content/GettingStarted/GettingStarted.htm
[71] METASPLOIT.com. Metasploit Framework User Guide [en línea]. Disponible en internet: https://metasploit.help.rapid7.com/docs
[72] Nmap Network Scanning. [en línea]. Disponible en internet: https://nmap.org/man/es/
[73] Barroso, David y Berrueta, Andrés. YERSINIA Framework for layer 2 attacks [en línea]. Disponible en Internet: http://www.yersinia.net/index.htm

- KALI: Herramienta muy popular para realizar auditorías de seguridad, basada en la distribución de Linux Debian, en la cual se incluyen muchas herramientas para realizar test de seguridad informática, sniffers, exploits, auditoria wireless, análisis forense y otras. [74]

6.7.2 Pruebas de Seguridad física

Con estas pruebas se buscan verificar las medidas de seguridad a nivel del perímetro para los activos de la red.

Actividad 1: Verificar con que controles se cuenta de acceso físico.

- El área debe contar con paredes sólidas y sin ninguna brecha que permita cualquier incidente.
- Contar con buenas cerraduras en puertas y ventanas.
- Contar con un sistema de control de intrusos o Registro de visitantes a la entrada.
- Ubicar los equipos de manera que se evite la manipulación de las conexiones.
- Los equipos deben estar protegidos dentro de gabinetes con cerradura o un cuarto con cerradura.

Actividad 2: Verificar el cableado de red en los equipos.

- Cableado rotulado debidamente.
- Que los cables estén ordenados correctamente.
- Los cables están protegidos para evitar cualquier interceptación o daño físico.

[74] Kali Linux. [en línea]. Disponible en internet: https://www.kali.org/kali-linux-documentation/

6.7.3 Pruebas de Seguridad en firewall

Estas pruebas buscan analizar el nivel de seguridad ofrecido por el equipo firewall que cuente la red, que se encarga del filtrado de tráfico hacia y fuera de la red por Internet. En la tabla 21 encontramos los comandos a usar con Nmap

Actividad 1: Verificar el funcionamiento del firewall.

Tabla 21. Comandos de Nmap para pruebas de firewall

Prueba	**Comando**
Verificar la posibilidad de escanear, desde un equipo en Internet, a través del *firewall* para enumeración de equipos	nmap –sP <Dirección de red/Sufijo de la Mascara>
Ejecutar un escaneo SYN desde un equipo en Internet hacia un equipo detrás del firewall, para descubrir puertos abiertos.	nmap –sS <Dirección IP> -P0
Ejecutar un escaneo ACK desde un equipo en Internet hacia un equipo detrás del firewall	nmap –sA <Dirección IP> -P0
Ejecutar un escaneo WIN desde un equipo en Internet hacia un equipo detrás del firewall	nmap –sW <Dirección IP> -P0
Ejecutar un escaneo NULL desde un equipo en Internet hacia un equipo detrás del firewall.	nmap –sN <Dirección IP> -P0
Ejecutar un escaneo FIN desde un equipo en Internet hacia un equipo detrás del firewall.	nmap –sF <Dirección IP> -P0

Desde un equipo en Internet testear la respuesta del firewall a paquetes con la bandera RST activada.	nmap --scanflags RST <Dirección IP> -P0
Realizar escaneos de tipo UDP para enumerar puertos UDP abiertos, cerrados o filtrados.	nmap –sU <Dirección IP> -p <rango_puertos> -P0
Realizar un sondeo de puertos, desde un equipo en Internet, con una dirección IP falsa para determinar si el firewall esté haciendo detección de direcciones IP falsas	nmap <Dirección IP> -e <Interfaz física local> -S <Dirección IP Falsa> -P0
Realizar un sondeo de puertos, desde un equipo en Internet, con una dirección MAC falsa para determinar si el *firewall* esté haciendo detección de direcciones MAC falsas hacia un equipo detrás del firewall.	nmap <Dirección IP> -e <Interfaz física local> -spoof-mac <Dirección MAC Falsa> -P0
Desde un equipo en Internet verificar la habilidad del firewall para manejar fragmentos de paquetes pequeños y evitar ataques por fragmentación.	nmap –f <Dirección IP> -P0 nmap –-mtu <valor_fragmento> <Dirección IP> -P0 [75]

Fuente: Guía de referencia de Nmap

6.7.4 Pruebas de Seguridad en servidores

Con estas pruebas se busca identificar en qué estado se encuentran los equipos que manejan servicios, información y datos sensibles en la empresa. Se desea detectar la presencia de vulnerabilidades que afecten el correcto funcionamiento de los servidores.

[75] Guía de referencia de Nmap [en línea]. Disponible en Internet: https://nmap.org/man/es/man-target-specification.html

Actividad 1- Análisis de puertos: Este análisis consiste en ejecutar diferentes tipos de pruebas o test dirigidos a los servidores para reconocer el estado de los puertos usados y la información de los servicios que se están ejecutando en dichos puertos.

Mediante este tipo de chequeos se puede identificar la presencia de *backdoors*, puertos abiertos y servicios que están activos innecesariamente.

En la tabla 22 se muestran los comandos de Nmap que se deben ejecutar desde Internet y/o segmento público de la red.

Tabla 22. Comandos para el análisis de puertos en servidor

TIPO	**COMANDO**
TCP SYN	*nmap -sS <Dirección IP> -P0*
VERSION	*nmap -sV <Dirección IP> -P0*
TCP ACK	*nmap -sA <Dirección IP> -P0*
VENTANA TCP	*nmap -sW <Dirección IP> -P0*
TCP NULL	*nmap -sN <Dirección IP> -P0*
TCP FIN	*nmap -sF <Dirección IP> -P0*
TCP XMAS	*nmap -sX <Dirección IP> -P0*
TCP RESET	*nmap --scanflags RST <Dirección IP> -P0*
UDP	*nmap -sU <Dirección IP> -p <rango_ puertos> -P0* [76]

Fuente: Guía de referencia de Nmap

Actividad 2 – Análisis de vulnerabilidades: Verificar la existencia de vulnerabilidades en los servidores que puedan afectar el funcionamiento de los mismos. Para esta actividad se puede usar la tabla 23:

[76] Ibid.

Tabla 23. Herramientas para identificación y análisis de vulnerabilidades

Prueba	**Herramienta**
Realizar en los servidores un escáner de vulnerabilidades. Analizar el informe y enumerar los puertos que estén abiertos, clasificando cada una de las vulnerabilidades asociadas a los puertos abiertos.	Nessus
Mediante la herramienta buscar en su base de datos de *exploits*, uno que haga referencia a las vulnerabilidades encontradas y comprobar la presencia de la vulnerabilidad.	Metasploit Framework 3

Fuente: Propiedad del autor

6.7.4 Pruebas de Seguridad en switches

Con esta prueba se identifican problemas de seguridad asociados a los switches de capa 3 utilizados en la red que permita la segmentación de ésta en VLAN's.

Actividad 1 – Análisis de vulnerabilidades: Con esta actividad que se encuentra en la tabla 24, se busca revisar e identificar la existencia de vulnerabilidades en los *switches* de capa 3 que puedan afectar el funcionamiento y desempeño normal de la red, además detectar posibles ataques para capturar tráfico.

Tabla 24. Herramientas para pruebas a switch

Prueba	**Herramienta**
Verificar si los switches son susceptibles a un ataque ARP spoofing	Ettercap
Realizar un análisis de tráfico y captura de paquetes para identificar los protocolos de capa de enlace utilizados en la red	Wireshark
Con la ayuda de la herramienta de ataque diseñada para aprovechar las vulnerabilidades de los protocolos de capa de enlace (Ej.: VTP, STP, DTP y CDP) llevar a cabo ataques a los switches en la red.	Yersinia

Fuente: Propiedad del autor

6.7.5 Pruebas de Seguridad en red inalámbrica 802.11

Con esta prueba se pretenden identificar problemas de seguridad en la red inalámbrica de la organización.

Actividad 1 – Inventario de los puntos de acceso (Access point): Inventariar los puntos de acceso instalados en la empresa con el objetivo de identificar cuales no están autorizados.

- Solicitar al encargado de administración de la red inalámbrica un listado de los puntos de acceso instalados en la red y autorizados por ellos.
- Identificar los puntos de acceso inalámbricos dentro de toda el área de la organización, mediante un equipo portátil con tarjeta de red inalámbrica y una herramienta de software. Para esta prueba se usa la herramienta NetStumbler.

Actividad 2 – Análisis general de la WLAN: Con un equipo portátil con conexión a la red inalámbrica realizar los siguientes pasos:

- Realizar un mapeo de la red donde se muestren los puntos de acceso (AP) inalámbrico, encontrando sus direcciones IP. Con la herramienta Nmap, usamos el siguiente comando: nmap –sP <Segmento de red: 10.0.0.0/16>
- Verificar si los puntos de acceso tienen habilitado un sistema de cifrado para el tráfico de la red (Ej.: WEP y WPA). Usamos la herramienta Wireshark
- Con un explorador de Internet ingresar a las direcciones de los AP e intentar acceder a la configuración con el usuario y contraseña *admin*.

6.7.6 Análisis de resultados de las pruebas de Seguridad

De acuerdo a las actividades realizadas anteriormente, se debe hacer el análisis de resultados del diagnóstico. Para realizar este análisis se utilizará la siguiente tabla

que permitirá identificar el grado de criticidad de seguridad que se encuentra un determinado equipo. Para su valoración utilizamos la tabla 25 con la siguiente escala:

- MA: muy alto
- A: alto
- M: medio
- B: bajo
- MB: muy bajo

Tabla 25. Resumen de pruebas, hallazgos y riesgos

Activo	Prueba	Hallazgo	Riesgo

Fuente: Propiedad del autor

7. MEDIDAS, PROCEDIMIENTOS Y BUENAS PRÁCTICAS PARA PREVENIR INCIDENTES RELACIONADOS CON EL TRATAMIENTO DE DATOS PERSONALES

Luego de llevar a cabo el diagnóstico de la seguridad en la empresa, se presentan las recomendaciones y medidas de seguridad que ayuden a resolver las deficiencias de seguridad encontradas. Estas medidas y controles de seguridad deben ser parte de una política de seguridad, por lo que a continuación se presenta una propuesta de una política que permita tener control mejor sobre los activos que conforman la organización.

7.1 POLÍTICA DE SEGURIDAD

Una política de seguridad debe estar compuesta por reglas y establecer responsabilidades para evitar que las amenazas impacten el negocio. Es un documento que define las directrices de la organización en materia de seguridad.

La política de seguridad se puede implementar mediante algunos mecanismos de seguridad que se constituyen en herramientas para la protección y seguridad del sistema. Estos elementos normalmente se apoyan en normativas que cubren áreas más específicas.

Los mecanismos de seguridad se dividen en tres grupos[77]:

- **"Prevención**: Evitan desviaciones respecto a la política de seguridad.
  Ejemplo: utilizar el cifrado en la transmisión de la información evita que un posible atacante capture y comprenda información en un sistema de red.

[77] MIFSUD, Elvira. MONOGRÁFICO: Introducción a la seguridad informática - Políticas de seguridad [en línea]. Disponible en Internet: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=4

- **Detección**: Detectan las desviaciones si se producen, violaciones o intentos de violación de la seguridad del sistema.
  Ejemplo: la herramienta Tripwire para la seguridad de los archivos.
- **Recuperación**: Se aplican cuando se ha detectado una violación de la seguridad del sistema para recuperar su normal funcionamiento.
  Ejemplo: las copias de seguridad."

El objetivo de la Política de Seguridad de Información de una organización es mostrar el estado de seguridad de la organización y servir como base para desarrollar los procedimientos concretos de seguridad.

La empresa debe disponer de un documento formalmente elaborado y ser divulgado entre todos los empleados.

No es necesario realizar un nivel tan detallado, pero tampoco se puede dejar como una declaración de meras intenciones. Lo más importante para que estas políticas tengan el efecto deseado, es lograr la concientización, el entendimiento y compromiso de todos los involucrados.

Las políticas deben contener claramente las medidas que serán adoptadas por la compañía. Estas deben ser revisadas paulatinamente y si es necesario actualizarlas.

Las políticas deben:

- "Definir qué es seguridad de la información
- Cuáles son sus objetivos principales y su importancia dentro de la organización
- Mostrar el compromiso de sus altos cargos con la misma
- Definir la filosofía respecto al acceso a los datos
- Establecer responsabilidades inherentes al tema

- Establecer la base para poder diseñar normas y procedimientos referidos a la:

    - Organización de la seguridad
    - Clasificación y control de los datos
    - Seguridad de las personas
    - Seguridad física y ambiental
    - Plan de contingencia
    - Prevención y detección de virus
    - Administración de los computadores

A partir de las políticas se podrá desarrollar, las normas y luego los procedimientos de seguridad que serán la guía para la realización de las actividades. Por lo tanto, la administración de la organización en cuestión debe encargarse de definirla, ya que afecta a todos los usuarios del sistema.

La seguridad informática de una empresa depende de que sus colaboradores (usuarios) conozcan las reglas a través de procesos de capacitación y de concienciación."[78]

Adicionalmente la seguridad informática de una empresa debe cubrir las siguientes áreas:

- Un mecanismo de seguridad física y lógica que se adapte a las necesidades de la compañía y al uso de los empleados
- Un procedimiento para administrar las actualizaciones
- Una estrategia de realización de copias de seguridad planificada adecuadamente
- Un plan de recuperación luego de un incidente

[78] Ibid.

- Un sistema documentado actualizado
- Por lo tanto y como resumen, la política de seguridad es el documento de referencia que define los objetivos de seguridad y las medidas que deben implementarse para tener la certeza de alcanzar estos objetivos.[79]

7.1.1 Modelo de una Política de Seguridad

El área de sistemas es la encargada de administrar el sistema de información que hace uso la empresa, además de ofrecer servicios de red a todos los usuarios de la compañía. Por lo anterior se hace necesario emitir la presente Política de Seguridad.

Propósito de la Política: El propósito de esta política es ayudar a minimizar el riesgo de daño o pérdida de la información por incidentes o actividades de delincuentes, las cuales también pueden afectar los servicios de la red. Para lo cual se establecen normas que permitan lograr una adecuada protección de la información, incluyendo las reglas de comportamiento de los usuarios y administradores del sistema de la red. Por medio de esta política se busca autorizar al personal encargado, de monitorear la red local con el fin de prevenir cualquier mal uso e investigar incidentes de seguridad que se presenten.

Alcance de la Política: La presente Política establece las normas para la seguridad de la información en la red de datos administrada por el área de sistemas, la cual afecta a todos los empleados y demás usuarios finales que hacen uso de los recursos informáticos de la empresa, quienes a partir de este momento se llamarán USUARIOS.

[79] MIFSUD. Elvira. MONOGRÁFICO: Introducción a la seguridad informática - Políticas de seguridad [en línea] disponible en internet: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=4

Responsabilidades: El área de sistemas es la responsable de socializar la Política de Seguridad entre quienes hagan uso de los sistemas de información de la empresa. De acuerdo al perfil del usuario, se dará a conocer la Política completa. Es responsabilidad de cada usuario cumplir con cada una de las directrices que se definan en esta Política de Seguridad.

Definiciones: Las siguientes definiciones son dadas con el fin de aclarar algunos conceptos para el conocimiento de la presente política:

- Información confidencial de la organización: Es toda información relacionada con la organización que, en caso de robo o pérdida, pueda generar daños o problemas de continuidad para la empresa.
- Sistema informático: Conjunto de hardware y software con el que cuenta la organización.
- Sistema de información: Es un conjunto de elementos (información, personas y recursos) que interactúan entre si para procesar la información y distribuirla de manera adecuada dentro de la empresa.

Uso del Correo Electrónico e Internet: El correo electrónico no debe ser utilizado para transmitir información confidencial de la empresa. En caso de que exista la necesidad de usar este medio para tal fin, se recomienda utilizar mecanismos como el cifrado para proteger la información de personas no autorizadas.

El correo electrónico debe ser de uso personal, cada usuario se hace responsable de asignar una contraseña segura y de hacer el uso correcto de éste.

El correo electrónico ni la Internet deben ser usados para publicar propaganda política, ni mensajes racistas, ni contenido sexual y ningún otro contenido que pueda afectar negativamente a los usuarios de dichos servicios.

El servicio de la Internet debe ser utilizado únicamente como un medio de consulta para fines laborales o para el cumplimiento de los objetivos organizacionales.

El área de sistemas deberá incentivar el buen uso de Internet, evitando que se haga uso indebido y malintencionado de Internet y de los servicios que sobre éste se brindan.

Administración de Cuentas de Usuario: Se debe definir claramente los perfiles de usuario de acuerdo a las funciones, roles que desempeña y de su tipo de vinculación dentro de la empresa. De acuerdo a esto los usuarios tendrán los permisos correspondientes para realizar determinadas modificaciones (Ej.: instalación de software en computadores personales) en los distintos sistemas informáticos.

El área de sistemas es la responsable de definir los perfiles de usuario y la única de crear las cuentas de usuario teniendo en cuenta los perfiles ya definidos.

Autenticación: El acceso a los servicios o sistemas que manejen información confidencial de la empresa, obligatoriamente, debe incluir un mecanismo de autenticación.

Todos los servicios informáticos deberían incluir autenticación de usuario, como contraseñas, certificados u otros mecanismos como doble factor de autenticación.

Se deberán establecer reglas para el uso de contraseñas seguras, como sólo permitir contraseñas que incluyan caracteres alfanuméricos y especiales dentro de la contraseña o cantidades mínimas de caracteres en la contraseña.

Los usuarios y contraseñas para acceder a los distintos servicios, computadoras y demás sistemas informáticos son personales y no deben compartirse con otros usuarios.

Las contraseñas deben ser memorizadas, y no se debe recurrir a la práctica de escribirlas en papeles ni en otro medio al cual puedan acceder otros usuarios.

El responsable del equipo no debe otorgar acceso al equipo a otras personas sin autorización del área de sistemas.

Control de Acceso: El acceso a las áreas que contengan sistemas con información confidencial (Ej.: servidores) o permitan acceso privilegiado a la red (Ej.: switch) deberá ser registrado con la fecha, hora de entrada y salida, y motivo de la visita.

La visita de personas que no pertenezcan a el área de sistemas a los cuartos de servidores y equipos deberá ser bajo supervisión del personal de El área de sistemas o una persona delegada para tal fin.

Se deberá generar mecanismos que restrinjan el acceso a personas no autorizadas a las áreas que contengan sistemas con información confidencial o permitan acceso privilegiado a la red de acuerdo al nivel de criticidad del área.

Se deben tener mecanismos que no permitan el acceso a los servidores por usuarios no autorizados.

Se deben establecer diferentes zonas lógicas en la red, en las que se separen los recursos de acceso público con los de acceso privado, filtrando tráfico de la red entre las dichas zonas.

Autorización de Acceso a la información y Sistemas: Se deben definir los diferentes niveles de autorización para los usuarios de acuerdo a sus roles dentro de la empresa.

La autorización para acceder a la información de la empresa y sistemas debe sólo ser concedida de acuerdo al nivel requerido por el rol del usuario.

La autorización para acceder a la información y sistemas debe ser verificada como mínimo en periodos de un año.

Seguridad física: Los equipos que procesen información sensible o crítica deben ser ubicados en lugares seguros, que tengan un perímetro de seguridad física definido y donde existan controles de acceso.

Los equipos de red deberán ser ubicados en lugares que cumplan con los requerimientos básicos de seguridad exigidos por el área de Informática.
Se deberá implementar mecanismos para protección contra incendio, tales como detectores de humo, extintores de fuego o los que se consideren necesarios.

Se debe evitar almacenar material combustible o que pueda ayudar a la propagación de un incendio en los cuartos con equipos que manejen información sensible o sean de gran importancia para el funcionamiento de la red.

Es recomendable el monitoreo de las condiciones ambientales, tales como temperatura, con el fin de controlar las condiciones que puedan afectar el funcionamiento de los equipos.

Software: En los equipos se deberán mantener actualizado aquel software del que se emita una mejora en seguridad o cualquiera que contribuya con el buen funcionamiento de éste.

En los equipos que manejen información sensible se deberá instalar la actualización del software garantizando que ésta no afecte con el funcionamiento del equipo.

El software instalado en los equipos debe cumplir con el licenciamiento apropiado y acorde a la propiedad intelectual a que dé lugar.

En los sistemas críticos se debería planear la actualización del software, el cual es recomendable realizar bajo un procedimiento de instalación emitido por el área de Informática.

Todo software que afecte la integridad y rendimiento de los recursos de la red no debe ser permitido.

Corresponde a El área de sistemas la autorización de la adquisición del software.

El área de sistemas es la responsable de llevar a cabo revisiones a los sistemas informáticos propiedad de la empresa con el fin de asegurar que sólo software licenciado se encuentre instalado en ellos.

El software utilizado en la empresa deberá ser usado exclusivamente para asuntos relacionados con las actividades de la empresa.

Instalación y mantenimiento de los equipos: El área de sistemas deberá llevar un inventario de todos los equipos propiedad de la empresa.

Los equipos que deban o estén conectados a la red de la empresa deberán estar sujetos a los requerimientos de instalación emitidos por El área de sistemas y tener la configuración de seguridad básica exigida por ella.

Es deber del responsable del equipo en conjunto con El área de sistemas dar cumplimiento a los requerimientos de instalación e informar sobre cualquier cambio que afecte la instalación del equipo. El responsable del equipo debe velar por la integridad física del equipo.

Es responsabilidad de El área de sistemas del mantenimiento preventivo y correctivo de lo equipos propiedad de la empresa. El área de sistemas puede otorgar mantenimiento preventivo y correctivo cuando lo estimen necesario, con previó aviso al responsable del equipo.

Se debe procurar mantener actualizados los equipos con el fin de mantener el buen funcionamiento de éste o mejorarlo.

Cuando se requiera reutilizar cualquier dispositivo se debe borrar la información que contenga mediante el uso de técnicas que permitan que dicha información no pueda ser recuperada.

En caso de que se necesite dar de baja un dispositivo, este debe ser destruido físicamente de tal forma que no pueda recuperarse la información.

Los equipos que vayan a ser reutilizados o eliminados deberán ser revisados, con el propósito de no eliminar software licenciado, ni información confidencial de los cuales no se tenga copia.

Se deberá contar con autorización previa de El área de sistemas para la reutilización o eliminación de un equipo.

Para cada equipo eliminado se deberá tener un documento que contenga el motivo por el cual se da de baja, el responsable en dar de baja el equipo, la fecha y cualquier otra información que se considere importante.

Acceso remoto desde un entorno de internet: Se deben implementar protocolos capaces de cifrar la comunicación que se establezca desde el exterior de la red en la cual se transmita información sensible.

El área de sistemas es la encargada de asignar los correspondientes accesos remotos a los servicios de la red con autorización del responsable del servicio, en los casos que la criticidad del servicio lo amerite, por ejemplo, acceso mediante VPN o sesión Telnet.

Desarrollo de servicios de red: La implementación de los servicios de red deberá tener el visto bueno del área de sistemas.

Al responsable del servicio de red le corresponde la implementación de la protección adecuada.

La programación e implementación de los servicios de red deberán estar de acuerdo a los requerimientos emitidos por el área de Informática.

Backup de la Información: La información que para la empresa se considere crítica o sensible deberá tener copias de seguridad.

Manejo de la información: El usuario no deberá divulgar o revelar información confidencial de la empresa a personas no autorizadas. En caso de ser necesario compartir información confidencial con cualquier persona, entidad o firma fuera de la empresa, se debe solicitar autorización al área de sistemas o el oficial de protección de datos, quienes a su vez darán el manejo adecuado para dicha solicitud.

Dentro de la empresa, la información confidencial se revelará a aquellas personas cuyas funciones ameriten tener tal conocimiento. Aquellas personas que manejan

información confidencial no deberán revelarla a ninguna otra persona de la empresa. Ningún usuario tiene, automáticamente, derecho a acceso a toda la información de la organización.

La persona que recibe información confidencial no deberá reproducirla, a menos que se le autorice por parte del dueño de la información. En caso que se autorice realizar copias de la información suministrada, éstas deben ser controladas.

Evaluaciones de seguridad: Las evaluaciones de seguridad deberían realizarse con regularidad con el fin de identificar posibles vulnerabilidades en el sistema. Toda información necesaria para la evaluación que se le suministre al evaluador o evaluadores deberá ser entregada bajo un compromiso de confidencialidad, que garantice no sea divulgada. El proceso de evaluación debería ayudar a encontrar las vulnerabilidades del sistema y a su vez los controles de seguridad adecuados para minimizarlas.

El proceso de evaluación debería asegurar que los resultados se documenten y hacerlo con regularidad podría ayudar a mejorar la Política de Seguridad.

7.2 MEDIDAS DE SEGURIDAD INFORMATICA

Para fortalecer la política de seguridad de la información es necesario adoptar medidas técnicas que apoyen la labor de seguridad y protección de la información y de los datos. A continuación, se describen algunas recomendaciones y medidas adicionales a tener en cuenta:

Hacer Uso de Protocolo de Buenas Contraseñas:

- No debe tener menos de ocho dígitos.
- Mezclar mayúsculas y minúsculas, letras, números y caracteres especiales.

- No debe contener nombres obvios o referentes a la organización.
- Debe cambiarse frecuentemente.

Hacer Uso de Encriptación de Datos:

- Hacer un cifrado de datos con lo que lograremos que:
  - Nadie lea la información en el transcurso de su envió.
  - Garantizar que el remitente sea quien dice ser.
  - El contenido del mensaje no sea modificado en el camino.

Hacer Uso de Software de Seguridad:

- El antivirus: estos detectan e impiden que se ejecute y elimina el software malicioso.
- El cortafuego: con ello permitimos o prohibimos la comunicación entre el software de nuestro equipo e Internet y evitar que atacantes haga funcionar una aplicación en nuestro ordenador sin autorización.
- Software Antispam: estos son filtros que detectan el correo indeseado.
- Software Antispyware: estos programas son orientados a la detección, bloqueo y eliminación de software espía.
- Filtros anti-phishing
- Programas de monitorización wifi
- Hacer uso de defensas pasivas

Partición de Disco Duro o Sistemas Raid:

- De esta manera guardar los datos en una partición distinta a la que se utiliza para instalar el S.O, en caso de tener que formatear el equipo no se necesita sacar todos los datos.

- Otra forma es tener en nuestro sistema un RAID o arreglo de discos, de tal forma que si existen daños en el disco duro principal este con replica en un segundo y no se pierda la información.

Implementar un Controlador de dominio:

- Con el fin de facilitar la administración de las cuentas de usuario, equipos en la red, carpetas compartidas, permisos y control de acceso, además de asegurar, en gran parte del cumplimiento de la política de seguridad, se recomienda la implementación de un servidor de dominio que permita agrupar los equipos y usuarios dentro de un dominio. De esta manera, cada persona que acceda a los recursos de la red se identifica con un único usuario, lo que facilita la auditoría de usuarios, ya que se puede rastrear los sucesos de cada uno de éstos, permitiéndole al administrador saber que usuario es el que comente una violación a la seguridad.
- También permite una mejor administración de las directivas de seguridad para todos los usuarios, porque no se requiere definir directivas en cada equipo conectado a la red.

Filtrado por MAC de conexiones físicas en la Intranet:

Una medida para evitar conexiones a la red de equipos no aprobados es filtrar por MAC. Esto ayuda a los administradores a saber que equipos están conectados a la red, y estar seguros de que cumplan con los requerimientos exigidos para operar de forma segura, de esta forma se reduce en significativamente que usuarios conecten equipos infectados y se propague un virus a los demás equipos.

Implementación de detección o prevención de intrusos (IDS o IPS):

- El sistema de detección de intrusos (IDS) está diseñado para detectar cualquier acceso no autorizado, ataque informático o cualquier violación a un equipo o a una red.
- Un sistema de prevención de intrusos (IPS) es un dispositivo capaz de realizar las funciones de un IDS más las de prevenir las violaciones informáticas detectadas en la red.
- Como medida técnica para reducir los ataques informáticos, se recomienda la implementación de estos sistemas en la red, que le permita a los administradores detectar con mayor facilidad de donde proviene los ataques y poder prevenir el éxito de éstos.
- Hay dispositivos como los UTM que integran estas funcionalidades aparte de tener un sistema de firewall, control de acceso, filtrado de aplicaciones, filtrado de sitios web, control de VPN entre otras características.

7.3 BUENAS PRÁCTICAS PARA PROTECCIÓN DE DATOS PERSONALES[80]

Las recomendaciones y medidas que se presentan a continuación deben ser aplicadas al tratamiento de la información en general y especialmente a los datos de carácter personal en cumplimiento de la Ley de protección de datos personales 1581 de 2012.

[80] Fundación Pública Andaluza Progreso y Salud. Código de buenas prácticas para la protección de datos personales. [en línea] Disponible en internet: http://www.cabimer.es/intranet/docs/LOPD_codigo_buenas_practicas.pdf

7.3.1 Buena practicas:

Todo el personal que acceda a información de la organización está obligado a conocer y observar las medidas, normas, protocolos, reglas, estándares y políticas que afecten a las funciones que desarrolla.

Cada persona se responsabiliza del puesto de trabajo que tiene asignado y debe cumplir con los procedimientos internos de la entidad con respecto a la protección de datos personales.

- Deberán guardar la confidencialidad de la información que conozcan en el desarrollo de su trabajo. Esta obligación de guardar secreto subsistirá aún después de finalizar las relaciones contractuales con la organización.
- Evitar revelar información corporativa, salvo en aquellos casos en que el desempeño de las funciones laborales así lo requieran. No sacar información ni datos personales de la organización salvo en los casos que lo requieran las funciones asignadas y, en su caso, con previa autorización.
- Cuando se abandona el puesto de trabajo, bien temporalmente o bien al finalizar el turno, se debe dejar en un estado que impida la visualización de los datos protegidos: bloqueando el equipo con contraseña o desconectándose de las aplicaciones y la red, y apagando el monitor.
- Frente a cualquier solicitud de ejercicio de derecho de acceso, rectificación, cancelación u oposición de los datos por parte de su titular, informar inmediatamente reenviando dicha solicitud a la dirección de correo establecida como canal de comunicación por la organización, teniendo claro que existen unos plazos legales ajustados para responder a dichas solicitudes.
- Con respecto a los computadores portátiles y demás de dispositivos de almacenamiento móviles (teléfonos móviles, memorias USB, etc.), se debe cumplir:
    - Mantenerlos siempre controlados, (no dejar en lugares públicos, taxis, etc.) para evitar su sustracción.

- Reducir y/o eliminar la información que no vaya a ser utilizada.

- En caso de pérdida o robo de un dispositivo de almacenamiento móvil (portátil, teléfono, memoria USB, etc.) se notificará inmediatamente como incidencia de seguridad al área de sistemas o encargada.
- Se debe proporcionar la ayuda que se requiera en lo que se refiere a mantener la calidad de los datos, lo cual implica controlar:

  - Que la información contenida en los ficheros únicamente sea tratada en relación con las finalidades para las que se haya obtenido.
  - Que los datos sean exactos, estén actualizados y sean cancelados cuando éstos hayan dejado de ser necesarios.

- Respecto al uso del correo electrónico e Internet, se debe prestar atención al envío de datos de carácter personal por medio del correo electrónico, tanto en el cuerpo del mensaje como en anexos y, si se realiza, deberá tratar esos mensajes y anexos como temporales y borrarlos en cuanto dejen de ser necesarios.
- No se pondrán utilizar cuentas de correo personales para el envío de información profesional de la organización, excepto en situaciones inevitables como por ejemplo cuando exista una urgencia y el sistema esté caído.
- Ficheros temporales creados extrayendo datos de las aplicaciones corporativas para la ejecución de una determinada tarea o proceso (ejemplo: listados en Word o Excel) no deben mantenerse indefinidamente ni en el ordenador ni en un directorio de red y una vez finalizada dicha tarea o proceso hay que eliminarlos.
- Mesas limpias: cada usuario, cada vez que se ausente de su mesa de trabajo o bien cuando termine su jornada laboral, deberá retirar toda aquella información que contenga información que pudiera ser de carácter confidencial.
- Utilización de fotocopiadoras, escáneres e impresoras: Al utilizar impresoras o fotocopiadoras, debe asegurarse de recoger los originales al finalizar y de que no quedan documentos con datos sensibles en la bandeja de salida. Si las

impresoras son compartidas con otros usuarios sin acceso a los datos que están siendo impresos, se deberán retirar los documentos conforme vayan siendo impresos.

El personal que intervenga en el tratamiento de la información y que incumpla lo descrito en el presente documento, normas o procedimientos relacionados con la seguridad y con la protección de datos de carácter personal, deberá saber que podrá ser sometido al régimen sancionador/disciplinario existente en la organización, así como a Ley 1581 de 20102 y del Código Penal respecto a la comisión de delitos informáticos. Todo ello sin perjuicio de las posibles consecuencias civiles y penales a las que hubiera lugar en su caso.

8. PROCESO DE REGISTRO DE BASES DE DATOS

Preparar a la organización para el proceso de registro de bases de datos ante la SIC es el proceso que se verá en este capítulo. Basado en la recopilación de información obtenida en las fases anteriores, se tienen muchos datos necesarios para realizar el registro RNBD.

Para hacer el registro ante la SIC, es requerido revisar el inventario de las bases de datos con información personal que reposen o no en las instalaciones de la empresa, bien sea en medio físico (papel) o electrónico (listas o archivos en cualquier formato, bases de datos relacionales, etc.). Este inventario correspondería al realizado en la Tabla 5: Inventario de bases de datos:

RESPONSABLE	BASE DATOS	# REG	TIPO DE DATO				CLASIFICA	FINALIDAD	ENCARGADO
Nombre Colaborador	Nombre de base datos		Publico	Semiprivado	Privado	Sensible	Tipo de carácter	Tratamiento del dato	Nombre del tercero
Carlos Solis	Prospectos	500	x				Publico	Mercadeo	
Juan Pérez	Proveedores	50	x	x			Uso interno	Contabilidad	
Juan Pérez	Empleados	35	x	x	x	x	Confidencial	RRHH	
Leidy Diaz	Clientes	250	x	x	x		Restringida	Facturación	
María Perea	Proyectos	15	x	x		x	Confidencial	Contratos	Abogado
Ruby Cano	HV Físicas	45	x	x	x	x	Confidencial	RRHH	ADECO

Fuente: Propiedad del autor

Además, es necesario tener claras las respuestas a cada una de las siguientes preguntas:

- “Cantidad de bases de datos con información personal.
- Cantidad de titulares por cada base de datos.
- Información detallada de los canales o medios que se tienen previstos para atender las peticiones y reclamos de los titulares.
- Tipos de datos personales contenidos en cada base de datos a los que se realiza Tratamiento, como: datos de identificación, ubicación, socioeconómicos, sensibles u otros.
- Ubicación de las bases de datos.
- Los datos de identificación y ubicación de los Encargados del tratamiento.
- Medidas de seguridad y/o controles implementados en la base de datos para minimizar los riesgos de un uso no adecuado de los datos personales tratados.
- Conocer si se cuenta con la autorización de los titulares de los datos contenidos en las bases de datos.
- Forma de obtención de los datos (directamente del titular o mediante terceros).
- Si se ha realizado transferencia o transmisión internacional de los datos personales contenidos en la base de datos.
- Si se ha realizado cesión de la base de datos.”[81]

8.1 INSCRIPCION EN EL RNBD

Teniendo resueltas las preguntas anteriores, el paso a seguir es inscribir la empresa en registro RNBD. Antes de hacer el registro del usuario, para tener acceso al sistema del RNBD es necesario que se cuente con la siguiente información:

[81] SIC. Registro nacional de bases de datos. {En línea}. {citado 2 de octubre de 2017} disponible en: http://www.sic.gov.co/registro-nacional-de-bases-de-datos

- Correo electrónico del responsable del tratamiento de datos personales (persona natural, persona jurídica o entidad pública) que tiene inscrito en el Registro Único Tributario RUT.
- Tener el RUT expedido por la plataforma de la DIAN con una vigencia inferior a 3 meses, el cual deberá ser subido al sistema RNBD al momento de hacer el registro inicial del responsable del Tratamiento.
- Saber quién tiene la administración del correo electrónico antes mencionado, ya que le será enviado el usuario y la clave de acceso, además de las notificaciones del proceso del registro de cada base de datos.

Para hacer la inscripción se debe ingresar por el siguiente link: http://www.sic.gov.co/registro-nacional-de-bases-de-datos el cual abrirá una ventana que contendrá unas opciones donde se ubicara la opción INSCRIPCION como se muestra en la figura 4.

Figura 4. Página web para la inscripción al RNBD

Fuente: Propiedad del Autor

Al dar clic en el botón de Inscripción, se abre una ventana que corresponde al siguiente url: https://rnbd.sic.gov.co/sisi/login , la cual tiene las opciones para el acceso (usuario y contraseña), en nuestro caso, se debe dar clic en la opción: Regístrese, como se ve en la figura 5.

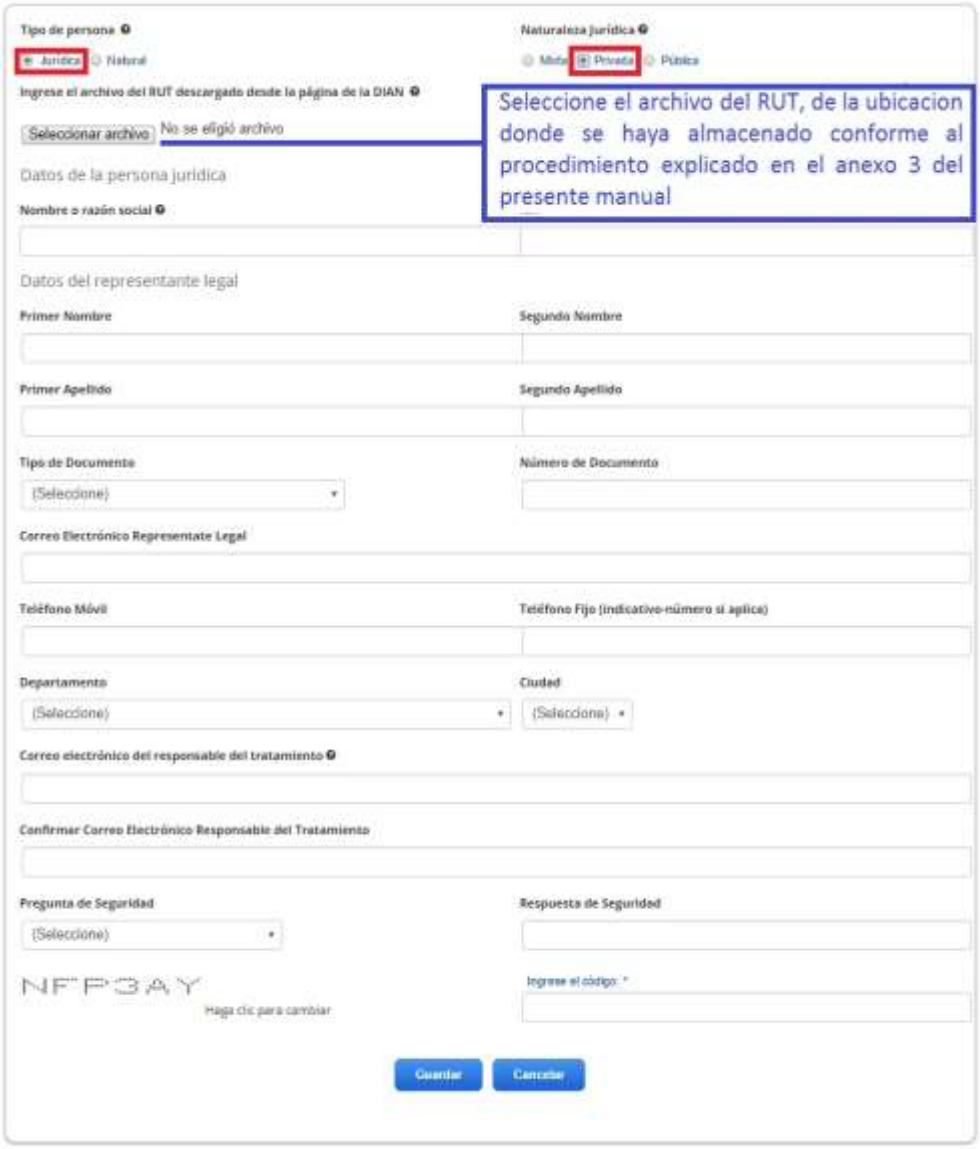
Figura 5. Acceso al RNBD

Fuente: Propiedad del Autor

Después de dar clic en Registrarse, la aplicación visualizara la ventana de la figura 6, en donde aparecen unas opciones de acuerdo al tipo de persona (jurídica o natural), para el caso de seleccionar Persona Jurídica, se debe seleccionar la naturaleza jurídica del responsable, es decir mixta, privada o pública.

La validación de los datos ingresados se hace por medio del RUT, el cual se debe cargar el archivo del RUT descargado directamente de la plataforma MUISCA de la DIAN, tal como se indica en el Anexo 5 Manual de Generación del RUT. Se debe tener en cuenta que en el campo NIT se ingresa sin dígito de verificación.

Figura 6. Formulario de inscripción al RNBD



Fuente: Manual de usuario RNBD

Después de ser validados los datos ingresados con el RUT, el sistema enviara la clave de ingreso al RNBD al correo registrado en el RUT al que se registró como correo electrónico del responsable. Esta clave podrá ser cambiada después del primer ingreso al RNBD.

La contraseña deberá estar conformada por al menos 6 caracteres combinando mayúsculas, minúsculas, letras, números y caracteres especiales (por ejemplo:

punto (.), punto y coma (;), porcentaje (%), pregunta (?), barra diagonal (/), más (+), asterisco (*), entre otros).

Al ingresar por primera vez al sistema, se podrá cambiar el correo electrónico registrado inicialmente con el cual se validó, es decir, que podrá cambiar el nombre del usuario registrado y será al nuevo correo a donde el sistema enviará las notificaciones.

Con la validación finalizada, el usuario ingresa al RNBD, a los módulos de: **Inscripción de bases de datos** y **Administración de usuarios,** como se muestra en la figura 7.

Figura 7. Opciones del RNBD

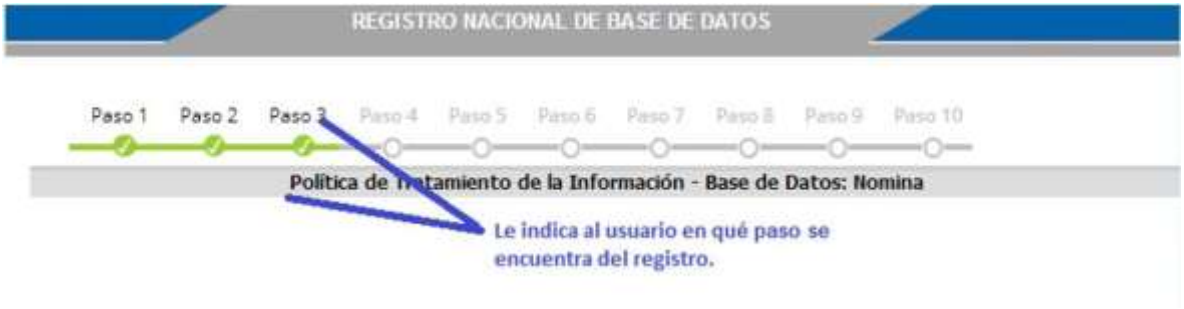
Fuente: Manual de usuario RNBD

El sistema RNBD muestra un menú en la parte superior izquierda los módulos al que se tiene acceso para inscribir las bases de datos. En la parte superior derecha muestra el nombre del usuario que está conectado y la opción de cerrar sesión. La información que se encuentra en la aplicación, podrá ser consultada por el usuario autorizado.

8.2 REGISTRO DE BASES DE DATOS

Por el módulo RNBD Inscripción de Bases de Datos, se ingresa la información de la base de datos a registrar. A medida que se va ingresando la información solicitada, el sistema le mostrará el avance, paso a paso, como se observa en la figura 8.

Figura 8. Avance en el proceso de registro



Fuente: Manual de usuario RNBD

La inscripción de las bases se inicia con el ingreso de los datos del responsable del Tratamiento, de acuerdo con la figura 9 donde se muestra el menú:

Figura 9. Opción Registro – Responsable del tratamiento

Fuente: Manual de usuario RNBD

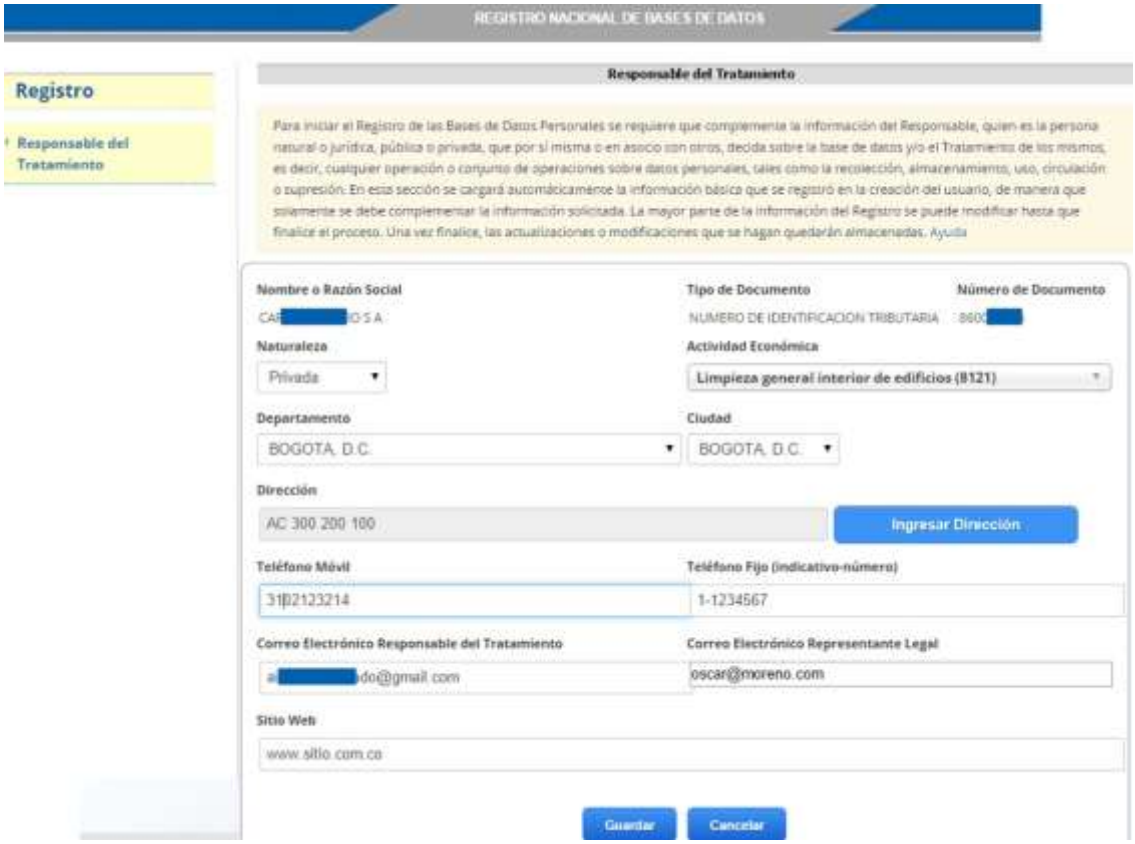
Dando clic en la opción Responsable del Tratamiento, se debe ingresar la información solicitada del Responsable, quien es la persona natural o jurídica que decide sobre la base de datos y/o el Tratamiento de los mismos.

“La información ingresada al sistema se puede modificar hasta antes de finalizar el proceso de inscripción de cada base de datos. Una vez finalizado dicho proceso y la aplicación entregue el número de radicado de la inscripción de la base de datos, se podrán realizar actualizaciones o modificaciones, para ello el sistema conservará el histórico de la información registrada por cada radicado y sólo le permitirá realizar

modificaciones sobre el último radicado. Una vez finalice los cambios se generará un nuevo radicado."[82]

La información solicitada se muestra en la figura 10.

Figura 10. Información del Responsable del tratamiento



Fuente: Manual de usuario RNBD

Después de ser guardada la información relacionada con el Responsable del Tratamiento, se podrá realizar el proceso de **Inscribir Bases de Datos** de acuerdo a la figura 11

[82] Manual de usuario RNBD {En línea}. {citado 2 de octubre de 2017} disponible en: https://rnbd.sic.gov.co/sisiAyuda/

Figura 11. Opción Registro – Inscribir Bases de Datos

Fuente: Manual de usuario RNBD

Aquí se ingresa el número de bases de datos con información personal que se realice tratamiento. Se ingresan de forma independiente cada una y la cantidad se puede aumentar en cualquier momento.

“El sistema no permite disminuir el número de bases de datos si ya se encuentran inscritas o cuyo proceso de inscripción haya iniciado. En caso de que por error inicie el registro de una base de datos, antes de finalizarla estando en el módulo “Inscribir Base de Datos” ingrese por la opción “Borrar Registro”, en caso de que no le aparezca, debe presionar la tecla F5 para refrescar la página, esto hará que pueda visualizar el enlace y así proceder con la eliminación de la Base de Datos que desea. Recuerde que sólo podrá eliminar bases de datos que se encuentren en modificación y no haya finalizado.”[83]

Inicialmente se puede registrar hasta 99 bases de datos, después de esta cantidad, se puede tener un cupo de hasta 10 más y a medida que va finalizando de la 100

[83] Manual de usuario RNBD {En línea}. {citado 2 de octubre de 2017} disponible en: https://rnbd.sic.gov.co/sisiAyuda/

en adelante, se habilita la cantidad de 10. De esta manera, al finalizar la 100, podrá inscribir hasta 110, etc.

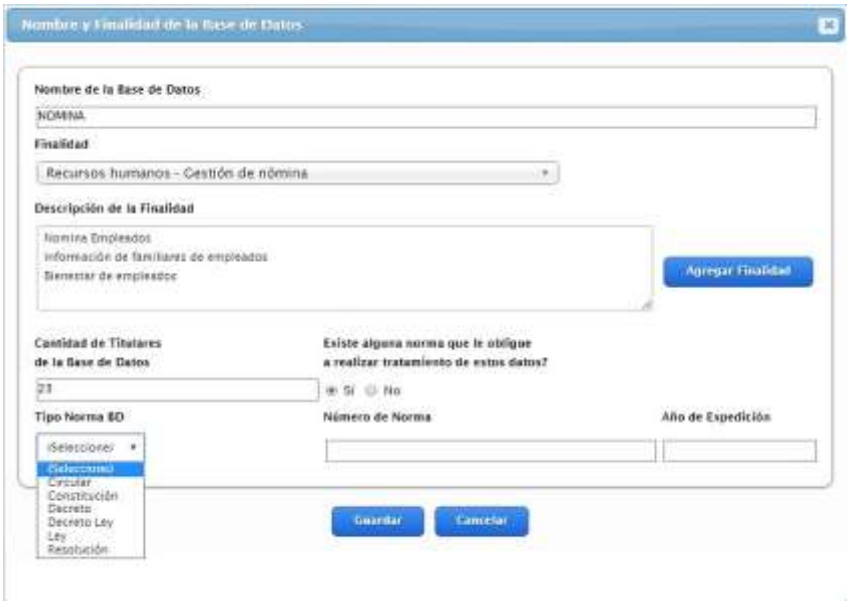
Para registrar una base de datos, se debe editar el registro correspondiente ingresando por la opción **Continuar registro,** como muestra la figura 12.

Figura 12. Inscribir Bases de Datos

Fuente: Manual de usuario RNBD

Dando clic en **Continuar Registro**, la aplicación mostrará el primer formulario para ingresar o modificar el **Nombre** y la **Finalidad** de la base de datos como muestra la figura 13.

Figura 13. Nombre y finalidad de la Base de Datos



Fuente: Manual de usuario RNBD

Nombre de la base de datos: Es el nombre como se llama o se reconoce la base de datos, este nombre es de libre elección.

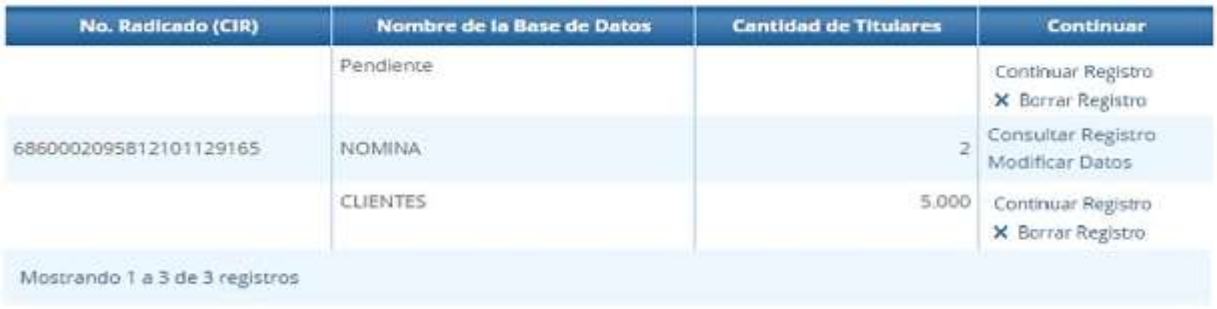
Finalidad: Es por qué o propósito de la recolección los datos personales. Se debe escoger una de las opciones de la lista y complementar con una explicación en el campo **Descripción de la Finalidad**, de acuerdo con la finalidad señalada en la política de tratamiento de datos. Cuando termine de llenar estos dos campos debe hacer clic en el botón **Agregar Finalidad.**

Cantidad de titulares de la base de datos: Es el número de titulares o personas naturales cuyos datos personales están almacenados en la base de datos que se está registrando. No se pueden contar datos de personas o titulares repetidos.

Norma: En caso de que la base de datos se construya por disposición de una norma que así lo exija, se escoge “SI” a la pregunta “¿Existe alguna norma que le obligue a realizar tratamiento de estos datos?”, llenando los siguientes campos: Tipo de norma, Número y Año de expedición de la misma.

Al terminar se da en la Opción **Guardar,** como se muestra en la figura 14.

Figura 14. Pantalla de Base de Datos inscritas

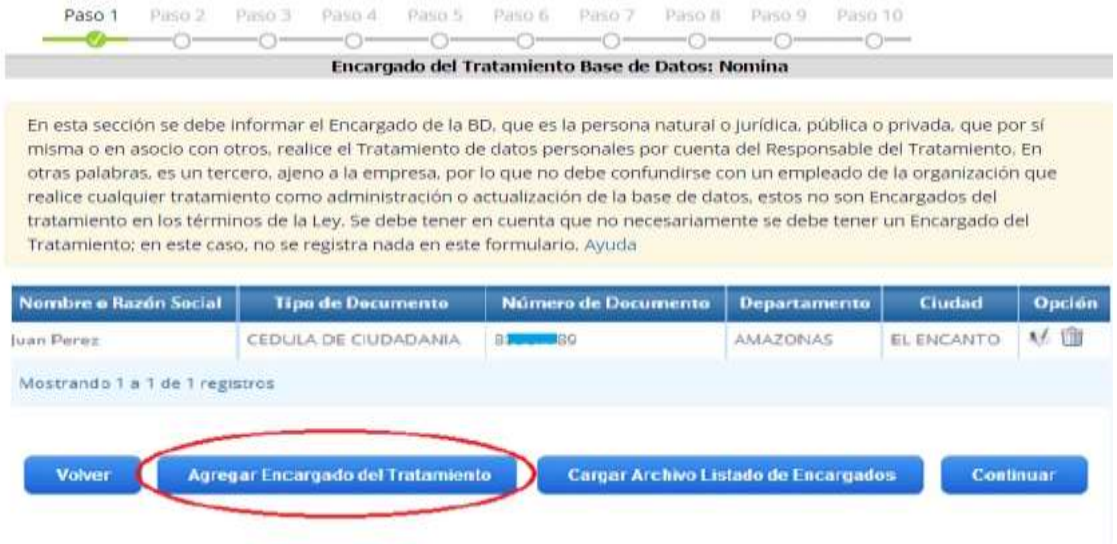


Fuente: Manual de usuario RNBD

Después de finalizado con estos pasos, se muestra el menú completo que conforma el módulo de **RNBD Inscripción de bases de datos** y se iniciara por el paso 1, con la opción **Encargado del Tratamiento**.

En esta parte, se ingresan los datos del **Encargado del Tratamiento**, si se tiene. Si la base de datos **no tiene Encargados**, puede continuar con el siguiente paso. Ver figura 15.

Figura 15. Ingresar encargado



Fuente: Manual de usuario RNBD

Para adicionar un Encargado, se deberá diligenciar los campos de la figura 16.

Los datos solicitados en esta ventana se deben llenar tantas veces como número de Encargados de la base de datos sean. Si se realiza transmisión internacional de datos, se debe escoger la opción “**Tiene domicilio fuera del país**” y diligenciara el formato para tal efecto

Figura 16. Datos del encargado

Fuente: Manual de usuario RNBD

Si se requiere modificar la información registrada, se puede hacer con las opciones **Editar** o **Eliminar** con los íconos respectivos, como se indica en la figura 17.

Figura 17. Editar o eliminar encargados

Fuente: Manual de usuario RNBD

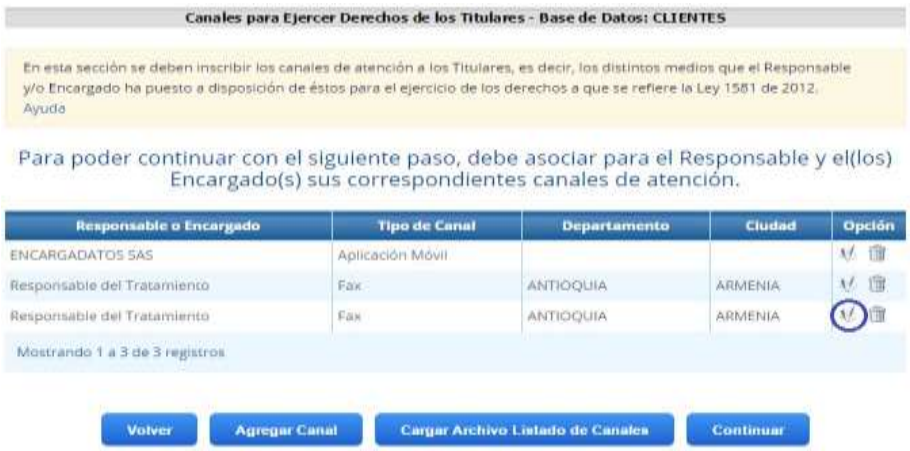
Para seguir con el proceso, se da clic en **Continuar** y para a la inscripción de los **Canales de Atención al Titular,** que son los medios de comunicación que se han dispuesto para atender a los titulares y sus derechos, como se muestra en la figura 18.

Figura 18. Crear canales de atención

Fuente: Manual de usuario RNBD

Si es requerido modificar los **Canales de Atención al Titular** el sistema mostrará la pantalla como aparece en la figura 19, en donde el usuario podrá editar los canales o eliminarlos.

Figura 19. Editar o eliminar canales



Fuente: Manual de usuario RNBD

Finalizado el anterior paso, se inicia con la subida de la **Política de Tratamiento de la Información** de los Responsables y, si cuenta con ella, la de los Encargados, como se visualiza en la figura 20.

Para subir el archivo solo se admiten archivos tipo pdf con un peso máximo de 2 MB.

Figura 20. Cargar la política de tratamiento de información

Fuente: Manual de usuario RNBD

Luego de cargada la Política de tratamiento de la información, se da clic en **Continuar,** para pasar a la **Forma de Tratamiento** de la base de datos, donde se especifica si el tratamiento de los datos se hace de forma manual o automatizado como se muestra en la figura 21.

Figura 21. Forma de tratamiento

Fuente: Manual de usuario RNBD

El usuario deberá ingresar la **Información contenida en la base de datos**, para lo cual se deberá elegir las subcategorías de datos almacenados en la base de datos, las cuales se encuentran agrupadas por categorías de acuerdo **con su naturaleza**, con el fin de facilitar la inscripción de los datos.

La primera categoría de datos es obligatoria, es decir que se debe indicar si la base contiene datos de personas mayores y/o menores de 18 años, como muestra la figura 22.

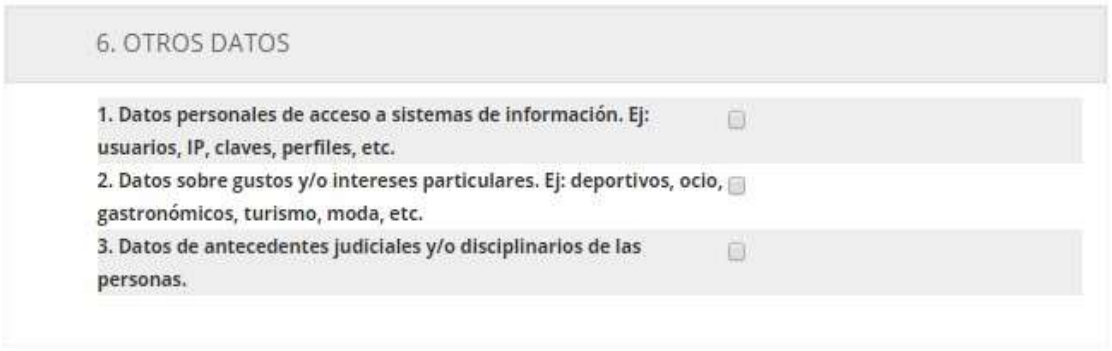
Figura 22. Información contenida en la base de datos

4. DATOS SENSIBLES

1. Datos relacionados con la salud de la persona en cuanto a órdenes y relación de pruebas complementarias como laboratorio, imagen, endoscópicas, patológicas, estudios, etc. ESTA SUBCATEGORÍA NO INCLUYE RESULTADOS NI DIAGNÓSTICOS.	☐
2. Datos relacionados con el estado de salud de la persona, que incluyen resultados de pruebas, laboratorios, estudios, diagnósticos médicos, generales o especializados, psicológicos o psiquiátricos, medicamentos y/o tratamientos médicos o terapéuticos de cualquier tipo, etc.	☐
3. Datos relacionados con la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, religiosas, políticas	☐
4. Datos de preferencia, identidad y orientación sexual de la persona, origen étnico-racial, etc.	☐
5. Población en condición vulnerable. Ej: personas de la tercera edad o menores de 18 años en condición de pobreza, personas con limitaciones sicomotoras, auditivas y visuales en condiciones de pobreza, personas víctimas de la violencia, personas en situación de desplazamiento forzado por violencia, madres gestantes o lactantes o cabeza de familia en situación de vulnerabilidad, menores en condición de abandono o protección, etc.	☐
6. Datos sobre personas en situación de discapacidad	☐

5. DATOS DE CONTENIDO SOCIOECONÓMICO

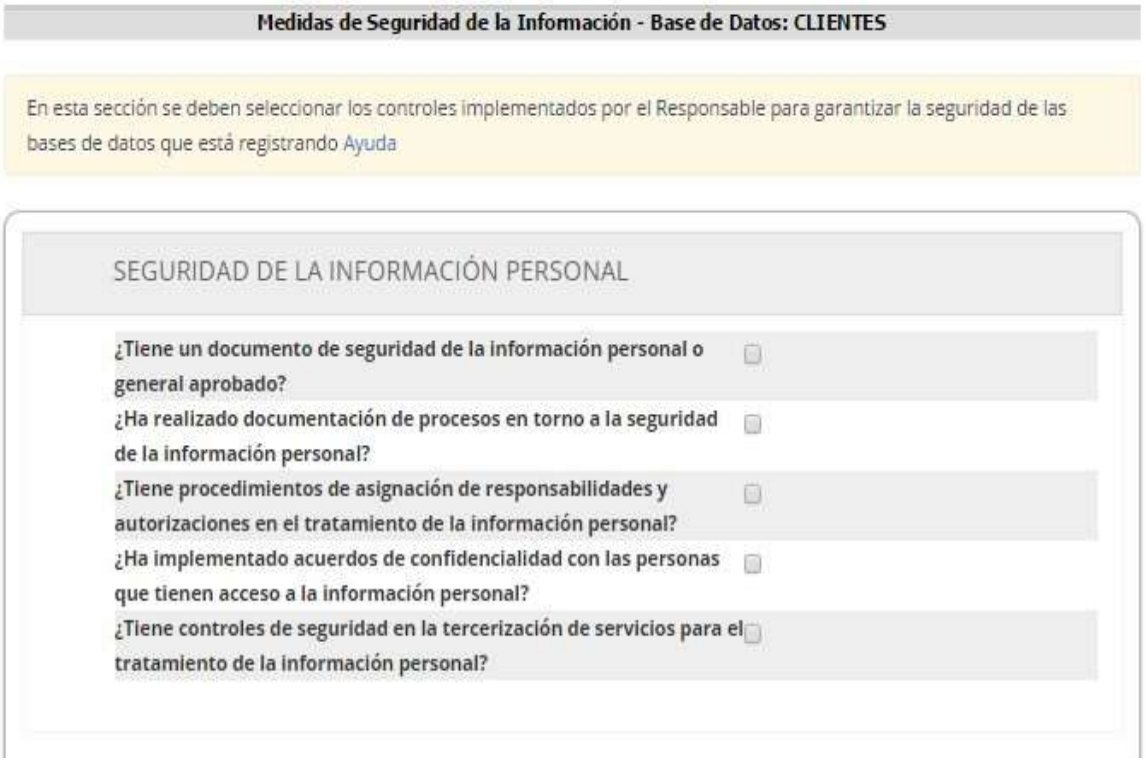
1. Datos financieros, crediticios y/o derechos de carácter económico de las personas.	☐
2. Datos socioeconómicos como estrato, propiedad de la vivienda, etc.	☐
3. Datos de información tributaria de la persona	☐
4. Datos patrimoniales de la persona. Ej: bienes muebles e inmuebles, ingresos, egresos, inversiones, etc.	☐
5. Datos relacionados con la actividad económica de la persona	☐
6. Datos relacionados con la historia laboral de la persona, experiencia laboral, cargo, fechas de ingreso y retiro, anotaciones, llamados de atención, etc.	☐
7. Datos relacionados con el nivel educativo, capacitación y/o historial académico de la persona, etc.	☐
8. Datos generales relacionados con afiliación y aportes al Sistema Integral de Seguridad Social. Ej: EPS, IPS, ARL, fechas de ingreso/retiro EPS, AFP, etc.	☐



Fuente: Manual de usuario RNBD

Terminado este punto y se de en guardar la información, se da clic en **Continuar y** la aplicación mostrará el paso 6, **Medidas de Seguridad de la Información,** en donde el usuario debe escoger los controles implementados por el Responsable del Tratamiento para garantizar la seguridad de la base de datos, si no se tienen controles realizados se deja en blanco. Ver figura 23.

Figura 23. Información de Medidas de seguridad de la información



SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

- ¿Tiene implementadas herramientas de gestión de riesgos en el tratamiento de datos personales? ☐
- ¿Tiene implementado un sistema de gestión de seguridad de la información o un programa integral de gestión de datos personales? ☐

SEGURIDAD DE LA INFORMACIÓN PERSONAL EN TORNO AL RECURSO HUMANO

- ¿Tiene implementados controles de seguridad de la información personal para el Recurso Humano antes de la vinculación y una vez finalizado el contrato laboral? ☐

CONTROL DE ACCESO A LA INFORMACIÓN PERSONAL

- ¿Tiene una política de control de acceso a la información personal, tanto en las instalaciones físicas como a nivel tecnológico? ☐
- ¿Cuenta con un procedimiento para la Gestión de usuarios con acceso a la información personal? ☐
- ¿Ha implementado una política específica para el acceso a la información personal de las bases de datos con información personal sensible? ☐
- ¿Tiene una política implementada de copia de respaldo de la información personal? ☐
- ¿Ha implementado una política de protección para el acceso remoto a la información personal? ☐

PROCESAMIENTO DE INFORMACIÓN PERSONAL

- ¿Cuenta con una política implementada para el correcto tratamiento de la información personal en las diferentes etapas del ciclo de vida del dato (recolección, circulación y disposición final)? ☐
- ¿Cuenta con un procedimiento implementado para la validación de datos de entrada y procesamiento de la información personal, para garantizar que los datos recolectados y procesados sean correctos y apropiados, como confirmación de tipos, formatos, longitudes, pertinencia, cantidad, uso, etc.? ☐
- ¿Cuenta con un control de seguridad de información para la validación de datos de salida? ☐
- ¿Cuenta con una política implementada para el intercambio físico o electrónico de datos (como por ejemplo durante el comercio electrónico para la compra y venta de productos o servicios), transporte y/o almacenamiento de información personal? ☐
- ¿Tiene un procedimiento o control implementado para la disposición final de la información personal (supresión, archivo, destrucción, etc.)? ☐

Fuente: Manual de usuario RNBD

Al guardar y dar clic en **Continuar,** el sistema pasa al punto 7, **Autorización del Titular.**

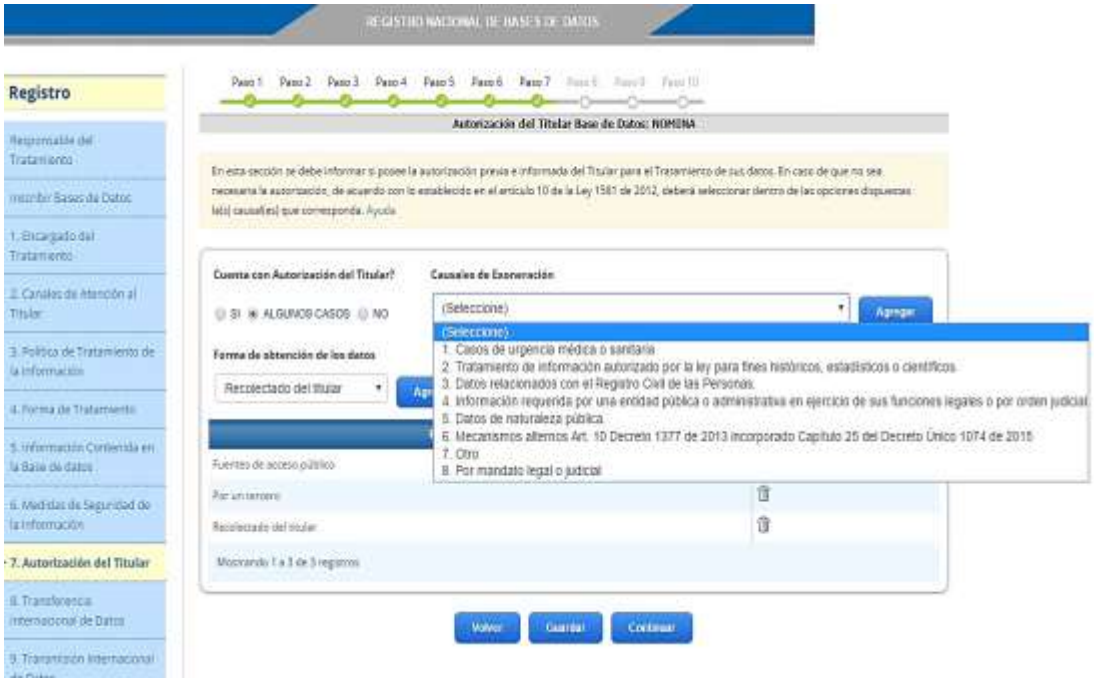
Se debe contestar **SI** se cuenta con las autorizaciones, si **No** se cuentan o Si se cuenta con autorización de los titulares en **Algunos Casos**, como se muestra en la la figura 24.

Figura 24. Autorización de titulares

Fuente: Manual de usuario RNBD

En caso de elegir (ALGUNOS CASOS/NO), se presenta el campo **Causales de Exoneración** como lo muestra la figura 25.

Figura 25. Causas de no tener Autorización del titular



Fuente: Manual de usuario RNBD

Se debe escoger la forma como se han obtenido los datos. Posterior al ingreso de los datos, se da clic en el botón **Agregar** con el fin de ver reflejados los datos en la Sección **Forma de Obtención de los datos.**
En caso de tener más de una forma de obtener los datos puede seleccionar otra opción de la lista y hacer clic nuevamente en el botón **Agregar.**

De esta forma vamos al con clic en **Continuar y** el sistema nos abre el paso 8 **Transferencia Internacional de Datos.**

En caso de realizar transferencia internacional de datos personales se deben agregar con el botón **Agregar Destinatario** y llenar los datos. De esta forma damos clic en el botón **Guardar,** de lo contrario debe hacer clic en el botón **Continuar.** Ver figura 26.

Figura 26. Transferencia Internacional de Datos

Fuente: Manual de usuario RNBD

Seguidamente, al dar clic en **Continuar**, la aplicación muestra el paso 9 **Transmisión Internacional de Datos** como muestra la figura 27.

Figura 27. Transmisión Internacional de Datos

Fuente: Manual de usuario RNBD

"En caso de que la transmisión se exceptúe de la prohibición de acuerdo con las causales contempladas en la norma podrá seleccionar una de ellas en el campo para ello dispuesto. De lo contrario podrá seleccionar si tiene contrato de transmisión, de no contar con este, se le preguntará por la declaración de conformidad, en caso de no contar con ninguno de estos requisitos aparecerá una advertencia sobre el riesgo en materia de protección de datos, para que solicite la declaración de Conformidad ante la Superintendencia de Industria y Comercio."[84]

Al **guarda** la información y dar clic en **Continuar**, la aplicación muestra el paso **10 Finalizar Registro de información**.

Al dar clic en Finalizar Registro, el sistema creara el número de radicación del registro de la base de datos, como aparece en la figura 28.

Figura 28. Finalización del registro de su base de datos

Fuente: Manual de usuario RNBD

[84] Ibid.

Si se está completamente seguro de finalizar la inscripción, clic en el botón "**Finalizar Registro**", de lo contrario, se puede devolverse para hacer modificaciones.

RECOMENDACIONES

Se recomienda recopilar la mayor cantidad de información relacionada con la empresa, estructura tecnológica y de procesos antes de iniciar con el proceso de registro RNBD.

Para la implementación de la Ley 1581 de protección de datos personales en las empresas, se recomienda que se haga un plan de trabajo basado en un cronograma que permita avanzar de manera significativa en todas las fases, pero hacerlo de forma secuencial de acuerdo a este modelo y basado en el principio de la responsabilidad demostrada.

No se recomienda hacer un registro RNBD a la carrera, sin contar con la documentación inicial y flujo de los datos en todo el proceso, ya que esto puede generar inconvenientes y reprocesos que, a la final, generaría malestar y una mala comunicación con la SIC, inclusive sanciones.

Dado que el vencimiento para el registro RNBD es enero de 2018, no significa que las empresas no deban estar cumpliendo con la Ley desde sus inicios. Se recomienda que las empresas que no han desarrollado este proceso, lo hagan de manera sistemática y a conciencia, de manera que se refleje en el registro la realidad de su organización.

Es importante recordar que la Ley establece unas fechas de actualización del registro que deben cumplirse para estar cumpliendo con exigencias de la norma.

Además, se deben revisar con detenimiento los riesgos y problemas de seguridad que den cabida a malos manejos e incidentes que puedan generar un llamado de atención por parte de los titulares y la SIC.

Si la organización no tiene el tiempo o las personas indicadas para realizar el registro y la implementación del sistema de gestión de protección de datos, se

recomienda contratar empresas especialistas en seguridad informática y protección de datos que puedan dirigir de una forma correcta las actividades y se genere una información confiable y de valor para la empresa que le permita continuar con su labor y responsabilidad de demostrar el cumplimiento ante el ente de control.

CONCLUSIONES

El proyecto presenta el modelo para la implementación de la Ley de protección de datos personales 1581 basado en el SGSI de la norma iso 27001, el cual aporta una guía para que las PYMES en Colombia logren reconocer el estado de la organización frente al cumplimiento de la norma y cumplir con el registro RNBD ante la SIC de forma correcta, siguiendo con el proceso de gestión protección de datos y seguridad de la información.

Aunque la implementación de la Ley de protección de datos personales en las empresas es un proceso que demanda tiempo, organización y recursos, una de las pautas iniciales es la identificación y clasificación de los datos, que si se hace de manera correcta y siguiendo esta guía se puede lograr y desarrollar de la mejor manera.

Las empresas que sigan las pautas dadas en este modelo podrán prepararse para el cumplimiento de la norma y de esta manera contar con la documentación básica requerida para tratamiento y correcta comunicación con el titular dueño de los datos, además de identificar sus problemas de seguridad, riesgos y vulnerabilidades que le permitan seguir con un plan de mejoramiento para salvaguardar el activo más preciado que tienen “la información y los datos”.

Es importante entender que más que una Ley que puede verse como impositiva y el registro RNBD un formalismo más, es tomar esta norma como una oportunidad para mejorar nuestros niveles de protección y seguridad de la información, que incluya procesos de concientización al personal y logre en la organización tener un estándar más alto que permita conservar la confianza de sus clientes y generar para sus propietarios los frutos de rentabilidad y productividad deseados.

Al seguir esta guía como está planteada, se podrá cumplir de forma correcta con el registro RNBD de las bases de datos ante la SIC, además de tener el conocimiento real de su organización a nivel de bases datos, tipos de datos, procedimientos y

seguridad de la información, permitirá a colaboradores y personal en general tener una cultura de protección y concientización sobre el cuidad por los datos personales, logran tener un país más responsable, productivo y de altos niveles de seguridad y confianza.

BIBLIOGRÁFIA

CUARTAS RODRIGUEZ, Eliseo. EL HABEAS DATA COMO DERECHO FUNDAMENTAL Y LA LEY 1581 DE 2012 Y SU DECRETO 1377 DE 2013. Universidad EAFIT, Escuela de derecho. Medellín, Colombia Julio de 2014.

ECHEVERRY, Juan Sebastián. METODOLOGÍA PARA EL DIAGNÓSTICO CONTINUO DE LA SEGURIDAD INFORMÁTICA DE LA RED DE DATOS DE LA UNIVERSIDAD MILITAR NUEVA GRANADA. Universidad Militar Nueva Granada. Bogotá, Colombia mayo 2009.

PRESIDENCIA DE LA REPUBLICA. GUÍA PARA LA CALIFICACIÓN DE LA INFORMACIÓN DE ACUERDO CON SUS NIVELES DE SEGURIDAD. Versión 6. Bogotá marzo de 2017

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método. Madrid, España octubre de 2012.

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos. Madrid, España octubre de 2012.

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III – Guía de técnicas. Madrid, España octubre de 2012.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Modelo de Seguridad y Privacidad de la Información. Bogotá, Colombia (s.f).

OIDOR GONZALEZ, Juan Carlos. DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI BAJO LA NORMA ISO/IEC 27001:2013 PARA LA EMPRESA “EN LÍNEA FINANCIERA”. Universidad Nacional Abierta y a Distancia. Popayán, Colombia diciembre de 2016.

SUAREZ SIERRA, Lorena. SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION SGSI. Universidad Nacional Abierta y a Distancia. Bogotá, Colombia julio de 2013.

WEBGRÁFIA

AGENCIA EFE. El Heraldo. Colombia pierde 5700 millones de dólares. {En línea}. {25 de mayo de 2017} disponible en: https://www.elheraldo.co/economia/ciberataques-en-colombia-dejan-perdidas-por-5700-millones-de-dolares-277787

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía del responsable de ficheros. {En línea}. {25 de mayo de 2017} disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf

ÁMBITO JURÍDICO. ¿Por qué se amplió el plazo para inscribir bases de datos en el registro nacional? {En línea}. {26 de mayo de 2017} disponible en: https://www.ambitojuridico.com/bancoconocimiento/mercantil-propiedad-intelectual-y-arbitraje/por-que-se-amplio-el-plazo-para-inscribir-bases-de-datos-en-el-registro-nacional

BALANTA, Heidy. Retos de los programas de protección de datos personales en Colombia. {En línea}. {10 de noviembre de 2017} disponible en: https://colombiadigital.net/opinion/columnistas/derecho-y-economia-digital/item/9578-retos-de-los-programas-de-proteccion-de-datos-personales-en-colombia.html

CARACOL RADIO. Multas por violación a ley de datos ascienden a 19.000 millones de pesos. {En línea}. {26 de mayo de 2017} disponible en: http://caracol.com.co/radio/2017/01/27/economia/1485540887_417956.html

CERTICÁMARA. ABC para proteger los datos personales, Ley 1581 de 2012 Decreto 1377 de 2013. {En línea}. {26 de mayo de 2017} disponible en: https://colombiadigital.net/actualidad/articulos-informativos/item/5543-abc-para-proteger-los-datos-personales-ley-1581-de-2012-decreto-1377-de-2013.html

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1266. Bogotá. (diciembre 31 de 2008). Diario Oficial 47219 de diciembre 31 de 2008. {En línea}. {31 de diciembre de 2017} disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488

COLOMBIA, CONGRESO DE LA REPUBLICA. Decreto 1377 de 2013. Bogotá. (junio 277 de 2013). Diario Oficial 48834 de junio 27 de 2013. {En línea}. {25 de mayo de 2017} disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley estatutaria 1581 de 2012. Bogotá. (octubre 17 de 2012). Diario Oficial 48587 de octubre 18 de 2012. {En línea}. {25 de mayo de 2017} disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

COLOMBIA, CONGRESO DE LA REPUBLICA. Decreto 1759 de 2016. Bogotá. (noviembre 9 de 2016). Diario Oficial 48834 de noviembre 9 de 2016. {En línea}. {25 de mayo de 2017} disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=62508

COLPRENSA. Hay 602 empresas sancionadas por violar la ley de protección de datos. {En línea}. {25 de mayo de 2017} disponible en: http://www.laopinion.com.co/economia/hay-602-empresas-sancionadas-por-violar-la-ley-de-proteccion-de-datos-127060

CONSTITUCIÓN POLÍTICA DE COLOMBIA. ¿Qué es la Constitución Política? {En línea}. {26 de mayo de 2017} disponible en: http://www.constitucioncolombia.com/historia.php

GARCIA, Laura. Metodología OSSTMM. {En línea}. {26 de mayo de 2017} disponible en: http://www.securitybydefault.com/2010/03/metodologia-osstmm.html

ISO 27000. El portal de ISO 27001 en español. {En línea}. {26 de mayo de 2017} disponible en: http://www.iso27000.es/sgsi.html#home

ITECH SAS. Responsabilidad Demostrada. {En línea}. {26 de mayo de 2017} disponible en: http://www.itechsas.com/blog/ley-1581-protecion-de-datos/responsabilidad/

MENDOZA, Miguel Ángel. Importancia de la protección de los datos. {En línea}. {25 de mayo de 2017} disponible en: http://www.welivesecurity.com/la-es/2015/10/16/importancia-datos-personales-proteccion/

OSPINA, Natalia. Protección de Datos Personales en Colombia: el camino que falta recorrer. {En línea}. {25 de mayo de 2017} disponible en: http://blogs.portafolio.co/abogado-tic/2016/12/01/proteccion-datos-personales-colombia-camino-falta-recorrer/

PAE, Portal de administración electrónica. MAGERIT. {En línea}. {26 de mayo de 2017} disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WSJBdWg1_IU

ROZO, Catalina. Que debes conocer de la ley 1581. {En línea}. {25 de mayo de 2017} disponible en: https://www.securityartwork.es/2015/06/10/que-debes-conocer-de-la-ley-1581-de-proteccion-de-datos-personales-colombiana/

SIC. Guía para la Implementación del Principio de Responsabilidad Demostrada. {En línea}. {26 de mayo de 2017} disponible en: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Guia-SIC-Accountability-28V2015.pdf

SIC. Protección de datos. Gobierno amplía hasta el 30 de junio de 2017 el plazo para que las empresas registren sus bases de datos. {En línea}. {25 de mayo de 2017} disponible en: http://www.sic.gov.co/noticias/gobierno-amplia-hasta-el-30-de-junio-de-2017-el-plazo-para-que-las-empresas-registren-sus-bases-de-datos

SIC. Súper intendencia de industria y comercio. Protección de datos personales. {En línea}. {25 de mayo de 2017} disponible en: http://www.sic.gov.co/proteccion-de-datos-personales

VEGA SUÁREZ, Ana Maritza. El cumplimiento de la normativa de protección de datos en Iberoamérica. {En línea}. {25 de mayo de 2017} disponible en: http://www.abogacia.es/2013/11/11/el-cumplimiento-de-la-normativa-de-proteccion-de-datos-en-iberoamerica/

ANEXOS

ANEXO A. Formato de autorización y tratamiento de datos personales

FORMATO PARA AUTORIZACIÓN Y TRATAMIENTO DE DATOS PERSONALES

Conforme a la ley 1581 de 2012 y demás Decretos reglamentarios, autorizo a la empresa XXXXXXXXXXXXXXXXXXXXXXX. para el tratamiento y manejo de mis datos personales el cual consiste en recolectar, almacenar, depurar, usar, analizar, circular, actualizar, con el fin de contactarlo para la gestión comercial de bienes y prestación de servicios. Los datos personales que serán sometidos a tratamiento son:

DATOS PERSONALES DEL TITULAR DE LA INFORMACIÓN				
Nombre completo y/o Razón Social				
No. Identificación				
Dirección de correspondencia				
Teléfonos				
Correo electrónico				
Tipo de relación	[ ] Cliente	[ ] Proveedor	[ ] Otro	

Declaro que soy responsable de la veracidad de los datos suministrados. Así mismo autorizo a la empresa XXXXXXXXXXXXXXXXXXXXXXXX a efectuar sus procedimientos de notificación y comunicación a la dirección de correspondencia y/o correo electrónico antes mencionados. Declaro que he sido informado que la empresa XXXXXXXXXXXXXXXXXXXXXXXX. es responsable de los datos personales obtenidos a través de sus distintos canales de comunicación.
Mis derechos como titular de los datos son los previstos en la constitución y la ley, especialmente el derecho a conocer, actualizar, rectificar y suprimir mi información personal; así como el derecho a revocar el consentimiento otorgado para el tratamiento de datos personales. Estos los puedo ejercer a través de los canales dispuestos por la empresa XXXXXXXXXXXXXXXXXXXXXXXX para la atención al público y observando la política de tratamiento de datos personales en nuestra página web: **www.empresa.com**.,el correo electrónico **protecciondatos@empresa.com** y las oficinas de atención al cliente en la Calle 3 # 3-33, Cali, Valle.

Atentamente,

NOMBRE Y FIMRA DEL TITULAR: _____

FECHA DE DILIGENCIAMIENTO: _____

Anexo B. Formato de política de tratamiento de información

POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

Razón social: **EMPRESA**.	Nit: 900888000 - 0
Dirección: Calle 3 # 3-33, Cali, Valle	Teléfono: (57) +2 4886022
Correo electrónico: protecciondatos@empresa.com	Página web: www. empresa.com

En cumplimiento de la Ley 1581 de 2012, por la cual se dictan disposiciones para la protección de datos personales, LA **EMPRESA**, en su calidad de responsable del tratamiento de datos personales de sus socios, clientes, colaboradores, contratistas y/o proveedores, entendiendo estos como personas naturales, sujetos de los derechos que otorga la normatividad vigente en materia de protección de datos, se compromete a garantizar en todo momento la seguridad de sus datos personales.

De acuerdo a lo contemplado en la normatividad vigente y aplicable en materia de protección de datos, LA **EMPRESA** se compromete a dar el tratamiento adecuado a todos y cada uno de los datos personales que le sean entregados y que a su vez son incorporados en nuestras bases de datos y/o archivos con las finalidades específicas para lo cual fueron dados.

LA EMPRESA siguiendo los requerimientos del artículo 9 de la ley 1581 de 2012 y articulo 4 y 5 del decreto 1377 de 2013, solicita su autorización previa para hacer uso de manera responsable del tratamiento (Art. 17 Ley 1581/2012) de los datos suministrados por usted, que han sido incluidos en las bases de datos y archivos de nuestra empresa.

FINALIDADES DEL TRATAMIENTO DE DATOS

El tratamiento de los datos personales de los Titulares que maneje la empresa se hará conforme a lo dispuesto por la Constitución Política de Colombia y a los contemplados por la ley 1581 de protección de datos personales. Así mismo, se someterá estrictamente a las finalidades descritas por el objeto social de la empresa, y concretamente para:

1. Facilitar los fines comerciales, corporativos, laborales, tributarios y contables de la empresa.

2. Realizar los fines de mercadeo y publicidad con el propósito de ofrecer nuevos productos o servicios de la empresa, lo que incluye el mantenimiento, actualización y custodia de la base de datos de clientes, empleados, ex empleados, contratistas y proveedores de la firma.
3. Cumplir con los procesos administrativos internos para el manejo de contratistas y proveedores de la empresa, y demás fines operativos de la misma.
4. Cumplir con la prestación de los servicios contratados por los clientes de la empresa enmarcados en el objeto social y de acuerdo a las solicitudes y necesidades de los clientes.
5. Cumplir con las demás finalidades que permitan el desarrollo de las actividades, funciones y operaciones comprendidas dentro del objeto social de la Firma y las otorgadas por la ley.
6. Envío de comunicaciones comerciales y publicitarias por cualquiera de los medios que se relacionan a continuación, tales como correo electrónico, SMS, MMS, REDES SOCIALES o cualquier otro medio electrónico o físico conocido en el presente o futuro.
7. Informar sobre cambios en las políticas de tratamiento de la información.
8. Tramitar encargos, solicitudes o cualquier tipo de petición que sea realizada por el titular de la información de carácter personal a través de cualquiera de las formas de contacto que se ponen a disposición del usuario en el sitio web de la compañía o donde ésta determine.
9. Enviar boletines informativos.
10. Elaborar estudios estadísticos.

DERECHOS Y DEBERES DE LOS TITULARES

El Titular de los Datos Personales tendrá los siguientes derechos:

a) Conocer, actualizar y rectificar los Datos Personales.
b) Solicitar pruebas de la autorización otorgada.
c) Ser informado, previa solicitud, respecto del uso que le ha dado a sus Datos personales.
d) Presentar consultas ante el Responsable o Encargado del Tratamiento.
e) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen, una vez haya agotado el trámite de consulta o reclamo ante el Responsable o el Encargado del tratamiento, según el Artículo 16 del Decreto 1377.

f) Acceder de manera gratuita a los Datos Personales que son objeto de Tratamiento.

El Titular de los Datos Personales debe mantener actualizada su información y garantizar, en todo momento, la veracidad de la misma. LA EMPRESA no se hará responsable, en ningún caso, por cualquier tipo de responsabilidad derivada por la inexactitud de la información suministrada por el Titular.

Los Titulares de la Información pueden ejercer sus derechos de revocar la autorización para el tratamiento de datos, conocer, actualizar, rectificar y suprimir sus Datos Personales, enviando correo electrónico a **protecciondatos@empresa.com** o si lo prefiere dirigir una comunicación escrita a la dirección **Calle 3 # 3-33, Cali, Valle** que el responsable de atender procesos de datos personales u oficial de protección de datos personales atenderá.

Los Titulares de los datos Personales, podrán solicitar la actualización, rectificación o la supresión total o parcial de datos. Igualmente, podrán solicitar la revocatoria de la autorización. La solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el Titular tenga un deber legal, contractual o comercial de permanecer en la base de datos. De acuerdo con el Artículo 16 del Decreto 1377, el Titular o causahabiente sólo podrá elevar queja ante la Superintendencia de Industria y Comercio una vez haya agotado el trámite de consulta o reclamo ante el Responsable o el Encargado del tratamiento.

La presente política aplica a partir del día 27 de octubre de 2017 y la información suministrada por los grupos de interés permanecerá almacenada durante el tiempo que sea razonable y necesario, a partir de la fecha del último Tratamiento, de acuerdo con las finalidades que justificaron dicho tratamiento y atendiendo a las disposiciones aplicables a la materia de que se trate y a los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información que debe cumplir la empresa.

Esta política podrá ser modificada en cualquier momento y de forma unilateral por parte de LA EMPRESA.

Oficial de Protección de Datos
Versión 1.0

Anexo C. Formato de encuesta para identificar Políticas seguridad

Empresa:		**Nº**		
Proceso	Seguridad de la Información			
Objetivo de Control	Seguridad de la Información a nivel general			
Cuestionario				
Pregunta		**SI**	**NO**	**N/A**
¿Existe algún archivo de tipo Log donde guarde información referida a las operaciones que realiza la Base de datos?				
¿Se lleva a cabo una comprobación, para verificar que los cambios efectuados son los solicitados por el interesado?				
¿Se documentan los cambios efectuados?				
¿Hay algún procedimiento para dar de alta a un usuario?				
¿Hay algún procedimiento para dar de baja a un usuario?				
¿Existe algún plan de contingencia ante alguna situación no deseada en la Base de Datos?				
¿Se cuenta con un inventario de todos los equipos que integran el centro de cómputo?				
¿Con cuanta frecuencia se revisa el inventario?				
¿Se posee de bitácoras de fallas detectadas en los equipos?				
¿Se cuenta con procedimientos definidos para la adquisición de nuevos equipos?				
¿Se cuenta con procedimientos definidos para el respaldo de la información?				
¿Existen metodologías de clasificación de información?				
¿Se realizan respaldos de información periódicamente?				
¿Cuenta con una política de seguridad?				
¿Cuenta con una política de privacidad y tratamiento de datos?				
Documentos probatorios presentados:				
TOTAL				

Anexo D. Manual de Generación del RUT

Esta guía paso a paso le ayudará a expedir una copia del RUT de la plataforma DIAN:

Advertencia: Debe contar con clave Muisca para iniciar el proceso de generación del RUT y el archivo no debe superar los tres (3) meses de haber sido descargado.

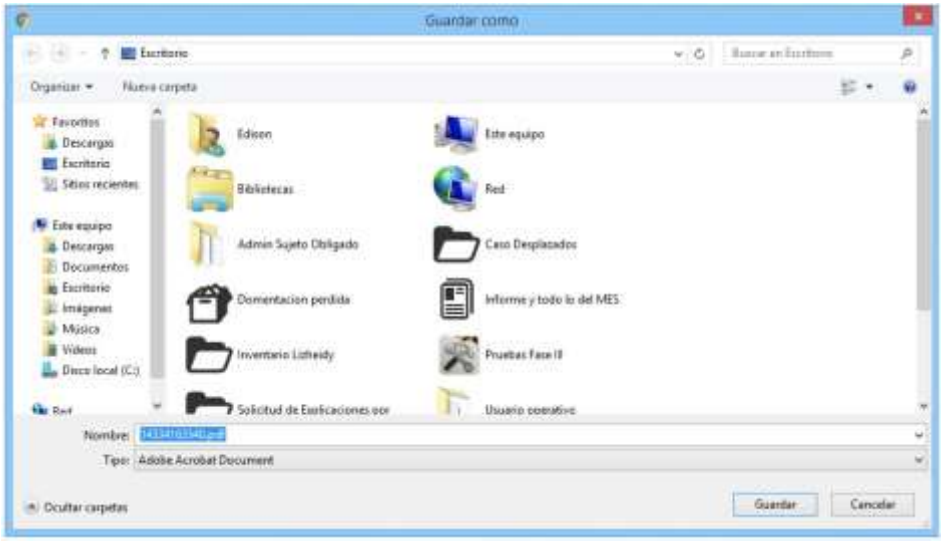
1. **Si cuenta con clave Muisca siga los pasos que se relacionan a continuación:**

    a) Ingrese en el navegador el enlace www.dian.gov.co página Oficial de la DIAN
    b) Seleccione el módulo “Usuarios Registrados” como lo indica la imagen:

    c) En la siguiente sección lo enviará al formulario de “Servicios en línea Muisca” donde podrá iniciar sesión de su cuenta según su tipo de naturaleza ingresando y seleccionando la información correspondiente; al final oprima el botón “Ingresar”.

d) Una vez haya iniciado sesión en la cuenta solo debe seleccionar la opción
"obtener copia RUT" para guardar el archivo en pdf.

e) Dependiendo de cómo tenga configurado su navegador, al darle click puede descargar el archivo directamente a descargas o abrir una ventana para que ingrese la ruta o sitio donde se quiere descargar el archivo, el cual debe guardar sin clave o contraseña de lectura.



2. Si no recuerda la clave Muisca siga los siguientes pasos para obtener la Clave y luego realice el proceso descrito en el punto anterior:

a) Ingrese en el navegador el enlace www.dian.gov.co página Oficial de la DIAN

b) Seleccione el módulo “Usuarios Registrados” y seleccione el hipervínculo “Ha olvidado su contraseña?” como lo indica la imagen:

c) Posteriormente seleccione el tipo y número de documento según corresponda y dé click en el botón “Recuperar Contraseña” esta función le

enviará al correo que tiene registrado en el RUT la nueva contraseña para ingresar al sistema y proceder conforme al procedimiento inicial para descargar la copia del RUT.

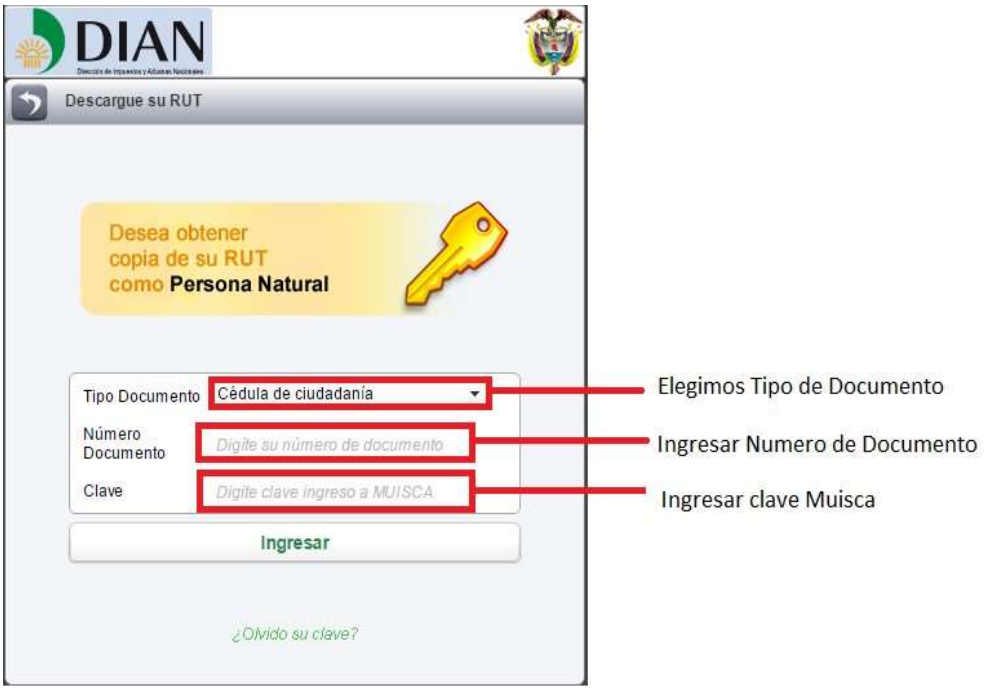
Método Alternativo

a) En el navegador escriba el enlace www.dian.gov.co “pagina Oficial de la DIAN

b) Se selecciona el módulo “En 2 pasos copia del RUT” y se da click.

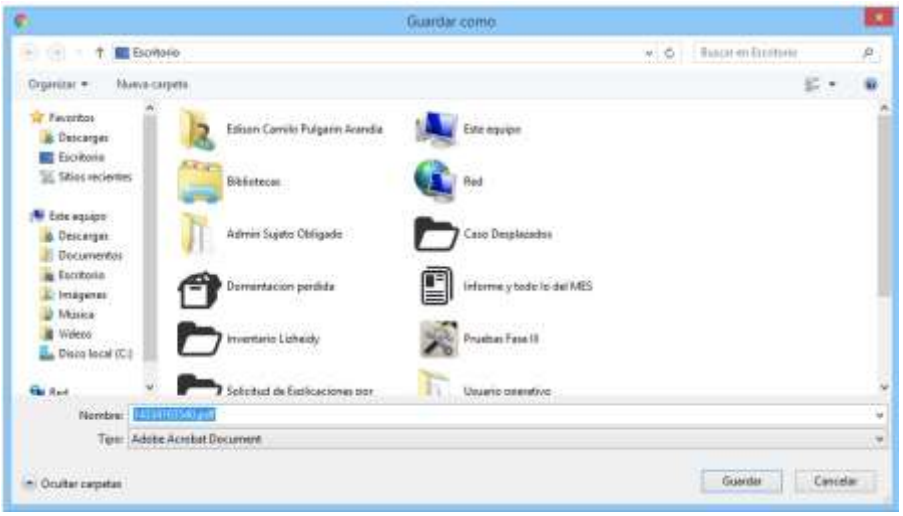
c) El sistema arroja una ventana en la que se debe seleccionar la opción dependiendo si es Persona Natural o es Persona Jurídica.

d) Después de haber seleccionado el tipo de persona, el sistema arroja una ventana en la cual se debe seleccionar el tipo de documento y en los cuadros de texto se ingresa el Número de documento y clave. Para poder dar click en el botón “Ingresar” y seguir el proceso.



e) Finalmente, el sistema muestra una ventana con el botón “Descargue su RUT” al darle click abre la ventana para dar la ruta o sitio donde se quiere descargar, el cual debe guardar sin clave o contraseña de lectura.

Imagen de ventana de descarga



2. Si no cuenta con clave Muisca siga los siguientes pasos para obtener la Clave y luego realice el proceso descrito en el punto anterior:

a) En el navegador se escribe el enlace www.dian.gov.co “pagina Oficial de la plataforma DIAN

b) En el módulo “En 2 pasos copia del RUT” dar click.

c) El sistema muestra una ventana en el cual se debe dar click en el enlace "¿Olvido su clave?" donde abre la página de Recuperación de Clave de acceso.

d) Ya estando en la página solo se debe seleccionar el tipo y número de documento de la persona, posteriormente se da click en el botón "Recuperar Contraseña" esta función le enviará al correo con el que hizo inscripción del RUT la contraseña.