UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS

Seguridad en los datos e implantación de la NTP-ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de Datos del RENIEC

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTOR:

Rojas Jaén, Moisés Clemente (ORCID: 0000-0003-3711-002X)

ASESOR:

Mgtr. Bermejo Terrones, Henry Paúl (ORCID: 0000-0002-3348-0181)

LÍNEA DE INVESTIGACIÓN:

Auditoria de Sistemas y Seguridad de la información

LIMA - PERÚ

2019

DEDICATORIA

A mi madre Rosa María Jaén Vda. De Rojas por todo el apoyo que me dio estos últimos años, a mi familia por su incansable e ilimitado apoyo, amor y comprensión en los días de ausencia, a mi hermana Beatriz que siempre me dio el aliento en los momentos más difíciles, y por encima de todo a Dios que guio mis pasos por el camino de la fe y la esperanza.

AGRADECIMIENTO

A la Universidad César Vallejo, a los docentes por brindarme una formación académica profesional, y especialmente a mi asesor Mgtr. Henry Paul Bermejo Terrones asesor de la presente investigación, por compartir su experiencia y conocimiento en la realización y desarrollo de la presente. A mis amigos que motivaron, apoyaron y alentaron el inicio, el proceso y la culminación de mi carrera, mi más sincero agradecimiento.

PÁGINA DEL JURADO

UCV UNIVERSIDAD CÉSAR VALLEJO	ACTA DE APROBACIÓN DE LA TESIS	Código : F07-PP-PR-02.02 Versión : 10 Fecha : 10-06-2019 Página : 1 de 9

El Jurado encargado de evaluar la tesis presentada por don (a)

- ROJAS JAÉN, MOISÉS CLEMENTE

cuyo título es:

SEGURIDAD EN LOS DATOS E IMPLANTACIÓN DE LA NTP-ISO/IEC 27001:2014 EN LA SUB GERENCIAS DE GESTIÓN DE BASE DE DATOS DEL RENIEC

Reunido en la fecha, escuchó la sustentación y la resolución de preguntas por el estudiante, otorgándole el calificativo de: ..18..(número) ..DIECIOCHO.....(letras).

Domingo, 22 de Diciembre del 2019
14:40 pm

.....
PRESIDENTE
Mgtr. PÉREZ FARFÁN IVÁN MARTIN

.....
SECRETARIO
Mgtr. GALVEZ TAPIA ORLEANS MOISES

.....
VOCAL
Mgtr. BERMEJO TERRONES HENRY PAÚL

Elaboró	Dirección de Investigación	Revisó	Representante de la Dirección / Vicerrectorado de Investigación y Calidad	Aprobó	Rectorado

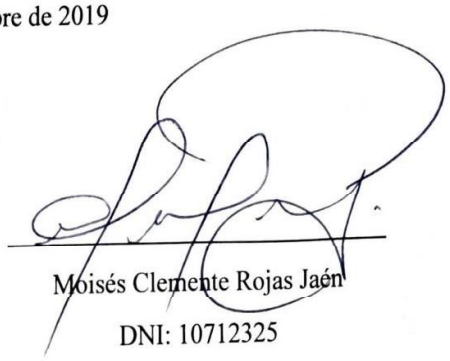
DECLARATORIA DE AUTENTICIDAD

Yo, Moisés Clemente Rojas Jaén, identificado con número de DNI 10712325, estudiante de la escuela académico profesional de Ingeniería de Sistemas, de la Facultad de Ingeniería de la Universidad Cesar Vallejo, con la investigación titulada "Seguridad en los datos e implantación de la NTP-ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de Datos del RENIEC" declaro bajo juramento que:

1. La tesis es de mi autoría.
2. He respetado las normas internacionales de citas y referencias para las fuentes consultadas. Por tanto, la tesis no ha sido plagiada ni total ni parcialmente.
3. La tesis no ha sido auto plagiada; es decir, no ha sido publicada ni presentada anteriormente para obtener algún grado académico previo o título profesional.
4. Los datos presentados en los resultados son reales, no han sido falseados, ni duplicados, ni copiados y por tanto los resultados que se presenten en la tesis se constituirán en aportes a la realidad investigada.

En tal sentido asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada por lo cual me someto a lo dispuesto en la normatividad vigente de la Universidad Cesar Vallejo.

Los Olivos, 22 de diciembre de 2019



Moisés Clemente Rojas Jaén
DNI: 10712325

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente proyecto de investigación lleva por título "**Seguridad en los Datos e Implantación de la NTP-ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de Datos del RENIEC**", que tiene como objetivo implantar la Norma Técnica Peruana ISO/IEC 27001:2014 para mejorar la seguridad de los datos en la Base de Datos de la Sub Gerencia de Gestión de Base de Datos del RENIEC.

Los sistemas tecnológicos que dan soporte a los procesos claves del RENIEC, generan grandes volúmenes de información, los que crecen constantemente a consecuencia de las operaciones diarias. Asumir, tratar y procesar la información creciente supone un gran reto, en la gestión de los datos, demarcando mucho más en la seguridad, puesto que siendo un activo clave que respalda la información de más de 38 millones de personas (mayores y menores), debe ser protegida, es por eso que la implantación de controles alineados a la NTP ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de datos, permite gestionar la Confidencialidad, Integridad y Disponibilidad implementando mejores políticas en base a la Misión, Visión y Objetivos de la Organización.

Este proyecto de investigación tiene un enfoque Cuantitativo, tipo Aplicada Experimental, diseño Pre-experimental, y un análisis de Pre-test y Post-test.

Lo que intenta demostrar este proyecto de investigación, es cuanto contribuye la implantación de la NTP ISO/IEC 27001:2014 en la gestión de la Confidencialidad, de la Integridad y de la Disponibilidad de la base de datos del RENIEC.

Las reuniones con las unidades orgánicas y con los especialistas de la Sub Gerencia de Gestión de Base de Datos, dieron como resultado la selección de los controles de la norma técnica necesarios para garantizar la seguridad de los datos, generar los indicadores y los documentos normativos, con la proyección de una posterior certificación en la ISO/IEC 27001:2013.

Palabras claves: Seguridad de la Información, confidencialidad, integridad, disponibilidad.

ABSTRACT

This research project is entitled "Data Security and Implementation of the NTP-ISO / IEC 27001: 2014 in the Sub Management of Database Management of RENIEC", which aims to implement the Peruvian Technical Standard ISO / IEC 27001: 2014 to improve data security in the Database of the Sub Management of Database Management of RENIEC.

The technological systems that support the key processes of RENIEC generate large volumes of information, which are constantly growing as a result of daily operations. Assuming, treating and processing the growing information is a great challenge, in the management of the data, demarcating much more in the security, since being a key asset that supports the information of more than 38 million people (older and younger), it must be protected, that is why the implementation of controls aligned to the NTP ISO / IEC 27001: 2014 in the Sub Management of Database Management, allows to manage Confidentiality, Integrity and Availability by implementing better policies based on the Mission, Vision and Objectives of the Organization.

This research project has a Quantitative approach, Applied Experimental type, Pre-experimental design, and a Pretest and Posttest analysis.

What this research project tries to demonstrate is how much the implementation of the NTP ISO / IEC 27001: 2014 contributes to the management of Confidentiality, Integrity and Availability of the RENIEC database.

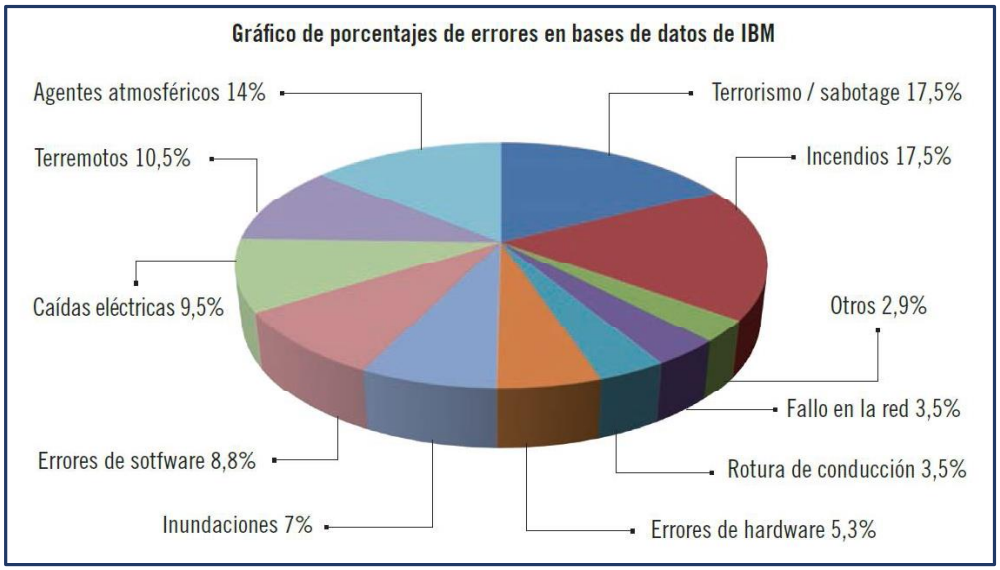
The meetings with the organic units and with the specialists of the Sub Management of Database Management, resulted in the selection of the controls of the technical norm necessary to guarantee the security of the data, generate the indicators and the normative documents, with the projection of a subsequent certification in ISO / IEC 27001: 2013.

Keywords: Security of the information, confidentiality, integrity, availability.

I. INTRODUCCIÓN

En Europa (2018), las compañías han tenido la inversión más alta en soluciones de ciberseguridad, convirtiéndose en una prioridad debido al incremento y a la tendencia de ataques que va en aumento. En España hubo más de 100,000 ciberataques en ese año de acuerdo a los datos reportados por el INCIBE y por CISCO (Rodríguez, 2018, parrafo 4).

FIGURA 1: FALLOS CATASTRÓFICOS



Fuente: San Martin Gonzales(2014)

Jean Claude Juncker, el presidente de la Comisión Europea declaraba que en Europa el año 2017 se produjeron aproximadamente 4,000 ciberataques diarios, de los más conocidos tenemos a malware, phishing, botnets y ransomware, que afectan directamente a las empresas privadas y organismos públicos, generando grandes daños a causa de robo de información, usurpación de identidades, y el pago de sobornos y su consecuente rescate para recobrar el dominio de equipos informáticos secuestrados a distancia (López, 2019, parrafo 3). Latinoamérica no ha sido la excepción, la firma ESET compañía eslovaca informo que el virus "ransomware", conocido con el ciber extorsión, ha tenido gran impacto en este lado del mundo, Colombia registra 28 % , el Perú un 17 %, en México un 15 %, Brasil llega a un 11 %, Argentina tiene 9 %, y los países de Chile, Ecuador y Venezuela un mínimo de 4 % (1).

FIGURA 2: TOP 10 BRECHAS DE DATOS DE LOS ÚLTIMOS AÑOS

Company	Accounts Hacked	Date of Hack
Yahoo	3 billion	Aug. 2013
Marriott	500 million	2014-2018
Yahoo	500 million	Late 2014
Adult FriendFinder	412 million	Oct. 2016
MySpace	360 million	May 2016
Under Armor	150 million	Feb. 2018
Equifax	145.5 million	July 2017
EBay	145 million	May 2014
Target	110 million	Nov. 2013
Heartland Payment Systems	100+ million	May 2008

Fuente: (1)

El Estado Peruano conocedor de esta problemática, el 8 de enero de 2016, aprueba de forma obligatoria en todas las instituciones del estado peruano, adscritas al Sistema Nacional de Informática, la implantación de la NTP ISO/IEC 27001:2014, mediante Resolución Ministerial N° 004-2016-PCM.

El Registro Nacional de Identificación y Estado Civil (RENIEC), es un organismo autónomo del Perú, tiene la misión de identificar a todos los peruanos, entregándoles el Documento Nacional de Identificación – DNI, registra los hechos vitales de cada ciudadano, nacimiento, matrimonio y defunción. Encargado por ley de preparar y entregar el Padrón Electoral para todos los procesos electorales.

El RENIEC de acuerdo a las políticas impulsadas por el estado peruano referente a la seguridad de la información, ha certificado cuatro procesos misionales en la ISO/IEC 27001:2013.

La Sub Gerencia de Gestión de Base de Datos (SGGBD) unidad orgánica de la Gerencia de Tecnología de la Información, está encargada de garantizar la integridad, confiabilidad, seguridad y el normal funcionamiento de la base de datos institucional, así como el de coordinar con las áreas operativas encargadas de los procesos misionales de la institución.

La finalidad de este proyecto, es determinar cuánto influye la implantación de esta norma técnica, en las métricas para el resguardo de la Base de Datos del RENIEC que está a cargo de la Sub Gerencia de Gestión de Base de Datos.

Este proyecto de investigación reviso varias tesis, tanto nacionales como internacionales, referente al contenido del actual proyecto de investigación; en los trabajos tenemos:

Tesis nacionales:

a) Presentada por **Hugo Daniel Olaza Aliano** del año 2017, con el título "Implementación de NTP ISO/IEC 27001:2013 para la Seguridad de Información en el Área de Configuración y Activos del Ministerio de Educación – Sede Centromin", utilizó el ciclo continuo en gestión de calidad PDCA (PHVA), realizar el Plan (Planificar), realizar la implementación - Do(Hacer), vigilar e inspeccionar – Check (verificar) y conservar y renovar constantemente – Act (Actuar), y se elaboró en base a un diseño experimental del tipo preexperimental, utilizó la técnica de recopilación de datos y como instrumento utiliza una ficha para la observación, la herramienta para recolectar datos se definió por juicio de expertos.

b) Presentada por **Daniel Elías Santos Llanos** del año 2016, con el título "Establecimiento, Implementación, Mantenimiento y Mejora de un Sistema de Gestión de Seguridad de La Información, Basado en la ISO/IEC 27001:2013, para una Empresa de Consultoría de Software" para obtener el título profesional de Ingeniero Informático en Lima-Perú, la investigación se realiza en el ámbito de intercambio de información entre cliente y proveedor, donde existe un riesgo alto de confidencialidad, planteando una solución basada en la Norma Técnica Peruana ISO/IEC 27001. Esta implantación facilita que los directivos y el personal que participan, puedan gestionar y tomar las decisiones adecuadas referente a las políticas de seguridad dentro de la empresa de Consultoría de Software, asegurando niveles altos de control en la información respecto a mantener la confidencialidad, proteger la integridad y ofrecer altos niveles de disponibilidad.

c) Presentada por Miguel Ángel Ayala Medrano del año 2017, con el título "Sistema de Gestión de Seguridad de Información para mejorar el proceso de gestión del riesgo en un hospital nacional, 2017", tuvo como finalidad cualificar la manera en que la implantación del Sistema de Gestión de Seguridad de la Información

interviene en la forma de cómo se gestionan los riegos de un Hospital Nacional, tomando en cuenta que el sistema de gestión de seguridad de la información es un sistema que se basa en el enfoque de los riesgos del negocio y que evalúa, monitorea y optimiza la seguridad de la información; asimismo, evaluar la probabilidad de que se produzcan y que de inmediato se tomen las acciones necesarias para aminorar todos los riesgos a un nivel aceptable.

d) Presentada por **Katherin Cinthia de la Sota Shicshe e Yvonne Jhosseln Mechan**, presentada el año 2018 con el título "Implementación de Controles y Cumplimiento de Requisitos de la ISO/IEC 27001:2013 para la Seguridad de Información en una pyme consultora" para optar el título profesional de Ingeniero de Computación y Sistemas en la ciudad de Lima. El objetivo del proyecto, se fundamentó en la perfección de los niveles de seguridad en la consultora VF CONSULTING S.A.C, para ello presentaron la implantación de la norma técnica peruana ISO/IEC 27001:2013. Este proyecto tomo como base la metodología del Ciclo de Deming (PHVA), los resultados proporcionaron bases para realizar la certificación de la referida norma. La investigación concluyo que es importante contar con un SGSI en cualquier empresa.

Tesis internacionales:

a) In the thesis of **Maryanne Ndungu and Sushila Kandel**, presented in 2015 with the title "INFORMATION SECURITY MANAGEMENT IN ORGANIZATIONS" to choose the degree in Information Technology in Finland. The purpose of the thesis is to explain the importance and value of information security in companies. Explains and highlights that the security of information is not only a technological issue but also a problem in the institutional culture of each organization. Therefore, it is emphasized that in every organization an organic unit exclusive to the security government must be included in its organizational structure. In addition, they indicate that for information to be secure, organizations must review their procedures, establishing the appropriate policies in a security approach. The thesis concludes that the security of information has become the main priority of any organization. They also indicate that the strategies implemented can not counter current threats, which is why they need to develop new models in architectures based on information security.

b) Presentada por **Jonier Pava Camacho, James Sarmiento Pérez y Bryan Forero Orjuela**, presentada el año 2018 con el título "Diagnóstico de Seguridad y Privacidad de la Información en la Alcaldía Municipal de Icononzo Tolima" para obtener el título profesional de Ingeniero de Sistemas en la ciudad de Bogotá – Colombia, se desarrolló para adecuar las políticas de seguridad y privacidad de la información, indicadas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y utilizo el Modelo de Seguridad y Privacidad de la Información (MSPI) determinada por este Ministerio. La investigación permitió determinar el estado en el que se encontraba la Alcaldía Municipal de Icononzo Tolima, respecto sus activos de información, localizo las debilidades y las falencias en sus sistemas, así como también realizo las recomendaciones para proteger, apoyar e implementar estrategias tecnológicas y de cultura organizacional, todo bajo el modelo de Seguridad y Privacidad de la Información del Gobierno en Línea (GEL) colombiano.

c) Presentada por **Bahareh Shojaie**, presentada el año 2018 con el título "Implementación de Seguridad de la Información. Sistemas de gestión basados en la Norma ISO / IEC 27001 en diferentes culturas" para lograr el título de doctorado en el Departamento de Informática de la Universidad en Hamburgo, se basa en verificar la potencialidad entre la cultura, política y económica de los países que lograron adoptar la norma ISO 27001 en los procesos de seguridad. La medición se realiza mediante un análisis cuantitativo, en términos de promedio de certificaciones emitidas entre los años 2014 al 2016. La relación que existe entre el comportamiento, la mentalidad y la cultura de cada país y la implantación de la norma internacional no ha sido investigada todavía.

De acuerdo a **Lapiedra** (2011), todas las empresas en el mundo, ya sean de gobierno o empresas privadas y de cualquier giro, en la actualidad, son generadores de datos, muchos de estos datos no tienen significado, pero muchos de ellos si sirven para dar a conocer el ámbito que los rodea, o para saber el estado de las organizaciones. Los datos son la materia prima necesaria para que, mediante un proceso, se conviertan en información, y este al ser relevante y oportuna, se transforma en una herramienta poderosa en las funciones de la planificación, el control y de la toma de decisiones (p. 5).

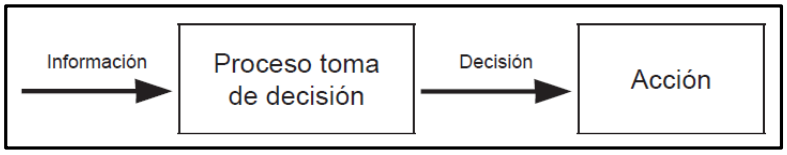
FIGURA 3: PROCESO DE TRANSFORMACIÓN DATOS - INFORMACIÓN

Fuente: Lapiedra , y otros(2011)

Asimismo, **Lapiedra** (2011),

Indica que la información es una agrupación de datos que han sido transformados de tal forma que contribuyan a minimizar la incertidumbre del futuro y, por tanto, apoyen en la toma de decisiones. La información simboliza los datos que han sido transformados de forma relevante para el personal operativo, funcionarios y dueños y/o accionistas de las empresas que lo reciban, es decir, tiene un valor real o percibido para las decisiones o las acciones a tomar (p. 6).

FIGURA 4: INFORMACIÓN PARA LA TOMA DE DECISIONES



Fuente: Lapiedra , y otros(2011)

De acuerdo a lo descrito por Lapiedra, la seguridad de los datos, está directamente relacionada con la seguridad de la información, ya que la información es resultado de un proceso cuya entrada principal son los datos.

Por otro lado, en la obra *"Salvaguarda y Seguridad de los Datos"* del autor **Enrique San Martin Gonzales**, indica que la seguridad de los datos tiene como proposito el de proteger a los datos y a los sistemas de información, controlar el acceso, supervisar que no sufran interrupcion y vigilar para impedir la eliminación no autorizada, la garantia de la información, la seguridad de los datos y la seguridad informatica son denominaciones que, aunque no signifiquen lo mismo, tienen un único propósito al proteger la confidencialidad, integridad y disponibilidad de la información.

En el libro *"Manual Integro de Itil v3",* su autor **Sergio Ríos**, indica que el objetivo de una Metrica, es llegar a comprobar si los objetivos se estan cumpliendo, mediante las mediciones, los controles y el analisis de los resultados o los datos obtenidos. Una de las maneras de establecer metricas pueden ser comparando los resultados que se han obtenido, analizando las mediciones de satisfaccion, analizando las mediciones de los controles de recursos, revisar y estudiar las no conformidades

En el taller *"Implementación de la Norma ISO 27001"*, dirigida por la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI, el ponente **Maurice Frayssinet Delgado**, indica que la seguridad de la información es el grupo de normas preventivas y reactivas de las empresas e instituciones, que proporcionan protección y resguardo de la información buscando conservar las dimensiones de la Confidencialidad, de la Disponibilidad y de la Integridad de esta.

De acuerdo a San Martin Gonzales, define a la dimensiòn **Confidencialidad,** como a la característica que imposibilita la divulgación de información a personas, procesos y/o aplicaciones no autorizadas. Es un derecho constitucional a la intimidad y que los datos propios o personales, o procesados, gestionados y administrados por una empresa, no hayan sido públicos ni expuestos a personas, entidades o grupos no autorizados.

El **Indicador** que utilizamos para esta dimensión es la **Métrica de Confidencialidad de la BD,** que corresponde a la evaluación y promedio del total de las conexiones realizadas por los usuarios y de la cantidad de las conexiones no autorizadas fallidas por día.

$$INCONF = \frac{TA - TA\_NA}{TA} * 100$$

- Dónde:

  INCONF: Índice de Confidencialidad de la base de datos

  TA: Sumatoria de todos los Usuarios Conectados x día

  TA_NA: Sumatoria de Conexiones no autorizados x día

La dimensión de la **Integridad**, se define como a la característica que tiene el objetivo de conservar los datos y protegerlos contra alteraciones no autorizadas. Estas

alteraciones pueden venir de usuarios, procesos y/o aplicaciones que tengan o no la intensión de alterar o eliminar información.

El **Indicador** que utilizamos para esta dimensión es la **Métrica de Integridad de la BD,** que corresponde a la evaluación y promedio de la cantidad de documentos recibidos en la SGGBD y la cantidad de documentos donde solicitan modificación directa a la base de datos.

$$ININTE = \frac{DS - DS\_MBD}{DS} * 100$$

Dónde:

ININTE:	Índice de Integridad de la base de datos.
DS:	Sumatoria de la totalidad de Documentos por tramite documentario a la SGGBD.
DS_MBD:	Sumatoria de la totalidad de documentos por tramite documentario que modificaron la base de datos.

La dimensión de la **Disponibilidad,** se define como la cualidad de la información que indica que esta deba encontrarse a disposición de las personas, procesos o aplicaciones para su uso, y que se asegure que no exista interrupciones que eviten el funcionamiento normal de las empresas o instituciones (p. 133).

El **Indicador** que utilizamos para esta dimensión es la **Métrica de Disponibilidad de la BD,** que corresponde a la evaluación y promedio de la cantidad de horas diarias de disponibilidad de la base de datos y de la cantidad de horas que la base de datos dejo de operar por problemas técnicos y operativos.

$$INCON = \frac{TH - TH\_PA}{TH} * 100$$

Dónde:

INCON: Índice de Disponibilidad de la base de datos.

TH: Sumatoria de la totalidad de horas diarias.

TH_PA: Sumatoria de la totalidad de horas paradas.

El Estado Peruano ha elaborado esta norma técnica NTP-ISO/IEC 27001-2013, basado en la ISO internacional de Sistema de Seguridad de la Información ISO/IEC 27001-2014, para que todos los organismos estatales implanten las políticas y normas necesarias para gestionar la protección de su información, basados en un marco de mejora continua.

La decisión de implementar este sistema, tiene que ser una determinación estratégica y debe estar implementado dentro de los procesos misionales de la organización.

La implementación se basa inicialmente en medir la importancia que brindara estas políticas, dentro de las necesidades y objetivos de la institución, y cuál sería el impacto, dependiendo de los fines de cada una de ellas (NTP-ISO/IEC 27001:2014, 2014, p.vii).

La norma resalta que toda organización debe de cumplir primero con requerimiento mínimo de la seguridad de la información, como son: se debe planificar, implementar y controlar todos los procesos de la empresa, así como también evaluar y valorar los riesgos, dándoles un tratamiento de acuerdo a su importancia. También indica las etapas que debe tener y llevar, así como: realizar el seguimiento, determinar la medición, estudiar el análisis, realizar la evaluación, implementar la auditoría interna y desarrollar la revisión por parte de la dirección y los responsables del SGSI.

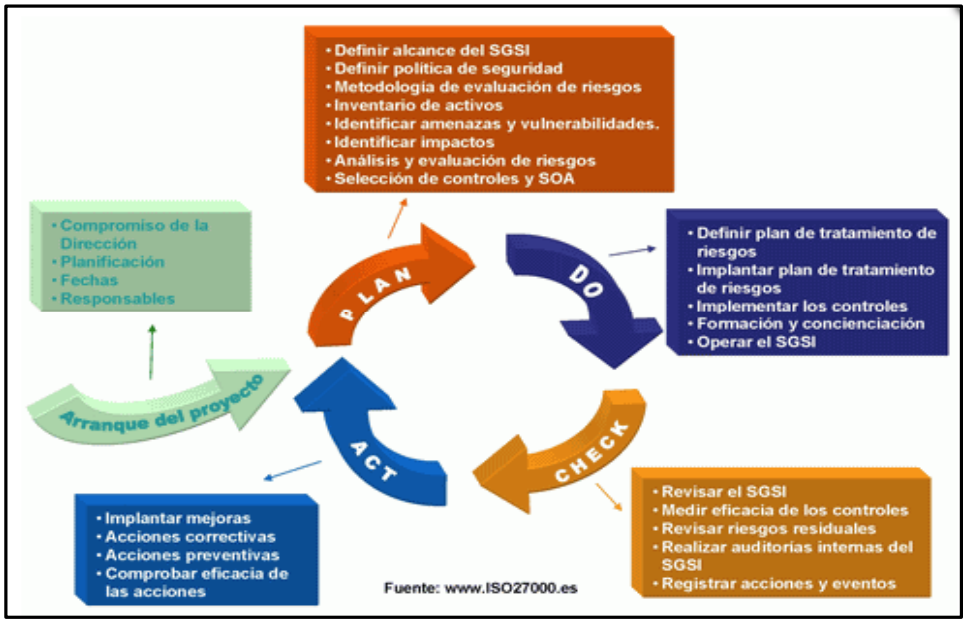
Las normas descritas anteriormente, ISO 27001 y 27002, son asistidas por la norma ISO/EIC 27005:2009, para poder administrar los riesgos en seguridad de información. Es necesario tener una visión metódica al momento de analizar los riesgos, ya que estos deben ser alineados a los objetivos organizacionales, directamente a sus requisitos para poder gestionar mejor el sistema de gestión de seguridad de información que se pretende implementar.

Brinda las directrices necesarias para que toda organización de acuerdo a sus necesidades y alineado a la gestión general del análisis de riesgo de toda la compañía,

para que sean enfrentados oportunamente, en el lugar y tiempo que sea necesario. Te brinda un marco conceptual para poder gestionar los riesgos mediante procesos continuos de revisión y control, estos deben ser analizados para medir su implicancia y las consecuencias posibles, antes de tomar decisiones de como atacar y minimizarlos en un nivel que sea aceptado por la organización.

De Acuerdo a la Organización Internacional de Normalización (2019), ISO es el organismo internacional autonomo de estandares no gubernamental, que tiene a mas de 164 paises con membresias internacionales y 783 comites tecnicos y subcomites, que tienen la mision de desarrollar los estandares. Por medio de los paises miembros, puede reunir expertos a nivel mundial, que permitan compartir sus conocimientos y el desarrollo de estandares internacionales basados en los requerimientos del mercado, que apoyan y dan solucion a grandes desafios que se presentan en varias lineas de procesos que comprende la calidad, la seguridad y la eficiencia, en tal sentido, el ISO por las políticas y procedimientos con las que son elaboradas para las diferentes líneas, cumple con los requisitos de una Metodología. Esta ISO utiliza el modelo del ciclo continuo PDCA, que tradicionalmente es utilizado en los sistemas para la gestión de la calidad.

FIGURA 5 : MODELO PDCA



Fuente: ISO-Organización Internacional de Normalización(2016)

Este proyecto se elabora para analizar el problema de "¿Cómo optimiza la seguridad de los datos la implantación de la NTP ISO/IEC-27001 en la Sub Gerencia de Gestión de Base de Datos del RENIEC?", asi como también de acuerdo a sus dimensiones que son:

- ¿Cómo optimiza en la Confidencialidad de los datos la implantación de la NTP ISO/IEC-27001 en la Sub Gerencia de Gestión de Base de Datos del RENIEC?
- ¿Cómo optimiza en la Integridad de los datos la implantación de la NTP ISO/IEC-27001 en la Sub Gerencia de Gestión de Base de Datos del RENIEC?
- ¿Cómo optimiza en la Disponibilidad de los datos la implantación de la NTP ISO/IEC-27001 en la Sub Gerencia de Gestión de Base de Datos del RENIEC?

La presente investigacion, se desarrolla en el RENIEC, que es una Institución comprometida al servicio del ciudadano, a la identificación en todo el territorio peruano y los peruanos con residencia en el extranjero, que tiene la noble misión de proteger el Registro Único de Identificación de las Personas Naturales (RUIPN), la emisión del DNI (Documento Nacional de Identificación), así como también el registro de hechos vitales (nacimiento, matrimonio y defunción). Siempre tomando en cuenta la gran importancia de la integridad, de la confidencialidad y de la disponibilidad de los datos y la información de los ciudadanos peruanos. Por lo tanto el activo más crítico que el RENIEC tiene es la información del registro de identidad de más de 38 millones de habitantes en todo el territorio peruano. La necesidad de demostrar con este proyecto de investigación sobre la implantación del ISO 27001, es causar un efecto positivo al aumentar sus métricas de valoración en el dato almacenado en su motor de base de datos, respecto a mantener la confidencialidad, asegurar la integridad y a la disponibilidad de los datos almacenados para el uso de todos los sistemas de información que se brinda.

La justificación tecnológica se basa en que los resultados de la investigación facilitan los diseños y la producción de técnicas, herramientas y grupos para la producción de activos económicos, industriales, científicos, etc., que estimulan la producción de los procesos de productividad y el aseguramiento de los activos más importantes de la institución. Los motores de base de datos que se utilizan para gestionar los datos, brindan gran parte de la seguridad y protección que se exige, así como la administración de los usuarios, los cambios y modificaciones y la disponibilidad de esta a los sistemas de información. Pero en los últimos años se ha demostrado que los ataques a los

motores de base de datos a nivel mundial han sido dirigidos hacia las brechas o vulneraciones sobre el personal que los administra, a pesar que existe políticas definidas y buenas prácticas, pero que no están bajo normas, marcos o estándares internacionales, como lo es la ISO 27001. La implantación de esta norma de seguridad, podrá determinar la gestión de la base de datos en esta plataforma tecnológica.

La justificación Socioeconómica, de acuerdo a Carrasco(2017), corresponde a los resultados de esta investigación que están dirigidos en beneficiar a la población, que ayuden a la realización de proyectos en apoyo en lo social y económico de la población. Este proyecto tiene un impacto social, puesto que se aplica en la base de datos de la información de la identidad de los ciudadanos peruanos, el cual debe tener una mayor cobertura de seguridad, dado que ayuda al gobierno en la ejecución de todos los programas sociales. Además, le da sostenibilidad a los servicios de información que el RENIEC brinda a las entidades privadas y gubernamentales (Bancos, Notarias, Sunat, Sunarp, Transporte y otros).

La justificación Institucional, aplica en la implantación definida en este proyecto de investigación, el cual aumentara los niveles de seguridad en los motores de datos y brindara mejores controles al personal que los administra, asegurando a la institución los servicios que brinda a la sociedad son confiables.

La justificación política-administrativa, según Carrasco(2017), indica si el resultado promueve al poder ejecutivo a tomar acciones administrativas y de ámbitos políticos en beneficio de los ciudadanos, directamente en la construcción de obras públicas, en la explotación de recursos y otras actividades a favor de la ciudadanía. El fortalecimiento de la seguridad en los datos de los ciudadanos, impulsara los proyectos que el estado peruano tenga con la población, en los niveles de programas sociales, administración de identidades, comercio electrónico, voto electrónico y otros. Las instituciones del estado necesitan que la información que se brinda para el uso de sus funciones, tenga un alto grado de seguridad y confiabilidad, y es lo que se persigue en la implantación de esta norma.

Esta Tesis, supone plantear la Hipótesis General "*La implantación de la NTP ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de Datos del RENIEC optimizara significativamente la seguridad en los datos*", y para las hipótesis específicas de las dimensiones se plantea:

- La implantación de la NTP ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de Datos del RENIEC optimizara significativamente en la Confidencialidad de la seguridad de los datos.
- La implantación de la NTP ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de Datos del RENIEC optimizara significativamente en la Integridad de la seguridad de los datos.
- La implantación de la NTP ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de Datos del RENIEC optimizara significativamente en la Disponibilidad en la seguridad de los datos.

El Objetivo General de esta Tesis, es "*Valorar la optimización en la seguridad de los datos al implantar la ISO 27001 en la Sub Gerencia de Gestión de Base de Datos del RENIEC*" y los objetivos específicos para sus dimensiones:

- Valorar la optimización en la Confidencialidad de la seguridad de los datos al implantar la ISO 27001 en la Sub Gerencia de Gestión de Base de Datos del RENIEC.
- Valorar la optimización en la Integridad de la seguridad de los datos al implantar la ISO 27001 en la Sub Gerencia de Gestión de Base de Datos del RENIEC.
- Valorar la optimización en la Disponibilidad de la seguridad de los datos al implantar la ISO 27001 en la Sub Gerencia de Gestión de Base de Datos del RENIEC.

II. MÉTODO

2.1. Tipo y diseño de Investigación

2.1.1. Método de Investigación: Pre-Experimental

Según indica **Hernandez, Fernadez, & Baptista** (2010), que un proyecto de investigacion determina el impacto que va a tener una o mas variables independientes en una o mas variables dependientes en un ambiente controlado (p. 121).

Según **Carrasco** (2017), el diseño preexperimental se refiere a la aplicación de una prueba previa a un determinado grupo, al estímulo o tratamiento experimental, para luego gestionarlo y tratarlo, y después de un determinado tiempo, aplicar nuevamente otra prueba o medición posterior (p. 64).

En este proyecto se utiliza el Diseño experimental, de tipo preexperimental, de un solo grupo en dos tiempos en la modalidad de preprueba y posprueba (pretest y posttest), que nos permitirá observar el comportamiento de la variable dependiente al inicio y al final del proyecto de la implantación y adecuación de la ISO 27001.

El esquema de este diseño:

G -> O1 -> X -> O2

Dónde:

G: Grupo a evaluar

X : determina a la variable independiente (NTP ISO/IEC 27001).

O1: medición previa (antes de la implantación) de la variable dependiente

(Seguridad en los Datos).

O2: medición posterior (después de la implantación) de la variable dependiente (Seguridad en los Datos).

Se aplica un pretest (O1-antes de la implantación) a un grupo (G) de sujetos, después el tratamiento (X-ISO 27001) y finalmente el posttest (O-después de la

implantación). El resultado es el impacto de optimización que ocurrió desde el pretest hasta finalizar la implantación con un post test. Este viene a ser la medida del cambio.

2.1.2. Aplicada

Según Carrasco (2017), define a la investigación aplicada, a la que se diferencia de otros por tener determinaciones prácticas inmediatas bien definidas, es decir, se indaga para actuar, transformar, modificar o producir cambios en un determinado sector definido de la realidad actual (p. 43).

La actual Investigación Aplicada, tiene por objetivo resolver un determinado planteamiento específico, orientado a determinar los efectos que pueden alterar la seguridad de los datos y la implantación de una norma técnica, el cual enriquecerán los procesos actuales.

2.2. Operacionalización de Variables

2.2.1. Definición Conceptual

Variable Independiente (VI): NTP ISO/IEC-27001

Es la norma técnica peruana de seguridad de la información, que es impulsada por el estado peruano, para que todos los organismos la implementen progresivamente en el entorno de seguridad de sus instituciones. Contiene 114 controles que cada institución definirá cuál de ellos está de acuerdo a la funcionalidad y objetivos de cada organismo. La norma brinda las metodologías necesarias para el control de calidad y mejora continua en seguridad de información.

Variable Dependiente (VD): Seguridad en los Datos

La seguridad de datos es la responsabilidad principal de las oficinas de TI en toda organización ya sea en el ámbito público o privado, pequeña o grande, o de cualquier tipo. Es custodiar los datos durante su ciclo de vida, por posibles ataques que cambien o modifiquen su contenido y que solo debe ser proporcionado a personas autorizadas.

2.2.2. Definición Operacional

Variable Independiente (VI): NTP ISO/IEC-27001

Son controles definidos y proporcionados por la ISO 27001, que facilitan la gestión en la seguridad de la información, ayudan a aumentar los niveles de aceptación y valoración de las métricas de la confidencialidad, la de integridad y la de disponibilidad de los datos de la base de datos del RENIEC.

Proporciona mecanismos de mejora continua, con el fin de mantener siempre vigilada las políticas creadas para salvaguardar la seguridad.

Variable Dependiente (VD): Seguridad en los Datos

Conjunto de políticas implementadas en la vigilancia de la protección de los motores de base de datos, con la finalidad de protegerlo sobre la intromisión de intrusos, posibles vulneraciones que alteren los datos, y sobre probables fallas que afecten la disponibilidad y que perjudiquen el acceso a los servicios de los sistemas de información.

2.2.3. Operacionalización

Según Bernal (2010), menciona que el concepto de Operacionalizar una variable significa traducir la variable a indicadores, es decir, traducir los conceptos hipotéticos a unidades de medición (p. 141).

Según Carrasco (2017), es el proceso en el cual se descompone o divide deductivamente todas las variables del problema de investigación, iniciando de los más general hasta lo más específico (p. 226).

.

TABLA 1: CUADRO DE OPERACIONALIZACIÓN

Variable	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Datos	Instrumento	Fuente de Información
Variable Dependiente: Seguridad de los Datos en la Base de Datos del RENIEC	La seguridad de datos es la responsabilidad principal de las oficinas de TI en toda organización ya sea en el ámbito público o privado, pequeña o grande, o de cualquier tipo. Es custodiar los datos durante ciclo de vida, por posibles ataques que cambien o modifiquen su contenido y que solo debe ser entregado a las personas autorizadas.	Conjunto de políticas implementadas en la vigilancia de la protección de los motores de base de datos, con la finalidad de protegerlo sobre la intromisión de intrusos, posibles vulneraciones que alteren los datos, y sobre probables fallas que afecten la disponibilidad y que perjudiquen el acceso a los servicios de los sistemas de infomación.	Confidencialidad	Métrica de Confidencialidad de la BD	Accesos a la Base de Datos	Ficha de Registro diario	Base de Datos del RENIEC
			Integridad	Métrica de Integridad de la BD	Modificación en la Base de Datos		
			Disponibilidad	Métrica de Disponibilidad de la BD	Hora de Actividad de la Base de Datos		

Referencia: Elaboración Propia

TABLA 2: RECOLECCIÓN DE DATOS

Indicador	Descripción	Técnica	Instrumento	Unidad de Medidas	Formula
Métrica de Confidencialidad de la BD	Corresponde a la evaluación y promedio del total de las conexiones realizadas por los usuarios y de la cantidad de las conexiones de no autorizadas fallidas por día.	Fichaje	Ficha de Registro	Unidades	$INCONF = \frac{TA - TA\_NA}{TA} * 100$ Donde: INCONF: Índice de Confidencialidad de la base de datos TA: Sumatoria de todos los Usuarios Conectados x día TA_NA: Sumatoria de Conexiones no autorizados x día
Métrica de Integridad de la BD	Corresponde a la evaluación y promedio de la cantidad de documentos recibidos en la SGGBD y la cantidad de documentos donde solicitan modificación directa a la base de datos.				$ININTE = \frac{DS - DS\_MBD}{DS} * 100$ Donde: ININTE: Índice de Integridad de la base de datos. DS: Sumatoria de la totalidad de Documentos por tramite documentario a la SGGBD. DS_MBD: Sumatoria de la totalidad de documentos por tramite documentario que modificaron la base de datos.
Métrica de Disponibilidad de la BD	Corresponde a la evaluación y promedio de la cantidad de horas diarias de disponibilidad de la base de datos y de la cantidad de horas que la base de datos dejo de operar por problemas técnicos y operativos.				$INCON = \frac{TH - TH\_PA}{TH} * 100$ Donde: INCON: Índice de Disponibilidad de la base de datos. TH: Sumatoria de la totalidad de horas diarias. TH_PA: Sumatoria de la totalidad de horas paradas.

Referencia: Elaboración Propia

2.3. Población, Muestra y Muestreo

2.3.1. Población (N)

De acuerdo a lo indicado por Carrasco (2017), define a la población al grupo de los componentes y elementos que pertenecen a un espacio determinado donde se está haciendo el estudio experimental (p.237)

La población para este proyecto de investigación corresponde a la totalidad de los registros de la tabla de auditoria de Login de la base de datos, de la Totalidad de Documentos recibidos en la SGGBD y de la Totalidad de horas Operativas del servicio de información.

2.3.2. Muestra (n)

Para Carrasco (2017) la muestra es la porción específica de una población, esta es representativa, objetiva y fidedigna, para que los resultados que obtengan sean los más óptimos y que se puedan generalizar para todos los elementos de la población (p.237).

El tipo de la muestra a utilizar es la muestra probabilística aleatoria simple.

De acuerdo a Carrasco 82017), indica que la muestra probabilística incluye en la selección a la totalidad de los elementos de la población y todos ellos tienen la misma posibilidad de formar parte de la muestra (p. 241).

Para efectos de este proyecto de investigación, el procedimiento a utilizar para conseguir el tamaño de la muestra será de acuerdo a la tabla de error de Fisher, Arkin y Colton.

De acuerdo a Carrasco (2017) la tabla de error es uno de los métodos más simples y prácticos utilizados para tratar a una población y la muestra que le corresponda. El punto principal es el nivel de confianza que son establecidos, así como el nivel de significación para determinar la muestra en base a una determinada población (p. 245).

FIGURA 6: TAMAÑO DE LA MUESTRA EXTRAÍDA DE POBLACIONES FINITAS PARA MÁRGENES DE ERROR DE 1 A 10% EN LA HIPÓTESIS DE P=50%

AMPLITUD DE LA POBLACION	TAMAÑO DE LA MUESTRA SEGÚN MARGEN DE ERROR					
	+ - 1	+ - 2	+ - 3	+ - 4	+ - 5	+ - 10
	0.01	0.02	0.03	0.04	0.05	0.10
N	n1	n2	n3	n4	n5	n10
500	-	-	-	-	222	83
1,000	-	-	-	385	386	91
1,500	-	-	638	441	316	94
2,000	-	-	714	476	333	95
2,500	-	1,250	769	500	345	96
3,000	-	1,364	811	520	353	97
3,500	-	1,468	843	530	359	98
4,000	-	1,538	870	541	364	98
4,500	-	1,607	891	546	367	98
5,000	-	1,667	909	556	370	98
6,000	-	1,765	938	566	375	99
7,000	-	1,842	959	574	378	99
8,000	-	1,905	976	580	381	99
9,000	-	1,957	989	584	383	99
10,000	5,000	2,000	1,000	588	385	99
15,000	6,000	2,143	1,034	600	390	100
20,000	6,667	2,222	1,053	606	392	100
25,000	7,143	2,273	1,064	610	394	100
50,000	8,333	2,381	1,087	617	397	100
100,000	9,091	2,439	1,099	621	398	100
+ de 100,000	10,000	2,500	1,111	625	400	100

Referencia: (2 pág. 246) Metodología de la Investigación Científica

2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad

2.4.1. Técnica

Observación

Para Carrasco (2017) determina que la observación es una técnica para recolectar datos, que capta las propiedades, características y cualidades, con la finalidad de procesarlos y transformarlos en información (p. 282).

Para poder lograr las métricas de este proyecto, los resultados obtenidos en los reportes diarios y catalogados en las fichas de observación para cada métrica, se procederá a evaluar de acuerdo a los formatos de la métricas e indicadores presentados en el anexo B.

2.4.2. Instrumento de investigación

Según Carrasco (2017) define a los instrumentos de investigación como a todo objeto que es utilizado para la recopilación de datos físicos y electrónicos de forma organizada, que permitan conseguir opiniones, respuestas y características diversas, que posteriormente puedan ser procesados, analizados y estudiados de acuerdo a la finalidad de la investigación (p.334).

En este proyecto, se generarán reportes mensuales, donde se evidenciará las medidas diarias y el grado de eficiencia de los controles implementados.

Estos reportes están presentados en el anexo B.

2.4.3. Ficha de Observación

Según Carrasco (2017) cataloga a la ficha de observación como un instrumento de fácil manejo, que tiene grandes utilidades de uso. En ella se registran las evidencias y acciones que tiene el observador y el ámbito de observación (p. 313).

Para cada métrica, se tiene una ficha de control que deberá de llenarse mensualmente para indicar el grado de eficiencia lograda. Esta ficha se presenta en el anexo B.

2.4.4. Validez

Para Carrasco (2017), es un atributo de cada instrumento de investigación, determinando que estos valoran de modo objetivo, con alta precisión, autenticidad y veracidad de todo aquello que se evalúa tanto de la variable o variables de la investigación (p. 336).

2.4.5. Confiabilidad

Para Carrasco (2017), la define como un atributo o propiedad de una herramienta de medición, que, al procesar en diferentes periodos de tiempo, obtienen el mismo

resultado aplicando una o más veces a un mismo individuo o a un grupo de individuos. Sus características principales son la objetividad, estabilidad, consistencia y la predictibilidad (p. 339).

Existen varios procesos para medir la confiabilidad de un instrumento de medición. Todos usan formulas y técnicas que crean coeficientes de fiabilidad. Esto se ilustra en la figura Nro. 2

FIGURA 7: INTERPRETACIÓN DE UN COEFICIENTE DE CONFIABILIDAD

Fuente: (3)

El resultado de la calificación de los expertos para las metricas fueron los siguientes:

TABLA 3: GRADO DE CONFIABILIDAD DE LA MÉTRICA DE CONFIDENCIALIDAD

METRICA DE CONFIDENCIALIDAD								
	Puntuación por Item							Confiabilidad
Experto	1	2	3	4	5	6	7	
Dra. Romero Valencia, Monica	75.00%	75.00%	75.00%	75.00%	75.00%	75.00%	75.00%	75.00%
Mgtr. Galvez Tapia, Orleans Moisés	80.00%	80.00%	80.00%	80.00%	80.00%	80.00%	80.00%	80.00%
Mgtr. Huarote Zegarra, Raúl	85.00%	90.00%	95.00%	90.00%	95.00%	95.00%	90.00%	91.43%
						Grado de Confiabilidad		82.14%

Referencia: Elaboración Propia

Interpretación: El grado de confiabilidad promedio de los 3 expertos consultados, es 82.14%, ACEPTABLE.

TABLA 4: GRADO DE CONFIABILIDAD DE LA MÉTRICA DE INTEGRIDAD

METRICA DE INTEGRIDAD								
	Puntuación por Item							Confiabilidad
Experto	1	2	3	4	5	6	7	
Dra. Romero Valencia, Monica	80.00%	80.00%	80.00%	80.00%	80.00%	80.00%	80.00%	80.00%
Mgtr. Galvez Tapia, Orleans Moisés	90.00%	90.00%	90.00%	90.00%	90.00%	90.00%	90.00%	90.00%
Mgtr. Huarote Zegarra, Raúl	85.00%	90.00%	95.00%	95.00%	90.00%	95.00%	95.00%	92.14%
							Grado de Confiabilidad	87.38%

Referencia: Elaboración Propia

Interpretación: El grado de confiabilidad promedio de los 3 expertos consultados, es 87.38%, ACEPTABLE.

TABLA 5: GRADO DE CONFIABILIDAD DE LA MÉTRICA DE DISPONIBILIDAD

METRICA DE DISPONIBILIDAD								
	Puntuación por Item							Confiabilidad
Experto	1	2	3	4	5	6	7	
Dra. Romero Valencia, Monica	78.00%	78.00%	78.00%	78.00%	78.00%	78.00%	78.00%	78.00%
Mgtr. Galvez Tapia, Orleans Moisés	90.00%	90.00%	90.00%	90.00%	90.00%	90.00%	90.00%	90.00%
Mgtr. Huarote Zegarra, Raúl	95.00%	90.00%	85.00%	90.00%	95.00%	95.00%	90.00%	91.43%
							Grado de Confiabilidad	86.48%

Referencia: Elaboración Propia

Interpretación: El grado de confiabilidad promedio de los 3 expertos consultados, es 86.48%, ACEPTABLE.

2.5. Procedimiento

Las mediciones que resulten de la aplicación del pre-test así como del post-test serán registrados en formatos de registros electrónicos, para posteriormente a través de un análisis estadístico se realizara las pruebas de hipótesis para determinar el cumplimiento de los objetivos planteados.

2.6. Métodos de análisis de datos

Para Bernal (2010), todo desarrollo de investigación debe analizar los datos obtenidos (individuales, dispersos o desordenados) que se obtuvieron de la población objeto del proyecto de investigación en el trabajo de campo, y tiene

como fin de brindar los resultados (datos en grupos depurados y con un orden específico), y a partir de ellos se realizara los análisis respectivos según los objetivos o hipótesis de la investigación o ambas. Este proceso debe realizarse con utilitarios informáticos estadísticos que se encuentra de acceso libre en el mercado (p. 198).

Para analizar los datos obtenidos se deberá de evaluar su consistencia de acuerdo a su correlación y a los niveles de acuerdo a las siguientes condiciones:

FIGURA 8: RANGOS DE LA CORRELACIÓN DE PEARSON

Coeficiente	Interpretación
r = 1	Correlación perfecta
0.80 < r < 1	Muy alta
0.60 < r < 0.80	Alta
0.40 < r < 0.60	Moderada
0.20 < r < 0.40	Baja
0 < r < 0.20	Muy baja
r = 0	Nula

Referencia: Jimenez (2018)

2.7. Aspectos éticos

Toda información que sea proporcionada por la Sub Gerencia de Gestión de Base de Datos al investigador, será tratada con discrecionalidad y se guardara la máxima confidencialidad, así mismo se respetara la propiedad intelectual y todos los derechos de autor de las citas utilizadas. También se mantendrá en restricto la identidad de los participantes del proyecto.

III. RESULTADOS

El estudio de la presente investigación, desea comprobar que tanto influye una norma técnica o un estándar internacional en la operatividad de un sistema de control informático, en este caso, vamos a evidenciar que la implantación de la NTP-ISO/IEC 27001:2014, en la Sub gerencia de Gestión de base de Datos del RENIEC, si influyo de forma positiva o negativa en la seguridad de los datos, en las dimensiones de la Confidencialidad, la Integridad y la Disponibilidad.

Para demostrar el resultado se realiza un análisis descriptivo e inferencial de la cantidad de datos obtenidos por medio de los instrumentos de recolección. Para Peña (2014), la estadística descriptiva se emplea para reducir y simplificar los datos que fueron procesados y transformados en información, para adecuar los modelos a una realidad estudiada (p. 25).

Asimismo, indica que la estadística inferencial ejecuta de forma contraria: dadas las frecuencias estudiadas de una variable, inferir el modelo probabilístico que ha generado los datos (p.258).

3.1. Análisis Descriptivo

En este análisis, vamos a resumir los datos recolectados en la muestra, para darnos un panorama general y así describir a los integrantes de la muestra. Al tratar con un análisis de variable cuantitativa, utilizaremos las medidas de tendencia central, como son la media, moda y mediana. Para el caso de esta investigación, la población de datos es igual a la muestra, para tal efecto, se evaluó el comportamiento de los indicadores implantados durante dos meses, el primero antes de la implantación, y el segundo después de haber implantado los controles de la NTP ISO/IEC 27001.

3.1.1. Indicador 1.- Índice de Confidencialidad de la Base de Datos

TABLA 6: MEDIDA DESCRIPTIVA DEL INDICADOR DE CONFIDENCIALIDAD ANTES Y DESPUÉS DE LA IMPLANTACIÓN

	Media	Mediana	Moda	Desviación Estándar	Mínimo	Máximo	Coeficiente de Variación
Índice antes	96,35	99	100	4,990	82	100	5,18%
Índice después	98,58	100	100	1,945	94	100	1,97%

Fuente: Elaboración Propia

El análisis dio como resultado una diferencia de Medias. El valor de la Media del índice antes es de 96.35 respecto al valor de la Media del índice después que es de 98,58. Esto significa que la influencia de la variable independiente causo efecto al momento de ser implantado. El índice de confidencialidad mínimo antes fue de 82 frente al índice de confidencialidad después que arrojo 94. La dispersión del índice de confidencialidad paso de 5.18% a 1.97%, se comprueba que la variabilidad respecto a los datos no difiere en gran medida, por lo que la comparación de los valores de las medias se considera adecuada.

3.1.2. Indicador 2.- Índice de Integridad de la Base de Datos

TABLA 7: MEDIDA DESCRIPTIVA DEL INDICADOR DE INTEGRIDAD ANTES Y DESPUÉS DE LA IMPLANTACIÓN

	Media	Mediana	Moda	Desviación Estándar	Mínimo	Máximo	Coeficiente de Variación
Índice antes	76,00	91,50	100	28,05	16	100	36,91%
Índice después	90,59	95,50	100	13,168	53	100	14,53%

Fuente: Elaboración Propia

El análisis dio como resultado una diferencia de Medias. El valor de la Media del índice antes es de 76.00 respecto al valor de la Media del índice después que es de 90.59. Esto significa que la influencia de la variable independiente causo efecto al momento de ser implantado. El índice de integridad mínimo antes fue de 16 frente al índice de integridad después que dio 53. La dispersión del índice de integridad paso de 36.91% a 14.53%, se comprueba que la variabilidad respecto a los datos

no difiere en gran medida, por lo que la comparación de los valores de las medias se considera adecuada.

3.1.3. Indicador 3.- Índice de Disponibilidad de la Base de Datos

TABLA 8: MEDIDA DESCRIPTIVA DEL INDICADOR DE DISPONIBILIDAD ANTES Y DESPUÉS DE LA IMPLANTACIÓN

	Media	Mediana	Moda	Desviación Estándar	Mínimo	Máximo	Coeficiente de Variación
Índice antes	96,35	100	100	7,495	73	100	7,78%
Índice después	99,97	100	100	0,180	99	100	0,17%

Fuente: Elaboración Propia

El análisis dio como resultado una diferencia de Medias. El valor de la Media del índice antes es de 96,35 respecto al valor de la Media del índice después que es de 99,97. Esto significa que la influencia de la variable independiente causo efecto al momento de ser implantado. El índice de disponibilidad mínimo antes fue de 73 frente al índice de disponibilidad después que dio 99. La dispersión del índice de disponibilidad paso de 36.91% a 18,65%, se comprueba que la variabilidad respecto a los datos no difiere en gran medida, por lo que la comparación de los valores de las medias se considera adecuada.

3.2. Análisis Inferencial

3.2.1. Prueba de Normalidad

Con la finalidad de seleccionar la prueba de hipótesis para la presente investigación, lo datos se sometieron a una prueba de normalidad para validar su distribución.

De acuerdo a Peña (2014), para hacer el análisis de normalidad se utiliza el estadístico de Shapiro y Wilks cuando las muestras sean menor a 30 datos (p. 470). En el presente caso de este estudio, se tienen muestras de hasta 31 datos que serán incluidos en este tipo de análisis estadístico.

Para todos los indicadores que vamos analizar, se tomará un nivel de confiabilidad del 5%, esto quiere decir que si el valor de Sig es:

Sig >= 0.05 estaremos frente a una distribución normal

Sig < 0.05 estaremos frente a una distribución no normal

Indicador 1.- Índice de Confidencialidad de la Base de Datos

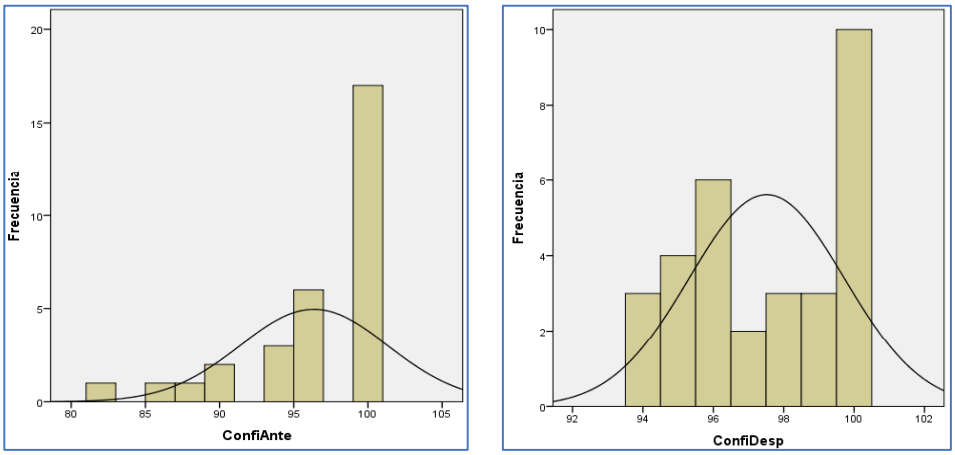
TABLA 9: PRUEBA DE NORMALIDAD DEL NÚMERO DE INFORMACIÓN DEL INDICADOR DE CONFIDENCIALIDAD ANTES Y DESPUÉS DE LA IMPLANTACIÓN

	Shapiro-Wilk		
	Estadístico	gl	Sig
Índice antes	0,758	31	0,000
Índice después	0,742	31	0,000

Fuente: Elaboración Propia

Los resultados obtenidos para el indicador de Confidencialidad, es de Sig.=0.000, para los índices antes y los índices después, esto se interpreta, que, de acuerdo al nivel de confiabilidad, el resultado refleja que estamos frente a una distribución no normal para la etapa de pre-test y del post-test. Esto significa que utilizaremos la prueba no paramétrica.

FIGURA 9*:* DIAGRAMA DE NORMALIDAD DE LOS DATOS



Referencia: Histograma de prueba de normalidad del promedio del índice de confidencialidad antes y después de la implantación.

Los histogramas reflejan una distribución no normal para los datos, no cumplimiento el requisito de normalidad.

Indicador 2.- Índice de Integridad de la Base de Datos

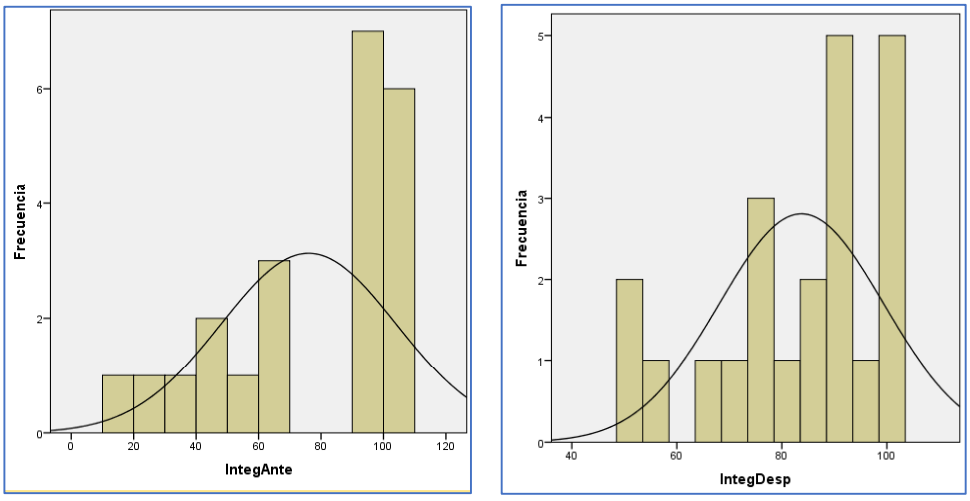
TABLA 10: PRUEBA DE NORMALIDAD DEL NÚMERO DE INFORMACIÓN DEL INDICADOR DE INTEGRIDAD ANTES Y DESPUÉS DE LA IMPLANTACIÓN

	Shapiro-Wilk		
	Estadístico	gl	Sig
Índice antes	0,813	22	0,001
Índice después	0,716	22	0,000

Fuente: Elaboración Propia

Los resultados obtenidos para el indicador de Integridad, para los índices antes el valor de Sig.=0.001 y para los índices después con un valor de Sig.=0.000, esto se interpreta, que de acuerdo al nivel de confiabilidad, el resultado refleja que estamos frente a una distribución no normal para la etapa de pre-test y del post-test. Esto significa que utilizaremos la prueba no paramétrica.

FIGURA 10: FIGURA: DIAGRAMA DE NORMALIDAD DE LOS DATOS



Referencia. Histograma de prueba de normalidad del promedio del índice de Integridad antes y después de la implantación

Los histogramas reflejan una distribución no normal para los datos, no cumplimiento el requisito de normalidad.

Indicador 3.- Índice de Disponibilidad de la Base de Datos

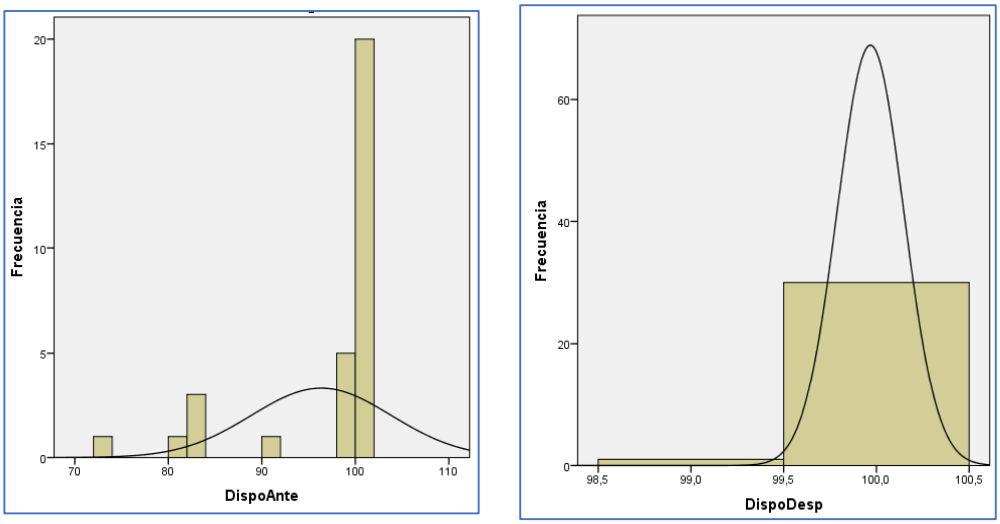
TABLA 11: PRUEBA DE NORMALIDAD DEL NÚMERO DE INFORMACIÓN DEL INDICADOR DE DISPONIBILIDAD ANTES Y DESPUÉS DE LA IMPLANTACIÓN

	Shapiro-Wilk		
	Estadístico	gl	Sig
Índice antes	0,548	31	0,000
Índice después	0,176	31	0,000

Fuente: Elaboración Propia

Los resultados obtenidos para el indicador de Disponibilidad, es de Sig.=0.000, para los índices antes y los índices después, esto se interpreta, que de acuerdo al nivel de confiabilidad, el resultado refleja que estamos frente a una distribución no normal para la etapa de pre-test y del post-test. Esto significa que utilizaremos la prueba no paramétrica.

FIGURA 11: DIAGRAMA DE NORMALIDAD DE LOS DATOS



Referencia. Histograma de prueba de normalidad del promedio del índice de integridad antes y después de la implantación de la NTP ISO/IEC 27001.

Los histogramas reflejan una distribución no normal para los datos, no cumplimiento el requisito de normalidad.

3.2.2. Prueba de Hipótesis

H1: La implantación de la ISO/IEC 27001 en la Sub Gerencia de Gestión de Base de Datos del RENIEC optimizará significativamente en la Confidencialidad de la seguridad de los datos.

A. Hipótesis de Investigación N° 01

I1=Indicador de Confidencialidad

Variables:

IC_a: Índice de Confidencialidad antes de la implantación.

IC_d: Índice de Confidencialidad después de la implantación.

$H1_0$: La implantación de la ISO/IEC 27001 NO mejora la confidencialidad de la seguridad de los datos.

$H1_a$: La implantación de la ISO/IEC 27001 mejora significativamente la confidencialidad de la seguridad de los datos.

$H1_0$: $IC_d <= IC_a$, el indicador después de la implantación es menor o igual que el indicador antes de la implantación.

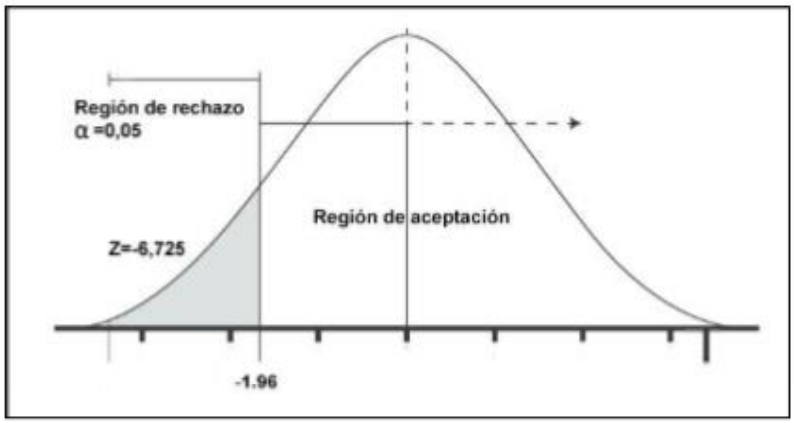
$H1_a$: **$IC_d > IC_a$,** el indicador después de la implantación es mayor que el indicador antes de la implantación.

TABLA 12: PRUEBA DE RANGOS DE WILCOXON PARA EL INDICADOR DE CONFIDENCIALIDAD ANTES Y DESPUÉS DE IMPLANTACIÓN.

Test	Z	Sig.(p)
Prueba de Rangos de Wilcoxon	-2,731	0.000

Fuente: Elaboración Propia

FIGURA 12: DIAGRAMA DE NORMALIDAD DE LOS DATOS



Referencia: **Pértegas Díaz, S., Pita Fernández, S.**

Lo indicado en la Tabla Nro. 12 y en la Figura Nro. 12, corresponde que el valor de Sig. es de 0.000, cayendo en la región conocida como rechazo, por lo que queda descartada la hipótesis nula($H1_0$), tomando como válida la hipótesis alterna(**$H1_a$**) que dice:

"La implantación de la ISO/IEC 27001 mejora significativamente la confidencialidad de la seguridad de los datos".

B. Hipótesis de Investigación N° 02

I2=Indicador de Integridad

Variables:

II_a: Índice de Integridad antes de la implantación.

II_d: Índice de Integridad después de la implantación.

$H1_0$: La implantación de la ISO/IEC 27001 NO mejora la integridad de la seguridad de los datos.

$H1_a$: La implantación de la ISO/IEC 27001 mejora significativamente la integridad de la seguridad de los datos.

$H1_0$: $II_d <= II_a$, el indicador después de la implantación es menor o igual que el indicador antes de la implantación.

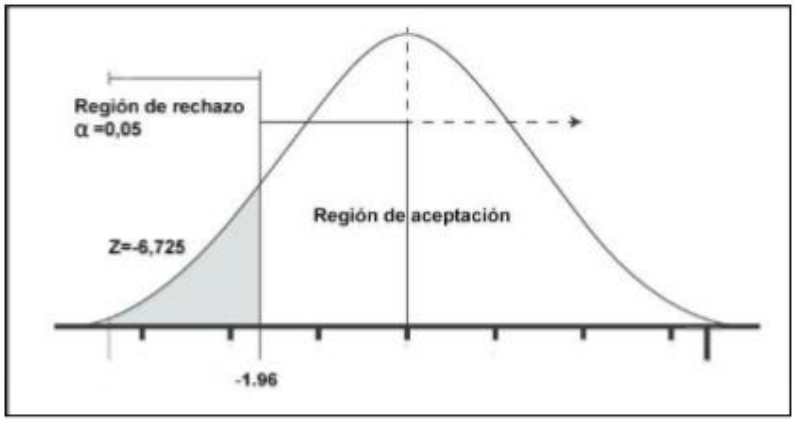
$H1_a$: $II_d > II_a$, el indicador después de la implantación es mayor que el indicador antes de la implantación.

TABLA 13: PRUEBA DE RANGOS DE WILCOXON PARA EL INDICADOR DE INTEGRIDAD

Test	Z	Sig.(p)
Prueba de Rangos de Wilcoxon	-2,113	0,035

Fuente: Elaboración Propia

FIGURA 13: DIAGRAMA DE NORMALIDAD DE LOS DATOS



Referencia: **Pértegas Díaz, S., Pita Fernández, S.**

Lo indicado en la Tabla Nro. 13 y en la Figura Nro. 13, corresponde que el valor de Sig. es de 0.035, cayendo en la región conocida como rechazo, por lo que queda descartada la hipótesis nula ($H1_0$), tomando como válida la hipótesis alterna (**$H1_a$**) que dice:

"La implantación de la ISO/IEC 27001 mejora significativamente la integridad de la seguridad de los datos".

C. Hipótesis de Investigación N° 03

I2=Indicador de Disponibilidad

Variables:

ID_a: Índice de Disponibilidad antes de la implantación.

ID_d: Índice de Disponibilidad después de la implantación.

$H1_0$: La implantación de la ISO/IEC 27001 NO mejora la disponibilidad de la seguridad de los datos.

$H1_a$: La implantación de la ISO/IEC 27001 mejora significativamente la disponibilidad de la seguridad de los datos.

$H1_0$: $II_d <= II_a$, el indicador después de la implantación es menor o igual que el indicador antes de la implantación.

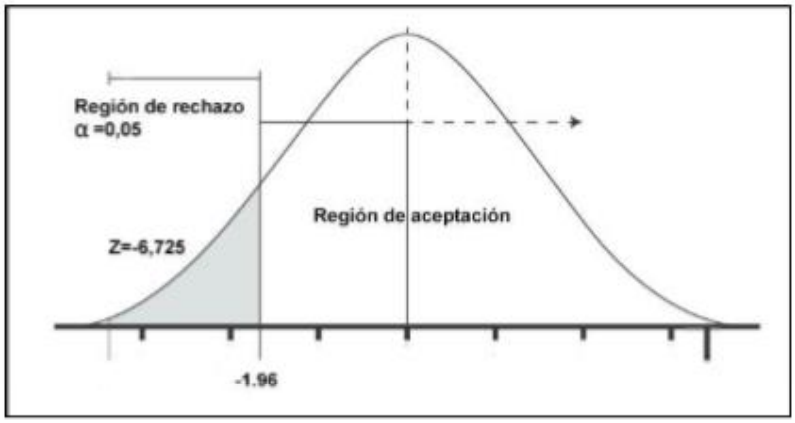
$H1_a$: $II_d > II_a$, el indicador después de la implantación es mayor que el indicador antes de la implantación.

TABLA 14:PRUEBA DE RANGOS DE WILCOXON PARA EL INDICADOR DE DISPONIBILIDAD

Test	Z	Sig.(p)
Prueba de Rangos de Wilcoxon	-2,824	0,005

Fuente: Elaboración Propia

FIGURA 14: DIAGRAMA DE NORMALIDAD DE LOS DATOS



Referencia: **Pértegas Díaz, S., Pita Fernández, S.**

Lo indicado en la Tabla Nro. 14 y en la Figura Nro. 14, corresponde que el valor de Sig. es de 0.005, cayendo en la región conocida como rechazo, por lo que queda descartada la hipótesis nula ($H1_0$), tomando como válida la hipótesis alterna(**$H1_a$**) que dice:

"La implantación de la ISO/IEC 27001 mejora significativamente la disponibilidad de la seguridad de los datos".

IV. DISCUSIÓN

A partir de los resultados obtenidos en el presente estudio, aceptamos la hipótesis general que establece que la Implantación de la NTP ISO/IEC 27001, optimizo significativamente la seguridad de los datos en la Base de Datos del RENIEC, lo que nos indica que las normas técnicas o los estándares internacionales (ISO), influyen dentro de los procesos importantes en una empresa y que impactan positivamente en el control y la gestión de los procesos, dándole un entorno de seguridad y confianza.

Estos resultados tienen relación con los que sostiene Olaza (2017) y Ayala (2017), donde la implantación de la norma técnica peruana, aumento los niveles en los indicadores de seguridad de información. Los autores expresan que el ordenamiento y la implantación de las técnicas y controles determinados por la ISO, reflejan resultados positivos en los estudios planteados respectivamente.

Los resultados para esta investigación señalan, que el indicador de la Confidencialidad, para el pre-test diagnosticó un índice de 96.35 y después de la implantación de la ISO, en fase de post-test aumentó a 98.58. Respecto al indicador de la Integridad, para el pre-test se determinó un índice de 76.00 y luego de la implantación en fase post-test aumento a 90.59, y para el indicador de Disponibilidad, para el pre-test se determinó un índice de 96.35 y luego de la implantación en fase post-test aumento a 99.97.

Para Ayala (2017), el diagnóstico sobre el indicador de nivel de riesgo, en el momento de pre-test diagnostico una medición de 3.72, y en el momento de post-test la medición disminuyo en 3.09, los resultados determinan que existió una disminución de 0.63, esto demuestra que la implantación de la ISO 27001, apoyo sustancialmente en el proceso de gestionar los riesgos en el Hospital Nacional PNP "Luis N. Sáenz".

Para Ayala (2017), el diagnóstico sobre el indicador de nivel de riesgo, en el momento de pre-test diagnostico una medición de 3.72, y en el momento de post-test la medición disminuyo en 3.09, los resultados determinan que existió una disminución de 0.63, esto demuestra que la implantación de la ISO 27001, apoyo sustancialmente en el proceso de gestionar los riesgos en el Hospital Nacional PNP "Luis N. Sáenz".

Para Olaza (2017), en su investigación, acerca de la exposición de los datos, la cantidad de información confidencial divulgada, al momento de tomar la muestra en el pre-test, diagnosticó un indicador de 6.07 y después de la implantación de la ISO/IEC 27001 en la medición post-test se redujo a 1.67. Los resultados determinan una reducción en este indicador de 4.4, por lo que se concluye que la implantación de la ISO ha logrado una reducción del 72.5% en el número de información confidencial divulgada del Área de Configuración y Activos del Ministerio de Educación – Sede Centromin.

En la investigación realizada por **Santos** (2016), demostró como resultado de las exigencias del proyecto y sus interesados, que pudieron implementar propuestas innovadoras asociadas a la metodología en la gestión de los riesgos de la seguridad de la información, la normalización de los planes del sistema y la verificación integral de cumplimiento de los componentes requeridos como requisitos por la ISO/IEC 27001, dio como resultado que la empresa consultora de software, incrementara su nivel de seguridad, garantizando a las organizaciones con las que contrata, un adecuado funcionamiento de las soluciones informáticas que automatizan sus procesos para el desarrollo, mantenimiento y calidad de software.

En la investigación realizada por **Sota-Mechan** (2018), tuvieron resultados de variaciones considerables en el total de los requisitos que se implementaron, el nivel de cumplimiento previo a la implantación de la ISO/IEC 27001, fue de 2% y después llego a un nivel de cumplimiento de 64%. La implementación de los controles de seguridad cumplió con los requisitos mínimos aceptables, relacionados a la Norma 27001, en consecuencia, se mejoró significativamente la seguridad de la información en la consultora. Al realizar el análisis de riesgos de los activos de información se pudo concluir que se ha identificado un nivel aceptable de riesgo, que con la implementación de los controles mínimos requeridos se ha reducido el nivel de exposición en el que podrían estar los activos de información más importantes de la organización.

Según la investigación realizada por **Maryanne Ndungu and Sushila Kandel**, (2015), su estudio concluye que, tras la aplicación generalizada de las tecnologías de la información y la comunicación, los sistemas TIC son ahora el núcleo básico y la reserva de todos los elementos de información que son fundamentales para las

organizaciones. En los últimos tiempos, los sistemas y redes de información interconectados llevaron a las organizaciones a una situación crítica que determina la necesidad de medidas explícitas para la protección de la información. Por un lado, los sistemas de TIC se están volviendo cada vez más complejos con el avance de la tecnología. Por otro lado, lanzar ataques dañinos contra los sistemas requiere habilidades menos complejas. La seguridad de la información nunca ha sido más importante de lo que es hoy. Las amenazas de hoy no se pueden contrarrestar con las estrategias del ayer. Las organizaciones necesitan un modelo actual y una arquitectura bien establecida de seguridad de la información, impulsado por el conocimiento de las amenazas, los activos, los motivos y objetivos de los posibles adversarios.

V. CONCLUSIONES

Con el análisis realizado a los resultados de la investigación, se puede concluir lo siguiente:

a) Se ha determinado que la implantación de la NTP ISO/IEC 27001, en la Sub Gerencia de Gestión de Base de Datos, optimizo significativamente los indicadores de seguridad en los datos. El cumplimiento de los controles propuestos por la norma, así como también la creación de nuevos controles de gestión, relacionados a la seguridad de la información, tuvo un efecto positivo al incrementar los resultados de los indicadores en las dimensiones de seguridad.

b) Se ha logrado el objetivo de valorar el índice de Confidencialidad, que en el análisis dio como resultado positivo en la diferencia de Medias, la Media del índice antes fue de 96,35 respecto a la Media después que es de 98,58. Esto significa que la influencia de la variable independiente causo efecto al momento de ser implantado. El índice de confidencialidad mínimo antes fue de 82 frente al índice de confidencialidad después que arrojo 94. La dispersión del índice de confidencialidad paso de 5.18% a 1.97%, se comprueba que la variabilidad respecto a los datos no difiere en gran medida, por lo que la comparación de las Medias se considera adecuada.

c) Se ha logrado el objetivo de valorar el índice de Integridad, que en el análisis dio como resultado positivo en la diferencia de Medias, la Media antes fue de 76,00 respecto a la Media después que fue de 90.59. Esto significa que la influencia de la variable independiente causo efecto al momento de ser implantado. El índice de integridad mínimo antes fue de 16 frente al índice de integridad después que dio 53. La dispersión del índice de integridad paso de 36.91% a 14.53%, se comprueba que la variabilidad respecto a los datos no difiere en gran medida, por lo que la comparación de las Medias se considera adecuada.

d) Se ha logrado el objetivo de valorar el índice de Disponibilidad, que en el análisis dio como resultado positivo en la diferencia de Medias, la Media del índice antes es de 96,35 respecto a la Media del índice después que es de 99,97. Esto significa que la influencia de la variable independiente causo efecto al momento de ser implantado. El índice de disponibilidad mínimo antes fue de 73 frente al índice de

disponibilidad después que dio 99. La dispersión del índice de disponibilidad paso de 36.91% a 18,65%, se comprueba que la variabilidad respecto a los datos no difiere en gran medida, por lo que la comparación de las Medias se considera adecuada.

e) De los estudios referenciados, y el presente estudio, se puede concluir que las normas internacionales, tales como la ISO/IEC 27001, causan efectos positivos para la gestión y la administración de seguridad de información. En cada organización debe establecer un espacio adecuado para las políticas, prácticas, gestión de riesgos, observación y mantenimiento de la gestión de la seguridad de la información, junto con las actividades cotidianas y las actividades a largo plazo para abordar los asuntos técnicos.

VI. RECOMENDACIONES

a) Se recomienda que la Gerencia de Tecnología de la Información del RENIEC, evalué la posibilidad de pasar a la siguiente etapa de la implantación de la NTP ISO/IEC 27001, esto quiere decir que se deberá de canalizar el pedido de certificación de la Sub Gerencia de Gestión de Base de Datos en la ISO/IEC 27001, el cual garantizará que los controles implementados podrán ser actualizados, así como también adicionar nuevos controles, como referencia a la mejora continua que determina la ISO investigada.

b) Se recomienda a la institución, continúe la implantación de la NTP ISO/IEC 27001, en las demás Sub Gerencias de la Gerencia de Tecnología de la Información, con la finalidad de seguir garantizando mejores beneficios y controles de seguridad de los datos y de la información.

c) Se recomienda a nuevos investigadores que deseen ahondar en la investigación de la implementación de sistemas de seguridad de información, en unidades orgánicas de TI o áreas de TI, que profundicen en los temas de infraestructura, seguridad perimetral y desarrollo de software con inclusión de la seguridad de la información y de los datos.

REFERENCIAS

AGENCIA EFE. Colombia encabeza los casos de ciberextorsiones en Latinoamérica en 2018. *America.* [En línea] Colombia 2018. [Fecha de Consulta: 10 de Mayo de 2019.] Disponible en https://www.efe.com/efe/america/tecnologia/colombia-encabeza-los-casos-de-ciberextorsiones-en-latinoamerica-2018/20000036-3805939.

AGESIC - GOBIERNO DE URUGUAY. Directrices para la aplicación de la Ley 18.331. *Portal Institucional.* [En línea] Uruguay 05 de Agosto de 2016. [Fecha de Consulta: 12 de 06 de 2019.] Disponible en https://www.agesic.gub.uy/innovaportal/v/509/1/agesic/documentos.html.

AMARO, José Antonio. Seguridad en internet. PAAKAT Revista de Tecnología y Sociedad. Centro Universitario de Ciencias Sociales y Humanidades, Universidad de Guadalajara, México 2017.[En linea] México Febrero del 2017. [Fecha de Consulta: 20 de Agosto de 2019]. Disponible en http://www.udgvirtual.udg.mx/paakat/index.php/paakat/article/view/280/html.

ANTTILA, Juhani. Integrating ISO/IEC 27001 and other Managerial Discipline Standards with Processes of Management in Organizations. IEEE Xplore-Digital Library. Prague, Czech Republic Fecha de la Conferencia 20-24 Agosto 2012. [Fecha de Consulta: 20 de Junio de 2019]. DOI: **10.1109/ARES.2012.93. Dis**ponible en https://ieeexplore.ieee.org/abstract/document/6329214.

ARÉVALO, J. G., **BAYONA**, R. Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: Análisis del riesgo de la información. Revista Tecnura. Colombia 24 de Agosto de 2015. doi:10.14483/udistrital.jour.tecnura.2015.4.a10. Disponible en https://revistas.udistrital.edu.co/index.php/Tecnura/article/view/9551.

BACA, Gabriela. *Introducción a la Seguridad Informática.* Mexico : Grupo Editorial Patria, S.A. de C.V., 2016. pág. 342. ISBN 978-607-744-471-8.

BELL, Timothy. *Auditoria Basada en Riesgos - Perspectiva Estrategica de Sistemas.* [ed.] Adriana Gutierrez. Bogotá D.C. : Kimpres Ltda., 2015. pág. 284. ISBN 978-958-648-512-8.

BERNAL, César. *Metodología de la Investigación.* Colombia : Pearson Educación de Colombia Ltda., 2010. pág. 320. ISBN 978-958-699-128-5.

CARRASCO, Sergio. *Metodología de la Investigación Cientifica.* Lima : San Marcos de Anibal Paredes Galvan, 2017. pág. 474. ISBN 978-9972-38-344-1.

CONCYTEC. Politica de Seguridad de la Información. *Resolución de Presidencia N° 114-2017-CONCYTEC-P.* Lima, Peru : Portal Institucional del CONCYTEC, 20 de Setiembre de 2017.

CONEXION ESAN. Los cinco principios de COBIT 5. [En línea] Perú 01 de Junio de 2016. [Fecha de la Consulta: 16 de Mayo de 2019.] Disponible en https://www.esan.edu.pe/apuntes-empresariales/2016/06/los-cinco-principios-de-cobit-5/.

COSTA, Jesús. *Seguridad Informática.* Madrid : RA-MA, 2014. pág. 307. ISBN 978-84-9964-313-7.

CRESPO, Esteban. Ecu@Risk, Una metodología para la gestión de Riesgos aplicada a las MPYMEs. Enfoque UTE. Quito-Ecuador Febrero de 2017. [Fecha de Consulta: 20 de Junio de 2019]. ISSN:1390-6542. Disponible en . http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-65422017000100107&lang=en

FRAYSSINET, Maurice. Taller de Implementación de la norma ISO 27001. Oficina Nacional de Gobierno Electronico e Informatica - ONGEI. [En línea] Perú 22 de Agosto de 2014. [Fecha de Consulta: 20 de 06 de 2019.] Disponible en www.ongei.gob.pe.

GARCIA, Elisenda. El Ciclo de Deming: La Gestión y Mejora de Procesos. [En línea] España 10 de Noviembre de 2016. [Fecha de Consulta: 04 de 06 de 2019.] Disponible en https://equipo.altran.es/author/elisenda-garcia/.

HERNANDEZ, Roberto. *Metodología de la Investigación.* Mexico DF : McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V., 2010. pág. 510. 968-422-931-3.

INDECOPI. NTP-ISO/IEC 27005:2009. Lima, Perú : Esta Norma Técnica Peruana ha sido preparado para proporcionar los requisitos para, 07 de Noviembre de 2009. pág. 100.

INTITUTO URUGUAYO DE NORMAS TECNICAS. UNIT-ISO/IEC 27002:2013. Montevideo, Uruguay : Instituto Uruguayo de Normas Tecnicas, Mayo de 2014. pág. 93.

ISO - Organización Internacional de Normalización. Organización Internacional de Normalización. [En línea] Secretaría Central de la ISO, 2019. [Fecha de Consulta: 16 de 07 de 2019.] Disponible en https://www.iso.org/standards.html.

JIMENEZ, Daniel. Coeficiente de Pearson. *Tesis e Investigaciones Analisis - SPSS.* [En línea] Mexico 30 de 05 de 2018. [Fecha de Consulta: 17 de 07 de 2019.] Disponible en https://www.tesiseinvestigaciones.com/estadiacutesticos-descriptivos/coeficiente-de-pearson.

LAPIEDRA, Rafael. *Introducción a la Gestión de Sistemas de información en la empresa.* Castellón de la Plana : Universitat Jaume I. Servei de Comunicación y Publicacion, 2011. pág. 72. ISBN 84-693-9894-6.

LOPEZ, José María. La Unión Europea y su papel en la ciberseguridad. *Hipertextual.* [En línea]España 18 de 04 de 2019. Fecha de Consulta: 14 de 05 de 2019.] Disponible en https://hipertextual.com/2019/04/union-europea-ciberseguridad-enisa.

MARTELO, Raul. Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI).Centro de Información

Tecnologica. Vol. 26.La Serena. Cartagena 2015. [Fecha de Consulta: 20 de Mayo de 2019]. ISSN:0718-0764. Disponible en https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-07642015000200015&lang=en.

MARTINEZ, Myriam. El Riesgo percibido y la Gestión de la Seguridad. Derechos de eu-repo/semantics/openAccess. Revista de la Universidad Industrial de Santander (Rev. Univ. Ind. Santander. Salud). [En Línea] España 18 de Agosto de 2018. [Fecha de Consulta: 22 de Junio de 2019]. Disponible en https://repositorioacademico.upc.edu.pe/handle/10757/575099.

PIATTINI-VELTHIUS, Mario. A reference ontology for harmonizing process- reference models. Revista Facultad de Ingeniería Universidad de Antioquia.Medellin-Colombia 2014. [Fecha de Consulta: 20 de Junio 2019]. ISSN 0120-6230. Disponible en http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-62302014000400004&lang=en.

TUNÇALP, D. Diffusion and Adoption of Information Security Management Standards Across Countries and Industries. Journal of Global Information Technology Management, Scotland 11 de Diciembre del 2014. 17, 221–227. [Fecha de Consulta: 20 de Junio de 2019]. ISSN:1097-198X. Disponible en http://doi.org/10.1080/1097198X.2014.982454

NTP-ISO/IEC 27001:2014. Técnicas de Seguridad. Sistemas de gestión de seguridad de la información. Lima, Perú : Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias - INDECOPI, 20 de Noviembre de 2014.

OLAZA, Hugo. Implementación de NTP ISO/IEC 27001 para la Seguridad de Información en el Área de Configuración y Activos del Ministerio de Educación – Sede Centromin. Trabajo de Titulación (Ingeniero de Sistema) Lima-Peru:Universidad Cesar Vallejo, 2017. 147 p.

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO/IEC 27000-Tecnicas de Seguridad de Información . España : s.n., 10 de Febrero de 2016.

PANDA MEDIACENTER. Marriott International, protagonista de la segunda mayor brecha de datos de la historia. *Noticias de Seguridad.* [En línea] EEUU 3 de Diciembre de 2018. [Fecha de Consulta: 25 Mayo de 2019] Disponible en https://www.pandasecurity.com/spain/mediacenter/seguridad/marriott-international-brecha-de-datos-masiva/.

PEÑA, Daniel. *Fundamentos de Estadistica.* Madrid : Alianza Editorial, S. A., 2014.pág. 688. ISBN: 978-84-206-8877-0.

POWERDATA. Seguridad de datos: En qué consiste y qué es importante en tu empresa. [En línea] España 27 de Febrero de 2016. [Fecha de Consulta: 16 de 05 de 2019.] Disponible en https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/seguridad-de-los-datos.

QUEZADA, Nel. *Metodología de la Investigación, estadistica aplicada en la investigación.* Argentina:Mcro,2010. Pág. 336. ISBN: 978-612-4034-50-3.

RENIEC. Registro Nacional de Identificación y Estado Civil. [En línea] Perú 12 de Diciembre 2009. [Fecha de Consulta: 25 de Mayo de 2019] Disponible en www.reniec.gob.pe.

RIOS, Sergio. ITIL v3 - Manual Integro. *B-able.* [En línea] España 2015. [Fecha de Consulta: 17 de Julio de 2019.] Disponible en www.biable.es.

RODRIGUEZ, Irene. Los ataques de los que todo el mundo ha hablado en 2018. *IMF Business School.* [En línea] España 26 de 12 de 2018. [Fecha de Consulta: 14 de 05 de 2019.] Disponible en https://blogs.imf-formacion.com/blog/tecnologia/ataques-mas-hablados-2018-201812/.

SAN MARTIN GONZALES, Enrique. *Salvaguarda y Seguridad de los datos.* Andalucia : IC Editorial - Innovación y Cualificación S. L., 2014. Pág. 296. ISBN 978-84-16207-27-5.

SHAMELI-SENDI, A., AGHABABAEI-BARZEGAR,R. Taxonomy of Information Security Risk Assessment (ISRA). *Computers & Security.*[En línea] Canada 12 de Noviembre de 2015.[Fecha de Consulta: 15 de Junio de 2019]. Disponible en http://dx.doi.org/10.1016/j.cose.2015.11.001.

TARÍ GUILLÓ, Juan Jose. *Calidad Total: fuente de ventaja competitiva.* Alicante : Espagrafic, 2015. pág. 302. 84-7908-522-3.

TUNÇALP, D. Diffusion and Adoption of Information Security Management Standards Across Countries and Industries. *Journal of Global Information Technology Management*, Scotland 11 de Diciembre del 2014. *17*, 221–227. [Fecha de Consulta: 20 de Junio de 2019]. ISSN:1097-198X. Disponible en http://doi.org/10.1080/1097198X.2014.982454

VALENCIA-DUQUE, Francisco. Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. RISTI- Revista Iberica de Sistemas y Tecnologias de Información. Portugal Junio de 2017. [Fecha de Consulta: 20 de Junio de 2019]. ISSN: 1646-9895. Disponible en http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1646-98952017000200006&lang=en

ZAIDMAN, Emilio. Seguridad Informática. [En línea]La Plata, Buenos Aires-Argentina 2017. [Fecha de Consultal: 16 de 05 de 2019.] Disponible en http://hdl.handle.net/10915/61109.

ANEXOS

ANEXO A: MATRIZ DE CONSISTENCIA

ANEXO A. MATRIZ DE CONSISTENCIA

PROBLEMA	OBJETIVOS	HIPÓTESIS	OPERACIONALIZACION DE VARIABLES			
			Variables	Dimensión	Indicador	Metodología
General	**General**	**General**	**Independiente**			
¿Cómo optimiza la seguridad de los datos la implantación de la NTP ISO/IEC-27001 en la Sub Gerencia de Gestión de Base de Datos del RENIEC?	Valorar la optimización en la seguridad de los datos al implantar la ISO 27001 en la Sub Gerencia de Gestión de Base de Datos del RENIEC.	La implantación de la NTP ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de Datos del RENIEC optimizara significativamente la seguridad en los datos.	NTP ISO/IEC-27001:2014			**Metodología** ISO/IEC 27001:2013
Específicos	**Específicos**	**Específicos**	**Dependiente**			**Tipo de Investigación** Aplicada Experimental
¿Cómo optimiza en la Confidencialidad de los datos la implantación de la NTP ISO/IEC-27001 en la Sub Gerencia de Gestión de Base de Datos del RENIEC?	Valorar la optimización en la Confidencialidad de la seguridad de los datos al implantar la ISO 27001 en la Sub Gerencia de Gestión de Base de Datos del RENIEC.	La implantación de la NTP ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de Datos del RENIEC optimizara significativamente en la Confidencialidad de la seguridad de los datos.	SEGURIDAD EN LOS DATOS	CONFIDENCIALIDAD	Métrica de Confidencialidad de la BD	**Tipo de Diseño** Pre experimental
¿Cómo optimiza en la Integridad de los datos la implantación de la NTP ISO/IEC-27001 en la Sub Gerencia de Gestión de Base de Datos del RENIEC?	Valorar la optimización en la Integridad de la seguridad de los datos al implantar la ISO 27001 en la Sub Gerencia de Gestión de Base de Datos del RENIEC.	La implantación de la NTP ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de Datos del RENIEC optimizara significativamente en la Integridad de la seguridad de los datos.		INTEGRIDAD	Métrica de Integridad de la BD	**Instrumento** Ficha de Observación
¿Cómo optimiza en la Disponibilidad de los datos la implantación de la NTP ISO/IEC-27001 en la Sub Gerencia de Gestión de Base de Datos del RENIEC?	Valorar la optimización en la Disponibilidad de la seguridad de los datos al implantar la ISO 27001 en la Sub Gerencia de Gestión de Base de Datos del RENIEC.	La implantación de la NTP ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de Datos del RENIEC optimizara significativamente en la Disponibilidad en la seguridad de los datos.		DISPONIBILIDAD	Métrica de Disponibilidad de la BD	

ANEXO B: INSTRUMENTO, POBLACIÓN

FICHA DE EVALUACION MENSUAL DE CUMPLIMIENTO DE LA METRICA

INDICADOR: METRICAS DE CONFIDENCIALIDAD					
IDENTIFICADOR :	SGSI_SGGBD01				
DEFINICION					
Grado de Implementación de políticas de privacidad y confidencialidad de la entidad					
OBJETIVO					
Buscar identificar el nivel de implementación de políticas de privacidad y confidencialidad de la Entidad					
TIPO DEL INDICADOR					
INDICADOR DE CUMPLIMIENTO					
DESCRIPCION DE VARIABLES		**FORMULA**		**FUENTE DE DATOS**	
VS01: ¿Cuál es el grado de intentos de accesos no Autorizados en la Base de Datos?		**INCONF=((TA-TA_NA)/TA) *100** **INCONF:** Indicador de Confidencialidad **TA:** Total de Acceso a la Base de Datos **TA_NA:** Total de Acceso no autorizado		**Reporte Mensual de Control de la Confidencialidad de la Información**	
TEMPORALIDAD:		GENERACION DIARIA DE LA INFORMACION			
METAS					
MINIMA:	**99.5%**	**SATISFACTORIA:**	**99.98%**	**SOBRESALIENTE**	**99.99%**
REVISION MENSUAL					
MES DE EVALUACION		**SUPERVISOR**			
OSERVACIONES					

Ficha de Recolección de Datos

REPORTE MENSUAL DEL CONTROL DE LA CONFIDENCIALIDAD DE LA INFORMACIÓN

Identificador:		SGSI_SGGBD01		
Indicador :		METRICA DE CONFIDENCIALIDAD		
Medicion :		MEDIR EL GRADO DE CONFIDENCIALIDAD EN LA BASE DE DATOS		
Mes :		Abril	Año :	2019
Dia	Total de Usuarios conectados en el dia	Total de Accesos Fallidos	% incidencia	Observaciones
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				
31				
	Promedio Mensual			

FICHA DE EVALUACION MENSUAL DE CUMPLIMIENTO DE LA METRICA

INDICADOR: METRICAS DE INTEGRIDAD					
IDENTIFICADOR :	SGSI_SGGBD02				
DEFINICION					
Grado de Implementación de mecanismos para la integridad de la información					
OBJETIVO					
Buscar identificar el nivel de implementación de políticas de integridad de la información de la Entidad					
TIPO DEL INDICADOR					
INDICADOR DE CUMPLIMIENTO					
DESCRIPCION DE VARIABLES		**FORMULA**		**FUENTE DE DATOS**	
VS02: ¿Cuántas modificaciones se realizaron a la Base de Datos?		**ININTE=(DS-DS_MBD)/DS *100** **ININTE:** Indicador de Integridad **DS:** Total de Documentos Solicitados **DS_MBD:** Total de Documentos solicitados que modifican la Base de Datos		**Reporte Mensual del Control de la Integridad de la Información**	
TEMPORALIDAD:		GENERACION DIARIA DE LA INFORMACION			
METAS					
MINIMA:	**95%**	**SATISFACTORIA:**	**97%**	**SOBRESALIENTE**	**98%**
REVISION MENSUAL					
MES DE EVALUACION			**SUPERVISOR**	**Moisés Clemente Rojas Jaén**	
OBSERVACIONES					

Ficha de Recolección de Datos

REPORTE MENSUAL DEL CONTROL DE LA INTEGRIDAD DE LA INFORMACIÓN

Identificador:		SGSI_SGGBD01		
Indicador :		METRICA DE INTEGRIDAD		
Medicion :		GRADO DE INTEGRIDAD DE LA BASE DE DATOS		
Mes :			Año :	
Dia	Total de Documentos Recibidos	Total de Documentos de Cambios a BD	% de incidencia	Observaciones
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				
31				
	Promedio Mensual			

FICHA DE EVALUACION MENSUAL DE CUMPLIMIENTO DE LA METRICA

INDICADOR: METRICAS DE DISPONIBILIDAD					
IDENTIFICADOR :	SGSI_SGGBD03				
DEFINICION					
Grado de Implementación de las políticas de disponibilidad del servicio a la información					
OBJETIVO					
Buscar identificar el nivel de implementación de políticas de continuidad del servicio de la información de la Entidad					
TIPO DEL INDICADOR					
INDICADOR DE CUMPLIMIENTO					
DESCRIPCION DE VARIABLES		**FORMULA**		**FUENTE DE DATOS**	
VS03: ¿Cuál fue el grado de disponibilidad del servicio de información de la Base de Datos?		**INCONT=((TH-TH_PA)/TH) *100** **INCONT:** Indicador de Continuidad de servicio **TH:** Total de Horas diarias **TH_PA:** Total de Horas sin Servicio de información		**Reporte Mensual de la Disponibilidad del servicio de información**	
TEMPORALIDAD:		GENERACION DIARIA DE LA INFORMACION			
METAS					
MINIMA:	**99.50%**	**SATISFACTORIA:**	**99.80%**	**SOBRESALIENTE**	**99.99%**
REVISION MENSUAL					
MES DE EVALUACION		**SUPERVISOR**		**Moisés Clemente Rojas Jaén**	
OBSERVACIONES					

Ficha de Recolección de Datos

REPORTE MENSUAL DE LA DISPONIBILIDAD DEL SERVICIO DE INFORMACIÓN

Identificador:		SGSI_SGGBD03		
Indicador :		METRICA DE DISPONIBILIDAD		
Medicion :		GRADO DE DISPONIBILIDAD DE LA BASE DE DATOS		
Mes :			Año :	
Dia	Horas dia	Horas de Corte	% de Disponibilidad	Observaciones
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				
31				
	Promedio Mensual			

MOISES CLEMENTE ROJAS JAEN
Sub Gerente de Gestión de Base de Datos
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: ROJAS JAEN Moises Clemente FAU 20295613820 hard
Motivo: Soy el autor del documento
Fecha: 14/06/2019 12:28:38-0500

INDICADOR: METRICAS DE CONFIDENCIALIDAD					
IDENTIFICADOR :	SGSI_SGGBD01				
DEFINICION					
Grado de Implementación de políticas de privacidad y confidencialidad de la entidad					
OBJETIVO					
Buscar identificar el nivel de implementación de políticas de privacidad y confidencialidad de la Entidad					
TIPO DEL INDICADOR					
INDICADOR DE CUMPLIMIENTO					
DESCRIPCION DE VARIABLES		**FORMULA**		**FUENTE DE DATOS**	
VS01: ¿Cuál es el grado de intentos de accesos no Autorizados en la Base de Datos?		**INCONF=((TA-TA_NA)/TA) *100** **INCONF:** Indicador de Confidencialidad **TA:** Total de Acceso a la Base de Datos **TA_NA:** Total de Acceso no autorizado		**Reporte Mensual de Control de la Confidencialidad de la Información**	
TEMPORALIDAD:		GENERACION DIARIA DE LA INFORMACION			
METAS					
MINIMA:	**99.5%**	**SATISFACTORIA:**	**99.98%**	**SOBRESALIENTE**	**99.99%**
REVISION MENSUAL					
MES DE EVALUACION	**ABRIL**	**SUPERVISOR**		**Moisés Rojas Jaén**	
OSERVACIONES					
La ficha de Recolección de Datos para la métrica de Confidencialidad arrojo un promedio mensual de 95.16%, muy por debajo de la mínima estipulada en este indicador antes de la implantación de la NTP ISO/IEC 27001:2014					

MOISES CLEMENTE ROJAS JAEN
Sub Gerente de Gestión de Base de Datos
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: ROJAS JAEN Moises Clemente FAU 20295813820 hard
Motivo: Soy el autor del documento
Fecha: 14/06/2019 12:17:49-0500

RENIEC

Ficha de Recolección de Datos

REPORTE MENSUAL DEL CONTROL DE LA CONFIDENCIALIDAD DE LA INFORMACIÓN

Identificador:		SGSI_SGGBD01		
Indicador :		METRICA DE CONFIDENCIALIDAD		
Medicion :		MEDIR EL GRADO DE CONFIABILIDAD EN LA BASE DE DATOS		
Mes :		Abril	Año :	2019
Dia	Total de Usuarios conectados en el dia	Total de Accesos Fallidos	% incidencia	Observaciones
1	136		100.00%	
2	149		100.00%	
3	133	5	96.24%	
4	131	7	94.66%	
5	134		100.00%	
6	96		100.00%	
7	77	1	98.70%	
8	131		100.00%	
9	132	5	96.21%	
10	134		100.00%	
11	151		100.00%	
12	134	6	95.52%	
13	94		100.00%	
14	81		100.00%	
15	136		100.00%	
16	131	16	87.79%	
17	127		100.00%	
18	74		100.00%	
19	139	5	96.40%	
20	85	12	85.88%	
21	141		100.00%	
22	140		100.00%	
23	136		100.00%	
24	112		100.00%	
25	134		100.00%	
26	131	51	61.07%	
27	153	49	67.97%	
28	75	10	86.67%	
29	141		100.00%	
30	130	16	87.69%	
31				
	Promedio Mensual		95.16%	

MOISES CLEMENTE ROJAS JAEN
Sub Gerente de Gestión de Base de Datos
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: ROJAS JAEN Moises Clemente FAU 20295613620 hard
Motivo: Soy el autor del documento
Fecha: 19/11/2019 17:33:09-0500

INDICADOR: METRICAS DE CONFIDENCIALIDAD					
IDENTIFICADOR :	SGSI_SGGBD01				
DEFINICION					
Grado de Implementación de políticas de privacidad y confidencialidad de la entidad					
OBJETIVO					
Buscar identificar el nivel de implementación de políticas de privacidad y confidencialidad de la Entidad					
TIPO DEL INDICADOR					
INDICADOR DE CUMPLIMIENTO					
DESCRIPCION DE VARIABLES		**FORMULA**		**FUENTE DE DATOS**	
VS01: ¿Cuál es el grado de intentos de accesos no Autorizados en la Base de Datos?		**INCONF=((TA-TA_NA)/TA) *100** **INCONF:** Indicador de Confidencialidad **TA:** Total de Acceso a la Base de Datos **TA_NA:** Total de Acceso no autorizado		**Reporte Mensual de Control de la Confidencialidad de la Información**	
TEMPORALIDAD:	GENERACION DIARIA DE LA INFORMACION				
METAS					
MINIMA:	**99.5%**	**SATISFACTORIA:**	**99.98%**	**SOBRESALIENTE**	**99.99%**
REVISION MENSUAL					
MES DE EVALUACION	**MAYO**	**SUPERVISOR**		**Moisés Rojas Jaén**	
OSERVACIONES					
La ficha de Recolección de Datos para la métrica de Confidencialidad arrojo un promedio mensual de 96.21%, muy por debajo de la mínima estipulada en este indicador antes de la implantación de la NTP ISO/IEC 27001:2014					

MOISES CLEMENTE ROJAS JAEN
Sub Gerente de Gestión de Base de Datos
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: ROJAS JAEN Moises Clemente FAU 20295613820 hard
Motivo: Soy el autor del documento
Fecha: 19/11/2019 17:33:27-0500

RENIEC

Ficha de Recolección de Datos

REPORTE MENSUAL DEL CONTROL DE LA CONFIDENCIALIDAD DE LA INFORMACIÓN

Identificador:		SGSI_SGGBD01		
Indicador :		METRICA DE CONFIDENCIALIDAD		
Medicion :		MEDIR EL GRADO DE CONFIABILIDAD EN LA BASE DE DATOS		
Mes :		Mayo	**Año :**	2019
Dia	**Total de Usuarios conectados en el dia**	**Total de Accesos Fallidos**	**% incidencia**	**Observaciones**
1	82	15	81.71%	
2	134		100.00%	
3	136	6	95.59%	
4	98		100.00%	
5	82	10	87.80%	
6	138		100.00%	
7	135	1	99.26%	
8	112		100.00%	
9	116	5	95.69%	
10	138		100.00%	
11	98	5	94.90%	
12	85		100.00%	
13	131	8	93.89%	
14	134		100.00%	
15	134	5	96.27%	
16	137		100.00%	
17	134		100.00%	
18	97	6	93.81%	
19	147		100.00%	
20	140	9	93.57%	
21	133		100.00%	
22	137	7	94.89%	
23	137		100.00%	
24	128	19	85.16%	
25	101		100.00%	
26	79	3	96.20%	
27	140		100.00%	
28	141	15	89.36%	
29	146	1	99.32%	
30	144	16	88.89%	
31	135			
	Promedio Mensual		96.21%	

RENIEC

MOISES CLEMENTE ROJAS JAEN
Sub Gerente de Gestión de Base de Datos
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: ROJAS JAEN Moises Clemente FAU 20295613620 hard
Motivo: Soy el autor del documento
Fecha: 19/11/2019 17:40:18-0500

INDICADOR: METRICAS DE CONFIDENCIALIDAD					
IDENTIFICADOR :	SGSI_SGGBD01				
DEFINICION					
Grado de Implementación de políticas de privacidad y confidencialidad de la entidad					
OBJETIVO					
Buscar identificar el nivel de implementación de políticas de privacidad y confidencialidad de la Entidad					
TIPO DEL INDICADOR					
INDICADOR DE CUMPLIMIENTO					
DESCRIPCION DE VARIABLES		**FORMULA**		**FUENTE DE DATOS**	
VS01: ¿Cuál es el grado de intentos de accesos no Autorizados en la Base de Datos?		**INCONF=((TA-TA_NA)/TA) *100** **INCONF:** Indicador de Confidencialidad **TA:** Total de Acceso a la Base de Datos **TA_NA:** Total de Acceso no autorizado		**Reporte Mensual de Control de la Confidencialidad de la Información**	
TEMPORALIDAD:	GENERACION DIARIA DE LA INFORMACION				
METAS					
MINIMA:	**99.5%**	**SATISFACTORIA:**	**99.98%**	**SOBRESALIENTE**	**99.99%**
REVISION MENSUAL					
MES DE EVALUACION	**OCTUBRE**	**SUPERVISOR**	**Moisés Rojas Jaén**		
OSERVACIONES					
La ficha de Recolección de Datos para la métrica de Confidencialidad arrojo un promedio mensual de 97.56%, muy por debajo de la minima estipulada en este indicador después de la implantación de la NTP ISO/IEC 27001:2014					

MOISES CLEMENTE ROJAS JAEN
Sub Gerente de Gestión de Base de Datos
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: ROJAS JAEN Moises Clemente FAU 20295613620 hard
Motivo: Soy el autor del documento
Fecha: 19/11/2019 17:42:08-0500

Ficha de Recolección de Datos

REPORTE MENSUAL DEL CONTROL DE LA CONFIDENCIALIDAD DE LA INFORMACIÓN

Identificador:		SGSI_SGGBD01		
Indicador :		METRICA DE CONFIDENCIALIDAD		
Medicion :		MEDIR EL GRADO DE CONFIDENCIALIDAD EN LA BASE DE DATOS		
Mes :		Octubre	**Año :**	2019
Dia	**Total de Usuarios conectados en el dia**	**Total de Accesos Fallidos**	**% incidencia**	**Observaciones**
1	132	4	96.97%	
2	144		100.00%	
3	150		100.00%	
4	141	7	95.04%	
5	98	2	97.96%	
6	82		100.00%	
7	134	7	94.78%	
8	85		100.00%	
9	135		100.00%	
10	143		100.00%	
11	136	5	96.32%	
12	97	1	98.97%	
13	80		100.00%	
14	135	5	96.30%	
15	137	5	96.35%	
16	136		100.00%	
17	138	7	94.93%	
18	136	5	96.32%	
19	104	1	99.04%	
20	91		100.00%	
21	151	6	96.03%	
22	136	6	95.59%	
23	132	6	95.45%	
24	133	8	93.98%	
25	140	2	98.57%	
26	113	2	98.23%	
27	91	2	97.80%	
28	141		100.00%	
29	135	8	94.07%	
30	136	8	94.12%	
31	116	4	96.55%	
	Promedio Mensual		97.56%	

MOISES CLEMENTE ROJAS JAEN
Sub Gerente de Gestión de Base de Datos
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: ROJAS JAEN Moises Clemente FAU 20295613820 hard
Motivo: Soy el autor del documento
Fecha: 14/06/2019 12:27:09-0500

INDICADOR: METRICAS DE INTEGRIDAD					
IDENTIFICADOR :	SGSI_SGGBD02				
DEFINICION					
Grado de Implementación de mecanismos para la integridad de la información					
OBJETIVO					
Buscar identificar el nivel de implementación de políticas de integridad de la información de la Entidad					
TIPO DEL INDICADOR					
INDICADOR DE CUMPLIMIENTO					
DESCRIPCION DE VARIABLES		**FORMULA**		**FUENTE DE DATOS**	
VS02: ¿Cuántas modificaciones se realizaron a la Base de Datos?		**ININTE=(DS-DS_MBD)/DS *100** **ININTE:** Indicador de Integridad **DS:** Total de Documentos Solicitados **DS_MBD:** Total de Documentos solicitados que modifican la Base de Datos		**Reporte Mensual del Control de la Integridad de la Información**	
TEMPORALIDAD:	GENERACION DIARIA DE LA INFORMACION				
METAS					
MINIMA:	**95%**	**SATISFACTORIA:**	**97%**	**SOBRESALIENTE**	**98%**
REVISION MENSUAL					
MES DE EVALUACION	**ABRIL**		**SUPERVISOR**	**Moisés Clemente Rojas Jaén**	
OBSERVACIONES					
La ficha de Recolección de Datos para la métrica de Integridad arrojo un promedio mensual de 82.44%, muy por debajo de la mínima estipulada en este indicador antes de la implantación de la NTP ISO/IEC 27001:2014					

MOISES CLEMENTE ROJAS JAEN
Sub Gerente de Gestión de Base de Datos
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: ROJAS JAEN Moises Clemente FAU 20295613820 hard
Motivo: Soy el autor del documento
Fecha: 14/06/2019 12:19:01-0500

RENIEC

Ficha de Recolección de Datos

REPORTE MENSUAL DEL CONTROL DE LA INTEGRIDAD DE LA INFORMACIÓN

Identificador:		SGSI_SGGBD01		
Indicador :		METRICA DE INTEGRIDAD		
Medicion :		GRADO DE INTEGRIDAD DE LA BASE DE DATOS		
Mes :		Abril	**Año :**	2019
Dia	**Total de Documentos Recibidos**	**Total de Documentos de Cambios a BD**	**% de incidencia**	**Observaciones**
1	6	0	100.00%	
2	56	3	94.64%	
3	25	0	100.00%	
4	46	26	43.48%	
5	41	1	97.56%	
6				
7				
8	45	23	48.89%	
9	25	0	100.00%	
10	23	0	100.00%	
11	50	13	74.00%	
12	55	23	58.18%	
13				
14				
15	7	1	85.71%	
16	63	11	82.54%	
17	38	18	52.63%	
18				
19				
20				
21				
22	53	0	100.00%	
23	17	3	82.35%	
24	4	0	100.00%	
25	15	10	33.33%	
26	45	1	97.78%	
27				
28				
29	23	0	100.00%	
30	45	1	97.78%	
31				
	Promedio Mensual		82.44%	

MOISES CLEMENTE ROJAS JAEN
Sub Gerente de Gestión de Base de Datos
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: ROJAS JAEN Moises Clemente FAU 20295613620 hard
Motivo: Soy el autor del documento
Fecha: 14/08/2019 12:27:54-0500

INDICADOR: METRICAS DE INTEGRIDAD					
IDENTIFICADOR :	SGSI_SGGBD02				
DEFINICION					
Grado de Implementación de mecanismos para la integridad de la información					
OBJETIVO					
Buscar identificar el nivel de implementación de políticas de integridad de la información de la Entidad					
TIPO DEL INDICADOR					
INDICADOR DE CUMPLIMIENTO					
DESCRIPCION DE VARIABLES		**FORMULA**		**FUENTE DE DATOS**	
VS02: ¿Cuántas modificaciones se realizaron a la Base de Datos?		**ININTE=(DS-DS_MBD)/DS *100** **ININTE:** Indicador de Integridad **DS:** Total de Documentos Solicitados **DS_MBD:** Total de Documentos solicitados que modifican la Base de Datos		**Reporte Mensual del Control de la Integridad de la Información**	
TEMPORALIDAD:		GENERACION DIARIA DE LA INFORMACION			
METAS					
MINIMA:	**95%**	**SATISFACTORIA:**	**97%**	**SOBRESALIENTE**	**98%**
REVISION MENSUAL					
MES DE EVALUACION	**MAYO**		**SUPERVISOR**	**Moisés Clemente Rojas Jaén**	
OBSERVACIONES					
La ficha de Recolección de Datos para la métrica de Integridad arrojo un promedio mensual de 78.03%, muy por debajo de la mínima estipulada en este indicador antes de la implantación de la NTP ISO/IEC 27001:2014					

MOISES CLEMENTE ROJAS JAEN
Sub Gerente de Gestión de Base de Datos
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: ROJAS JAEN Moises Clemente FAU 20295613620 hard
Motivo: Soy el autor del documento
Fecha: 14/08/2019 12:19:16-0500

RENIEC

Ficha de Recolección de Datos

REPORTE MENSUAL DEL CONTROL DE LA INTEGRIDAD DE LA INFORMACIÓN

Identificador:		SGSI_SGGBD01		
Indicador :		METRICA DE INTEGRIDAD		
Medicion :		GRADO DE INTEGRIDAD DE LA BASE DE DATOS		
Mes :		Mayo	**Año :**	2019
Dia	**Total de Documentos Recibidos**	**Total de Documentos de Cambios a BD**	**% de incidencia**	**Observaciones**
1				
2	17	11	35.29%	
3	31	26	16.13%	
4	2	0	100.00%	
5				
6	35	3	91.43%	
7	29	1	96.55%	
8	54	22	59.26%	
9	56	1	98.21%	
10	10	4	60.00%	
11				
12				
13	42	0	100.00%	
14	10	1	90.00%	
15	47	24	48.94%	
16	39	0	100.00%	
17	8	0	100.00%	
18	2	0	100.00%	
19				
20	53	19	64.15%	
21	76	6	92.11%	
22	25	0	100.00%	
23	9	0	100.00%	
24	21	16	23.81%	
25				
26				
27	55	32	41.82%	
28	17	1	94.12%	
29	13	0	100.00%	
30	72	2	97.22%	
31	55	20	63.64%	
	Promedio Mensual		78.03%	

MOISES CLEMENTE ROJAS JAEN
Sub Gerente de Gestion de Base de Datos
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: ROJAS JAEN Moises Clemente FAU 20295613620 hard
Motivo: Soy el autor del documento
Fecha: 19/11/2019 17:46:32-0500

INDICADOR: METRICAS DE INTEGRIDAD					
IDENTIFICADOR :	SGSI_SGGBD02				
DEFINICION					
Grado de Implementación de mecanismos para la integridad de la información					
OBJETIVO					
Buscar identificar el nivel de implementación de políticas de integridad de la información de la Entidad					
TIPO DEL INDICADOR					
INDICADOR DE CUMPLIMIENTO					
DESCRIPCION DE VARIABLES		**FORMULA**		**FUENTE DE DATOS**	
VS02: ¿Cuántas modificaciones se realizaron a la Base de Datos?		**ININTE=(DS-DS_MBD)/DS *100** **ININTE:** Indicador de Integridad **DS:** Total de Documentos Solicitados **DS_MBD:** Total de Documentos solicitados que modifican la Base de Datos		**Reporte Mensual del Control de la Integridad de la Información**	
TEMPORALIDAD:	GENERACION DIARIA DE LA INFORMACION				
METAS					
MINIMA:	**95%**	**SATISFACTORIA:**	**97%**	**SOBRESALIENTE**	**98%**
REVISION MENSUAL					
MES DE EVALUACION	**OCTUBRE**		**SUPERVISOR**	**Moisés Clemente Rojas Jaén**	
OBSERVACIONES					
La ficha de Recolección de Datos para la métrica de Integridad arrojo un promedio mensual de 83.70%, muy por debajo de la minima estipulada en este indicador después de la implantación de la NTP ISO/IEC 27001:2014					

MOISES CLEMENTE ROJAS JAEN
Sub Gerente de Gestión de Base de Datos
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: ROJAS JAEN Moises Clemente FAU 20295613620 hard
Motivo: Soy el autor del documento
Fecha: 19/11/2019 17:42:33-0500

RENIEC

Ficha de Recolección de Datos

REPORTE MENSUAL DEL CONTROL DE LA INTEGRIDAD DE LA INFORMACIÓN

Identificador:		SGSI_SGGBD01		
Indicador :		METRICA DE INTEGRIDAD		
Medicion :		GRADO DE INTEGRIDAD DE LA BASE DE DATOS		
Mes :		Octubre	**Año :**	2019
Dia	**Total de Documentos Recibidos**	**Total de Documentos de Cambios a BD**	**% de incidencia**	**Observaciones**
1	7	0	100.00%	
2	18	2	88.89%	
3	38	12	68.42%	
4	29	1	96.55%	
5				
6				
7	63	5	92.06%	
8				
9	35	17	51.43%	
10	16	0	100.00%	
11	42	3	92.86%	
12				
13				
14	7	0	100.00%	
15	45	11	75.56%	
16	32	4	87.50%	
17	33	8	75.76%	
18	28	12	57.14%	
19				
20				
21	30	7	76.67%	
22	24	3	87.50%	
23	19	0	100.00%	
24	19	9	52.63%	
25	26	2	92.31%	
26				
27				
28	23	2	91.30%	
29	60	0	100.00%	
30	29	8	72.41%	
31	34	6	82.35%	
	Promedio Mensual		83.70%	

MOISES CLEMENTE ROJAS JAEN
Sub Gerente de Gestión de Base de Datos
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: ROJAS JAEN Moises Clemente FAU 20295613620 hard
Motivo: Soy el autor del documento
Fecha: 14/06/2019 12:26:54-0500

INDICADOR: METRICAS DE DISPONIBILIDAD					
IDENTIFICADOR :	SGSI_SGGBD03				
DEFINICION					
Grado de Implementación de las políticas de disponibilidad del servicio a la información					
OBJETIVO					
Buscar identificar el nivel de implementación de políticas de continuidad del servicio de la información de la Entidad					
TIPO DEL INDICADOR					
INDICADOR DE CUMPLIMIENTO					
DESCRIPCION DE VARIABLES		**FORMULA**		**FUENTE DE DATOS**	
VS03: ¿Cuál fue el grado de disponibilidad del servicio de información de la Base de Datos?		**INCONT=((TH-TH_PA)/TH) *100** **INCONT:** Indicador de Continuidad de servicio **TH:** Total de Horas diarias **TH_PA:** Total de Horas sin Servicio de información		**Reporte Mensual de la Disponibilidad del servicio de información**	
TEMPORALIDAD:		GENERACION DIARIA DE LA INFORMACION			
METAS					
MINIMA:	99.50%	**SATISFACTORIA:**	99.80%	**SOBRESALIENTE**	99.99%
REVISION MENSUAL					
MES DE EVALUACION	**ABRIL**		**SUPERVISOR**	**Moisés Clemente Rojas Jaén**	
OBSERVACIONES					
La ficha de Recolección de Datos para la métrica de DISPONIBILIDAD arrojo un promedio mensual de 97.26%, muy por debajo de la mínima estipulada en este indicador antes de la implantación de la NTP ISO/IEC 27001:2014					

MOISES CLEMENTE ROJAS JAEN
Sub Gerente de Gestión de Base de Datos
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: ROJAS JAEN Moises Clemente FAU 20295613820 hard
Motivo: Soy el autor del documento
Fecha: 14/06/2019 12:18:30-0500

RENIEC

Ficha de Recolección de Datos

REPORTE MENSUAL DE LA DISPONIBILIDAD DEL SERVICIO DE INFORMACIÓN

Identificador:		SGSI_SGGBD03		
Indicador :		METRICA DE DISPONIBILIDAD		
Medicion :		GRADO DE DISPONIBILIDAD DE LA BASE DE DATOS		
Mes :		Abril	Año :	2019
Dia	Horas dia	Horas de Corte	% de Disponibilidad	Observaciones
1	24.00		100.00%	
2	24.00	0.15	99.38%	
3	24.00		100.00%	
4	24.00		100.00%	
5	24.00	0.20	99.17%	
6	24.00		100.00%	
7	24.00	4.20	82.50%	
8	24.00		100.00%	
9	24.00		100.00%	
10	24.00		100.00%	
11	24.00	0.55	97.71%	
12	24.00		100.00%	
13	24.00		100.00%	
14	24.00	4.35	81.88%	
15	24.00		100.00%	
16	24.00	0.15	99.38%	
17	24.00		100.00%	
18	24.00	0.40	98.33%	
19	24.00	0.17	99.31%	
20	24.00	0.13	99.44%	
21	24.00	4.45	81.46%	
22	24.00		100.00%	
23	24.00		100.00%	
24	24.00	0.45	98.13%	
25	24.00		100.00%	
26	24.00		100.00%	
27	24.00		100.00%	
28	24.00	4.50	81.25%	
29	24.00		100.00%	
30	24.00		100.00%	
31				
	Promedio Mensual		97.26%	

RENIEC

MOISES CLEMENTE ROJAS JAEN
Sub Gerente de Gestión de Base de Datos
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: ROJAS JAEN Moises Clemente FAU 20295613620 hard
Motivo: Soy el autor del documento
Fecha: 14/06/2019 12:27:41-0500

INDICADOR: METRICAS DE DISPONIBILIDAD					
IDENTIFICADOR :	SGSI_SGGBD03				
DEFINICION					
Grado de Implementación de las políticas de disponibilidad del servicio a la información					
OBJETIVO					
Buscar identificar el nivel de implementación de políticas de continuidad del servicio de la información de la Entidad					
TIPO DEL INDICADOR					
INDICADOR DE CUMPLIMIENTO					
DESCRIPCION DE VARIABLES		**FORMULA**		**FUENTE DE DATOS**	
VS03: ¿Cuál fue el grado de disponibilidad del servicio de información de la Base de Datos?		INCONT=((TH-TH_PA)/TH) *100 **INCONT:** Indicador de Continuidad de servicio **TH:** Total de Horas diarias **TH_PA:** Total de Horas sin Servicio de información		**Reporte Mensual de la Disponibilidad del servicio de información**	
TEMPORALIDAD:		GENERACION DIARIA DE LA INFORMACION			
METAS					
MINIMA:	**99.50%**	**SATISFACTORIA:**	**99.80%**	**SOBRESALIENTE**	**99.99%**
REVISION MENSUAL					
MES DE EVALUACION	**MAYO**		**SUPERVISOR**	**Moisés Clemente Rojas Jaén**	
OBSERVACIONES					
La ficha de Recolección de Datos para la métrica de DISPONIBILIDAD arrojo un promedio mensual de 96.39%, muy por debajo de la mínima estipulada en este indicador antes de la implantación de la NTP ISO/IEC 27001:2014					

MOISES CLEMENTE ROJAS JAEN
Sub Gerente de Gestión de Base de Datos
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: ROJAS JAEN Moises Clemente FAU 20295813620 hard
Motivo: Soy el autor del documento
Fecha: 14/06/2019 12:18:45-0500

RENIEC

Ficha de Recolección de Datos

REPORTE MENSUAL DE LA DISPONIBILIDAD DEL SERVICIO DE INFORMACIÓN

Identificador:		SGSI_SGGBD03		
Indicador :		METRICA DE DISPONIBILIDAD		
Medicion :		GRADO DE DISPONIBILIDAD DE LA BASE DE DATOS		
Mes :		**Mayo**	**Año :**	**2019**
Dia	**Horas dia**	**Horas de Corte**	**% de Disponibilidad**	**Observaciones**
1	24	6.5	72.92%	
2	24		100.00%	
3	24	0.14	99.42%	
4	24		100.00%	
5	24	4.15	82.71%	
6	24		100.00%	
7	24	0.15	99.38%	
8	24		100.00%	
9	24		100.00%	
10	24	0.14	99.42%	
11	24		100.00%	
12	24	4.5	81.25%	
13	24		100.00%	
14	24		100.00%	
15	24	0.25	98.96%	
16	24		100.00%	
17	24		100.00%	
18	24		100.00%	
19	24	4.25	82.29%	
20	24		100.00%	
21	24		100.00%	
22	24	0.15	99.38%	
23	24		100.00%	
24	24		100.00%	
25	24		100.00%	
26	24	4.15	82.71%	
27	24		100.00%	
28	24		100.00%	
29	24		100.00%	
30	24		100.00%	
31	24	2.5	89.58%	
	Promedio Mensual		96.39%	

MOISES CLEMENTE ROJAS JAEN
Sub Gerente de Gestión de Base de Datos
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: ROJAS JAEN Moises Clemente FAU 20295613620 hard
Motivo: Soy el autor del documento
Fecha: 19/11/2019 17:48:43-0500

INDICADOR: METRICAS DE DISPONIBILIDAD					
IDENTIFICADOR :	SGSI_SGGBD03				
DEFINICION					
Grado de Implementación de las políticas de disponibilidad del servicio a la información					
OBJETIVO					
Buscar identificar el nivel de implementación de políticas de continuidad del servicio de la información de la Entidad					
TIPO DEL INDICADOR					
INDICADOR DE CUMPLIMIENTO					
DESCRIPCION DE VARIABLES		**FORMULA**		**FUENTE DE DATOS**	
VS03: ¿Cuál fue el grado de disponibilidad del servicio de información de la Base de Datos?		**INCONT=((TH-TH_PA)/TH) *100** **INCONT:** Indicador de Continuidad de servicio **TH:** Total de Horas diarias **TH_PA:** Total de Horas sin Servicio de información		**Reporte Mensual de la Disponibilidad del servicio de información**	
TEMPORALIDAD:		GENERACION DIARIA DE LA INFORMACION			
METAS					
MINIMA:	99.50%	**SATISFACTORIA:**	99.80%	**SOBRESALIENTE**	99.99%
REVISION MENSUAL					
MES DE EVALUACION	**OCTUBRE**	**SUPERVISOR**	**Moisés Clemente Rojas Jaén**		
OBSERVACIONES					
La ficha de Recolección de Datos para la métrica de DISPONIBILIDAD arrojo un promedio mensual de 99.98%, meta SATISFACTORIA estipulada en este indicador después de la implantación de la NTP ISO/IEC 27001:2014					

MOISES CLEMENTE ROJAS JAEN
Sub Gerente de Gestión de Base de Datos
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: ROJAS JAEN Moises Clemente FAU 20295613020 hard
Motivo: Soy el autor del documento
Fecha: 18/11/2019 17:42:21-0500

RENIEC

Ficha de Recolección de Datos

REPORTE MENSUAL DE LA DISPONIBILIDAD DEL SERVICIO DE INFORMACIÓN

Identificador:		SGSI_SGGBD03		
Indicador :		METRICA DE DISPONIBILIDAD		
Medicion :		GRADO DE DISPONIBILIDAD DE LA BASE DE DATOS		
Mes :		Octubre	**Año :**	2019
Dia	**Horas dia**	**Horas de Corte**	**% de Disponibilidad**	**Observaciones**
1	24		100.00%	
2	24		100.00%	
3	24		100.00%	
4	24		100.00%	
5	24		100.00%	
6	24		100.00%	
7	24		100.00%	
8	24		100.00%	
9	24		100.00%	
10	24		100.00%	
11	24		100.00%	
12	24		100.00%	
13	24		100.00%	
14	24		100.00%	
15	24		100.00%	
16	24		100.00%	
17	24		100.00%	
18	24		100.00%	
19	24		100.00%	
20	24		100.00%	
21	24		100.00%	
22	24		100.00%	
23	24		100.00%	
24	24		100.00%	
25	24		100.00%	
26	24		100.00%	
27	24		100.00%	
28	24	0.14	99.42%	
29	24		100.00%	
30	24		100.00%	
31	24		100.00%	
	Promedio Mensual		99.98%	

ANEXO C: FICHA DE JUICIO DE EXPERTOS

UCV
UNIVERSIDAD CÉSAR VALLEJO

TABLA DE EVALUACIÓN DE EXPERTOS

APELLIDOS Y NOMBRES DEL EXPERTO: Romero Valencia Monica
TÍTULO Y/O GRADO:
PhD ( ) Doctor (X) Magister ( ) Ingeniero ( ) Licenciado ( ) Otros ( )
Universidad que labora: Universidad César Vallejo
Fecha: 15/6/19

TESIS: SEGURIDAD EN LOS DATOS E IMPLANTACIÓN DE LA NTP-ISO/IEC 27001:2014 EN LA SUB GERENCIA DE GESTIÓN DE BASE DE DATOS DEL RENIEC

INDICADOR: METRICAS DE CONFIDENCIALIDAD

FORMULA: **INCONF=((TA-TA_NA) / TA) *100**

INCONF: Indicador de Confidencialidad
TA: Total de Acceso a la Base de Datos
TA_NA: Total de Acceso no autorizado

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar el instrumento que se empleará mediante una serie de preguntas marcando un valor porcentual. Asimismo, le exhortamos en la corrección de los ítems indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia del instrumento.

ITEMS	PREGUNTAS	Deficiente 0-20%	Regular 21%-50%	Bueno 51%-70%	Muy Bueno 71%-80%	Excelente 81%-100%
1	¿El instrumento de medición cumple con el diseño adecuado?				75	
2	¿El instrumento de recolección de datos tiene relación con el título de la investigación?				75	
3	¿El instrumento de recolección de datos tiene relación con las variables de investigación?				75	
4	¿El instrumento de recolección de datos facilitará el logro de los objetivos de investigación?				75	
5	¿El instrumento analiza los datos de la organización?				75	
6	¿El instrumento de medición explica en forma precisa y clara el grado de cumplimiento de la meta o resultado?				75	
7	¿El resultado del instrumento es entendible para ser correctamente analizado?				75	
TOTAL						

Fuente: Vargas Pinto: Tesis Business Intellenge para el pronóstico de ventas en la empresa Zona Cel S.A.C, 2018

PROMEDIO TOTAL:

EL INSTRUMENTO PUEDE SER APLICADO: SI ( ) NO ( )

SUGERENCIAS: _____

UCV
UNIVERSIDAD CÉSAR VALLEJO

TABLA DE EVALUACIÓN DE EXPERTOS

APELLIDOS Y NOMBRES DEL EXPERTO: Romero Valencia Monica.
TÍTULO Y/O GRADO:
PhD ( ) Doctor (X) Magister ( ) Ingeniero ( ) Licenciado ( ) Otros ( )
Universidad que labora: Universidad César Vallejo
Fecha: 15/6/19

TESIS: SEGURIDAD EN LOS DATOS E IMPLANTACIÓN DE LA NTP-ISO/IEC 27001:2014 EN LA SUB GERENCIA DE GESTIÓN DE BASE DE DATOS DEL RENIEC

INDICADOR:	METRICAS DE INTEGRIDAD	
FORMULA:	**ININTE=(DS-DS_MBD / DS) *100**	**ININTE:** Indicador de Integridad **DS:** Total de Documentos Solicitados **DS_MBD:** Total de Documentos solicitados que modifican la Base de Datos

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar el instrumento que se empleará mediante una serie de preguntas marcando un valor porcentual. Asimismo, le exhortamos en la corrección de los ítems indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia del instrumento.

ITEMS	PREGUNTAS	Deficiente 0-20%	Regular 21%-50%	Bueno 51%-70%	Muy Bueno 71%-80%	Excelente 81%-100%
1	¿El instrumento de medición cumple con el diseño adecuado?				80	
2	¿El instrumento de recolección de datos tiene relación con el título de la investigación?				80	
3	¿El instrumento de recolección de datos tiene relación con las variables de investigación?				80	
4	¿El instrumento de recolección de datos facilitará el logro de los objetivos de investigación?				80	
5	¿El instrumento analiza los datos de la organización?				80	
6	¿El instrumento de medición explica en forma precisa y clara el grado de cumplimiento de la meta o resultado?				80	
7	¿El resultado del instrumento es entendible para ser correctamente analizado?				80	
TOTAL						

Fuente: Vargas Pinto: Tesis Business Intellenge para el pronóstico de ventas en la empresa Zona Cel S.A.C, 2018

PROMEDIO TOTAL:

EL INSTRUMENTO PUEDE SER APLICADO: SI ( ) NO ( )

SUGERENCIAS: _____

UCV
UNIVERSIDAD CÉSAR VALLEJO

TABLA DE EVALUACIÓN DE EXPERTOS

APELLIDOS Y NOMBRES DEL EXPERTO: Romero Valencia Monica
TÍTULO Y/O GRADO:
PhD ( ) Doctor (X) Magister ( ) Ingeniero ( ) Licenciado ( ) Otros ( )
Universidad que labora: Universidad César Vallejo
Fecha: 15/6/19

TESIS: SEGURIDAD EN LOS DATOS E IMPLANTACIÓN DE LA NTP-ISO/IEC 27001:2014 EN LA SUB GERENCIA DE GESTIÓN DE BASE DE DATOS DEL RENIEC

INDICADOR:	METRICAS DE DISPONIBILIDAD	
FORMULA:	**INCONT=((TH-TH_PA) / TH) *100**	**INCONT:** Indicador de Disponibilidad de servicio **TH:** Total de Horas diarias **TH_PA:** Total de Horas sin Servicio de información

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar el instrumento que se empleará mediante una serie de preguntas marcando un valor porcentual. Asimismo, le exhortamos en la corrección de los ítems indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia del instrumento.

ITEMS	PREGUNTAS	Deficiente 0-20%	Regular 21%-50%	Bueno 51%-70%	Muy Bueno 71%-80%	Excelente 81%-100%
1	¿El instrumento de medición cumple con el diseño adecuado?				78	
2	¿El instrumento de recolección de datos tiene relación con el título de la investigación?				78	
3	¿El instrumento de recolección de datos tiene relación con las variables de investigación?				78	
4	¿El instrumento de recolección de datos facilitará el logro de los objetivos de investigación?				78	
5	¿El instrumento analiza los datos de la organización?				78	
6	¿El instrumento de medición explica en forma precisa y clara el grado de cumplimiento de la meta o resultado?				78	
7	¿El resultado del instrumento es entendible para ser correctamente analizado?				78	
TOTAL						

Fuente: Vargas Pinto: Tesis Business Intellenge para el pronóstico de ventas en la empresa Zona Cel S.A.C, 2018

PROMEDIO TOTAL:

EL INSTRUMENTO PUEDE SER APLICADO: SI ( ) NO ( )

SUGERENCIAS: _____

UCV
UNIVERSIDAD CÉSAR VALLEJO

TABLA DE EVALUACIÓN DE EXPERTOS

APELLIDOS Y NOMBRES DEL EXPERTO: Gálvez Tapia Orleans Moisés.
TÍTULO Y/O GRADO:
PhD ( ) Doctor ( ) Magister (✓) Ingeniero ( ) Licenciado ( ) Otros ( )
Universidad que labora: Universidad César Vallejo
Fecha: 12 / 06 / 2019

TESIS: SEGURIDAD EN LOS DATOS E IMPLANTACIÓN DE LA NTP-ISO/IEC 27001:2014 EN LA SUB GERENCIA DE GESTIÓN DE BASE DE DATOS DEL RENIEC

INDICADOR:	METRICAS DE CONFIDENCIALIDAD	
FORMULA:	**INCONF=((TA-TA_NA) / TA) *100**	**INCONF:** Indicador de Confidencialidad **TA:** Total de Acceso a la Base de Datos **TA_NA:** Total de Acceso no autorizado

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar el instrumento que se empleará mediante una serie de preguntas marcando un valor porcentual. Asimismo, le exhortamos en la corrección de los ítems indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia del instrumento.

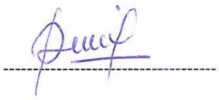
ITEMS	PREGUNTAS	Deficiente 0-20%	Regular 21%-50%	Bueno 51%-70%	Muy Bueno 71%-80%	Excelente 81%-100%
1	¿El instrumento de medición cumple con el diseño adecuado?				80%	
2	¿El instrumento de recolección de datos tiene relación con el título de la investigación?				80%	
3	¿El instrumento de recolección de datos tiene relación con las variables de investigación?				80%	
4	¿El instrumento de recolección de datos facilitará el logro de los objetivos de investigación?				80%	
5	¿El instrumento analiza los datos de la organización?				80%	
6	¿El instrumento de medición explica en forma precisa y clara el grado de cumplimiento de la meta o resultado?				80%	
7	¿El resultado del instrumento es entendible para ser correctamente analizado?				80%	
TOTAL						

Fuente: Vargas Pinto: Tesis Business Intellenge para el pronóstico de ventas en la empresa Zona Cel S.A.C, 2018

PROMEDIO TOTAL:

EL INSTRUMENTO PUEDE SER APLICADO: SI (✓) NO ( )

SUGERENCIAS: _____



UCV
UNIVERSIDAD CÉSAR VALLEJO

TABLA DE EVALUACIÓN DE EXPERTOS

APELLIDOS Y NOMBRES DEL EXPERTO: Gálvez Tapia Orleans Moisés
TÍTULO Y/O GRADO:
PhD ( ) Doctor ( ) Magister (✓) Ingeniero ( ) Licenciado ( ) Otros ( )
Universidad que labora: Universidad César Vallejo
Fecha: 19/07 / 2019

TESIS: SEGURIDAD EN LOS DATOS E IMPLANTACIÓN DE LA NTP-ISO/IEC 27001:2014 EN LA SUB GERENCIA DE GESTIÓN DE BASE DE DATOS DEL RENIEC

INDICADOR: METRICAS DE INTEGRIDAD

FORMULA: **ININTE=(DS-DS_MBD / DS) *100**

ININTE: Indicador de Integridad
DS: Total de Documentos Solicitados
DS_MBD: Total de Documentos solicitados que modifican la Base de Datos

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar el instrumento que se empleará mediante una serie de preguntas marcando un valor porcentual. Asimismo, le exhortamos en la corrección de los ítems indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia del instrumento.

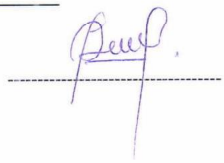
ITEMS	PREGUNTAS	Deficiente 0-20%	Regular 21%-50%	Bueno 51%-70%	Muy Bueno 71%-80%	Excelente 81%-100%
1	¿El instrumento de medición cumple con el diseño adecuado?					90%
2	¿El instrumento de recolección de datos tiene relación con el título de la investigación?					90%
3	¿El instrumento de recolección de datos tiene relación con las variables de investigación?					90%
4	¿El instrumento de recolección de datos facilitará el logro de los objetivos de investigación?					90%
5	¿El instrumento analiza los datos de la organización?					90%
6	¿El instrumento de medición explica en forma precisa y clara el grado de cumplimiento de la meta o resultado?					90%
7	¿El resultado del instrumento es entendible para ser correctamente analizado?					90%
TOTAL						

Fuente: Vargas Pinto: Tesis Business Intellenge para el pronóstico de ventas en la empresa Zona Cel S.A.C, 2018

PROMEDIO TOTAL:

EL INSTRUMENTO PUEDE SER APLICADO: SI (✓) NO ( )

SUGERENCIAS: _____



UCV
UNIVERSIDAD CÉSAR VALLEJO

TABLA DE EVALUACIÓN DE EXPERTOS

APELLIDOS Y NOMBRES DEL EXPERTO: Gálvez Tapia Orleans Moisés.
TÍTULO Y/O GRADO:
PhD ( ) Doctor ( ) Magister (✓) Ingeniero ( ) Licenciado ( ) Otros ( )
Universidad que labora: Universidad César Vallejo
Fecha: 19 / 07 / 2019

TESIS: SEGURIDAD EN LOS DATOS E IMPLANTACIÓN DE LA NTP-ISO/IEC 27001:2014 EN LA SUB GERENCIA DE GESTIÓN DE BASE DE DATOS DEL RENIEC

INDICADOR:	METRICAS DE DISPONIBILIDAD	
FORMULA:	**INCONT=((TH-TH_PA) / TH) *100**	**INCONT:** Indicador de Disponibilidad de servicio **TH:** Total de Horas diarias **TH_PA:** Total de Horas sin Servicio de información

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar el instrumento que se empleará mediante una serie de preguntas marcando un valor porcentual. Asimismo, le exhortamos en la corrección de los ítems indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia del instrumento.

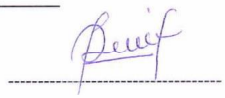
ITEMS	PREGUNTAS	Deficiente 0-20%	Regular 21%-50%	Bueno 51%-70%	Muy Bueno 71%-80%	Excelente 81%-100%
1	¿El instrumento de medición cumple con el diseño adecuado?					90%
2	¿El instrumento de recolección de datos tiene relación con el título de la investigación?					90%
3	¿El instrumento de recolección de datos tiene relación con las variables de investigación?					90%
4	¿El instrumento de recolección de datos facilitará el logro de los objetivos de investigación?					90%
5	¿El instrumento analiza los datos de la organización?					90%
6	¿El instrumento de medición explica en forma precisa y clara el grado de cumplimiento de la meta o resultado?					90%
7	¿El resultado del instrumento es entendible para ser correctamente analizado?					90%
TOTAL						

Fuente: Vargas Pinto: Tesis Business Intellenge para el pronóstico de ventas en la empresa Zona Cel S.A.C, 2018

PROMEDIO TOTAL:

EL INSTRUMENTO PUEDE SER APLICADO: SI (✓) NO ( )

SUGERENCIAS: _____



UCV
UNIVERSIDAD CÉSAR VALLEJO

TABLA DE EVALUACIÓN DE EXPERTOS

APELLIDOS Y NOMBRES DEL EXPERTO: Huarote Zegarra Raul
TÍTULO Y/O GRADO:
PhD ( ) Doctor ( ) Magister (✓) Ingeniero ( ) Licenciado ( ) Otros ( )
Universidad que labora: Universidad César Vallejo
Fecha: 12/06/19

TESIS: SEGURIDAD EN LOS DATOS E IMPLANTACIÓN DE LA NTP-ISO/IEC 27001:2014 EN LA SUB GERENCIA DE GESTIÓN DE BASE DE DATOS DEL RENIEC

INDICADOR:	METRICAS DE CONFIDENCIALIDAD	
FORMULA:	**INCONF=((TA-TA_NA) / TA) *100**	**INCONF:** Indicador de Confidencialidad **TA:** Total de Acceso a la Base de Datos **TA_NA:** Total de Acceso no autorizado

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar el instrumento que se empleará mediante una serie de preguntas marcando un valor porcentual. Asimismo, le exhortamos en la corrección de los ítems indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia del instrumento.

ITEMS	PREGUNTAS	Deficiente 0-20%	Regular 21%-50%	Bueno 51%-70%	Muy Bueno 71%-80%	Excelente 81%-100%
1	¿El instrumento de medición cumple con el diseño adecuado?					95
2	¿El instrumento de recolección de datos tiene relación con el título de la investigación?					90
3	¿El instrumento de recolección de datos tiene relación con las variables de investigación?					95
4	¿El instrumento de recolección de datos facilitará el logro de los objetivos de investigación?					90
5	¿El instrumento analiza los datos de la organización?					95
6	¿El instrumento de medición explica en forma precisa y clara el grado de cumplimiento de la meta o resultado?					95
7	¿El resultado del instrumento es entendible para ser correctamente analizado?					90
TOTAL						

Fuente: Vargas Pinto: Tesis Business Intellenge para el pronóstico de ventas en la empresa Zona Cel S.A.C, 2018

PROMEDIO TOTAL:

EL INSTRUMENTO PUEDE SER APLICADO: SI (✓) NO ( )

SUGERENCIAS: _____

UCV
UNIVERSIDAD CÉSAR VALLEJO

TABLA DE EVALUACIÓN DE EXPERTOS

APELLIDOS Y NOMBRES DEL EXPERTO: Alvarado Zegarra Raul.
TÍTULO Y/O GRADO:
PhD ( ) Doctor ( ) Magister (✓) Ingeniero ( ) Licenciado ( ) Otros ( )
Universidad que labora: Universidad César Vallejo
Fecha: 18/07/19.

TESIS: SEGURIDAD EN LOS DATOS E IMPLANTACIÓN DE LA NTP-ISO/IEC 27001:2014 EN LA SUB GERENCIA DE GESTIÓN DE BASE DE DATOS DEL RENIEC

INDICADOR:	METRICAS DE INTEGRIDAD	
FORMULA:	**ININTE=(DS-DS_MBD / DS) *100**	**ININTE:** Indicador de Integridad **DS:** Total de Documentos Solicitados **DS_MBD:** Total de Documentos solicitados que modifican la Base de Datos

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar el instrumento que se empleará mediante una serie de preguntas marcando un valor porcentual. Asimismo, le exhortamos en la corrección de los ítems indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia del instrumento.

ITEMS	PREGUNTAS	Deficiente 0-20%	Regular 21%-50%	Bueno 51%-70%	Muy Bueno 71%-80%	Excelente 81%-100%
1	¿El instrumento de medición cumple con el diseño adecuado?					85
2	¿El instrumento de recolección de datos tiene relación con el título de la investigación?					90
3	¿El instrumento de recolección de datos tiene relación con las variables de investigación?					95
4	¿El instrumento de recolección de datos facilitará el logro de los objetivos de investigación?					95
5	¿El instrumento analiza los datos de la organización?					90
6	¿El instrumento de medición explica en forma precisa y clara el grado de cumplimiento de la meta o resultado?					95
7	¿El resultado del instrumento es entendible para ser correctamente analizado?					95
TOTAL						

Fuente: Vargas Pinto: Tesis Business Intellenge para el pronóstico de ventas en la empresa Zona Cel S.A.C, 2018

PROMEDIO TOTAL:

EL INSTRUMENTO PUEDE SER APLICADO: SI (✓) NO ( )

SUGERENCIAS: _____

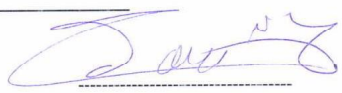


TABLA DE EVALUACIÓN DE EXPERTOS

APELLIDOS Y NOMBRES DEL EXPERTO: Huarote Zegarra Raul.
TÍTULO Y/O GRADO:
PhD ( ) Doctor ( ) Magister (✓) Ingeniero ( ) Licenciado ( ) Otros ( )
Universidad que labora: Universidad César Vallejo
Fecha: 18 / 07 / 19.

TESIS: SEGURIDAD EN LOS DATOS E IMPLANTACIÓN DE LA NTP-ISO/IEC 27001:2014 EN LA SUB GERENCIA DE GESTIÓN DE BASE DE DATOS DEL RENIEC

INDICADOR:	METRICAS DE DISPONIBILIDAD	
FORMULA:	**INCONT=((TH-TH_PA) / TH) *100**	**INCONT:** Indicador de Disponibilidad de servicio **TH:** Total de Horas diarias **TH_PA:** Total de Horas sin Servicio de información

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar el instrumento que se empleará mediante una serie de preguntas marcando un valor porcentual. Asimismo, le exhortamos en la corrección de los ítems indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia del instrumento.

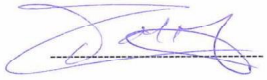
ITEMS	PREGUNTAS	Deficiente 0-20%	Regular 21%-50%	Bueno 51%-70%	Muy Bueno 71%-80%	Excelente 81%-100%
1	¿El instrumento de medición cumple con el diseño adecuado?					95
2	¿El instrumento de recolección de datos tiene relación con el título de la investigación?					90
3	¿El instrumento de recolección de datos tiene relación con las variables de investigación?					85
4	¿El instrumento de recolección de datos facilitará el logro de los objetivos de investigación?					90
5	¿El instrumento analiza los datos de la organización?					95
6	¿El instrumento de medición explica en forma precisa y clara el grado de cumplimiento de la meta o resultado?					95
7	¿El resultado del instrumento es entendible para ser correctamente analizado?					90
TOTAL						

Fuente: Vargas Pinto: Tesis Business Intellenge para el pronóstico de ventas en la empresa Zona Cel S.A.C, 2018

PROMEDIO TOTAL:

EL INSTRUMENTO PUEDE SER APLICADO: SI (✓) NO ( )

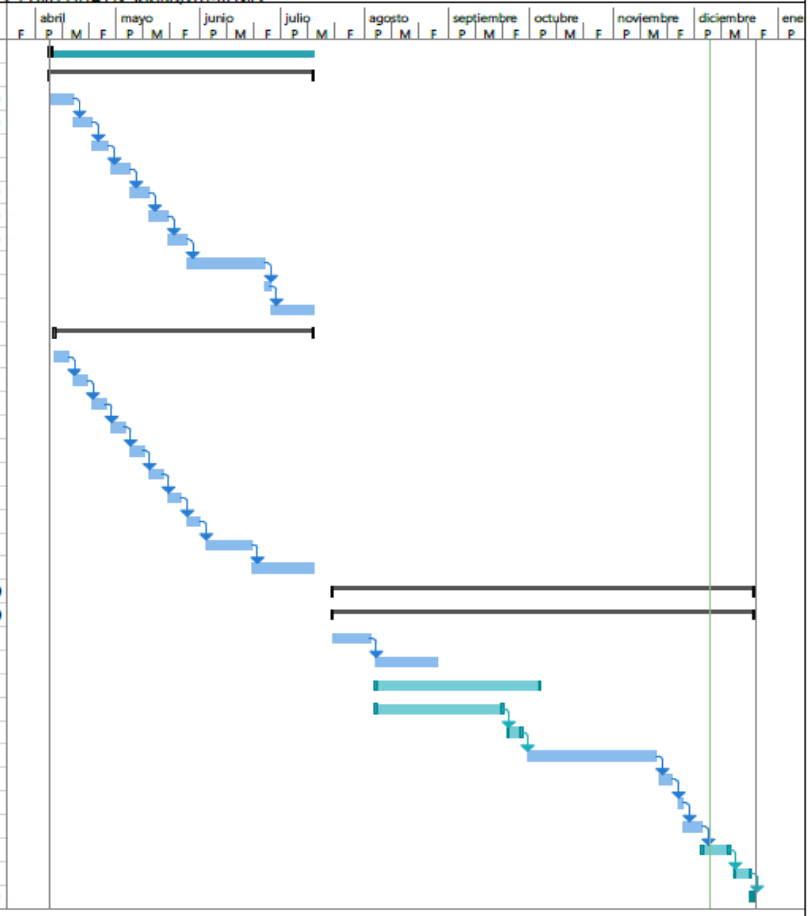
SUGERENCIAS: _____



ANEXO D: CRONOGRAMA DE ACTIVIDADES

CRONOGRAMA DE IMPLANTACION NTP-ISO/IEC 27001:2014 EN SGGBD/GTI-RENIEC

Id	Nombre de tarea	Comienzo	Fin
1	**PLANIFICACION**	**sáb 6/04/19**	**sáb 6/04/19**
2	**Elaboración de Proyecto**	**sáb 6/04/19**	**vie 12/07/19**
3	Presentación del Titulo del Proyecto	sáb 6/04/19	dom 14/04/19
4	Realidad Problemática	lun 15/04/19	dom 21/04/19
5	Trabajos Previos	lun 22/04/19	sáb 27/04/19
6	Teoria Relacionada al Tema	lun 29/04/19	dom 5/05/19
7	Justificacion Hipotesis y Objetivos	lun 6/05/19	dom 12/05/19
8	Diseño de investigación, Variable y Operacionalización	lun 13/05/19	dom 19/05/19
9	Población, Muestra, Herramientas y Recursos	lun 20/05/19	dom 26/05/19
10	Verificación y Evaluación Turnitin	lun 27/05/19	lun 24/06/19
11	Presentación de Informes	mar 25/06/19	mié 26/06/19
12	Sustentación del Proyecto	jue 27/06/19	vie 12/07/19
13	**Planificación de la Implantación**	**lun 8/04/19**	**vie 12/07/19**
14	Revision del Estado Actual en la SGGBD	lun 8/04/19	vie 12/04/19
15	Revision de los Controles de la NTP 27001 a Implantar	lun 15/04/19	vie 19/04/19
16	Revision de los Activos	lun 22/04/19	vie 26/04/19
17	Revision de las Metricas	lun 29/04/19	vie 3/05/19
18	Revision de los Riesgos	lun 6/05/19	vie 10/05/19
19	Reuion con las UUOO sobre los nuevos controles	lun 13/05/19	vie 17/05/19
20	Revision de nuevos formatos	lun 20/05/19	vie 24/05/19
21	Aprobación de los formatos y matrices de control	lun 27/05/19	vie 31/05/19
22	Creacion de la Directiva Gestion de Eventos en la BD	lun 3/06/19	mié 19/06/19
23	Creacion de la Directiva Monitoreo, supervision, y auditoria del uso d	jue 20/06/19	vie 12/07/19
24	**DESARROLLO**	**sáb 20/07/19**	**dom 22/12/19**
25	**Implantación de la NTP 27001**	**sáb 20/07/19**	**dom 22/12/19**
26	Generación del Pre Test	sáb 20/07/19	vie 2/08/19
27	Implantación de los Controles	lun 5/08/19	mar 27/08/19
28	Marcha Blanca del Uso de los Formatos de la Directiva de Eventos	lun 5/08/19	vie 4/10/19
29	Creacion de Lineamientos para el uso de los controles del SGSI	lun 5/08/19	vie 20/09/19
30	Implementacion de controles	lun 23/09/19	vie 27/09/19
31	Seguimiento y Aplicabilidad	lun 30/09/19	sáb 16/11/19
32	Generacion del Post test	lun 18/11/19	vie 22/11/19
33	Informe de Resultados de la Implantación	lun 25/11/19	mar 26/11/19
34	Revision por la Gerencia de Tecnologia y aceptación de la Implantaci	mié 27/11/19	mar 3/12/19
35	Presentacion de la Tesis	mié 4/12/19	vie 13/12/19
36	Revision de la Tesis	lun 16/12/19	sáb 21/12/19
37	Sustentación de Tesis	dom 22/12/19	dom 22/12/19



Proyecto: NTP_ISO_27001

Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
solo duración
Informe de resumen manual
Resumen manual
solo el comienzo
solo fin
Tareas externas
Hito externo
Fecha límite
Progreso
Progreso manual

ANEXO E: INFORME TÉCNICO DE IMPLANTACIÓN DE LA NTP ISO/IEC 27001:2014

Lima, 05 de Noviembre de 2019

INFORME TÉCNICO

SEGURIDAD EN LOS DATOS E IMPLANTACIÓN DE LA NTP-ISO/IEC 27001:2014 EN LA SUB GERENCIA DE GESTIÓN DE BASE DE DATOS DEL RENIEC

La Sub Gerencia de Gestión de Base de Datos (SGGBD), de acuerdo a indicaciones dadas por la Gerencia de Tecnología de la Información (GTI) y en coordinación con la Oficina de Seguridad y Defensa Nacional (OSDN), ha realizado la implantación de la NTP-ISO/IEC 27001:2014 en los procesos de esta Sub Gerencia.

La Norma Técnica Peruana proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para la organización.

El sistema de gestión de la seguridad de información preserva la confidencialidad, integridad y disponibilidad de la información aplicando un proceso de gestión de riesgos y proporciona confianza a las partes interesadas en el sentido en que los riesgos se manejan adecuadamente.

Es importante que el sistema de gestión de la seguridad de la información sea parte de y esté integrado con los procesos de la organización y la estructura de gestión general y que la seguridad de la información se considere en el diseño de procesos, sistemas y controles de la información.

Por lo que describimos los puntos y acciones en la estructura de la ISO 27001 adecuadas para el desarrollo en la SGGBD.

I. OBJETIVO Y CAMPO DE APLICACIÓN

Especificar los elementos principales del modelo de Implantación de Seguridad de la Información del Proceso Monitoreo y Administración de las Bases de Datos del Registro Nacional de Identificación y Estado Civil en adelante RENIEC, a cargo de la SGGBD de la GTI, con el fin de cumplir los requisitos establecidos en la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistema de gestión de seguridad de la información: Requisitos.

II. REFERENCIAS NORMATIVAS

La implantación de los modelos de seguridad de información en la SGGBD ha sido diseñada de acuerdo a lo establecido:

1. La Norma Internacional ISO/IEC 27001:2013 "Tecnología de la Información. Técnicas de seguridad. Sistema de gestión de seguridad de la información Requisitos". Segunda edición, del 01 de octubre de 2013.
2. La Norma Técnica Peruana NTP-ISO/IEC 27001:2014 "Tecnología de la Información. Técnicas de seguridad. Sistema de gestión de seguridad de la información Requisitos".
3. La Norma Internacional ISO/IEC 27000:2014 "Tecnología de la Información – Técnicas de Seguridad. Sistema de gestión de seguridad de información: Requisitos".
4. La Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la NTP-ISO/IEC 27001:2014 "TECNOLOGIAS DE LA INFORMACION. Técnicas de seguridad. Sistemas de gestión de seguridad de la información: Requisitos 2° Edición en todas las entidades del Sistema Nacional de Informática, del 08 de enero de 2016.
5. La Resolución Ministerial N° 0166-2017-PCM, modifica el artículo 5 de la R.M. N° 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información, del 20 de junio de 2017.

III. TÉRMINOS Y DEFINICIONES

Para propósitos de este documento, se aplican los términos y definiciones proporcionados en ISO/IEC 27000, de las que se presentan en este informe:

ABREVIACIÓN	NOMBRES
JNAC	Jefatura Nacional
GG	Gerencia General
ER	Escuela Registral
CGSI	Comité Interno de Seguridad de Información
OSDN	Oficina de Seguridad y Defensa Nacional
ISO	Organización Internacional de Estandarización
PHVA	Planificar, Hacer, Verificar y Actual
GCI	Gerencia de Calidad e Innovación
GTI	Gerencia de Tecnología de la Información
POI	Plan Operativo Institucional
PEI	Plan Estratégico Institucional
RAD	Representante de la Alta Dirección
ROF	Reglamente de Organización y Funciones
SITD	Sistema Integrado de Tramite Documentario
SGGBD	Sub Gerencia de Gestión de Base de Datos
SGIS	Sub Gerencia de Ingeniería de Software

IV. CONTEXTO DE LA ORGANIZACIÓN

4.1. De la organización y su contexto

Registro Nacional de Identificación y Estado Civil (RENIEC) es un organismo público autónomo que cuenta con personería jurídica de derecho público interno y goza de atribuciones exclusivas y excluyentes en materia registral, técnica, administrativa, económica y financiera.

El RENIEC tiene como activo principal la información de todos los peruanos registrados e identificados.

4.2. Contexto de la Organización

De conformidad al Reglamento de Organización y Funciones del RENIEC, las funciones de la SGGBD son:

Artículo 147.- *La Sub Gerencia de Gestión de Base de Datos es la Unidad Orgánica encargada de garantizar la integridad, confiabilidad, seguridad y el funcionamiento de la base de datos institucional en un nivel óptimo de calidad y performance. Responsable de administrar la base de datos institucional, estableciendo coordinaciones necesarias con las diferentes áreas, realizando el seguimiento para su permanente actualización.*

Artículo 148.- *Son funciones específicas de la Sub Gerencia de Gestión de Base Datos:*

a) Planificar y controlar las actividades de instalación, configuración y mantenimiento de las bases de datos de la institución que dan soporte a los sistemas de producción y de servicios de información;

b) Diseñar y mantener el modelo lógico de las bases de datos del RENIEC, permitiendo su eficiente utilización en los sistemas operacionales, de gestión y de análisis de información;

c) Garantizar la integridad, confiabilidad y seguridad en el acceso y modificaciones de la Base de Datos del RENIEC;

d) Planificar, coordinar, diseñar e implementar los proyectos de almacenamiento de los datos, datos biométricos y de las imágenes;

e) Supervisar la aplicación de las normas, estándares y procedimientos establecidos para la creación de objetos de bases de datos;

f) Elaborar el Padrón Electoral así como los archivos de actualización emitidos cada trimestre según la Ley Orgánica de Elecciones, garantizando los niveles de seguridad para el traslado y entrega al Jurado Nacional de Elecciones - JNE y a la Oficina Nacional de Procesos Electorales-ONPE;

g) *Establecer y operar un sistema de Bases de Datos con la información pertinente para la planificación, investigación y monitoreo de los registros;*

h) *Establecer mecanismos de control histórico, auditoria y fiscalización de los datos que conforman el Registro Único de Identificación de las Personas Naturales — RUIPN y de los Registros Civiles, salvaguardando su integridad, confiabilidad y seguridad de la información;*

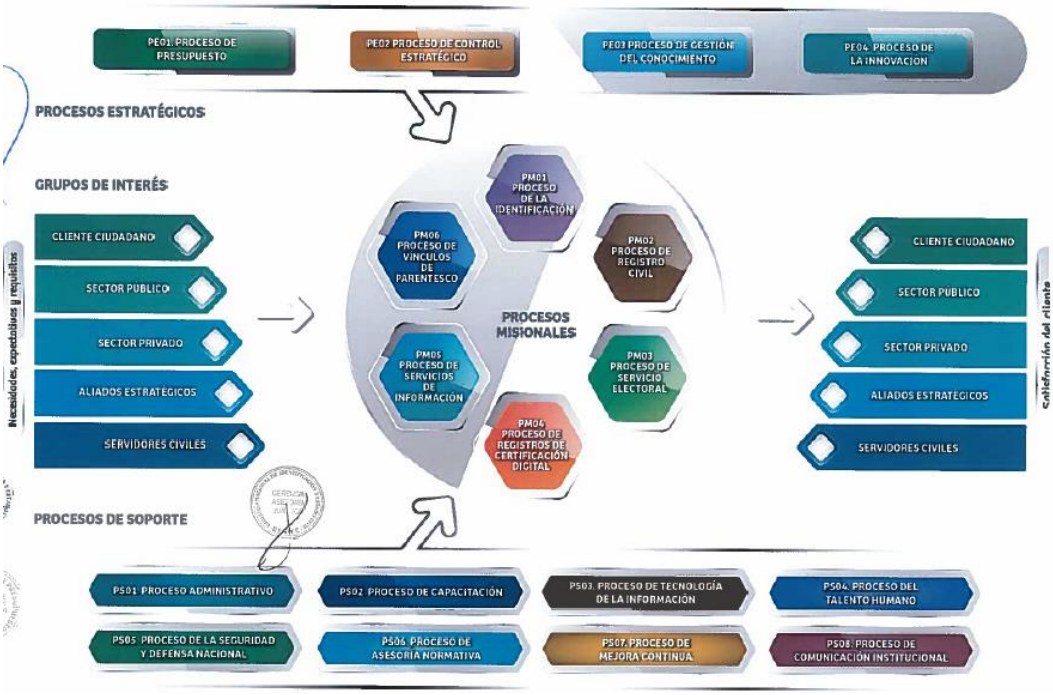
i) *Participar en el diseño de los proyectos de sistemas del RENIEC, evaluando las mejores alternativas de solución para la captura, procesamiento, acceso y almacenamiento de los datos, imágenes y datos biométricos, asimismo participar en las pruebas e implantación de los mismos en coordinación con las unidades orgánicas de la Gerencia de Tecnología de la Información;*

j) *Validar que los datos estén organizados adecuadamente y soporten las soluciones informáticas;*

k) *Participar en la elaboración de los planes de seguridad y contingencia de los sistemas de información y los recursos informáticos a nivel de la institución;*

l) *Las demás funciones que se le asignen en el ámbito de su competencia.*

El RENIEC aplica la gestión por procesos la cual permite lograr un sistema de trabajo enfocado en la mejora continua del funcionamiento de las actividades de la organización mediante la identificación de procesos y la mejora de los mismos. Actualmente, RENIEC cuenta con procesos claves, estratégicos y de soporte, como se aprecia en el siguiente cuadro.



Se han definido como procesos misionales a:

- PM01. Proceso de la Identificación
- PM02. Proceso de Registros Civiles
- PM03. Proceso de Servicio Electoral
- PM04. Proceso de Registro de Certificación Digital
- PM05. Proceso de Servicios de Información
- PM06. Proceso de Vínculos de Parentesco

La Sub Gerencia de Gestión de Base de Datos está a cargo de la administración de todas las Bases de Datos que soportan a los procesos misionales de la institución.

Asimismo, el Plan Estratégico Institucional vigente del RENIEC define como

MISIÓN

"Registrar la identidad, los hechos vitales y los cambios de estado civil de las personas; Participar del sistema electoral; Promover el uso de la identificación y certificación digital, con inclusión social y enfoque intercultural"

VISIÓN

"Ciudadanos identificados con acceso a servicios amigables e innovadores en tiempo real, integrados digitalmente a través de la entidad de registro del Estado peruano que garantiza su identidad y seguridad jurídica, y que contribuye a la modernización del Estado y al desarrollo del país"

El RENIEC, hace uso intensivo de las Tecnologías de Información que soportan todos sus procesos de negocio, permitiendo de esta manera el logro de los objetivos estratégicos y el cumplimiento de su Misión y Visión, antes definidos.

Dentro del ROF del RENIEC, en el Capítulo III DE LAS ATRIBUCIONES Y FUNCIONES, en su Artículo 10°, entre otras funciones, en los literales j); k); p); y q); se establecen las siguientes funciones relacionadas a la seguridad de la información:

j) Velar por el irrestricto respeto del derecho a la intimidad e identidad de la persona y los demás derechos inherentes a ella derivados de su inscripción en el registro;
k) Garantizar la privacidad de los datos relativos a las personas que son materia de inscripción;
p) Mantener la confidencialidad de la información relativa a los solicitantes y titulares de certificados digitales;
q) Medir y mejorar su eficacia, la calidad de su desempeño, para asegurar el cumplimiento de sus funciones, utilizando las mejores prácticas de gestión disponibles;

Asociando de esta manera sus funciones con los pilares de la seguridad de la información como son las confidencialidad, disponibilidad e integridad de la información. En tal sentido, la seguridad de la información es requisito indispensable del RENIEC para cumplir con parte importante de sus funciones, para ello, debe ser apoyada por una óptima gestión de la seguridad de la

información a nivel institucional, implantando controles adecuados y planificados cuidadosamente.

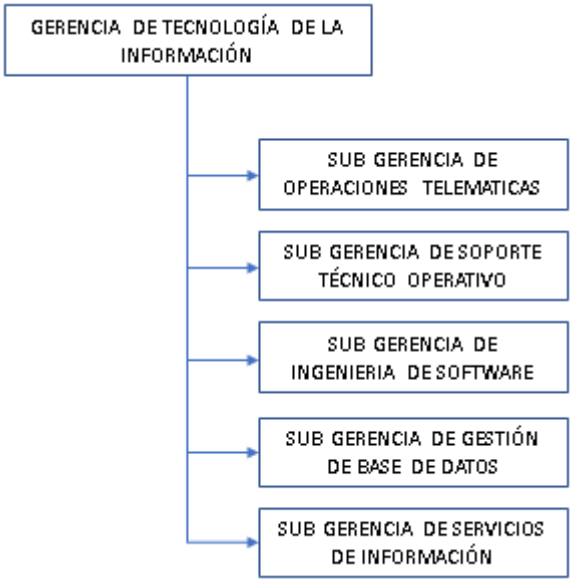
Con la implantación de la NTP-ISO/IEC 27001:2014, además de garantizar la confidencialidad, integridad y disponibilidad de la información de la base de datos y generar confianza en los clientes (persona natural y jurídica), el RENIEC da cumplimiento a lo dispuesto por la Resolución Ministerial 004-2016-PCM, en relación al uso de la referida norma.

4.3. Dueño del proceso de Monitoreo y Administración de la Base de Datos del RENIEC.

La Sub Gerencia de Gestión de Base de Datos, depende directamente de la Gerencia de Tecnología de la Información, órgano de línea, responsable del sistema funcional de gobierno electrónico e informática de la institución a nivel nacional e internacional, encargado de brindar servicios de información y comunicación oportuna y veraz, mediante la implementación de plataformas tecnológicas de vanguardia y de acuerdo con los objetivos y estrategias institucionales, generando valor a los procesos estratégicos, misionales y de apoyo a través del uso de tecnologías de información y comunicaciones.

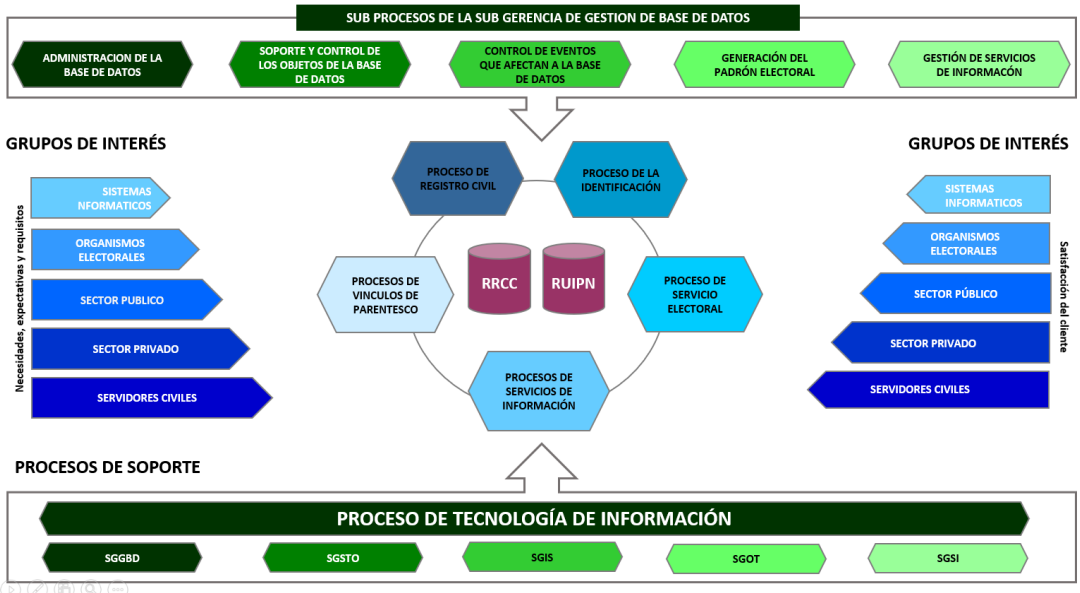
Asimismo, se encarga de administrar los recursos informáticos, custodiar la información, asegurar la continuidad de los procesos, velar por la seguridad de información y la calidad de los sistemas de información de RENIEC y promover el adecuado uso de las tecnologías de la información. Gestiona la administración y operación de toda la infraestructura tecnológica del RENIEC.

ESTRUCTURA ORGÁNICA DE LA GERENCIA DE TECNOLOGÍA DE LA INFORMACIÓN



Las funciones de cada una de las Sub Gerencias se encuentran descritas en el Reglamento de Organización y Funciones del RENIEC (ROF) vigente, aprobado mediante Resolución Jefatural N° 073-2016/JNAC/RENIEC.

Diagrama de Interacción de los servicios con el proceso de Monitoreo y Administración de la Base de Datos



4.3.1. De las necesidades y expectativas de las partes interesadas

El proceso de implantación ha identificado a las partes interesadas del proceso de Monitoreo y Administración de la Base de Datos, así como a sus necesidades y expectativas.

4.3.2. Alcance de la Implantación de la NTP-ISO/IEC 27001:2014

El Alcance de la implantación de la referida norma técnica, aplica a los procesos que se generan en la Sub Gerencia de Gestión de Base de Datos:

1) **Administración de las bases de datos**
   Tiene la finalidad de mantener operativa la Base de Datos, en un formato de 24x7x365, para que los sistemas que dan soporte a los procesos misionales puedan cumplir con sus objetivos. Además, deben de garantizar la confidencialidad, integridad y disponibilidad de la información.
2) **Soporte y Control de los Objetos de la Base de Datos**
   Encargados de revisar estrictamente todos los objetos que serán creados en la Base de Datos, apegándose a los estándares de creación de objetos, cuantificando los procesos de ejecución de sentencias balanceadas que se realizarán directo dentro del motor de base de datos.
3) **Control de Eventos que afectan a la Base de Datos**
   Gestionar con las áreas y grupos de interés, acerca de los eventos ocasionados en los sistemas informativos y los datos almacenados en ellos, llevando un control seguimiento y trazabilidad de cambios que se realicen en este proceso.
4) **Generación del Padrón Electoral**
   Elaboración, procesamiento y custodia de los padrones electorales que son utilizados en los procesos electorales convocados por el poder ejecutivo, para las elecciones Generales y de Congreso de la Republica, Municipalidades y Regionales, Revocatorias, Complementarias y todas las que definan el voto popular.
5) **Gestión de Servicios de Información**

Mantener operativo los servicios de información utilizadas por las entidades públicas y privadas que hayan realizado un convenio con el RENIEC para la utilización de la información, controlando el uso adecuado y la actividad de los usuarios. Asimismo, apoya en el proceso de la facturación en coordinación con la Sub Gerencia de Tesorería.

4.3.3. Sistema de Gestión de Seguridad de la Información

La Alta Dirección ha establecido, implementado, mantiene y mejora un Sistema de Gestión de Seguridad de la Información acorde a los requisitos de la Norma Técnica Peruana NTP ISO/IEC 27001:2014.

V. LIDERAZGO

5.1. Liderazgo y Compromiso

El RAD evidencia su liderazgo y compromiso con el desarrollo e implantación del Sistema de Gestión de Seguridad de la Información en el proceso de Monitoreo y Administración de las Bases de Datos del RENIEC, a través de la realización de las siguientes actividades:

ACTIVIDADES	EVIDENCIAS
Asegurando que la política y los objetivos de seguridad de la información son establecidos y mantenidos con la dirección estratégica de la organización.	-Plan Estratégico Institucional -Plan Operativo Institucional de la Oficina de Seguridad y Defensa Nacional a través de la Sub Gerencia de Seguridad de la Información define como actividad "Programar, controlar y supervisar las actividades de Mantenimiento de los procesos certificados: Identificación de Ciudadanos (GRI), Registros Civiles (GRC), Planta PKI (GRCD) y Padrón Electoral (GRE).
Asegurando la integración de los requisitos del Sistema de Gestión de la Seguridad de la Información estén disponibles.	EL RENIEC, ha certificado y viene manteniendo el Sistema de Gestión de Seguridad de la Información en los procesos misionales de la institución: • Certificado Digital • Registros Civiles • Registro de identificación • Padrón Electoral Plan de Tratamiento de Riesgos y Oportunidades de Seguridad de la Información, en cumplimiento de la DI-370-OSDN/006 "Gestión de Riesgos de Seguridad de la Información" e IN-208-OSDN/001 "Gestión de Riesgos de Seguridad de la Información" La SGGBD/GTI dispone a su personal incluir en todos los documentos normativos y otros mecanismos necesarios para asegurar la seguridad de la información. Documento de Declaración de Aplicabilidad de la SGGBD, en cumplimiento de la DI-372-OSDN/006.
Asegurando que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles.	El RENIEC a través de la Gerencia de Planificación y Presupuestos, formula el PIA con los órganos en el cual se considera la asignación de presupuesto para el mantenimiento de los Sistemas de Gestión de Seguridad de la Información
Comunicando la importancia de una efectiva gestión de la Seguridad de la Información y conformidad con los requisitos del Sistema de Gestión de Seguridad de la Información	El RENIEC a través de la Gerencia General como RAD, y haciendo uso de la herramienta de tramite documentario, emite comunicados a todas las Áreas en relación a la importancia de la Seguridad de la Información. Asimismo, la Gerencia de Tecnología de la Información traslada la comunicación a todo el personal que está dentro del alcance del SGSI, solicitando el cumplimiento estricto de lo dispuesto.
Asegurando que los sistemas de gestión de seguridad de la información logren sus resultados previstos	El Articulo Segundo de la Resolución Jefatural N° 069-2017/JNAC/RENIEC, aprueba la reconstitución del comité de Gestión de Seguridad de la Información del RENIEC en cumplimiento de la Resolución Ministerial N° 004-2016-PCM (22MAY2017). La OSDN, a través de la Sub Gerencia de Seguridad de la Información, como órgano responsable de la implementación y mantenimiento del

	Sistema de Gestión de Seguridad de la Información del Proceso de Monitoreo y Administración de las Base de Datos, asesora a la SGGBD para establecer los indicadores base para la medición del cumplimiento de los objetivos de seguridad de la información.

ACTIVIDADES	EVIDENCIAS
Dirigiendo y apoyando a las personas para que contribuyan a la efectividad del Sistema de Gestión de Seguridad de la Información	Plan de Desarrollo de Personas a cargo de la Oficina de Seguridad y Defensa Nacional, que en coordinación con la Escuela Registral se brindara los cursos o talleres en temas de seguridad de la información.
Promoviendo la mejora continua	La implementación del Sistema de Gestión de Seguridad de la Información del Proceso de Monitoreo y Administración de las Bases de Datos, implica una gestión de mejora continua, ya que está basado en el modelo de gestión de procesos de Deming: Planificar – Hacer – Verificar – Actuar(PHVA). Documentos Normativos: Directiva Gestión por procesos del RENIEC DNI-366-GCI/007, Directiva de Tratamiento de Hallazgos DI-421-GCI/012, Guía de Procedimiento Mejora de procesos del RENIEC GP 378-GCI/001 y Guía de Procedimiento Metodología de Documentación de Procesos del RENIEC GP-379-GCI/002.
Apoyando los roles de gestión relevantes para demostrar su liderazgo según corresponda a sus áreas de responsabilidad	La Gerencia General en su rol de RAD apoyando la implantación y mantenimiento de los procesos del RENIEC. El RENIEC, traslada a la OSDN la responsabilidad de liderar la implementación y mantenimiento de la seguridad de la información a nivel institucional. Comité de Gestión de Seguridad de la Información como instancia de máximo nivel encargada de la seguridad de la información.

5.2. Política

La Alta Dirección ha definido y aprobado la Política de Seguridad de la Información del RENIEC mediante Resolución Jefatural N° 073-2015-JNAC-RENIEC, y es como sigue:

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Registro Nacional de Identificación y Estado Civil tiene como activo principal la información de todos los peruanos registrados e identificados; preserva su confidencialidad, integridad y disponibilidad en cada uno de sus procesos, a través de incorporación de controles, procedimientos y metodologías definidas, personal capacitado, tecnología adecuada y mecanismos de mejora continua en el cumplimiento del marco legal vigente y estándares internacionales.

La Alta Dirección ejerce las acciones necesarias para asegurar que la Política de Seguridad de la Información:

a) Sea adecuada a las necesidades de la organización y de los clientes.
b) Incluya el compromiso para satisfacer los requisitos para la mejora continua.
c) Proporcione un marco de referencia para establecer y revisar los objetivos de seguridad de la información.
d) Sea comunicada, entendida en interiorizada por todo el personal a través de lo siguiente:
    - ✓ Publicación de la Pagina web del RENIEC
    - ✓ Publicación en periódicos murales y/o lugares visibles
    - ✓ Presentándola en reuniones a los trabajadores
    - ✓ Revisando su cumplimiento durante las auditorias y supervisiones del Sistema de Gestión de Seguridad de la Información.
    - ✓ Sistema Integrado de Tramite Documentario (SIA-SITD)
    - ✓ Publicación en htttps//intranet.reniec.gob.pe
e) Sea analizada durante la Revisión por la Dirección, para su continua adecuación y eficacia.

VI. PLANIFICACIÓN

6.1. Acciones para tratar los riesgos y las oportunidades

El RENIEC, a través de la Oficina de Seguridad y Defensa Nacional, mediante la Directiva DI 372-OSDN/006 “Gestión de Riesgos de Seguridad de la Información” e Instructivo INS-208-OSDN-001 “Gestión de Riesgos de Seguridad de Información”, establece los lineamientos para identificar, analizar, evaluar, y tratar los riesgos de seguridad de la información a los que se encuentra expuesto, hasta obtener un nivel aceptable del riesgo y garantizar la seguridad de la información en las áreas que cuenten o implementen un Sistema de Gestión de Seguridad de la Información.

6.2. Generalidades

La Sub Gerencia de Gestión de Base de Datos

a) Asegura los resultados esperados a través de los lineamientos y las especificaciones descritas en el presente informe.
b) Desarrolla acciones para la prevención o reducción de efectos indeseados, en coordinación con las sub gerencias de la Gerencia de Tecnología de la Información, a fin de cumplir los objetivos y requisitos del Sistema de Gestión de Seguridad de la Información.
c) Promueve la mejora continua.
d) Identifica los riesgos y oportunidades para su tratamiento y seguimiento, aplicando la Directiva DI-372-OSDN/006 "Gestión de Riesgos de Seguridad de la Información".
e) Aplica las estrategias, controles y evaluación del riesgo residual descritos en la Directiva DI-372-OSDN/006 "Gestión de Riesgos de Seguridad de la Información".

6.3. Valoración del Riesgo de Seguridad de la Información

Las actividades de identificación, análisis, evaluación y tratamiento de riesgos de seguridad de la información se encuentran definidas en la Directiva DI-372-OSDN/006 "Gestión de Riesgos de Seguridad de la Información" e Instructivo INS-208-OSDN-001 "Gestión de Riesgos de Seguridad de la Información" de la Oficina de Seguridad y Defensa Nacional, que establece los criterios contra los cuales se evalúan los riesgos de seguridad de la información, los lineamientos para identificar, analizar, evaluar, y tratar los riesgos de seguridad de la información a los que se encuentran expuestos los productos y servicios que presta la Gerencia de Registro Electoral, hasta obtener un nivel aceptable del riesgo y garantizar la seguridad de la Información en las áreas que cuenten o implementen un Sistema de Gestión de Seguridad de la Información.

El Dueño de Proceso Monitoreo y Administración de las Bases de Datos, a través de los Gestores Operativos y Gestor Líder de Seguridad de la

Información, con el asesoramiento de la Oficina de Seguridad y Defensa Nacional, identifica las amenazas y oportunidades, generando así un "Plan de Tratamiento de Riesgos y Oportunidades de Seguridad de la Información" bajo los criterios de disponibilidad, confidencialidad e integridad de la información. Se mantiene información documentada de este proceso.

6.4. Tratamiento del Riesgo de Seguridad de la Información

Los lineamientos para identificar, analizar, evaluar y tratar los riesgos del Sistema de Seguridad de la Información se encuentran definidos en la Directiva DI-372-OSDN/006 "Gestión de Riesgos de Seguridad de la Información" e Instructivo INS-208-OSDN-001 "Gestión de Riesgos de Seguridad de la Información" de la Oficina de Seguridad y Defensa Nacional, para lo cual el Dueño del Proceso, La Sub Gerencia de Gestión de Base de Datos establecen estrategias, responsables y tiempo estimado, para el tratamiento del riesgo, seleccionando los controles e impulsores que sean necesarios hasta obtener un nivel aceptable del riesgo.

El Dueño del Proceso Monitoreo y Administración de las Bases de Datos, y las Sub Gerencias de la Gerencia de Tecnología de la Información, gestionan la implementación de los controles o impulsores definidos en el "Plan de Tratamiento de Riesgos y Oportunidades de Seguridad de la Información" e informan a la Oficina de Seguridad y Defensa Nacional, cualquier cambio en el proceso.

Se han establecido controles e impulsores necesarios para el Sistema de Gestión de Seguridad de la Información del proceso Monitoreo y Administración de las Bases de Datos, los mismos que se encuentran expresados en la **Declaración de Aplicabilidad** que incluye la justificación de las inclusiones, ya sea que se implementen o no, así como la justificación de excluir controles del Anexo A de la Norma Técnica Peruana NTP ISO/IEC 27001:2014.

6.5. Gestión de Incidentes de Seguridad de la Información

La SGGBD/GTI a través de la DI-374-OSDN/008 "Gestión de incidentes de Seguridad de la Información", asegura que los eventos, vulnerabilidades e incidentes de seguridad que se presenten y afecten a los activos de información,

sean comunicados y atendidos oportunamente, empleando los procedimientos definidos, y tomar oportunamente las acciones correctivas.

6.6. Objetivos de seguridad de la información y planificación para conseguirlos

La Alta Dirección ha definido y aprobado los Objetivos Generales de Seguridad de la Información del RENIEC mediante Resolución Jefatural N° 073-2015/JNAC/RENIEC, los cuales son:

OBJETIVOS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

- *Proteger la confidencialidad de la información asegurando que sea accesible a organismos o personas autorizadas.*
- *Salvaguardar la integridad de la información para garantizar su exactitud y totalidad, así como sus métodos de procesamiento.*
- *Mantener la disponibilidad de la información y los sistemas de información que soportan los procesos de RENIEC para garantizar que los organismos o personas autorizadas tengan acceso a la información cuando lo requieran.*
- *Establecer, implementar, operar, monitorear, revisar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información del RENIEC.*

El Dueño del Proceso ha definido y aprobado los Objetivos Específicos de Seguridad de la Información que apoyan al cumplimiento de los Objetivos Generales de Seguridad de la Información, siendo lo siguiente:

OBJETIVOS ESPECÍFICOS DE SEGURIDAD DE LA INFORMACIÓN

- *Solicitar oportunamente las altas y bajas de los usuarios en los sistemas*
- *Asegurar la eficiencia en la atención de los eventos y/o vulnerabilidades que afectan al proceso de padrón electoral*
- *Garantizar la operatividad de los equipos necesarios a fin de salvaguardar la información*
- *Asegurar el mantenimiento del Sistema de Gestión de Seguridad de la Información*
- *Garantizar la efectividad de los controles de seguridad de la*

a

o

planifica las actividades a realizar para lograr los objetivos específicos de seguridad de la información.

VII. SOPORTE

7.1. Recursos

El Dueño del Proceso, la Sub Gerencia de Gestión de Base de Datos, elaboran anualmente su respectivo Plan Operativo Institucional y Cuadro de Necesidades en base al Presupuesto Institucional asignado dentro del cual deberán de incluir las necesidades de recursos humanos, infraestructura, equipos, sistemas y otros que apoyen a la del Sistema de Gestión de Seguridad de la Información.

7.2. Competencias

El Dueño del Proceso, la Sub Gerencia de Gestión de Base de Datos, determina las necesidades de competencias del personal que realizan las actividades que afectan la conformidad de los requisitos del Sistema de Gestión de Seguridad de la Información, teniendo como marco de referencia a la, Guía de Procedimientos GP-414-ER/SGFC/001 “Formación y Capacitación de la Escuela Registral” y Reglamento RE-207-ER/001 “Reglamento de la Escuela Registral”.

Los requisitos mínimos de competencia para desarrollar actividades específicas del Proceso Monitoreo y Administración de las Bases de Datos son definidos por los funcionarios responsables de los procesos del Sistema de Gestión de Seguridad de la Información.

La Gerencia de Talento Humano es responsable de administrar y organizar los legajos del personal siguiendo lo establecido en la DI-406-GTH/007 “Administración del Legajo del Servidor Civil en el Reniec”. Todo el personal del Proceso Monitoreo y Administración de las Bases de Datos es responsable de remitir su documentación personal que asegure la actualización de sus legajos personales.

7.3. Concientización

La Oficina de Seguridad y Defensa Nacional en atención a las necesidades de formación y sensibilización en seguridad de la información del personal de la SGGBD/GTI, coordina con la Escuela Registral la programación y realización, definiéndose en el Plan de Desarrollo de Personas.

La Escuela Registral a través de la Sub Gerencia de Formación y Capacitación realiza las actividades de coordinación previas, durante y después de la ejecución de los cursos de capacitación. Para los fines del caso, se dispone del documento normativo RE-207-ER/001 Reglamento de la Escuela Registral.

Además, a nivel interno, El Dueño del Proceso, a través de los Gestores Operativos, realiza actividades de concientización en materia de seguridad de la información al personal de la SGGBD.

7.4. Comunicación

El RENIEC cuenta con una estructura de comunicación interna moderna, ágil y flexible, que facilita la comunicación entre todos los niveles de la organización, la cual está procedimentada en la Directiva DI-417-SGEN/010 *"Gestión Documental del RENIEC*".

Los métodos formales para la elaboración, aprobación y difusión de documentos normativos están definidos en la DI-200-GPP/001 "Lineamientos para la Formulación de los Documentos Normativos del *RENIEC* ", además a fin de asegurar el uso efectivo de la información, se cuenta con la GP-399-GAJ/SGSJ/004, "Sistematización de documentación y normatividad interna y externa del *RENIEC*".

Así mismo, a fin de vincular a todos los miembros de los Sistemas de Gestión en todos los distintos niveles jerárquicos y áreas, mejorar el desempeño y fortalecer el sentimiento de pertenencia, se utilizan las siguientes herramientas de comunicación interna:

HERRAMIENTAS	TEMAS
• Reuniones de trabajo. • Mesas de trabajo. • Correo electrónico. • Video conferencias. • Intranet RENIEC • Micro sitio SGGBD. • Fondos de pantalla. • Periódico mural.	• Cumplimiento de la política y objetivos de seguridad de la información. • Resultados de la gestión de riesgos de seguridad de la información. • Reporte de eventos y vulnerabilidades. • Auditorías y acciones correctivas. • Resultados de la Revisión del SGSI. • Cambios y mejoras en el SGSI. • Otros temas relevantes para la seguridad de la información.

7.5. Información documentada

7.5.1. Generalidades

La Implantación del Sistema de Seguridad de la Información de la Sub Gerencia de Gestión de Base de Datos, incluye:

a) La información documentada requerida por la Norma Técnica Peruana ISO/IEC 27001:2014.
b) Información documentada establecida como necesaria para la efectividad del mismo.

7.5.2. Creación, actualización y control de la información documentada

El Registro Nacional de Identificación y Estado Civil, a través de la Directiva DI-200-GPP/001 "Lineamientos para la Formulación de los Documentos Normativos del RENIEC", establece lineamientos que orienten a las áreas del RENIEC en el proceso de formulación, aprobación publicación, difusión, implementación, revisión, actualización y derogación de los Documentos Normativos para "normalizar" sus procesos de gestión tanto operativa como administrativa con el propósito de construir un ordenamiento jurídico interno que sea coherente y estructurado a partir de preceptos normativos correctamente formulados que respondan a las necesidades de la entidad para poder brindar y garantizar de manera efectiva e integral un servicio y una atención de calidad que satisfaga al ciudadano; así como, las exigencias de los organismos rectores de los sistemas administrativos y sistemas funcionales que se aplican en el RENIEC.

Los Gestores Líderes y Operativos conservarán los documentos del SGSI en lugares seguros en coordinación con la Oficina de Administración.

7.5.3. Información Documentada

Documentos normativos que apoyan al Sistema de Gestión de Seguridad de la Información

Los documentos normativos que apoyan al Sistema de Gestión de Seguridad de la Información del proceso del Padrón Electoral, garantizan que éste cuente con los documentos estrictamente necesarios y maneje la dinámica de la mejora continua. En la medida que se evidencie la eficacia de las acciones tomadas y la madurez del sistema de gestión, los procesos y documentos se ajustarán y evolucionarán; a fin de cumplir con las necesidades de seguridad de la información; jerarquizados y clasificados de la siguiente manera según Grafico N° 03:

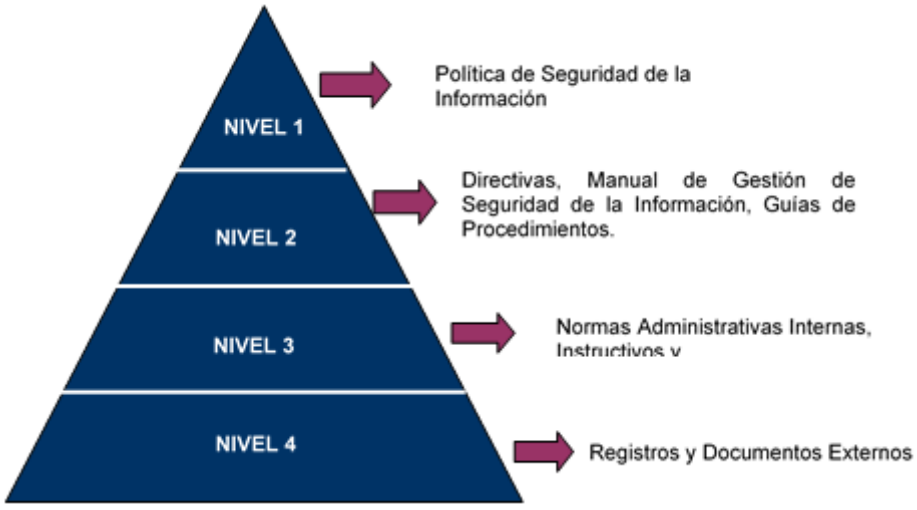


GRAFICO N° 03: ESTRUCTURA DE LA DOCUMENTACIÓN DEL SGSI

Informe de Implantación de Seguridad de la Información

Los documentos normativos utilizados para la implantación del Sistema de Gestión de Seguridad de la Información en la SGGBD son registrados por el

Gestor Líder u Operativo de Seguridad de la Información en la "Lista Maestra de Documentos del Proceso de Monitoreo y Administración de las Bases de Datos.

Clasificación de la Información

El RENIEC a través de la Directiva DI-373-OSDN/007 "Clasificación de la Información del Sistema de Gestión de Seguridad de la Información", establece lineamientos a seguir para la clasificación, etiquetado y tratamiento de la información con independencia del medio de soporte en el que se encuentre.

Disponibilidad de la Información

Las versiones vigentes de los documentos normativos se exhiben en la Intranet. Las copias impresas de documentos normativos, se consideran como "*Copia no controlada*".

Para asegurar que los documentos normativos vigentes aplicables estén disponibles para todo el personal, se cuenta con los siguientes medios:

- Link en la intranet RENIEC (documentos normativos).
- Copia física no controlada (En caso se requiera).

La Gerencia de Asesoría Jurídica a través de la Sub Gerencia de Sistematización Jurídica, establece los lineamientos y acciones a seguir para una adecuada sistematización y control de los documentos de origen externo, que afecten al Sistema de Gestión de Seguridad de la Información contemplada en la Guía de Procedimientos GP-399-GAJ/SGSJ/004, "Sistematización de Documentación y Normativa Interna y Externa del RENIEC".

Los documentos normativos del Sistema de Gestión de Seguridad de la Información son registrados por el Gestor Líder u Operativo, en el "Inventario de documentos".

A fin de asegurar que los documentos normativos vigentes aplicables a los procesos se encuentren disponibles para el personal que no cuenten con equipos informáticos, se identificará un punto de uso. Para ello o cuando se requiera, el Gestor Líder u Operativo dispondrá de copias físicas debidamente identificadas

con el sello “Copia Controlada”, registrándola en la “Lista de distribución de documentos” .

Registros que apoyan al Sistema de Gestión de Seguridad de la Información

La SGGBD, mantiene sus registros conforme a la Directiva DI-349-GCI/004 “Control de Registros” del RENIEC, en la que se establece lineamientos para identificar, almacenar, proteger, recuperar, retener y disponer de los registros.
Siendo el Gestor Líder u Operativo, el responsable de los registros propios del SGSI de su respectivo proceso.

VIII. OPERACIÓN

8.1. Planificación y control operacional

La implantación de la NTP ISO/IEC 27001:2014 en Proceso Monitoreo y Administración de las Bases de Datos planifica, implementa y controla los procesos necesarios para cumplir con los requisitos de seguridad de la información detallados en el numeral 6.1 y 6.2 del presente informe.

8.2. Evaluación del Riesgo de Seguridad de la Información

La implantación de la NTP ISO/IEC 27001:2014 en Proceso Monitoreo y Administración de las Bases de Datos, realiza evaluaciones de riesgos y oportunidades de seguridad de la información a intervalos planificados, según lo dispuesto por la Oficina de Seguridad y Defensa Nacional que indica que la periodicidad será de forma anual para la actualización de los documentos de la gestión de riesgos y oportunidades de la DI-372-OSDN/006 “Gestión de Riesgos de Seguridad de la Información” e INS-208-OSND/001 “Gestión de Riesgos de Seguridad de la Información”.

8.3. Tratamiento del Riesgo de Seguridad de la Información

La implantación de la NTP ISO/IEC 27001:2014 en Proceso Monitoreo y Administración de las Bases de Datos, conforme a lo previsto en la Directiva DI-372-OSDN/006 “Gestión de Riesgos de Seguridad de la Información” e INS-208-OSND/001 “Gestión de Riesgos de Seguridad de la Información”, se planifican las actividades, responsables, fechas, etc., para tratar los riesgos de nivel importante y crítico, y realizar el seguimiento mediante el “Plan de Tratamiento de Riesgos y Oportunidades de Seguridad de la Información”.

IX. EVALUACIÓN DEL DESEMPEÑO

9.1. Monitoreo, medición, análisis y evaluación

Con el fin de demostrar la conformidad con los requisitos de la normatividad vigente y mejorar continuamente la eficacia de la La implantación de la NTP ISO/IEC 27001:2014 en Proceso Monitoreo y Administración de las Bases de Datos, en coordinación con la Oficina de Seguridad y Defensa Nacional, establece indicadores relacionados con la medición de los Objetivos Específicos de Seguridad de la Información. Para ello se llevan a cabo actividades para el seguimiento y medición de los indicadores; de manera que se evidencie la capacidad de los procesos para alcanzar los resultados planificados en cuanto a la efectividad y eficacia del Sistema de Gestión de Seguridad de la Información.

Los indicadores diseñados para el seguimiento del Sistema de Gestión de Seguridad de la Información, así como los resultados alcanzados se registran en el formato “Sistema de Gestión de Seguridad de la Información – SGSI, Cuadro de Mando Operativo – CMO” .

9.2. Auditoría Interna

La Gerencia de Calidad e Innovación, planifica y desarrolla las Auditorías Internas de los Sistemas de Gestión implementados, según los Lineamientos

establecidos en el documento DI-400-GCI/011 “Auditorías Internas de los Sistemas de Gestión del RENIEC", en la que se definen:

- Lineamientos generales para la planificación, desarrollo y evaluación de las auditorías de los sistemas de gestión.
- Informe sobre los resultados y mantener los registros asociados de las auditorias.

ANEXO F:. DESARROLLO DE LA IMPLANTACIÓN DE LA NORMA ISO 27001

DESARROLLO DEL PROYECTO DE IMPLANTACIÓN DE LA NTP-ISO/IEC 27001:2014 EN LA SUB GERENCIA DE GESTIÓN DE BASE DE DATOS

La seguridad de la información es una disciplina asociada tradicionalmente a la gestión de TIC, cuyo propósito es mantener niveles aceptables de riesgo de la información organizacional y de los dispositivos tecnológicos que permiten su recolección, procesamiento, acceso, intercambio, almacenamiento, transformación y adecuada presentación. Ha sido definida por la norma ISO/IEC 27000 como la preservación de la confidencialidad, integridad y disponibilidad de la información (ISO/IEC, 2014).

Existen diversas formas de llevar a cabo una implantación para la ISO/IEC 27001:2014 en una organización, no obstante, para lograr cierto nivel de éxito y disminuir la incertidumbre en sus resultados, se debe adoptar un enfoque que permita abordar, desde una perspectiva sistémica, la forma de cumplir con los elementos que hacen parte de éste. El enfoque propuesto se basa en la metodología del ciclo continuo de Deming – PDCA (Plan – Do – Check – Act), tambien conocido en sus siglas en castellano PHCA y se combinará con la experiencia de los participantes de la Sub Gerencia de Gestión de Base de Datos que participaron en el proceso.

La estructura de los controles de seguridad de la información se encuentra conformada por 14 dominios, 35 objetivos de control y 114 controles, los cuales se encuentran divididos entre controles organizacionales, controles técnicos y controles normativos, como se puede apreciar en la Figura Nro. 2.

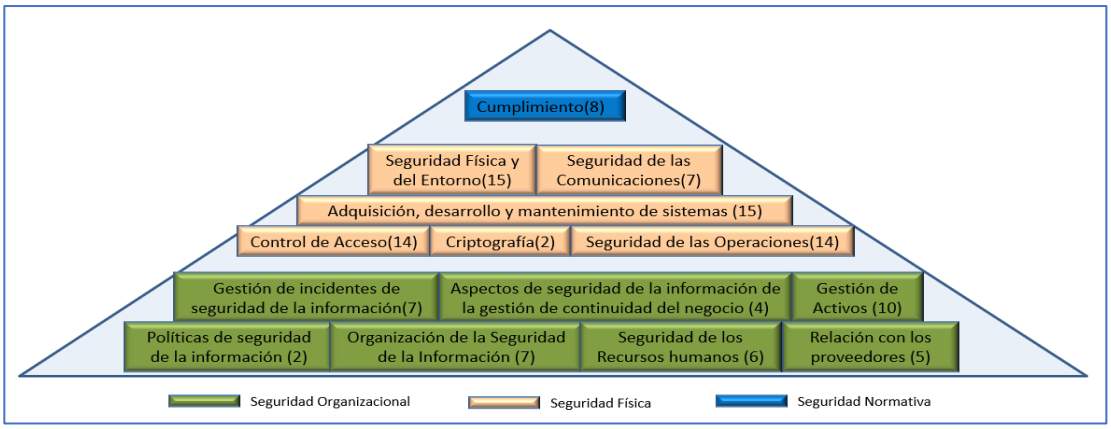


Figura Nro. 2 – Estructura de los Controles de la Norma IEC 27001

I. INICIO DEL PROYECTO

La implantación de la NTP-ISO/IEC 27001:2014, en la Sub Gerencia de Gestión de Base de Datos, permite identificar, analizar, evaluar, controlar y/o mitigar los riesgos a los que está expuesta la Base de Datos del RENIEC. Consiste en la adaptación de los requisitos mínimos requeridos en la norma como la implantación de controles aplicables del Anexo A de la norma en mención.

La implementación consiste en las siguientes etapas:

PLANIFICAR PLAN	HACER DO	VERIFICAR CHECK	ACTUAR ACT
• Contexto de la organización • Liderazgo • Planeación • Soporte	• Operación	• Evaluación de Desempeño	• Mejora

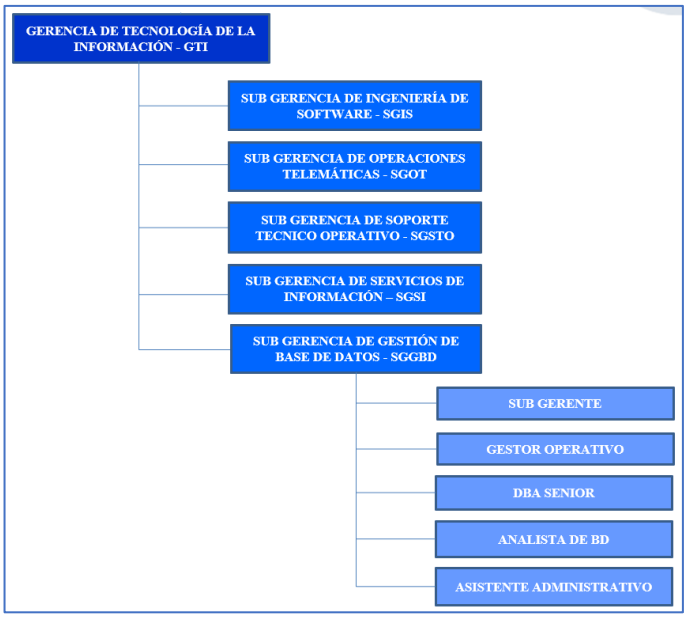
El proyecto de implantación de seguridad se ha definido para el Proceso de Monitoreo y Seguridad de la Base de Datos del RENIEC, a cargo de la Sub Gerencia de Gestión de base de Datos de la Gerencia de Tecnología de la Información.

El proyecto de desarrollo para la implantación de la NTP-ISO/IEC 27001:2014, se inició con la aprobación por parte de la Gerencia de Tecnología de la Información mediante el Memorando N° 001413-2019/GTI/RENIEC de fecha 18 de Julio del 2019.

Para el desarrollo de la implantación del ISO 27001, se creó el grupo conformado por el siguiente equipo de la Sub Gerencia de Gestión de Base de Datos:

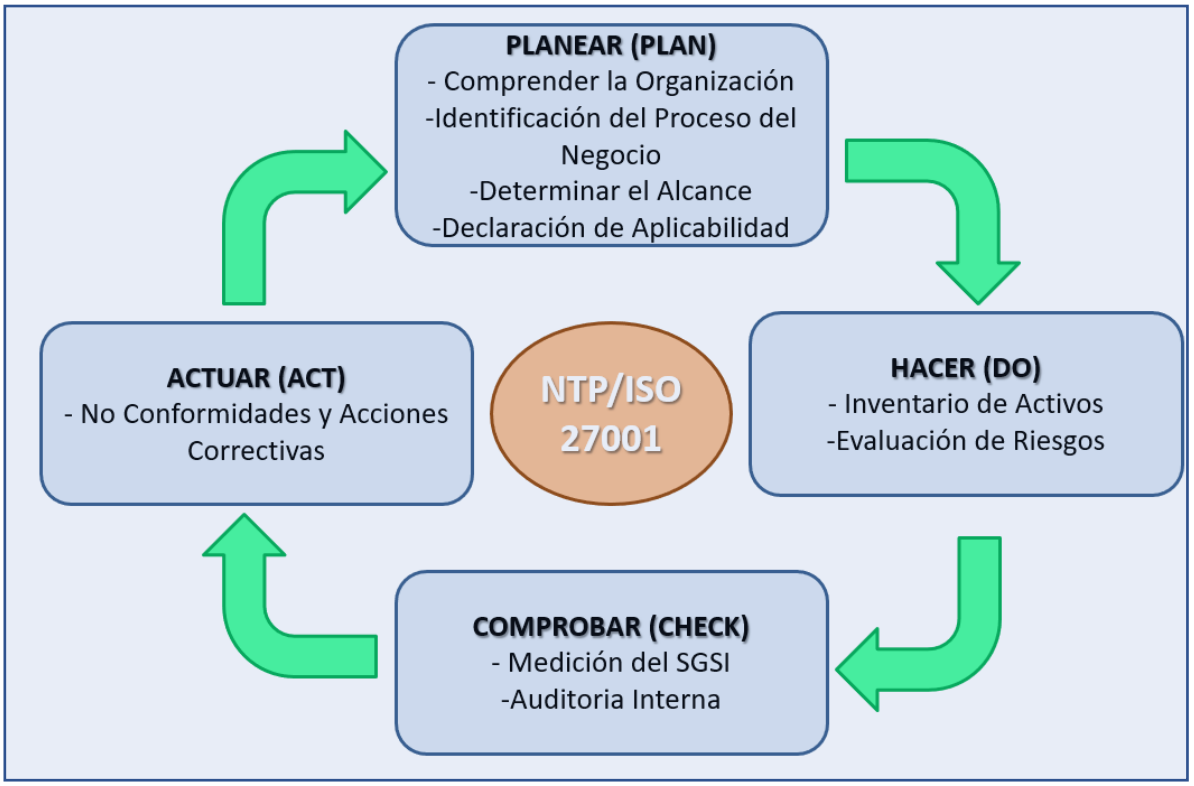
Ítem	Nombres y Apellidos	Cargo
1	Moisés Clemente Rojas Jaén	Sub Gerente
2	Rosario Samanez Serafin	Administrador Senior de Base de Datos
3	Carolina Armas Vela	Administrador Senior de Base de Datos
4	Eliana Zapata Quiñonez	Analista Senior de Base de Datos
5	Katherine Doza Cordova	Asistente Administrativo Documental

Esta estructura organizacional aprobada por la Gerencia de Tecnología de la Información para el desarrollo de la implantación:



1.1. ETAPAS DE LA IMPLANTACIÓN DE LA NTP-ISO/IEC 27001:2014

Ciclo de Deming



Fuente: Elaboración Propia

1.2. PLANEAR

1.2.1. COMPRENDER LA ORGANIZACIÓN Y SU CONTEXTO

El Registro Nacional de Identificación y Estado Civil RENIEC, es una organización autónoma del estado peruano, que tiene como misión principal el de la Identificación de todos los peruanos, el Registro de los Hechos Vitales, la elaboración del Padrón Electoral y de la gestión de los Certificados Digitales.

Para conocer mejor la Sub Gerencia de Gestión de Base de Datos, de la Gerencia de Tecnología de la Información, se elaboró una Matriz de FODA cruzada, para hallar las posibles estrategias a utilizar en el plan de implantación:

MATRIZ FODA CRUZADO

INTERNAS / EXTERNAS	FORTALEZAS	DEBILIDADES
	F1.-Gran soporte a los procesos de mejora continua de las áreas operativas y administrativas. F2.-El uso de tecnologías avanzada para la atención de rectificación de datos, con el uso de aplicaciones en equipos de telefonía celular, permite disminuir los tiempos de atención y economía de los ciudadanos. F3.-Buen soporte tecnológico para la gestión de imagen institucional, presencia en redes sociales y transparencia de la información. F4.-Soporte tecnológico que se brinda a las campañas de inscripción de RRCC y de DNI, permite el cumplimiento de metas y objetivos estratégicos. F5.-Se cuenta con personal especializado con experiencia en las distintas etapas de generación de aplicaciones informáticas: proyecto, diseño, producción, calidad y monitoreo. F6.-Alta disponibilidad de la infraestructura tecnológica propia del RENIEC, permite una comunicación y transferencia constante a nivel nacional. F7.-La institución hace uso de una serie de herramientas tecnológicas, como base de datos Oracle, lenguaje de programación Java, software de oficina, que genera seguridad, confianza e idoneidad en las comunicaciones, así como transparencia y trazabilidad de los procesos.	D1.-Falta de una planificación integral /corporativa de las TIC y débil incorporación de buenas prácticas internacionales para la operatividad y soporte de los motores de bases de datos. D2.- Falta de un plan formal de capacitación y certificación especializada - profesional para el grupo de Administradores y Analistas de BD en conceptos de seguridad de información. D3.- Limitada infraestructura / componentes TIC (hardware, software, base de datos, comunicaciones), seguridad y disposición de las instalaciones. D4-Falta de comunicación e integración entre unidades organicas operativas y las de soporte para acciones correctivas frente a problematicas de informacion D5.-Contar con personal tecnico especializado unico en los procesos criticos de alta disponibilidad D6.-Acceso a las bases de datos productivas por personal de desarrollo. D7.- Falta de definicion de centros de computos alternos para la continuidad operativa informatica. D8.- Uso de usuarios de previlegios con super usuarios con acceso a la base de datos. D9.- Falta de monitoreo de los equipos que contiene la base de datos en oficinas registrales. D10.- Falta de sistemas de video vigilancia en la SGGBD.
OPORTUNIDADES	**ESTRATEGIAS FO**	**ESTRATEGIAS DO**
O1.-Convenios con Organismos Registrales de otros países, como Argentina, Chile y Colombia, entre otros, para el intercambio de mejores practicas en el uso de las tecnología de la información, mejorará en el RENIEC implementar mejores niveles de seguridad de la informacion en las dimensiones de confidencialidad, integridad y disponibilidad. O2.-La informacion de la base de datos del RENIEC la convierte en un referente para ser usada en el movimiento migratorio tanto de los ciudadano peruanos como los que residen en el extranjero. O3.-La informacion de la base de datos del RENIEC debera de ser utilizada en la realizacion de los arboles genealógicos de los ciudadanos peruanos. O4.-La infraestrucctura tecnologica de alto nivel permite crear nuevos proyectos al servicio de los ciudadania.	F2 - O4 / Se unificaran las grandes bases de datos de los procesos misionales (emision de DNI y RRCC) con el respaldo de la insfraestructura tecnologica con la que cuenta el RENIEC. F5 - O3 / Planeamiento para el cumplimiento de la Ley que designa al RENIEC como gestor de la base de datos de vinculados hasta la etapa de diseño e implementación para el año 2020. F6 - O2 / Se debera de realizar convenios institucionales con Migraciones, RREE y Poder Judicial para el desarollo del control migratorio de ciudadanos peruanos asi como de extranjeros utilizando la infraestructura TIC del RENIEC.	D8 - O1 / Realizacion de convenios con el apoyo de paises extranjeros para la implementacion de centros de computos alternos.
AMENAZAS	**ESTRATEGIAS FA**	**ESTRATEGIAS DA**
A1.-Ataques informáticos de virus, malware, hackers y spyware pueden poner en riesgo las aplicaciones informáticas y los sistemas de información. A2.-La simplificación administrativa dispuesta por el Ejecutivo, que obvia la presentación de algunos documentos de sustento y verificación de datos para la inscripción en RRCC y la emisión del DNI, puede vulnerar la seguridad jurídica de los documentos registrales y de identificación. A3.-La oferta de empleos en la administración pública y sector privado, con mayor remuneración que los percibidos actualmente por los analistas informáticos especializados, genera fuga de talentos afectando la continuidad de los servicios que brinda la GTI. A4.-Posibilidad de fuga de información por acceso inadecuados del personal de desarrollo. A5.-Factores naturales externos terremotos, incendios y atentados en los centro de datos. A6.- Abuso de informacion privilegiada y operaciones no autorizadas por los super usuarios de la base de datos. A7.- Robo de equipos en las oficinas registrales que contienen bases de datos con informacion critica. A8.- Robo de equipos o vulneraciones de accesos por personal no autorizado.	F7 - A1 / Elaborar planes de control contra ataques a los sistemas informaticos utilizando las herramientas tecnologicas que tiene el RENIEC. F4 - A2 / Desarrollar programas de mantenimientos a los sistemas de captura en los tramites de DNI y RRCC controlados por los sistemas biometricos tanto para el personal que usa el aplicativo como tambien para identificas a los ciudadanos utilizando la biometria facila y dactilar. F5 - A3 / Fortalecer los procesos de capacitacion profesional del personal especializado en procesos critico informaticos asi como la evaluacion de los cargos y remuneraciones, para evitar que la inversion del talento humano se pierda.	D7 - A4 / Elaborar una metodologia de trabajo donde los administradores de base de datos puedan entregar la informacion necesaria al grupo de desarrollo en casos de incidentes generados por los aplicativos y puedan realizar la trazabilidad y la resolución de los problemas. D8 - A5 / Desarrollar grupos de trabajo con personal de servicios generales y GTI para desarrollar los estudios necesarios y encontrar las mejores ubicaciones donde se podria instalar los centros de computos alternos.

La Implantación de la NTP ISO/IEC 27001:2014, busca identificar aquellos factores internos y externos relacionados a la seguridad de la información, los cuales se muestran a continuación:

LINEAMIENTOS ESTRATÉGICOS

LINEAMIENTOS ESTRATÉGICOS	OBJETIVOS
VALOR	Mejora del Servicio. Atención a Sectores Vulnerables. Innovación y Uso Intensivo de Tecnología.
ESTABILIDAD	Mayor eficiencia en los procesos misionales
PRESTIGIO	Orientar cultura de servicio al ciudadano

Fuente: Elaboración Propia

FACTORES INTERNOS

FACTORES INTERNOS	RELACIONADOS CON LA SEGURIDAD
DESARROLLO DE SISTEMAS	Mayor demanda de seguridad en los servicios de tecnología, desarrollados in-house y de los adquiridos.
TALENTO HUMANO	El compromiso del personal del RENIEC, que se encuentre comprometido en la Seguridad de la Información
ADMINISTRACIÓN DE BASE DE DATOS	Se requiere mantener confidencialidad, integridad y disponibilidad de la información de todos los habitantes mayores y menores de edad del Estado Peruano

Fuente: Elaboración propia

FACTORES EXTERNOS

FACTORES EXTERNOS	RELACIONADOS CON EL SGSI
POLÍTICO – LEGAL	Cumplir con los dispuesto por la Oficina Nacional de Gobierno Electrónico, mediante las leyes y regulaciones relacionadas con la seguridad de la información
IDENTIDAD	Aumento de los ataques a Centro de datos en el Perú, e intento de afectar la seguridad de los datos en el RUIPN del RENIEC

SOCIAL - CULTURAL	El desarrollo basado en una cultura de Seguridad de Información a nivel social y personal.
TECNOLÓGICO	Nuevas tecnologías para proteger ataques a los centro de datos

Para comprender a la organización en el contexto de seguridad se dispone de el Plan Estratégico Informático 2018, en el mismo, se señala el marco contextual de la institución y las diferentes líneas estratégicas que asignan responsables, actividades y proyectos a ser cumplidos a mediano y largo plazo en el RENIEC.

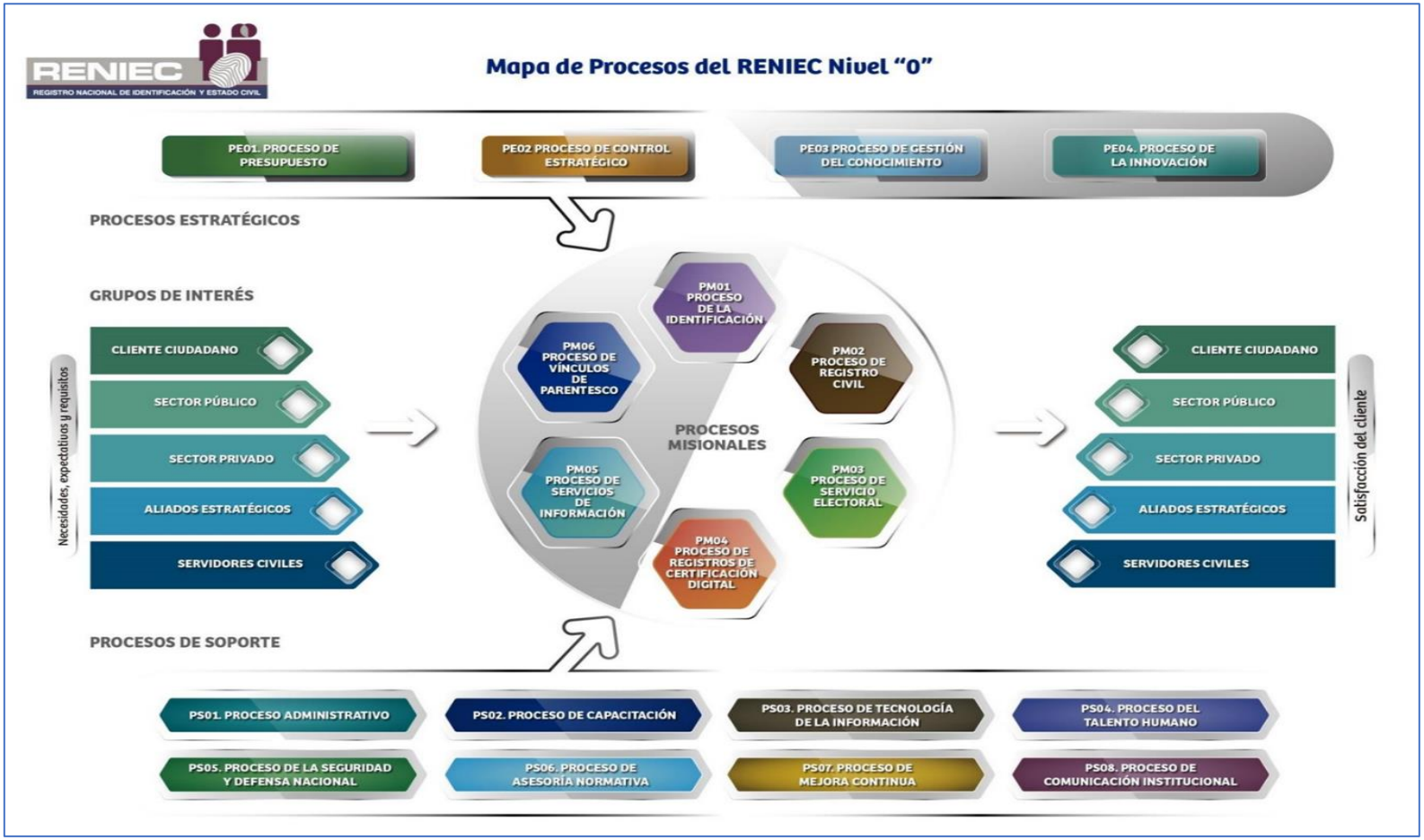
Es importante remarcar, que el Plan Estratégico Informático 2018 fue elaborada por especialistas de la Gerencia de Tecnología de la Información y la Gerencia de Calidad e Innovación y mediante la sistematización de material de apoyo al diagnóstico y construcción de ideas, dando como resultado el esclarecimiento de las necesitadas y expectativas dicho en la Norma ISO, "*identifica las necesidades y requisitos del cliente, requisitos legales y reglamentarios aplicables*", por tanto, este documento es primordial en el cumplimiento de los requisitos de calidad

1.2.2. IDENTIFICACIÓN DE LOS PROCESOS DEL NEGOCIO

Los procesos son mecanismos de comportamiento que diseñan los hombres para mejorar la productividad de algo, para establecer un orden o eliminar algún tipo de problema, mantienen relacionadas sus tareas para conseguir un resultado bien definido; por lo tanto, toman una entrada y le agregan valor para producir una salida.

El RENIEC, mantiene una estructura organizativa en gestión de procesos, por lo que, todos los procesos Misionales, de Soporte y de Gestión están mapeados en el siguiente cuadro.

FIGURA Nro. 1: MAPA DE PROCESOS RENIEC



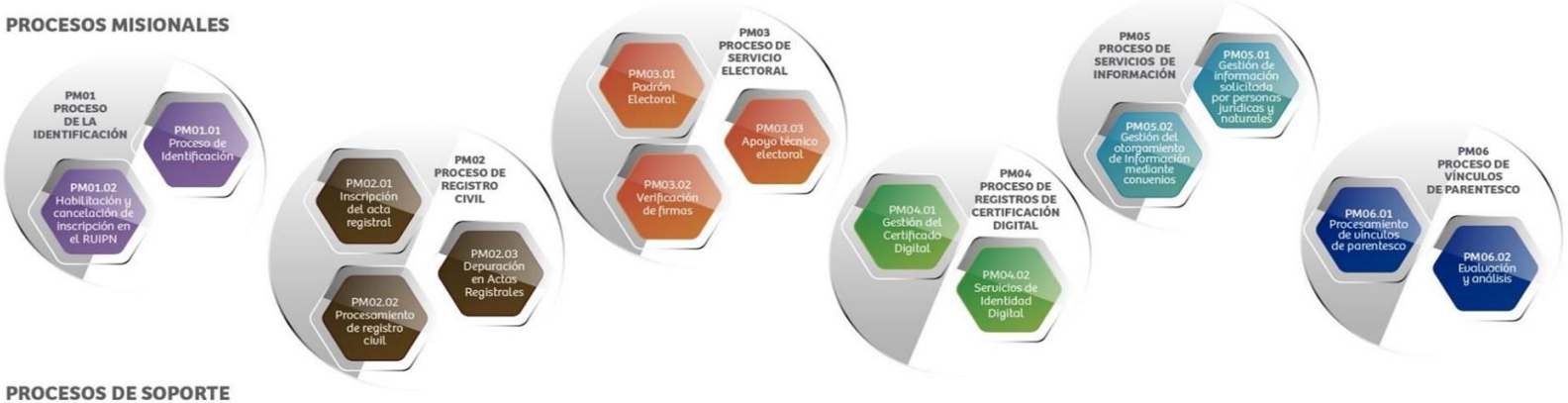
FUENTE: Elaboración propia

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

Diagrama de Procesos Nivel "1"

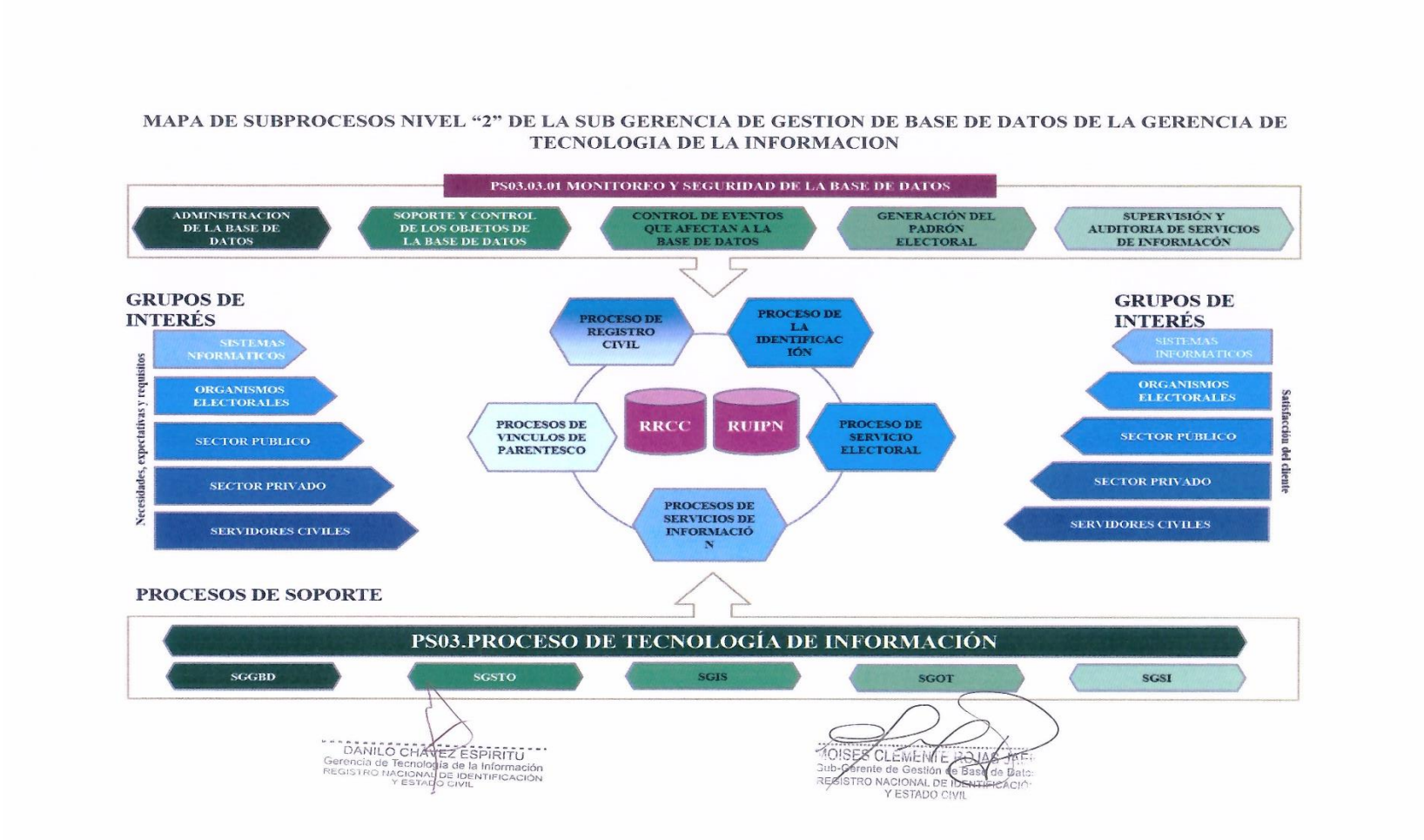
PROCESOS ESTRATÉGICOS

PROCESOS MISIONALES



PROCESOS DE SOPORTE

Para el proyecto de implantación de la ISO/IEC 27001, se presentó a la Gerencia de Tecnología de la Información el siguiente mapa de proceso de la Sub Gerencia de Gestión de Base de Datos, el cual fue aprobado y refrendado por el Gerente de TI.



Los sub procesos del proceso de Monitoreo y Seguridad de la base de datos son los encargados de darle valor y seguridad a los procesos misionales, estos sub procesos son los siguientes:

Administración de la Base de Datos.- Corresponde a la gestión de monitorear, controlar y supervisar constantemente las bases de datos operativas de la institución, dándole el soporte necesario para su confidencialidad, integridad y disponibilidad.

Soporte y Control de los Objetos de la Base de Datos.- Corresponde a la gestión de supervisar y controlar, los objetos que se ejecutaran directamente en la base de datos, midiendo su ejecución y procesamiento, revisión de las sentencias y procesos que realizara, para evitar incidentes que paralicen las líneas productivas de la institución.

Control de Eventos que afecten a la Base de Datos. - Corresponde a la gestión de controlar todos los requerimientos de eventos en la información o los datos generados por las líneas de procesamiento de los procesos core de la institución.

Generación del Padrón Electoral.- Es la gestión política de preparar y entregar el Padrón Electoral de los ciudadanos hábiles al voto, en cada proceso electoral convocado por la Presidencia del Consejo de Ministros.

Gestión de Servicios de Información. - Corresponde a la administración y control de los servicios de datos puestas al servicio del estado peruano y de las empresas privada, para fortalecer la seguridad ciudadana, apoyando en la identificación de las personas.

1.2.3. DETERMINAR EL ALCANCE DE LA IMPLANTACIÓN DE LA NTP ISO/IEC 27001:2014

Se ha definido el siguiente alcance para la implantación de la Norma Técnica Peruana del sistema de gestión de seguridad de la información:

DESCRIPCIÓN DEL ALCANCE	
El alcance de la implantación de la NTP ISO/IEC 27001:2014 es en el proceso: ***"Monitoreo y Seguridad de la Base de Datos"*** El lugar donde se implantará la norma técnica del SGSI es: Centro de Monitoreo de la Sub Gerencia de Gestión de Base de Datos de la Gerencia de Tecnología de la Información, ubicada en Av. Javier Prado Este 2392 – San Borja.	
REQUISITOS	**CARACTERÍSTICAS**
Lograr implantar la NTP ISO/IEC 27001:2014	Cumplimiento de la Norma
Participación de Auditorías Internas y Externas, como adjunto a los procesos a certificarse	Auditoría Interna del Proceso de Padrón Electoral en la ISO-27001:2014.
CRITERIOS DE ACEPTACIÓN DEL PRODUCTO	
CONCEPTOS	**CRITERIOS DE ACEPTACIÓN**
1.- TÉCNICOS	Se debe de cumplir el 100% el cronograma de trabajo
2.- CALIDAD	Se debe obtener la aceptación de la GTI de la implantación de la norma técnica.
3.- ADMINISTRATIVOS	Todos los entregables deben ser aprobados por la Gerencia de Tecnología de la Información
ENTREGABLES DEL PROYECTO	
FASE DEL PROYECTO	**PRODUCTO ENTREGADO**
DIAGNÓSTICO	Informe Técnico de Implantación.
CONTEXTO DE LA ORGANIZACIÓN	- Identificación de las partes interesadas "Matriz de Expectativas y Necesidades de las Partes Interesadas" - Alcance del SGSI - Matriz FODA Cruzada
LIDERAZGO	- Política de SI - Roles y responsabilidades del SGSI
PLANEACIÓN	- Metodología de gestión de riesgos

	- Declaración de aplicabilidad
SOPORTE	- Plan de capacitación - Plan de concienciación - Requisitos de Competencias - Documentos del SGSI
OPERACIÓN	- Gestión de cambios - Matriz de evaluación de riesgos - Plan de tratamiento de riesgos
EVALUACIÓN DEL DESEMPEÑO	- Programa de auditoria - Plan de auditoría interna - Informe de auditoría interna - Revisión de gestión
AUDITORIA EXTERNA	Haber sido auditados por una empresa externa en ISO 27001, como proceso de soporte al proceso certificado.

EXCLUSIONES DEL PROYECTO
Para el proyecto no se consideran los siguientes controles del anexo A de la norma ISO/IEC 27001:2013 A.6.2.1 / A.6.2.2 Política de dispositivos móviles / Trabajo remoto. Dentro del alcance del SGSI no se contempla el uso de dispositivos móviles ni teletrabajo o trabajo remoto.10.1.1 Política sobre el uso de controles criptográficos / 10.1.2 Gestión de claves. Dentro del alcance del SGSI no se contempla el uso de controles criptográficos A.11.2.6 Dentro del alcance del SGSI no se contempla el uso de equipos fuera de las instalaciones A.13.2.2 Acuerdos sobre mensajería de información. Dentro del alcance del SGSI no se contempla transferencia de información a terceros. A.14.1.1 Dentro del alcance del SGSI no se contempla desarrollo de producto de software A.14.2.1 hasta A.14.2.9 Dentro del alcance del SGSI no se contempla desarrollo de producto de software A.14.3.1 Dentro del alcance del SGSI no se contempla desarrollo de producto de software A.18.1.5 No hay regulación de controles criptográficos

RESTRICCIONES DEL PROYECTO	
INTERNOS A LA ORGANIZACIÓN	**EXTERNOS A LA ORGANIZACION**
Los entregables deberán presentarse en la fecha propuesta en el cronograma	El cliente definirá los requisitos de seguridad aplicables al sistema de gestión

Fuente: Elaboración Propia

El alcance del Sistema de la Gestión de la Seguridad de la Información del proceso de Monitoreo y Seguridad de la Base de Datos:

Administración de las bases de datos, Soporte y Control de los Objetos de la Base de Datos, Control de Eventos que afectan a la Base de Datos, Generación del Padrón Electoral y Supervisión y Auditoría de los Sistemas de Información

Producto / Servicio	Breve Descripción	Proceso	Unidad Orgánica	Sede
Administración de las bases de datos	Mantener operativa la Base de Datos en un formato de 24*7*365, para que los sistemas que dan soporte a los procesos misionales puedan cumplir con sus objetivos. Garantizar la confidencialidad, integridad y disponibilidad de la información.	Administración de las bases de datos	GT /SGGBD	Sede San Borja Av. Javier Prado Este 2392 San Borja
Soporte y Control de los Objetos de la Base de Datos	Gestionar los objetos de las Base de Datos, apegándose a los estándares de creación de objetos, cuantificando los procesos de ejecución de sentencias balanceadas que se realizarán directo dentro del motor de base de datos.	Soporte y Control de los Objetos de la Base de Datos	GTI/SGGBD	Sede San Borja Av. Javier Prado Este 2392 San Borja
Control de Eventos que afectan a la Base de Datos	Gestionar con las áreas y grupos de interés acerca de los eventos ocasionados en los sistemas informativos y los datos almacenados en ellos, llevando un control, seguimiento y trazabilidad de cambios que se realicen en este proceso.	Control de Eventos que afectan a la Base de Datos	GTI/SGGBD	Sede San Borja Av. Javier Prado Este 2392 San Borja
Generación del Padrón Electoral	Generar el Padrón Electoral, que es la relación de electores hábiles para votar en un proceso electoral. Siendo denominado: • Lista de padrón inicial a la fecha del cierre para la convocatoria electoral. • Padrón preliminar, antes de la aprobación del JNE. • Padrón electoral final (definitivo), con la aprobación del JNE.	Generación del Padrón Electoral	GTI/SGGBD	Sede San Borja Av. Javier Prado Este 2392 San Borja
Supervisión y Auditoría de los Sistemas de Información	Supervisar y mantener un control de los accesos de usuarios externos (entidades públicas y privadas) y usuarios internos (UU.OO) a traves de los sistemas de información, para su uso adecuado.	Supervisión y Auditoría de los Sistemas de Información	GTI/SGGBD	Sede San Borja Av. Javier Prado Este 2392 San Borja

MOISES CLEMENTE ROJAS [illegible]
Sub-Gerente de Gestión de Base de Datos

ROSARIO SAMANEZ SERAFIN
Sub Gerencia de Gestión de Base de Datos (e)

RENIEC

MATRIZ DE EXPECTATIVAS Y NECESIDADES DE LAS PARTES INTERESADAS

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI

CONTROL DE VERSIONES					
Versión	**Elaborado por**	**Revisado por**	**Aprobado por**	**Fecha**	**Motivo**
01	Moisés Rojas Jaén Rosario Samanez Serafín Carolina Armas Vela Eliana Zapata Quiñones	**Moisés Rojas Jaén** (Sub Gerente de Gestión de Base de Datos)	**Danilo Chávez Espiritu** (Gerente de Tecnología de la Información)	4/12/2019	Implementación del Sistema de Gestión de Seguridad de la Información

Proceso Misional:		**PS03. Proceso de Tecnología de la Información** **SGGBD: Monitoreo y Administración de la Base de Datos**			
Productos y/o Servicios	**Proceso**	**Partes interesadas (Interna/Externa)**	**Expectativas y Necesidades**	**Requisitos**	**Fuentes**
Administración de las Bases de Datos	Administración de las Bases de Datos	Colaboradores	• Buen Clima Laboral • Bienestar Laboral • Oportunidades de Desarrollo Profesional	• Plan de desarrollo de las personas • Equipos informáticos y materiales de trabajo adecuados • Condiciones óptimas para el desarrollo de las actividades • Disponibilidad de DN vigentes • Horas de trabajo de acuerdo a normativa	• Plan de Desarrollo de Personas • Cronogramas de mantenimiento • Tramite Documentario • Intranet • Contratos
		Agencias RENIEC a nivel nacional Entidades Públicas Entidades Privadas Ciudadanos	• Disponibilidad, Confidencialidad e Integridad de la Información en las Base de Datos	• Cumplimiento de la normativa vigente de Seguridad de la Información • Mantener actualizados los backups de las Bases de Datos • Mantener la custodia y control de los accesos a la Base de Datos	• NTP-ISO/27001:2014 Sistema de Gestión de la Seguridad de la Información • NAI N° 415-GTI-SGGBD/005 "Seguridad y Auditoria en las Bases de Datos del RENIEC" - Primera Versión
Soporte y Control de los Objetos de la Base de Datos	Soporte y Control de los Objetos de la Base de Datos	Colaboradores	• Buen Clima Laboral • Bienestar Laboral • Oportunidades de Desarrollo Profesional	• Plan de desarrollo de las personas • Equipos informáticos y materiales de trabajo adecuados • Condiciones óptimas para el desarrollo de las actividades • Disponibilidad de DN vigentes • Horas de trabajo de acuerdo a normativa	• Plan de Desarrollo de Personas • Cronogramas de mantenimiento • Tramite Documentario • Intranet • Contratos
		Sub Gerencia de Ingeniería de Software Unidades Orgánicas	• Optimización del procesamiento de datos • Gestión de los objetos de las Bases de Datos	• Cumplimiento de la normativa vigente	• NTP-ISO/27001:2014 Sistema de Gestión de la Seguridad de la Información • NAI N° 414-GTI-SGGBD/004 "Atención de Requerimientos en las Bases de Datos de Producción" - Primera Versión
Control de Eventos que afectan a la Base de Datos	Control de Eventos que afectan a la Base de Datos	Colaboradores	• Buen Clima Laboral • Bienestar Laboral • Oportunidades de Desarrollo Profesional	• Plan de desarrollo de las personas • Equipos informáticos y materiales de trabajo adecuados • Condiciones óptimas para el desarrollo de las actividades • Disponibilidad de DN vigentes • Horas de trabajo de acuerdo a normativa	• Plan de Desarrollo de Personas • Cronogramas de mantenimiento • Tramite Documentario • Intranet • Contratos
		Gerencia Registros de Identificación Gerencia de Registros Civiles Gerencia de Operaciones Registrales Gerencia de Tecnología de Información	• Gestionar los eventos que están relacionados con la información almacenada en las Bases de Datos.	• Cumplimiento de la normativa vigente	• DI N° 442-2019-GTI/002 "Gestión de eventos relacionados con la información en las Bases de Datos del RENIEC"
Generación del Padrón Electoral	Generación del Padrón Electoral	Colaboradores	• Buen Clima Laboral • Bienestar Laboral • Oportunidades de Desarrollo Profesional	• Plan de desarrollo de las personas • Equipos informáticos y materiales de trabajo adecuados • Condiciones óptimas para el desarrollo de las actividades • Disponibilidad de DN vigentes • Horas de trabajo de acuerdo a normativa	• Plan de Desarrollo de Personas • Cronogramas de mantenimiento • Tramite Documentario • Intranet • Contratos
		Organizaciones Políticas Jurado Nacional de Elecciones	• Disponibilidad de Padrón Preliminar • Disponibilidad del Padrón Electoral final	• Cumplimiento de la normativa vigente • Cumplimiento del cronograma de entrega de acuerdo a ley • Mantener datos integros y actualizados	• Normativa Interna Vigente • Ley 26859, Ley Orgánica de Elecciones y sus modificatorias
		Entes externos	• Disponibilidad del Padrón Electoral final	• Cumplimiento de la normativa vigente	• Normativa Interna Vigente • Ley 26859, Ley Orgánica de Elecciones y sus modificatorias
		Colaboradores	• Buen Clima Laboral • Bienestar Laboral • Oportunidades de Desarrollo Profesional	• Plan de desarrollo de las personas • Equipos informáticos y materiales de trabajo adecuados • Condiciones óptimas para el desarrollo de las actividades • Disponibilidad de DN vigentes • Horas de trabajo de acuerdo a normativa	• Plan de Desarrollo de Personas • Cronogramas de mantenimiento • Tramite Documentario • Intranet • Contratos

RENIEC

MATRIZ DE EXPECTATIVAS Y NECESIDADES DE LAS PARTES INTERESADAS

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI

CONTROL DE VERSIONES					
Versión	**Elaborado por**	**Revisado por**	**Aprobado por**	**Fecha**	**Motivo**
01	Moisés Rojas Jaén Rosario Samanez Serafín Carolina Armas Vela Eliana Zapata Quiñones	**Moisés Rojas Jaén** (Sub Gerente de Gestión de Base de Datos)	**Danilo Chávez Espiritu** (Gerente de Tecnología de la Información)	4/12/2019	Implementación del Sistema de Gestión de Seguridad de la Información

Proceso Misional:		**PS03. Proceso de Tecnología de la Información** **SGGBD: Monitoreo y Administración de la Base de Datos**			
Productos y/o Servicios	**Proceso**	**Partes interesadas (Interna/Externa)**	**Expectativas y Necesidades**	**Requisitos**	**Fuentes**
Supervisión y Auditoría de los Servicios de Información	Supervisión y Auditoría de los Servicios de Información	Unidades Orgánicas Entidades Públicas Entidades Privadas Ciudadanos	• Gestionar los convenios de los servicios de información. • Sistema de Gestión de Usuarios (Módulo SIO) • Disponibilidad, Confidencialidad e Integridad de la Información en las Base de Datos	• Cumplimiento de la normativa vigente • Cumplimiento de los convenios interinstitucionales. • Cumplimiento del TUPA - RENIEC	• GP-284-GI/SGGBD/001(2010) : Administración de los Servicios Consulta en Línea y Verificación Biométrica • GP-285-GI/SGGBD/001(2010): Fiscalización posterior a la Administración de los Servicios Consultas en Líneas y Verificación Biométrica. • Ley N° 27806 - Ley de Transparencia y Acceso a la Información Pública. • Resolución Jefatural N° 156-2017/JNAC/RENIEC: Resolución que aprueba el TUPA - RENIEC

MOISES CLEMENTE ROJAS JAEN
Sub-Gerente de Gestión de Base de Datos
REGISTRO NACIONAL DE IDENTIFICACIÓN
Y ESTADO CIVIL

ROSARIO SAMANEZ SERAFIN
Sub Gerencia de Gestión de Base de Datos (e)
REGISTRO NACIONAL DE IDENTIFICACIÓN
Y ESTADO CIVIL

Liderazgo y Compromiso

La alta dirección demuestra su compromiso al definir los roles y responsabilidades, los recursos necesarios, al definir la política y los objetivos de los sistemas de seguridad de la información.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El RENIEC, ha estipulado la siguiente Política de Seguridad de Información Institucional:

El Registro Nacional de Identificación y Estado Civil tiene como activo principal la información de todos los peruanos registrados e identificados; preserva su confidencialidad, integridad y disponibilidad en cada uno de sus procesos, a través de incorporación de controles, procedimientos y metodologías definidas, personal capacitado, tecnología adecuada y mecanismos de mejora continua en el cumplimiento del marco legal vigente y estándares internacionales.

Roles y Responsabilidades del SGSI

Comité de Gestión de Seguridad de la Información (CGSI)

Es la instancia permanente de carácter no técnico y de máximo nivel, encargado de la seguridad de la información a nivel institucional.

Está constituido mediante Resolución Jefatural N° 069-2017/JNAC/RENIEC que aprueba la reconstitución del Comité de Gestión de Seguridad de la Información, el mismo que está integrado por los siguientes miembros:

• Jefe Nacional	:	Presidente
• Jefe de la Oficina de Seguridad y Defensa Nacional	:	Secretario Técnico
• Gerente de Administración	:	Miembro

• Gerente de Planificación y Presupuesto	:	Miembro
• Gerente de Tecnología de la Información	:	Miembro
• Gerente de Asesoría Jurídica	:	Miembro
• Oficial de Seguridad de la Información	:	Miembro
• Un representante del Gabinete de Asesores	:	Miembro

El CGSI se encargará de las siguientes funciones:

- Asegurar que el sistema de gestión de seguridad de la información y los objetivos de seguridad de la información sean establecidas y compatibles con la dirección estratégica de la organización.
- Asegurar la integración de los requisitos del sistema de seguridad de la información en los procesos de la organización.
- Asegurar los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles.
- Comunicar la importancia de una efectiva gestión de seguridad de la información y en conformidad con los requisitos del sistema de gestión de seguridad de la información.
- Asegurar que el sistema de gestión de seguridad de la información logre su(s) resultado(s) previsto(s).
- Dirigir y apoyar a los colaboradores para que contribuyan con la efectividad del sistema de gestión de seguridad de la información.
- Promover la mejora continua.
- Apoyar a otros roles relevantes de gestión para demostrar su liderazgo tal como se aplica en sus áreas de responsabilidad, y
- Otras funciones que se le asigne en el ámbito de su competencia.

Oficina de Seguridad y Defensa Nacional

La Oficina de Seguridad y Defensa Nacional es el órgano de asesoramiento de la Alta Dirección, encargado del planeamiento, programación, ejecución y

supervisión de las acciones de gestión del riesgo de desastres, seguridad y defensa nacional, gestión de seguridad de la Información a nivel institucional en concordancia con las disposiciones normativas correspondientes. Responsable de la gestión del sistema de seguridad institucional que garantice la protección de las personas, de los bienes, activos de información, las instalaciones y el normal funcionamiento de los servicios del RENIEC.

Son funciones específicas de la OSDN en relación a la seguridad de la información:

- Coordinar con la Gerencia de Planificación y Presupuesto a través de la Secretaría General la articulación de la Política de Seguridad y Defensa Nacional con el Plan Estratégico Institucional – PEI.
- Conducir la implementación del Sistema de Gestión de Seguridad de la Información en la institución de acuerdo a la normatividad vigente, en el ámbito de su competencia.
- Informar a la Jefatura Nacional la situación institucional en materia de seguridad de la información.
- Desarrollar, en el ámbito de su competencia, las acciones orientadas a implementar el funcionamiento del Sistema de Seguridad de la Información de acuerdo con los lineamientos establecidos por la Alta Dirección y las normas legales pertinentes.
- Coordinar con la Gerencia General y la Gerencia de Tecnología de la Información las acciones de implementación, desarrollo y cumplimiento de las disposiciones vigentes sobre la seguridad de la información.
- Promover la difusión de la Seguridad de la Información en coordinación con la Alta Dirección y la Escuela Registral.

Sub Gerencia de Seguridad de la Información

La Sub Gerencia de Seguridad de la Información es la unidad orgánica encargada de la gestión del sistema de seguridad de la información del RENIEC, responsable de desarrollar e implantar un sistema de gestión de la seguridad que permita identificar y dar respuesta a los nuevos riesgos de la institución.

Son funciones específicas de la Sub Gerencia de Seguridad de la Información:

- Proponer las políticas, planes, programas y actividades relacionadas al Sistema de Gestión de Seguridad de la Información, para reducir los riesgos que afecten la confidencialidad, integridad y disponibilidad de la información en los procesos institucionales.

- Establecer, implementar, monitorear, revisar y mejorar el Sistema de Gestión de Seguridad de la Información en el RENIEC, en el cumplimiento del marco legal vigente y estándares internacionales.

- Planear, organizar, programar, ejecutar y supervisar las acciones de Seguridad de la Información de acuerdo a la normatividad vigente y estándares internacionales.

- Formular, supervisar y monitorear la implementación del Plan de Seguridad de la Información del RENIEC, garantizando su correcta ejecución en el cumplimiento del marco legal vigente y estándares internacionales.

- Proponer mejoras o iniciativas en materia de seguridad de la información al Comité de Gestión o al Oficial de Seguridad de la información en materia de gestión de riesgos, activos de información, procesamiento de la información, mejoras al Sistema de Gestión de Seguridad de la Información (SGSI), entre otros.

- Definir una metodología de evaluación de riesgos apropiada para el Sistema de Gestión de Seguridad de la Información y las necesidades de la organización, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable.

- Administrar el desarrollo y la aplicación de las políticas de seguridad, normas y procedimientos para garantizar el mantenimiento continuo de la seguridad de la información y la protección de activos.

- Coordinar con la Gerencia General, Secretaría General, Gerencia de Tecnología de la Información y sus áreas la implementación de las políticas, normativas y controles para reducir los riesgos de seguridad de la información en la institución.

- Supervisar las áreas respecto a la implementación de los controles de seguridad de la información en el ámbito de su competencia.

- Capacitar y sensibilizar al personal frente a la cultura de seguridad en toda la institución.

- Gestionar mejoras a nivel de procedimientos y aplicaciones informáticas utilizadas dentro del ámbito de su competencia.

- Las demás funciones que se le asignen en el marco de su competencia.

Oficial de Seguridad de la Información

Es el responsable de coordinar la implementación del Sistema de Gestión de Seguridad de la Información en la entidad.

Dueño del Proceso

Es la persona que tiene la responsabilidad y confianza para el éxito del diseño, desarrollo, ejecución y desempeño de un proceso completo.

Responsable del Sub proceso

Es la persona a quien el Dueño del proceso encarga la conducción de una parte del proceso, es decir, de un sub proceso.

Gestor Líder de Seguridad de la Información

La SGGBD asignará al Gestor Líder el rol, responsabilidades y autoridad para cumplir con las siguientes funciones:

- Velar por el cumplimiento de la Política de Seguridad de la Información, documentos, directivas y normas relacionadas.
- Coordinar con la OSDN cualquier tema relevante relacionado a la seguridad de la información o del SGSI.
- Reportar a la OSDN cualquier evento o vulnerabilidad de seguridad de la información según la DI-374-OSDN/008 "Gestión de Incidentes de Seguridad de la Información"
- Hacer seguimiento a los eventos o vulnerabilidades reportados por los procesos que conforman el alcance.
- Gestionar las acciones para la clasificación, etiquetado, y tratamiento de la información del SGSI.
- Liderar el Equipo de Riesgos de Seguridad de la Información.
- Elaborar la Declaración de Aplicabilidad en concordancia con el Plan de Tratamiento de Riesgos y Oportunidades de Seguridad de la Información.

- Monitorear la ejecución del Plan de Tratamiento de Riesgos y Oportunidades de Seguridad de la Información.
- Monitorear la ejecución de actividades de capacitación y sensibilización en seguridad de la información.
- Conservar la información documentada necesaria por el Sistema de Gestión de Seguridad de la Información en coordinación con la Oficina de Administración de Archivos.
- Planificar y monitorear la evaluación de desempeño del Sistema de Gestión de Seguridad de la Información a través de los indicadores de gestión, la cual será reportada a la OSDN.
- Coordinar la elaboración y actualización del Plan de Continuidad Operativa.
- Gestionar la programación de las auditorías internas/externas del Sistema de Gestión de Seguridad de la Información.
- Monitorear el cierre de los hallazgos que deriven de las auditorías internas y externas, así como reportar a la OSDN y CIGSI el estado de las acciones que se implementen.
- Otras funciones que se le asigne en el ámbito de su competencia.

La designación de Gestores Líderes de Seguridad de la Información es hecha de conocimiento de la Oficina de Seguridad y Defensa Nacional mediante hoja de elevación.

Equipo de Riesgos

Es el grupo multifuncional conformado por el Gestor(es) Líder(es) y Operativo(s) de Seguridad de la Información del Proceso Monitoreo y Seguridad de la Base de Datos y un personal de la OSDN. Sus funciones son:

- Elaborar el inventario de activos de información.
- Elaborar la "Identificación, Análisis y Evaluación de Riesgos y Oportunidades de Seguridad de la Información".
- Elaborar el "Plan de Tratamiento de Riesgos y Oportunidades de Seguridad de la Información" y la evaluación del riesgo residual.

- Elaborar y remitir al CIGSI y a la OSDN, el informe de la identificación, análisis evaluación y tratamiento de los riesgos y oportunidades del SGSI.
- Otras funciones que se asigne en el ámbito de su competencia.

Gestor Operativo de Seguridad de la Información

Los Gestores Operativos de Seguridad de la Información cumplen las siguientes funciones:

- Integrar el equipo de riesgos y ejecutar las actividades que demanden de la gestión de riesgos de seguridad de la información.
- Participar en la elaboración de la Declaración de Aplicabilidad en concordancia con el Plan de Tratamiento de Riesgos y Oportunidades de Seguridad de la Información.
- Ejecutar las actividades de capacitación y sensibilización en seguridad de la información.
- Conservar la información documentada necesaria por el Sistema de Gestión de Seguridad de la Información en coordinación con la Oficina de Administración de Archivos.
- Ejecutar y/o gestionar las acciones que demanden del "Plan de Tratamiento de Riesgos y Oportunidades de Seguridad de la Información".
- Ejecutar la evaluación de desempeño del Sistema de Gestión de Seguridad de la Información a través de los indicadores de gestión.
- Aplicar cuando corresponda, la ejecución del Plan de Continuidad Operativa de la GRE en coordinación con el Gestor Líder de Seguridad de la Información.
- Participar y coordinar en el desarrollo de las auditorías internas/externas, brindando la información que corresponda para su ejecución.
- Ejecutar y/o gestionar las actividades que demanden el cierre de los hallazgos detectados en las auditorías internas y externas.
- Velar por los activos de información que estén debidamente inventariados, y sean utilizados de acuerdo a los procedimientos establecidos, garantizando su uso aceptable.
- Realizar la clasificación, el etiquetado o marcado de la información, donde corresponde.
- Reportar y gestionar la ejecución de las acciones que demanden las vulnerabilidades, eventos e incidentes de seguridad de la información.

- Comunicar los temas de su gestión al Gestor Líder de Seguridad de la Información.
- Proponer y coordinar la implementación o ejecución de controles relacionados a la seguridad de la información en el ámbito de su competencia.
- Otras funciones que se le asigne en el ámbito de su competencia.

La designación de Gestores Operativos de Seguridad de la Información es hecha de conocimiento de la Oficina de Seguridad y Defensa Nacional mediante hoja de elevación

1.2.4. DECLARACIÓN DE APLICABILIDAD

Se definen que controles del anexo A de la norma ISO 27001:2013 que son aplicables al sistema de gestión, para el presenta trabajo se han considerado los que se presentan a continuación:

Nro.	DECLARACIÓN DE APLICABILIDAD								
	Requerimiento de la NTP ISO				Aplicabilidad	Justificación			
	Clausula	Objetivo de Control / Control		Descripción del Objetivo de Control		1	2	3	Comentario
	Política de Seguridad	5.1 Dirección de la gerencia para la seguridad de la información							
1		5.1.1	Políticas para la seguridad de la información	Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la gerencia, publicado y comunicado a los empleados y a las partes externas	SI				Se aplica por cumplimiento regulatorio
2		5.1.2	Revisión de las políticas para la seguridad de la información	Las políticas para la seguridad de la información deben ser revisadas a intervalos planificados o si ocurren cambios significativos para asegurar su conveniencia, adecuación y efectividad continúa.	SI				Se aplica por cumplimiento regulatorio
	Organización de la seguridad de la información	6.1. Organización interna							
3		6.1.1	Roles y responsabilidades para la seguridad de la información	Todas las responsabilidades de seguridad de la información deben ser definidas y asignadas.	SI				Se aplica por cumplimiento regulatorio
4		6.1.2	Segregación de funciones	Las funciones y áreas de responsabilidad en conflicto deben ser segregadas para reducir oportunidades de modificación no autorizada o no intencional o mal uso de los activos	SI				Se aplica por cumplimiento normativo interno
5		6.1.3	Contacto con autoridades	Contactos apropiados con autoridades relevantes deben ser mantenidos.	SI				Se aplica por cumplimiento de buenas prácticas
6		6.1.4	Contacto con grupos especiales de interés	Contactos apropiados con grupos especiales de interés u otros foros de especialistas en seguridad deben ser mantenidos.	SI				Se aplica por cumplimiento de buenas prácticas
7		6.1.5	Seguridad de la información en la gestión de Proyectos	La seguridad de la información debe ser tratada en la gestión de proyectos, sin importar el tipo de proyecto.	SI				Se aplica por cumplimiento normativo
		6.2 Dispositivos móviles y teletrabajo							
8		6.2.1	Política de dispositivos móviles	Una política y medidas de seguridad de soporte deben ser adoptadas para gestionar los riesgos por el uso de dispositivos móviles.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
9		6.2.2	Teletrabajo	Una política y medidas de seguridad de apoyo deben ser implementadas para proteger información a la que se accede	SI				La entidad no tiene la necesidad de aplicar el teletrabajo

Nro.	DECLARACIÓN DE APLICABILIDAD								
	Requerimiento de la NTP ISO				Aplicabilidad	Justificación			
	Clausula	Objetivo de Control / Control		Descripción del Objetivo de Control		1	2	3	Comentario
	SEGURIDAD DE LOS RECURSOS HUMANOS	7.1 Antes del empleo							
10		7.1.1	Selección	La verificación de los antecedentes de todos los candidatos a ser empleados debe ser llevadas a cabo en concordancia con las leyes, regulaciones y ética relevantes, y debe ser proporcional a los requisitos del negocio, la clasificación de la información a la que se tendrá acceso y los riesgos percibidos.	SI		5		Se aplica por cumplimiento de disposiciones para entidades públicas
11		7.1.2	Términos y condiciones del empleo	Los acuerdos contractuales con los empleados y contratistas deben estipular responsabilidades de éstos y de la organización respecto de la seguridad de la información.	SI		5		Se aplica por cumplimiento normativo, aplicación en el PTR y por cumplimiento de disposiciones para entidades públicas
		7.2 Durante el empleo							
12		7.2.1	Responsabilidades de la gerencia	La gerencia debe requerir a todos los empleados y contratistas aplicar la seguridad de la información en concordancia con las políticas y procedimientos establecidos por la organización.	SI				Se aplica por cumplimiento de disposiciones para entidades públicas
13		7.2.2	Conciencia, educación y capacitación sobre la seguridad de la información	Todos los empleados de la organización y, cuando fuera relevante, los contratistas deben recibir educación y capacitación sobre la conciencia de la seguridad de la información, así como actualizaciones regulares sobre políticas y procedimientos de la organización, según sea relevante para la función del trabajo que cumplen.	SI				Se aplica por cumplimiento de disposiciones para entidades públicas
14		7.2.3	Proceso disciplinario	Debe haber un proceso disciplinario formal y comunicado para tomar acción contra empleados que hayan cometido una infracción a la seguridad de la información.	SI				Se aplica por cumplimiento de disposiciones para entidades públicas
		7.3 Terminación y cambio de empleo							
15		7.3.1	Terminación o cambio de responsabilidades del empleo	Las responsabilidades y deberes de seguridad de la información que siguen siendo válidos luego de la terminación o cambio de empleo deben ser definidos, comunicados al empleado o contratista y forzar su cumplimiento.	SI				Se aplica por cumplimiento de disposiciones para entidades públicas

Nro.	DECLARACIÓN DE APLICABILIDAD									
	Requerimiento de la NTP ISO				Aplicabilidad	Justificación				
	Cláusula	Objetivo de Control / Control		Descripción del Objetivo de Control		1	2	3	Comentario
	GESTIÓN DE ACTIVOS	8.1 Responsabilidad por los activos							
16		8.1.1	Inventario de activos	Información, otros activos asociados con información e instalaciones de procesamiento de información deben ser identificados y un inventario de estos activos debe ser elaborado y mantenido.	SI		✓		Se aplica por cumplimiento normativo
17		8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario deben ser propios.	SI				Se aplica por cumplimiento normativo
18		8.1.3	Uso aceptable de los activos	Las reglas para el uso aceptable de la información y activos asociados con la información y con las instalaciones de procesamiento de la información deben ser identificadas, documentadas e implementadas.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
19		8.1.4	Retorno o devolución de activos	Todos los empleados y usuarios de partes externas deben retornar todos los activos de la organización en su posesión a la conclusión de su empleo, contrato o acuerdo.	SI				Se aplica por cumplimiento normativo
		8.2 Clasificación de la información							
20		8.2.1	Clasificación de la información	La información debe ser clasificada en términos de los requisitos legales, valor, criticidad y sensibilidad respecto a una divulgación o modificación no autorizada.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
21		8.2.2	Etiquetado de la información	Un conjunto apropiado de procedimientos para el etiquetado de la información debe ser desarrollado e implementado en concordancia con el esquema de clasificación de la información adoptado por la organización.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
22		8.2.3	Manejo de activos	Los procedimientos para el manejo de activos deben ser desarrollados e implementados en concordancia con el esquema de clasificación de la información adoptada por la organización.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR

1)Plan de Tratamiento de Riesgo 2) Requisito Legal u Obligación Contractual 3) Buenas Practicas

Nro	DECLARACIÓN DE APLICABILIDAD								
	Requerimiento de la NTP ISO				Aplicabilidad	Justificación			
	Clausula	Objetivo de Control / Control		Descripción del Objetivo de Control		1	2	3	Comentario
	GESTIÓN DE ACTIVOS	8.3 Manejo de los medios							
23		8.3.1	Gestión de medios removibles	Se debe implementar procedimientos para la gestión de medios removibles en concordancia con el esquema de clasificación adoptado por la organización.	SI				Se aplica por cumplimiento normativo
24		8.3.2	Eliminación o disposición de medios	Se debe poner a disposición los medios de manera segura cuando ya no se requieran, utilizando procedimientos formales.	SI				Se aplica por cumplimiento normativo
25		8.3.3	Transferencia de medios físicos	Los medios que contienen información deben ser protegidos contra el acceso no autorizado, el mal uso o la corrupción durante el transporte.	SI				Se aplica por cumplimiento normativo
	CONTROL DE ACCESO	9.1 Requisitos de la empresa para el control de acceso							
26		9.1.1	Política de control de acceso	Una política de control de acceso debe ser establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información.	SI				Se aplica por cumplimiento normativo
27		9.1.2	Acceso a redes y servicios de red	Los usuarios deben tener acceso solamente a la red y a servicios de red que hayan sido específicamente autorizados a usar.	SI				Se aplica por cumplimiento normativo
		9.2 Gestión de acceso de usuario							
28		9.2.1	Registro y baja de usuario	Un proceso formal de registro y baja de usuarios debe ser implementado para permitir la asignación de derechos de acceso.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
29		9.2.2	Aprovisionamiento de acceso a usuarios	Un proceso formal de aprovisionamiento de acceso a usuarios debe ser implementado para asignar o revocar los derechos de acceso para todos los tipos de usuarios a todos los sistemas y servicios.	SI				Se aplica por cumplimiento normativo
30		9.2.3	Gestión de derechos de acceso privilegiados	La asignación y uso de derechos de acceso privilegiado debe ser restringida y controlada.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
31		9.2.4	Gestión de información de autentificación	La asignación de información de autenticación secreta debe ser controlada a través de un proceso de gestión formal.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR

Nro	DECLARACIÓN DE APLICABILIDAD								
	Requerimiento de la NTP ISO				Aplicabilidad	Justificación			
	Clausula	Objetivo de Control / Control		Descripción del Objetivo de Control		1	2	3	Comentario
32		9.2.5	Revisión de derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
33		9.2.6	Revisión de derechos de acceso de usuarios	Los derechos de acceso a información e instalaciones de procesamiento de información de todos los empleados y de los usuarios de partes externas deben removerse al término de su empleo, contrato o acuerdo, o ajustarse según el cambio.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
		9.3 Responsabilidades de los usuarios							
34		9.3.1	Uso de información de autentificación secreta	Los usuarios deben ser exigidos a que sigan las prácticas de la organización en el uso de la información de autenticación secreta.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
		9.4 Control de acceso a sistema y aplicación							
35		9.4.1	Restricción de acceso a la información	El acceso a la información y a las funciones del sistema de aplicación debe ser restringido en concordancia con la política de control de acceso.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
36		9.4.2	Procedimientos de ingreso seguro	Donde la política de control de acceso lo requiera, el acceso a los sistemas y a las aplicaciones debe ser controlado por un procedimiento de ingreso seguro.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
37		9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
38		9.4.4	Uso de programas utilitarios privilegiados	El uso de programas utilitarios que podrían ser capaces de pasar por alto los controles del sistema y de las aplicaciones debe ser restringido y controlarse estrictamente.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
39		9.4.5	Control de acceso al código fuente de los programas	El acceso al código fuente de los programas debe ser restringido.	SI				Se aplica por cumplimiento normativo

Nro	DECLARACIÓN DE APLICABILIDAD								
	Requerimiento de la NTP ISO				Aplicabilidad	Justificación			
	Clausula	Objetivo de Control / Control		Descripción del Objetivo de Control		1	2	3	Comentario
		10.1 Controles criptográficos							
40	CRIPTOGRAFIA	10.1.1	Política sobre el uso de controles criptográficos	Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	SI				Se aplica por cumplimiento normativo
41		10.1.2	Gestión de claves	Una política sobre el uso, protección y tiempo de vida de las claves criptográficas debe ser desarrollada e implementada su ciclo de vida.	SI				Se aplica por cumplimiento normativo
	SEGURIDAD FÍSICA Y AMBIENTAL	11.1 Áreas seguras							
42		11.1.1	Perímetro de seguridad física	Perímetros de seguridad deben ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de la información.	SI				Se aplica por cumplimiento de disposiciones para entidades públicas y de defensa civil y aplicación en el PTR
43		11.1.2	Controles de ingreso físico	Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite el acceso sólo al personal autorizado.	SI				Se aplica por cumplimiento de disposiciones para entidades públicas y de defensa civil y aplicación en el PTR
44		11.1.3	Asegurar oficinas, áreas e instalaciones	Seguridad física para oficinas, áreas e instalaciones debe ser diseñada e implementada.	SI				Se aplica por cumplimiento de disposiciones para entidades públicas y de defensa civil y aplicación en el PTR
45		11.1.4	Protección contra amenazas externas y ambientales	Protección física contra desastres naturales, ataque malicioso o accidentes debe ser diseñada y aplicada.	SI				Se aplica por cumplimiento de disposiciones para entidades públicas y de defensa civil y aplicación en el PTR
46		11.1.5	Trabajo en áreas seguras	Procedimientos para el trabajo en áreas seguras debe ser diseñado y aplicado.	SI				Se aplica por cumplimiento de disposiciones para entidades públicas y de defensa civil y aplicación en el PTR
47		11.1.6	Áreas de despacho y carga	Los puntos de acceso, como las áreas de despacho, carga y otros puntos en donde personas no autorizadas pueden ingresar al local deben ser controlados, y si fuera posible, aislados de las instalaciones de procesamiento de la información para evitar el acceso no autorizado.	SI				Se aplica por cumplimiento de disposiciones para entidades públicas y de defensa civil y aplicación en el PTR

Nro	DECLARACIÓN DE APLICABILIDAD								
	Requerimiento de la NTP ISO				Aplicabilidad	Justificación			
	Clausula	Objetivo de Control / Control		Descripción del Objetivo de Control		1	2	3	Comentario
	SEGURIDAD FÍSICA Y AMBIENTAL	11.2 Seguridad de los equipos							
48		11.2.1	Emplazamiento y protección de los equipos	Los equipos deben ser ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
49		11.2.2	Servicios de suministro	Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
50		11.2.3	Seguridad del cableado	El cableado de energía y telecomunicaciones que llevan datos o servicios de información de soporte debe ser protegido de la interceptación, interferencia o daño.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
51		11.2.4	Mantenimiento de equipos	Los equipos deben mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
52		11.2.5	Remoción de activos	Los equipos, la información o el software no deben ser retirados de su lugar sin autorización previa.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
53		11.2.6	Seguridad de equipos y activos fuera de las instalaciones	La seguridad debe ser aplicada a los activos que están fuera de su lugar tomando en cuenta los distintos riesgos de trabajar fuera de las instalaciones de la organización.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
54		11.2.7	Reutilización o eliminación segura de equipos	Todos los elementos del equipo que contengan medios de almacenamiento deben ser verificados para asegurar que cualquier dato sensible y software con licencia se haya eliminado o se haya sobre escrito de manera segura antes de su disposición o reutilización.	SI				Se aplica por cumplimiento normativo
55		11.2.8	Equipo de usuarios desatendidos	Los usuarios deben asegurarse de que el equipo desatendido tenga la protección apropiada.	SI				Se aplica por cumplimiento normativo
56		11.2.9	Política de escritorio limpio y pantalla limpia	Una política de escritorio limpio de papeles y de medios de almacenamiento removibles, así como una política de pantalla limpia para las instalaciones de procesamiento de la información.	SI				Se aplica por cumplimiento normativo

Nro	DECLARACIÓN DE APLICABILIDAD								
	Requerimiento de la NTP ISO				Aplicabilidad	Justificación			
	Clausula	Objetivo de Control / Control		Descripción del Objetivo de Control		1	2	3	Comentario
		12. 1 Procedimientos y responsabilidades operativas							
57	SEGURIDAD DE LAS OPERACIONES	12.1.1	Procedimientos operativos documentados	Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que los necesitan.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
58		12.1.2	Gestión del cambio	Los cambios en la organización, procesos de negocio, instalaciones de procesamiento de la información y sistemas que afecten la seguridad de la información deben ser controlados.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
59		12.1.3	Gestión de la capacidad	El uso de recursos debe ser monitoreado, afinado y se debe hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
60		12.1.4	Separación de los entornos de desarrollo, pruebas y operaciones	Los entornos de desarrollo, pruebas y operaciones deben ser separados para reducir los riesgos de acceso no autorizado o cambios al entorno operativo.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
		12.2 Protección contra códigos maliciosos							
61		12.2.1	Controles contra códigos maliciosos	Controles de detección, prevención y recuperación para proteger contra códigos maliciosos deben ser implementados, en combinación con una concientización apropiada de los usuarios.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
		12.3 Copias de seguridad (Respaldo)							
62		12.3.1	Copias de seguridad de la información	Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR

Nro.	DECLARACIÓN DE APLICABILIDAD									
	Requerimiento de la NTP ISO				Aplicabilidad	Justificación				
	Cláusula	Objetivo de Control / Control		Descripción del Objetivo de Control		1	2	3	Comentario
	SEGURIDAD DE LAS OPERACIONES	12. 4 Registros y monitoreo							
63		12.4.1	Registro de eventos	Registros (logs) de eventos de actividades de usuarios, excepciones, fallas y eventos de seguridad de la información deben ser producidos, mantenidos y regularmente revisados.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
64		12.4.2	Protección de información de registros	Las instalaciones para registros (logs) y la información de los registros (logs) deben ser protegidas contra la adulteración y el acceso no autorizado.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
65		12.4.3	Registros del administrador y el operador	Las actividades del administrador del sistema y del operador del sistema deben ser registradas y los registros (logs) deben ser protegidos y revisados regularmente.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
66		12.4.4	Sincronización del reloj	Los relojes de todos los sistemas de procesamiento de la información relevantes dentro de una organización o dominio de seguridad deben estar sincronizados a una fuente de tiempo de referencia única.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
		12.5 Control del Software operacional							
67		12.5.1	Instalación del software en sistemas operacionales	Procedimientos deben ser implementados para controlar la instalación de software en sistemas operacionales.	SI				Se aplica por cumplimiento normativo
		12.6 Gestión de la vulnerabilidad técnica							
68		12.6.1	Control de vulnerabilidades técnicas	Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debe ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debe ser evaluada y las medidas apropiadas deben ser tomadas para resolver el riesgo asociado.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
69		12.6.2	Restricciones sobre la instalación de software	Reglas que gobiernen la instalación de software por parte de los usuarios deben ser establecidas e implementadas.	SI				Se aplica por cumplimiento normativo
		12.7 Consideraciones para la auditoria de sistemas de información							
70		12.7.1	Controles de auditoria de sistemas de información	Requisitos de las auditorías y las actividades que involucran la verificación de sistemas operacionales deben ser cuidadosamente planificados y acordados para minimizar la interrupción a los procesos del negocio.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR

Nro	DECLARACIÓN DE APLICABILIDAD								
	Requerimiento de la NTP ISO				Aplicabilidad	Justificación			
	Clausula	Objetivo de Control / Control		Descripción del Objetivo de Control		1	2	3	Comentario
	SEGURIDAD DE LAS COMUNICACIONES	13.1 Gestión de seguridad de la red							
71		13.1.1	Controles de la red	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y las aplicaciones.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
72		13.1.2	Seguridad de los servicios de red	Mecanismos de seguridad, niveles de servicio y requisitos de gestión de todos los servicios de red deben ser identificados e incluidos en acuerdos de servicios de red, ya sea que estos servicios se provean internamente o sean tercerizados.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
73		13.1.3	Segregación en Redes	Grupos de servicios de información, usuarios y sistemas de información deben ser segregados en redes.	SI				Se aplica por cumplimiento normativo
		13.2 Transferencia de información							
74		13.2.1	Políticas y procedimientos de transferencia de la información	Políticas, procedimientos y controles de transferencia formales deben aplicarse para proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación.	SI				Se aplica por cumplimiento normativo
75		13.2.2	Acuerdo sobre transferencia de información	Los acuerdos deben dirigir la transferencia segura de información del negocio entre la organización y partes externas.	SI				Se aplica por cumplimiento normativo
76		13.2.3	Mensajes electrónicos (correo)	La información involucrada en mensajería electrónica debe ser protegida apropiadamente.	SI				Se aplica por cumplimiento normativo
77		13.2.4	Acuerdos de confidencialidad o no divulgación	Requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información debe ser identificado, revisados regularmente y documentados.	SI				Se aplica por cumplimiento normativo

1)Plan de Tratamiento de Riesgo 2) Requisito Legal u Obligación Contractual 3) Buenas Practicas

Nro.	DECLARACIÓN DE APLICABILIDAD									
	Requerimiento de la NTP ISO				Aplicabilidad	Justificación				
	Clausula	Objetivo de Control / Control		Descripción del Objetivo de Control		1	2	3	Comentario	
	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	14.1 Requisitos de seguridad de los sistemas de información								
78		14.1.1	Análisis y especificación de requisitos de seguridad de la información	Requisitos relacionados a la seguridad de la información deben ser incluidos dentro de los requisitos para nuevos sistemas de información o mejoras a los sistemas de información existente.	SI				Se aplica por cumplimiento normativo	
79		14.1.2	Aseguramiento de servicios de aplicaciones sobre redes públicas	La información involucrada en servicios de aplicaciones que pasa sobre redes públicas debe ser protegida de actividad fraudulenta, disputa de contratos o divulgación no autorizada y modificada.	SI				Se aplica por cumplimiento normativo	
80		14.1.3	Protección de transacciones en servicios de aplicación	La información involucrada en las transacciones de servicios de aplicación debe ser protegida para prevenir transmisión incompleta, ruteo incorrecto, alteración no autorizada, duplicación o respuesta no autorizada de mensajes.	SI				Se aplica por cumplimiento normativo	
		14.2 Seguridad en los procesos de desarrollo y soporte								
81		14.2.1	Política de desarrollo seguro	Reglas para el desarrollo de software y sistemas deben ser establecidas y aplicadas a desarrollos dentro de la organización.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR	
82		14.2.2	Procedimientos de control de cambio del sistema	Cambios a los sistemas dentro del ciclo de vida del desarrollo deben ser controlados por medio del uso de procedimientos formales de control de cambios.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR	
83		14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	Cuando se cambian las plataformas operativas, las aplicaciones críticas para el negocio deben ser revisadas y probadas para asegurar que no haya impacto adverso en las operaciones o en la seguridad de la organización.	SI				Se aplica por cumplimiento normativo	
84		14.2.4	Restricciones sobre cambios a los paquetes de software	Modificaciones a los paquetes de software deben ser disuadidas, limitadas a los cambios necesarios y todos los cambios deben ser estrictamente controlados.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR	
85		14.2.5	Principios de ingeniería de sistemas seguros	Principios para la ingeniería de sistemas seguros deben ser establecidos, documentados, mantenidos y aplicados a cualquier esfuerzo de implementación de sistemas de información.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR	

1)Plan de Tratamiento de Riesgo 2) Requisito Legal u Obligación Contractual 3) Buenas Practicas

Nro.	DECLARACIÓN DE APLICABILIDAD									
	Requerimiento de la NTP ISO				Aplicabilidad	Justificación				
	Clausula	Objetivo de Control / Control		Descripción del Objetivo de Control		1	2	3	Comentario
86	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	14.2.6	Entorno de desarrollo seguro	Las organizaciones deben establecer y proteger apropiadamente los ambientes de desarrollo para los esfuerzos de desarrollo e integración de	SI				Se aplica por cumplimiento normativo
87		14.2.7	Desarrollo contratado externamente	La organización debe supervisar y monitorear la actividad de desarrollo de sistemas contratado externamente.	SI				Se aplica por cumplimiento normativo
88		14.2.8	Pruebas de seguridad del sistema	Pruebas de funcionalidad de la seguridad deben ser llevadas a cabo durante el desarrollo.	SI				
89		14.2.9	Pruebas de aceptación del sistema	Programas de pruebas de aceptación y criterios relacionados deben ser establecidos para nuevos sistemas de información, actualizaciones y nuevas versiones.	SI				
		14.3 Datos de prueba							
90		14.3.1	Protección de los datos de prueba	Los datos de prueba deben ser seleccionados cuidadosamente y protegidos.	SI				
	RELACIONES CON LOS PROVEEDORES	15.1 Seguridad de la información en las relaciones con proveedores							
91		15.1.1	Política de seguridad de la información para las relaciones con los proveedores	Requisitos de seguridad de la información para mitigar los riesgos asociados deben ser acordados con el proveedor y documentados.	SI				
92		15.1.2	Requisitos de seguridad en contratos o acuerdos con proveedores	Todos los requisitos relevantes de seguridad de la información deben ser establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar,	SI				
93		15.1.3	Cadena de suministro de tecnología de información y comunicación	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información.	SI				
		15.2 Gestión de entrega de servicios del proveedor							
94		15.2.1	Monitoreo y revisión de servicios de los proveedores	Las organizaciones deben monitorear, revisar y auditar regularmente la entrega de servicios por parte de los proveedores.	SI				
95		15.2.2	Gestión de cambios a los servicios de proveedores	Los cambios a la provisión de servicios deben ser gestionados tomando en cuenta la criticidad de la información del negocio, sistemas y procesos involucrados y una reevaluación de riesgos.	SI				

Nro.	DECLARACIÓN DE APLICABILIDAD								
	Requerimiento de la NTP ISO				Aplicabilidad	Justificación			
	Clausula	Objetivo de Control / Control		Descripción del Objetivo de Control		1	2	3	Comentario
	GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	16.1 Gestión de incidentes de seguridad de la información y mejoras							
96		16.1.1	Responsabilidades y procedimientos	Las responsabilidades de gestión y los procedimientos deben ser establecidos para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.	**SI**				Se aplica por cumplimiento normativo
97		16.1.2	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información deben ser reportados a través de canales de gestión apropiados tan rápido como sea posible.	**SI**				Se aplica por cumplimiento normativo
98		16.1.3	Reporte de debilidades de seguridad de la información	Empleados y contratistas que usan los sistemas y servicios de información de la organización deben ser exigidos a advertir y reportar cualquier debilidad observada o de la que se sospecha en cuanto a seguridad de la información en los sistemas o servicios.	**SI**				Se aplica por cumplimiento normativo y aplicación en el PTR
99		16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	Los eventos de seguridad de la información deben ser evaluados y deben decidirse si son clasificados como incidentes de seguridad de la información.	**SI**				Se aplica por cumplimiento normativo
100		16.1.5	Respuesta a incidentes de seguridad de la información	Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.	**SI**				Se aplica por cumplimiento normativo
101		16.1.6	Aprendizaje de los incidentes de seguridad de la información	El conocimiento adquirido a partir de analizar y resolver los incidentes de seguridad de la información debe ser utilizado para reducir la probabilidad o el impacto de incidentes futuros.	**SI**				Se aplica por cumplimiento normativo
102		16.1.7	Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	**SI**				Se aplica por cumplimiento normativo

Nro.	DECLARACIÓN DE APLICABILIDAD									
	Requerimiento de la NTP ISO				Aplicabilidad	Justificación			
	Clausula	Objetivo de Control / Control		Descripción del Objetivo de Control		1	2	3	Comentario
	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO	17.1 Continuidad de la seguridad de la información							
103		17.1.1	Planificación de continuidad de seguridad de la información	La organización debe determinar sus requisitos de seguridad de la información y continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
104		17.1.2	Implementación de continuidad de seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de seguridad de la información durante una situación adversa.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
105		17.1.3	Verificación, revisión y evaluación de continuidad de seguridad de la información	La organización debe verificar los controles de continuidad de seguridad de la información que han establecido e implementado a intervalos regulares para asegurarse que son válidos y efectivos durante situaciones adversas.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
		17.2 Redundancias							
106		17.2.1	Disponibilidad de las instalaciones de procesamiento de información	Las instalaciones de procesamiento de la información deben ser implementadas con redundancia suficiente para cumplir con los requisitos de disponibilidad.	SI				Se aplica por cumplimiento normativo y aplicación en el PTR
	CUMPLIMIENTO	18.1 Cumplimiento de requisitos legales y contractuales							
107		18.1.1	Identificación de requisitos contractuales y legislación aplicable	Todos los requisitos legislativos, estatutarios, regulatorios y contractuales relevantes, así como el enfoque de la organización para cumplir con estos requisitos deben ser explícitamente identificados, documentados y mantenidos al día para cada sistema de información y para la organización.	SI				Se aplica en cumplimiento de las nuevas tendencias y lineamientos con el fin de que sea útil en el desarrollo y solución de situaciones que involucren la
108		18.1.2	Derechos de propiedad intelectual (DPI)	Procedimientos apropiados deben ser implementados para asegurar el cumplimiento de requisitos legislativos, regulatorios y contractuales relacionados a los derechos de propiedad intelectual y uso de productos de software propietario.	SI				La institución registra el software desarrollado inhouse en INDECOPI

Nro.	DECLARACIÓN DE APLICABILIDAD									
	Requerimiento de la NTP ISO					Aplicabilidad	Justificación			
	Clausula	Objetivo de Control / Control		Descripción del Objetivo de Control			1	2	3	Comentario
109	CUMPLIMIENTO	18.1.3	Planificación de continuidad de seguridad de la información	Los registros deben ser protegidos de cualquier pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio.		SI				Se aplica por cumplimiento normativo
110		18.1.4	Protección de datos y privacidad de la información de carácter personal	La privacidad y la protección de datos personales deben aseguradas tal como se requiere en la legislación y regulación relevantes donde sea aplicable.		SI				Se aplica por cumplimiento normativo
111		18.1.5	Regulación de controles criptográficos	Controles criptográficos deben ser utilizados en cumplimiento con todos los acuerdos, legislación y regulación relevantes.		SI				Se aplica por cumplimiento normativo
		18.2 Revisión de la seguridad de la información								
112		18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la organización para manejar la seguridad de la información y su implementación (por ejemplo, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) debe ser revisado independientemente a intervalos planeados o cuando ocurran cambios significativos.		SI				Se aplica por cumplimiento normativo
113		18.2.2	Cumplimiento de políticas y normas de seguridad	Los gerentes deben revisar regularmente el cumplimiento del procesamiento de la información y de los procedimientos dentro de su área de responsabilidad con las políticas, normas y otros requisitos de seguridad apropiados.		SI				Se aplica por cumplimiento normativo y aplicación en el PTR
114		18.2.3	Revisión del cumplimiento técnico	Los sistemas de información deben ser revisados regularmente respecto al cumplimiento de las políticas y normas de seguridad de la información de la organización.		SI				Se aplica por cumplimiento normativo

N°	DECLARACIÓN DE APLICABILIDAD EN LA SUB GERENCIA DE BASE DE DATOS						
	REQUERIMIENTO DE LA NTP ISO 27001			IMPLEMENTACIÓN DE CONTROLES			
	Clausula	Objetivo de Control / Control		DESCRIPCIÓN DE LO IMPLEMENTADO	ÁREA RESPONSABLE	UUOO RESPONSABLE	OBSERVACIONES
1	POLITICAS DE SEGURIDAD	5.1.1	Políticas para la seguridad de la información	(1) DI-288-GI/020 "Lineamientos Generales de Seguridad de la Información". (2) DI 327, 328 GTI	(1) GTI (2) GTI	Todos	
3		6.1.1	Roles y responsabilidades para la seguridad de la información	'Estructura de la Organización de la Seguridad de la Información (en Manual del SGSI).	GTI	Todos	
4		6.1.2	Segregación de funciones	'(1) Perfiles de puestos (Contratos de Trabajo). Matriz de competencias. (2) Documentos de asignación de roles o funciones.	GTI	Todos	Falta documento de asignación de funciones
26	CONTROL DE ACCESO	9.1.1	Política de control de acceso	(1) DI-328-GTI/022 "Seguridad Informática de la red del RENIEC" (2) DI-327-GTI/021 "Servicios de Comunicación para Usuarios Finales"(3) NAI-415-GTI-SGGBD/005 "Seguridad y Auditoria en las Bases de Datos del Reniec",	(1) GTI	1, 2)SGOT 3) SGGBD	
27		9.1.2	Acceso a redes y servicios de red	(1) DI-328-GTI/022 "Seguridad Informática de la red del RENIEC" (2) DI-327-GTI/021 "Servicios de Comunicación para Usuarios Finales" (3) NAI-415-GTI-SGGBD/005 "Seguridad y Auditoria en las Bases de Datos del Reniec",	(1) GTI	1, 2)SGOT 3) SGGBD	
37		9.4.3	Sistema de gestión de contraseñas	(1) DI-328-GTI/022 "Seguridad Informática de la red del RENIEC" (2 DI-327-GTI/021 "Servicio de Comunicación para Usuarios Finales del RENIEC" (3) NAI-415-GTI-SGGBD/005 "Seguridad y Auditoria en las Bases de Datos del Reniec"	(1) GTI	1, 2)SGOT 3) SGGBD	

N°	DECLARACIÓN DE APLICABILIDAD EN LA SUB GERENCIA DE BASE DE DATOS							
	REQUERIMIENTO DE LA NTP ISO 27001				IMPLEMENTACIÓN DE CONTROLES			
	Clausula	Objetivo de Control / Control			DESCRIPCIÓN DE LO IMPLEMENTADO	ÁREA RESPONSABLE	UUOO RESPONSABLE	OBSERVACIONES
39	CONTROL DE ACCESO	9.4.5	Control de acceso al código fuente de los programas		Nai-338-Gi/001 "Proceso De Gestión De La Configuración"GP-287-Gi/SGGBD/004 "Creación, Modificación O Recompilación De Objetos En Las Bases De Datos En Producción"	(1) GTI	SGIS, SGGBD	
47	SEGURIDAD FÍSICA Y AMBIENTAL	11.1.6	Áreas de despacho y carga		'(1) área de recepción de la GTI (2) cámara de video vigilancia (3) personal de seguridad (4) Control de acceso biométrico	GTI / OSDN / SGEN	TODOS	
55		11.2.8	Equipo de usuarios desatendidos		'(1) Configuración de bloqueo de la sesión de los equipos (2) DI-328-GTI/022 "Seguridad Informática de la red del RENIEC"	(1) GTI (2) GTI	TODOS	
56		11.2.9	Política de escritorio limpio y pantalla limpia		'(1) Configuración de bloqueo de la sesión de los equipos (2) DI-328-GTI/022 "Seguridad Informática de la red del RENIEC"	(1) GTI (2) GTI	TODOS	
57	SEGURIDAD DE LAS OPERACIONES	12.1.1	Procedimientos operativos documentados		Ver la intranet institucional documentos normativos	(1) GTI	TODOS	
59		12.1.3	Gestión de la capacidad		(1) NAI- 391 GTI/SGOT/012 “Monitoreo de Seguridad Informática, de la Red de Datos del RENIEC y Gestión de Incidentes”	(1) GTI	SGOT, SGSTO, SGGBD	Falta documento normativo: SGSTO y SGGBD
63		12.4.1	Registro de eventos		(1) NAI- 391 GTI/SGOT/012 “Monitoreo de Seguridad Informática, de la Red de Datos del RENIEC y Gestión de Incidentes”	(1) GTI	SGOT, SGSTO, SGGBD	Falta documento normativo: SGSTO y SGGBD
64		12.4.2	Protección de información de registros		(1) DI-328-GTI/022 "Seguridad Informática de la red del RENIEC"	(1) GTI	SGOT, SGSTO, SGGBD	Falta documento normativo la SGSTO y SGGBD
65		'12.4.3	Registros del administrador y el operador		(1) DI-328-GTI/022 "Seguridad Informática de la red del RENIEC"	(1) GTI	SGOT,SGSTO, SGGBD	Falta documento normativo la SGSTO y SGGBD
70		12.7.1	Controles de auditoria		DI 400 - Auditorías Internas de los Sistemas de Gestión del RENIEC	(1) GTI	TODOS	

1) Plan de Tratamiento de Riesgo 2) Requisito Legal u Obligación Contractual 3) Buenas Practicas

1.3. HACER (DO)

Para un buen análisis de riesgos se ha establecido las siguientes actividades y etapas:

- Identificar los activos y/ grupos de activos de información relevantes para el negocio.
- Identificar los eventos potenciales que pueden tener un efecto positivo o negativo sobre los activos de información
- Determinar la probabilidad de ocurrencia del evento.
- Estimar el nivel de impacto en función de la confidencialidad, integridad o disponibilidad.
- Estimar el nivel del riesgo
- Evaluar la prioridad para la atención del riesgo
- Identificar las acciones necesarias (Tratamiento de los riesgos)
- Calcular el riesgo residual

1.3.1. INVENTARIO DE ACTIVOS

Cada activo es clasificado según su tipo para lo cual se han identificado los siguientes tipos de activos de información:

TIPO DE ACTIVO	DESCRIPCIÓN
Servicios	Servicios que implican el acceso a datos o información, recibidos de terceros.
Datos e Información	Bases de datos, Archivos electrónicos, Documentos y registros en papel.
Software	Software base, Aplicaciones, Sistemas Operativos y utilitarios.
Hardware	Servidores, Desktop, Laptops, Storage, Librería de Cintas, etc.
Redes de Comunicación	Switches, Routers, Firewalls, Access point, Sistemas de telefonía, etc.
Soportes de Información	Cintas de backups, DVD (Microformas)
Equipamiento Auxiliar	Aire acondicionado, UPS, Grupo electrógeno, Alarmas, Detectores de humo, Extintores de fuego, Medidores de temperatura, etc.
Instalaciones	Datacenters, Bóvedas, Sedes, Oficinas, Salas, Almacenes, Cintotecas, etc.
Personas	Personal interno, Personal externo, Proveedores, Clientes.

Valorización del activo de información

El valor del activo de información estará en función del impacto que podría tener en las siguientes dimensiones: Confidencialidad, Integridad y Disponibilidad.

CRITERIOS PARA LA VALORACIÓN DE LOS ACTÍVOS DE INFORMACIÓN			
NIVEL	**CONFIDENCIALIDAD**	**INTEGRIDAD**	**DISPONIBILIDAD**
	La falla o pérdida de un activo origina la divulgación o revelamiento no autorizado de información; produciendo un impacto que afecta los intereses de la organización (prestigio, económico, legal, competencia, etc.)	La falla o pérdida de un activo origina la alteración de la información (dejando de ser exacta y completa); produciendo un impacto que afecta los intereses de la organización (prestigio, económico, legal, competencia, etc.)	La falla o pérdida de un activo origina la interrupción del acceso y disponibilidad de la información; produciéndose un impacto que afecta los intereses de la organización (prestigio, económico, legal, competencia, etc.)
Muy Alto (5)	Impacto irreversible	Impacto irreversible	Impacto irreversible
Alto (4)	Impacto severo	Impacto severo	Impacto severo
Medio (3)	Impacto moderado	Impacto moderado	Impacto moderado
Bajo (2)	Impacto parcial	Impacto parcial	Impacto parcial
Muy Bajo (1)	Sin impacto	Sin impacto	Sin impacto

El valor del activo será el promedio de los 3 valores registrados por cada dimensión citada anteriormente, aquellos activos con un valor del riesgo mayor o igual a 3 pasaran al análisis del riesgo.

GESTIÓN DEL RIESGO														
IDENTIFICACIÓN DE ACTIVOS						RESPONSABILIDAD			VALORIZACIÓN DEL ACTIVO				DESCRIPCION
									C	I	D		
CLASIFICACIÓN	N°	NOMBRE DEL ACTIVO	DESCRIPCIÓN	FUNCIÓN	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO DEL ACTIVO	USUARIO DEL ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DEL ACTIVO	
DATOS (INFORMACIÓN)	1	Documentos normativos	Documentos de cumplimiento obligatorio que contiene las disposiciones emitidas por la Sub Gerencia. Estos documentos contemplan: Normas Administrativas Internas - NAI.	Regular, desarrollar o dirigir las funciones y procesos de gestión interna	Intranet y fiile server (Formato Digital),	'SGGBD	'SGGBD	'GTI	5	5	1	4	NO SIGNIFICATIVO
	2	Lineamientos	Documentos que permite indicar las acciones a seguir con respecto al monitoreo de elaboración de reportes de continuidad de la Base de Datos Institucional.	Regular, desarrollar o dirigir las funciones y procesos de gestión interna	File server carpeta SGBD (Formato Digital)	'SGGBD	'SGGBD	'GTI	8	5	5	6	IMPORTANTE
	3	Estándares de base de datos	Documento técnico que permite la denominación de los objetos de la Base de Datos Institucional.	Nombrar adecuadamente los objetos de la Base de Datos Institucional.	File server carpeta SGBD (Formato Digital)	'SGGBD	'SGGBD	'GTI	8	5	1	5	IMPORTANTE
	4	Reporte de rendimiento de la base de datos	Documento que contiene el comportamiento de la Base de Datos Institucional en un período determinado.	Monitoreo del comportamiento de la Base de Datos Institucional.	File server carpeta SGBD (Formato Digital)	'SGGBD	'SGGBD	'GTI	8	5	5	6	IMPORTANTE
	5	Actas de pase de producción	Documento técnico que permite la formalización de los requerimientos de pase a producción, referidos a creación y/o modificación de los objetos de la Base Datos Institucional (requerimiento, detalle de las modificaciones de datos y alteraciones de estructuras (tablas, Store Proccedures, Funciones, etc.))	Seguimiento de control de cambios de los objetos de la Base de Datos Institucional.	File server carpeta SGBD (Formato Digital)	'GTI	SGGBD	'GTI	8	5	5	6	IMPORTANTE

GESTIÓN DEL RIESGO														
IDENTIFICACIÓN DE ACTIVOS						RESPONSABILIDAD			VALORIZACIÓN DEL ACTIVO				DESCRIPCIÓN
									C	I	D		
CLASIFICACIÓN	N°	NOMBRE DEL ACTIVO	DESCRIPCIÓN	FUNCIÓN	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO DEL ACTIVO	USUARIO DEL ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DEL ACTIVO	
DATOS (INFORMACIÓN)	6	Acta de creación, modificación y/o desactivación de usuarios de base de datos.	Documento técnico que permite otorgar o denegar los privilegios de accesos a la Base de Datos Institucional.	Controlar los usuarios que accedan a la Base de Datos Institucional.	File server carpeta SGBD (Formato Digital)	GTI	SGGBD	GTI	8	5	5	6	IMPORTANTE
	7	Correo de atención de requerimientos de Base de Datos	Correo electrónico derivado a la cuenta de los administradores de base de datos, en el cual con previa autorización se ejecuta un dml, ddl y/o dcl en la Base de Datos Institucional. (Personal que tiene autorización de acceso al correo).	Atención de los requerimientos informáticos en la Base de Datos Institucional.	En los *.pst de los administradores de base de datos (formato digital)	'SGGBD	'SGGBD, SGOT	'RENIEC y Entidades externas	8	5	10	8	CRITICO
	8	Documentos administrativos	Oficios, informes, memorandos, hojas de elevación, proveídos, cartas, hoja de envió.	Mantener evidencia de las gestiones propias de la Sub Gerencia.	STD (Formato Digital), file físico (Formato Físico)	'SGGBD	'SGGBD	'RENIEC y Entidades externas	5	5	5	5	IMPORTANTE
	9	Agenda de Sub Gerencia	Registro de las actividades del Sub Gerente de Gestión de Base de Datos en formato *.pst.	Organizar las actividades diarias del Sub Gerente de gestión de Base de Datos.	Computadora del asistente administrativo y del Sub Gerente (Formato Digital).	'Sub Gerente SGGBD	'Asistente Administrativo de la SGGBD	'Sub Gerente SGGBD	8	5	10	18	CRITICO
	10	Control de visitas a la Sub Gerencia	Registro de visitas externas a la SGGBD	Mantener el registro de visitas externas.	Archivo físico en la SGGBD	'SGGBD	'Asistente Administrativo de la SGGBD	'SGGBD	1	5	1	3	NO SIGNIFICATIVO

GESTIÓN DEL RIESGO														
IDENTIFICACIÓN DE ACTIVOS						RESPONSABILIDAD			VALORIZACIÓN DEL ACTIVO				DESCRIPCIÓN
									C	I	D		
CLASIFICACIÓN	N°	NOMBRE DEL ACTIVO	DESCRIPCIÓN	FUNCIÓN	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO DEL ACTIVO	USUARIO DEL ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DEL ACTIVO	
DATOS (INFORMACIÓN)	11	Reporte de mantenimiento de la Base de Datos Institucional	Registro de control de cambios de configuración de la Base de Datos Institucional	Control de cambios de configuración de la Base de Datos Institucional.	File server carpeta SGBD (Formato Digital)	'SGGBD	'SGGBD	'SGGBD	8	5	5	6	IMPORTANTE
	12	Cuaderno de cargos	Registro de entrega de diversos activos: -CD's (información a demanda) -Sobres con diversas informaciones del trámite documentario. -Otros.	Mantener el control de los registros de entrega de diversos activos.	Archivo físico en la SGGBD	'SGGBD	'Asistente Administrativo de la SGGBD	'SGGBD	5	5	1	4	NO SIGNIFICATIVO
	13	Lista de Padrón Inicial (LPI)	Relación de ciudadanos hábiles para un determinado proceso electoral en formato digital y físico a la fecha de cierre.	Fiscalizar el ubigeo del domicilio de los ciudadanos hábiles para un determinado proceso electoral.	Base de datos de la Línea de Producción DNI	'SGGBD	'SGGBD	'GRE, JNE	8	5	5	6	IMPORTANTE
	14	Lista de Jurados Electorales Especiales (JEE)	Relación de los candidatos para ser un jurado electoral especial en formato digital y físico (actas de sorteo para la selección aleatoria de ciudadanos candidatos a ser miembro y suplente del JEE).	Listar los candidatos a ser posibles miembros del JEE.	Equipo de cómputo asignado a la SGGBD para el sorteo de JEE.	'SGGBD	'SGGBD	'GRE, JNE	8	10	5	8	CRITICO
	15	Padrón Electoral	Relación de ciudadanos hábiles para un determinado proceso electoral en formato digital.	Indicar al JNE la relación de los ciudadanos hábiles para un determinado proceso y ejerzan su derecho a voto.	Base de Datos Institucional	'SGGBD	'SGGBD	'GRE, ONPE y JNE	8	5	5	6	IMPORTANTE

GESTIÓN DEL RIESGO														
IDENTIFICACIÓN DE ACTIVOS						RESPONSABILIDAD			VALORIZACIÓN DEL ACTIVO				DESCRIPCIÓN
									C	I	D		
CLASIFICACIÓN	N°	NOMBRE DEL ACTIVO	DESCRIPCIÓN	FUNCIÓN	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO DEL ACTIVO	USUARIO DEL ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DEL ACTIVO	
DATOS (INFORMACIÓN)	16	Bases de Datos Institucional	Repositorio de información de los sistemas informáticos de la Institución.	Almacenar y consultar la información que genera los sistemas informáticos de la Institución.	Servidores de la Institución.	'SGGBD	'SGSTO	'SGIS, SGGBD	8	5	10	8	CRITICO
	17	Informe de capacidad de almacenamiento servidores	Documento mediante el cual se informa el crecimiento de la Base de Datos Institucional en un período de tiempo.	Informar a la SGSTO acerca del crecimiento de la Base de Datos Institucional a fin de preveer la disponibilidad de espacio libre.	PC asignadas como Servidores de Base de Datos de Agencias	'SGGBD	'SGGBD	'Agencias a Nivel Nacional	5	5	5	5	IMPORTANTE
	18	Informe de cotejo masivo de datos	Documento que contiene la cantidad de registros procesados y resultado del cotejo masivo.	Informar a la entidad solicitante el resultado del cotejo masivo.	Sistema de Trámite Documentario	'SGGBD	'SGGBD	'Entidades Externas	8	5	1	5	IMPORTANTE
	19	Bases de Datos de Agencias	Repositorio de información de los sistemas informáticos de la Institución para las agencias con tipo de conexión conmutada, ADSL, VSAT.	Almacenar y consultar la información que genera los sistemas informáticos de la Institución.	Agencias RENIEC a nivel nacional	'SGGBD	'SGGBD	'Personal de las Agencias a Nivel Nacional	5	5	5	5	IMPORTANTE
SOFTWARE	20	Sistema Integrado de Trámite Documentario	Aplicativo desarrollado por la GTI para la gestión documentaria de la Institución.	Generar y consultar la trazabilidad de la documentación administrativa de la Institución.	Equipo informático asignado al personal del área	'SGEN	'SGIS,SGSTO,SGGBD	'SGGBD	5	5	5	5	IMPORTANTE

GESTIÓN DEL RIESGO														
IDENTIFICACIÓN DE ACTIVOS						RESPONSABILIDAD			VALORIZACIÓN DEL ACTIVO				DESCRIPCIÓN
									C	I	D		
CLASIFICACIÓN	N°	NOMBRE DEL ACTIVO	DESCRIPCIÓN	FUNCIÓN	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO DEL ACTIVO	USUARIO DEL ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DEL ACTIVO	
SOFTWARE	21	Sistema de Control patrimonial	Aplicativo que registra la asignación de bienes al personal del área.	Registra los bienes asignados al personal del área.	Equipo informático asignado al personal del área	'GAD - SGCP	'SGIS,SGSTO,SGGBD	'SGGBD	5	5	1	4	NO SIGNIFICATIVO
	22	SIO - Sistema Integrado Operativo	Módulo de consultas generales del SIO	Consulta de ciudadanos.	Equipo informático asignado al personal del área	'GRI	'SGIS,SGSTO,SGGBD	'SGGBD	5	10	5	7	IMPORTANTE
	23	Oracle Enterprise Edition	Manejador de base de datos	Gestor de base de datos	Sede Operativa, Sede Administrativa, Sede San Borja	'SGGBD	'SGGBD, SGSTO	'SGGBD	8	5	10	8	CRITICO
	24	Oracle Cluster Edition	Software de alta disponibilidad para base de datos Oracle	Maneja la alta disponibilidad. (Activo-Activo)	Computadora del asistente administrativo y del Sub Gerente (Formato Digital).	'SGGBD	'SGGBD, SGSTO	'SGGBD	8	5	10	8	CRITICO
	25	Pl/SQL Developer	PL / SQL Developer es un entorno de desarrollo integrado que está específicamente dirigido al desarrollo de unidades de programa almacenadas para Base de Datos Oracle. PL / SQL	Desarrollar y revisar scripts de procedimientos almacenados y otros.	Equipo informático asignado al personal del área	'SGGBD	'SGGBD	'SGGBD	8	5	1	5	IMPORTANTE
	26	Toad	TOAD es una aplicación informática de desarrollo SQL y administración de base de datos, considerada una herramienta útil para los DBAs (administradores de base de datos). Actualmente está disponible para las siguientes bases de datos: Oracle Database, Microsoft SQL Server, IBM DB2, y MySQL.	Administrar y dar mantenimiento de la base de datos.	Equipo informático asignado al personal del área	'SGGBD	'SGGBD	'SGGBD	8	5	1	5	IMPORTANTE

GESTIÓN DEL RIESGO														
IDENTIFICACIÓN DE ACTIVOS						RESPONSABILIDAD			VALORIZACIÓN DEL ACTIVO				DESCRIPCIÓN
									C	I	D		
CLASIFICACIÓN	N°	NOMBRE DEL ACTIVO	DESCRIPCIÓN	FUNCIÓN	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO DEL ACTIVO	USUARIO DEL ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DEL ACTIVO	
SOFTWARE	27	UltraEdit	UltraEdit es un editor de texto comercial.	Permite crear scripts masivos manejando filas y columnas grupales.	Equipo informático asignado al personal del área	SGGBD	SGGBD	SGGBD	8	5	1	5	IMPORTANTE
	28	Putty	PuTTY es un cliente SSH y Telnet con el que podemos conectarnos a servidores remotos iniciando una sesión en ellos que nos permite ejecutar comandos.	Acceder a servidores de base de datos remotamente.	Equipo informático asignado al personal del área	SGGBD	SGGBD	SGGBD	8	5	1	5	IMPORTANTE
	29	Oracle Cliente	Herramienta de acceso a base de datos.	Acceder a la base de datos remotamente.	Equipo informático asignado al personal del área	SGGBD	SGGBD	SGGBD	8	5	5	6	IMPORTANTE
	30	Oracle Administrador	Herramienta de acceso a base de datos y configuración.	Acceder a la base de datos remotamente.	Equipo informático asignado al personal del área	SGGBD	SGGBD	SGGBD	8	5	10	8	CRITICO
	31	GridControl	Herramienta para monitorear y dar mantenimiento a las Bases de Datos.	Monitorear la base de datos remotamente.	Servidor asignado para la instalación del producto	SGGBD	SGGBD	SGGBD	8	5	10	8	CRITICO

GESTIÓN DEL RIESGO														
IDENTIFICACIÓN DE ACTIVOS						RESPONSABILIDAD			VALORIZACIÓN DEL ACTIVO				DESCRIPCIÓN
									C	I	D		
CLASIFICACIÓN	N°	NOMBRE DEL ACTIVO	DESCRIPCIÓN	FUNCIÓN	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO DEL ACTIVO	USUARIO DEL ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DEL ACTIVO	
SOFTWARE	32	Sistema de Consultas en Línea	Sistema de control de usuarios que van a tener acceso al sistema de Consultas en Línea.	Administración y mantenimiento de los usuarios del Servicio de Consultas en Línea.	BD de la Línea de Producción del DNI	'SGGBD – CEL	SSGBD	SSGBD	8	5	10	8	CRITICO
HARDWARE	33	Estaciones de trabajo - DBAS Senior	Equipo informático mediante el cual un DBA Senior de la SGGBD realiza sus actividades.	Generar, almacenar y automatizar información respecto a las actividades de la Sub Gerencia.	Primer Piso Sede San Borja	'SGSTO, GAD-SGCP	SSGBD	SSGBD	8	5	10	8	CRITICO
	34	Estaciones de trabajo	Equipo informático mediante el cual un colaborador de la SGGBD realiza sus actividades.	Generar, almacenar y automatizar información respecto a las actividades de la Sub Gerencia.	Primer Piso Sede San Borja	'SGSTO, GAD-SGCP	SSGBD	SSGBD	8	5	5	6	IMPORTANTE
	35	Computadora personal portátil - LAPTOP	Ordenador personal que se puede mover o transportar con relativa facilidad.	Generar, almacenar y automatizar información respecto a las actividades de la Sub Gerencia.	Primer Piso Sede San Borja	'SGSTO, GAD-SGCP	SSGBD	SSGBD	8	5	5	6	IMPORTANTE
	36	Reproductor grabador de DVD - DVD grabador	Dispositivo electrónico que permite la lectura y grabación de DVD mediante el empleo de un rayo láser y la posterior transformación de este en impulsos eléctricos que la computadora interpreta.	Grabar información respecto a las actividades de la Sub Gerencia.	Primer Piso Sede San Borja	'SGSTO, GAD-SGCP	SSGBD	SSGBD	5	5	1	4	NO SIGNIFICATIVO

GESTIÓN DEL RIESGO													
IDENTIFICACIÓN DE ACTIVOS						RESPONSABILIDAD			VALORIZACIÓN DEL ACTIVO				DESCRIPCIÓN
									C	I	D		
CLASIFICACIÓN	N°	NOMBRE DEL ACTIVO	DESCRIPCIÓN	FUNCIÓN	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO DEL ACTIVO	USUARIO DEL ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DEL ACTIVO	
HARDWARE	37	Sistema de videoconferencia	Equipos que permiten la comunicación simultánea bidireccional de audio y vídeo, que permite mantener reuniones con grupos de personas situadas en lugares alejados entre sí.	Comunicación simultánea bidireccional de audio y vídeo, que permite mantener reuniones con grupos de personas situadas en lugares alejados entre sí. Adicionalmente, pueden ofrecerse facilidades telemáticas o de otro tipo como el intercambio de gráficos, imágenes fijas, transmisión de ficheros desde el ordenador, etc.	Primer Piso Sede San Borja	'SGSTO, GAD-SGCP	'SGGBD	'SGGBD	5	5	1	4	NO SIGNIFICATIVO
	38	Tableta PAD	Dispositivo electrónico que tiene un tamaño intermedio entre el ordenador y el móvil. Sus características principales son las siguientes: su ligereza, su manejo intuitivo utilizando las manos, su elevada autonomía de uso y la no dependencia de otros accesorios complementarios.	Visualizar información respecto a las actividades de la Subgerencia	Primer Piso Sede San Borja	'SGSTO, GAD-SGCP	'SGGBD	'SGGBD	5	1	1	3	NO SIGNIFICATIVO
PERSONAS	39	Sub Gerente	Profesional en Ingeniería de Sistemas, Computación o Informática con Certificación en Administración de Base de Datos Oracle y experiencia laboral mínimo de 06 años en Administración y afinamiento de Base de Datos Oracle Corporativa y en la Administración Pública. Con conocimientos en Administración Gerencial y Administración de Proyectos.	Planificar y controlar las actividades de instalación, configuración y mantenimiento de las bases de datos de la institución que dan soporte a los sistemas de producción y de servicios de información.	Primer Piso Sede San Borja	GTI	'SGGBD	'SGGBD	5	5	10	7	IMPORTANTE

GESTIÓN DEL RIESGO														
IDENTIFICACIÓN DE ACTIVOS						RESPONSABILIDAD			VALORIZACIÓN DEL ACTIVO				DESCRIPCIÓN
									C	I	D		
CLASIFICACIÓN	N°	NOMBRE DEL ACTIVO	DESCRIPCIÓN	FUNCIÓN	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO DEL ACTIVO	USUARIO DEL ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DEL ACTIVO	
PERSONAS	40	Asistente Administrativo	Egresado Técnico Profesional o VII ciclo universitario en Administración e Informática o Contabilidad o Secretariado o Ingeniería de Sistemas y experiencia laboral mínima de 03 años.	'- Recepción de documentos internos y externos. - Seguimiento de documentación. - Verificación de estado de trámites en el SITD - Recepción y monitoreo de llamadas telefónicas. - Redacción de documentos. - Otras actividades que sean asignadas por el Sub Gerente de Base de Datos.	Primer Piso Sede San Borja	GTI	'SGGBD	'SGGBD	5	5	5	5	IMPORTANTE
	41	Administrador de Base de Datos Senior	Profesional en Ingeniería de Sistemas, Computación o Informática con Certificación en Administración de Base de Datos Oracle y experiencia laboral mínimo de 06 años en Administración y afinamiento de Base de Datos Oracle Corporativa.	'- Administración, mantenimiento y monitoreo de Base de Datos Institucional. - Realizar actividades de pase a producción para el soporte de los sistemas informáticos. - Monitorear e implementar controles de seguridad de la Base de Datos Institucional. - Cumplir con las normas, políticas, procedimientos y estándares para la administración y seguridad de la Base de Datos Institucional, así como los sistemas y recursos. - Asesorar en actividades relacionadas de su competencia, a las demás unidades orgánicas. - Otras que le asigne el Sub Gerente de Gestión de Base de Datos.	Primer Piso Sede San Borja	GTI	'SGGBD	'SGGBD	8	5	10	8	CRITICO

GESTIÓN DEL RIESGO														
IDENTIFICACIÓN DE ACTIVOS						RESPONSABILIDAD			VALORIZACIÓN DEL ACTIVO				DESCRIPCIÓN
									C	I	D		
CLASIFICACIÓN	N°	NOMBRE DEL ACTIVO	DESCRIPCIÓN	FUNCIÓN	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO DEL ACTIVO	USUARIO DEL ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DEL ACTIVO	
PERSONAS	42	Administrador de Base de Datos	Profesional en Ingeniería de Sistemas, Computación o Informática con Cursos en Administración de Base de Datos Oracle y experiencia laboral mínima de 05 años en Administración y afinamiento de Base de Datos Oracle Corporativa.	'- Administración, mantenimiento y monitoreo de la Base de Datos Institucional. - Realizar actividades de pase a producción para el soporte de los sistemas informáticos. - Asistir a los desarrolladores con sus conocimientos de SQL y de construcción de procedimientos almacenados y triggers, entre otros. - Monitorear e implementar controles de seguridad de la Base de Datos Institucional. - Cumplir con las normas, políticas, procedimientos y estándares para la administración y seguridad de la Base de Datos Institucional, así como los sistemas y recursos. - Asesorar en actividades relacionadas de su competencia, a las demás unidades orgánicas. - Otras que le asigne el Sub Gerente de Gestión de Base de Datos.	Primer Piso Sede San Borja	GTI	SGGBD	SGGBD	8	5	5	6	IMPORTANTE

GESTIÓN DEL RIESGO														
IDENTIFICACIÓN DE ACTIVOS						RESPONSABILIDAD			VALORIZACIÓN DEL ACTIVO				DESCRIPCIÓN
									C	I	D		
CLASIFICACIÓN	N°	NOMBRE DEL ACTIVO	DESCRIPCIÓN	FUNCIÓN	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO DEL ACTIVO	USUARIO DEL ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DEL ACTIVO	
PERSONAS	43	Analista de Base de Datos	Bachiller en Ingeniería de Sistemas, Computación o Informática con conocimientos de Base de Datos Oracle y experiencia laboral mínimo 03 años.	'- Realizar actividades de pase a producción para el soporte de los sistemas informáticos. - Generar información que necesita la Institución. - Monitorear la Bases de Datos Institucional. - Prever, detectar e informar oportunamente incidentes y ocurrencias que alteren la normal operatividad de la Base de Datos Institucional. Proponer mejoras a las normas, políticas, procedimientos y estándares para la administración de la Base de Datos Institucional, así como a los sistemas y recursos informáticos. - Asistir a los desarrolladores con sus conocimientos de SQL y de construcción de procedimientos almacenados y triggers, entre otros. - Realizar las ejecuciones correspondientes para la generación de los padrones electorales. Analizar, verificar y/o actualizar la información relacionada a los procesos electorales. Asesorar en actividades relacionadas, de su competencia, a las demás unidades organizacionales. - Ejecutar otras funciones inherentes al cargo que le asigne el Sub Gerente de Gestión de Base de Datos.	Primer Piso Sede San Borja	GTI	SGGBD	SGGBD	5	5	5	5	IMPORTANTE

GESTIÓN DEL RIESGO														
IDENTIFICACIÓN DE ACTIVOS						RESPONSABILIDAD			VALORIZACIÓN DEL ACTIVO				DESCRIPCIÓN
									C	I	D		
CLASIFICACIÓN	N°	NOMBRE DEL ACTIVO	DESCRIPCIÓN	FUNCIÓN	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO DEL ACTIVO	USUARIO DEL ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DEL ACTIVO	
PERSONAS	44	Operador de Base de Datos	Título Técnico Profesional en Computación o Informática o Egredaso Universitario en Ingeniería de Sistemas o Computación o Informática o Software con conocimientos de Base de Datos Oracle y experiencia laboral mínima de 02 años.	'- Administración, mantenimiento y monitoreo de la Base de Datos Institucional. - Realizar actividades de pase a producción para el soporte de los sistemas informáticos. - Monitorear e implementar controles de seguridad de la Bases de Datos Institucional. - Cumplir con las normas, políticas, procedimientos y estándares para la administración y seguridad de la Base de Datos Institucional, así como los sistemas y recursos. - Asesorar en actividades relacionadas de su competencia, a las demás unidades orgánicas. - Otras que le asigne el Sub Gerente de Gestión de Base de Datos.	Primer Piso Sede San Borja	GTI	SGGBD	SGGBD	5	5	5	5	IMPORTANTE
	45	Asistente de Base de Datos	Personal con Título Técnico Profesional en Computación e Informática o Egresado Universitario en Sistemas, Informática o Computación con conocimientos de Base de Datos y experiencia en instituciones públicas.	'- Asegurar y monitorear que las conexiones de la Base de Datos Institucional estén funcionando permanentemente y de manera correcta. - Resolver en primera instancia o dar aviso sobre problemas de conexión y desconexión de la Base de Datos Institucional. - Cumplir con los requisitos de las normas ISO 9001, en cuanto a políticas, objetivos, documentación, roles y responsabilidades. - Consolidar el comportamiento de la Bases de Datos Institucional. - Otras funciones que le asigne el Sub Gerente de Gestión de Base de Datos en relación a sus competencias técnicas especializadas.	Primer Piso Sede San Borja	GTI	SGGBD	SGGBD	5	5	5	5	IMPORTANTE

GESTIÓN DEL RIESGO														
IDENTIFICACIÓN DE ACTIVOS						RESPONSABILIDAD			VALORIZACIÓN DEL ACTIVO				DESCRIPCIÓN
									C	I	D		
CLASIFICACIÓN	N°	NOMBRE DEL ACTIVO	DESCRIPCIÓN	FUNCIÓN	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO DEL ACTIVO	USUARIO DEL ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DEL ACTIVO	
PERSONAS	46	Soporte Administrativo de Consultas en Línea	Titulo Técnico Profesional o Egresado universitario en Sistemas, Computación o Informática.	'- Atención a los usuarios de servicios de consultas en línea, vía telefónica, correo electrónico y otros medios de comunicación. - Apoyo en las labores operativas en la administración y mantenimiento de los usuarios del Servicio de Consultas al Registro Único de Identificación de Personas Naturales. - Administrar y mantener operativos las cuentas de usuarios del servicio de consultas al RUIPN. - Soporte a los usuarios de Consultas en Línea para el normal uso de los servicios de consultas de acuerdo al nivel de seguridad asignado al usuario. - Soporte a la solución de problemas presentados a los usuarios reportados por correo electrónico o vía teléfono. - Preveer, detectar e informar oportunamente incidentes y ocurrencias que alteren la normal operatividad de las consultas del RUIPN. - Preparar y presentar informes relacionados a las funciones desempeñadas, en forma periódica y/o eventual. - Mantener la confidencialidad de la información a la que tiene acceso.	Primer Piso Sede San Borja	GTI	SGGBD	SGGBD	5	5	5	5	IMPORTANTE

GESTIÓN DEL RIESGO													
IDENTIFICACIÓN DE ACTIVOS						RESPONSABILIDAD			VALORIZACIÓN DEL ACTIVO				DESCRIPCIÓN
									C	I	D		
CLASIFICACIÓN	N°	NOMBRE DEL ACTIVO	DESCRIPCIÓN	FUNCIÓN	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO DEL ACTIVO	USUARIO DEL ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DEL ACTIVO	
PERSONAS	47	Apoyo Administrativo	Personal con Estudios Técnicos profesionales último ciclo o universitarios del tercer año en Derecho o Sociología o Administración o Contabilidad o Computación o Negocios Internacionales y experiencia laboral mínimo de 02 años.	'- Recepción de documentos internos y externos. - Seguimiento de documentación. - Verificación de estado de trámites en el SITD - Recepción y monitoreo de llamadas telefónicas. - Redacción de documentos. - Las demás funciones que se le asignen en el ámbito de su competencia.	Primer Piso Sede San Borja	GTI	SGGBD	SGGBD	5	5	5	5	IMPORTANTE
ENTORNO	48	Sub Gerencia de Gestión de Base Datos	Espacio físico donde se encuentra la Sub Gerencia de Gestión de Base Datos	Albergar y proteger los activos asignados a la SGGBD	Primer Piso Sede San Borja	SGGBD	SGGBD	SGGBD	8	5	10	8	CRITICO
SERVICIOS	49	Servicio de Internet	Servicio que brinda conexión a Internet.	Acceso internet limitado.	Configurado en cada estación autorizado.	SGOT	SGOT, SGGBD	SGGBD	5	5	10	7	IMPORTANTE
	50	Telefonía Móvil	Sistema de comunicación para la transmisión de sonidos a larga distancia que permite hacer y recibir llamadas desde cualquier lugar, siempre que sea dentro del área de cobertura del servicio que lo facilita.	Comunicación vía telefónica entre los colaboradores de la Institución.	De uso personal del colaborador asignado por la Institución	GAD	SGGBD / GAD / SERVICIOS GENERALES	'SGGBD	5	5	10	7	IMPORTANTE

GESTIÓN DEL RIESGO														
IDENTIFICACIÓN DE ACTIVOS						RESPONSABILIDAD			VALORIZACIÓN DEL ACTIVO				DESCRIPCIÓN
									C	I	D		
CLASIFICACIÓN	N°	NOMBRE DEL ACTIVO	DESCRIPCIÓN	FUNCIÓN	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO DEL ACTIVO	USUARIO DEL ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DEL ACTIVO	
SERVICIOS	51	Suministro de energía	Servicio de suministro de energía eléctrica.	Proporcionar energía eléctrica para el funcionamiento de los equipos informáticos.	Sede San Borja, Piso 1	'GAD	GAD/SERVICIOS GENERALES	'SGGBD	5	5	10	7	IMPORTANTE
	52	Servicio Soporte Técnico ORACLE	Servicio de consultas para casuísticas presentadas en la base de datos con motor ORACLE.	Consultar registrar y analizar casuísticas presentadas en los motores de base de datos Oracle.	Web	'SGSTO	'SGSTO, SGGBD	'SGSTO, SGGBD	8	5	10	8	CRITICO
PROCESOS DE NEGOCIO Y SERVICIOS	53	Servicio Soporte Técnico ORACLE	Tecnología que permite integrar en una misma red - basada en protocolo IP - las comunicaciones de voz y datos.	Facilitar las comunicaciones al personal del RENIEC para el desarrollo de sus actividades.	Sede San Borja, Piso 1	'SGOT	'SGOT	'RENIEC	5	5	5	5	IMPORTANTE
	54	Servicio de Videoconferencia	Servicio que permite la comunicación simultánea bidireccional de audio y vídeo, que permite mantener reuniones con grupos de personas situadas en lugares alejados entre sí.	Realizar reuniones y coordinaciones con entidades externas e internas	Sede San Borja, Piso 1	'SGOT	'SGGBD	'SGGBD	5	5	1	4	NO SIGNIFICATIVO
	55	Servicio de VPN (Virtual Private Network)	Extensión de una red privada de la Institución a través del internet. Se establece una conexión virtual punto a punto mediante el uso de conexiones dedicadas, encriptación o una combinación de ambos.	Acceso a los recursos de la red interna desde un equipo fuera de las instalaciones de la Institución.	Servidor de VPN, Sede Operativa	'SGOT	'SGOT	'SGGBD	8	5	10	8	CRITICO

GESTIÓN DEL RIESGO													
IDENTIFICACIÓN DE ACTIVOS						RESPONSABILIDAD			VALORIZACIÓN DEL ACTIVO				DESCRIPCIÓN
									C	I	D		
CLASIFICACIÓN	N°	NOMBRE DEL ACTIVO	DESCRIPCIÓN	FUNCIÓN	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO DEL ACTIVO	USUARIO DEL ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DEL ACTIVO	
PROCESOS DE NEGOCIO Y SERVICIOS	56	Servicio de Mensajería Interna (Microsoft Lync)	Programa que permite la comunicación en tiempo real por medio de mensajes escritos con personal previamente autorizado.	Comunicación entre colaboradores de la institución en tiempo real.	Configurado en cada estación autorizado.	'SGSTO - Mesa de ayuda.	Mesa de Ayuda, SGGBD	'SGGBD	5	1	1	3	NO SIGNIFICATIVO
	57	Servicio de Firma Digital	Es una modalidad de firma electrónica que utiliza una técnica de criptografía asimétrica (basada en el sistema de “parejas de claves”) y garantiza la autoría, la integridad y la aceptación de los documentos electrónicos "suscritos" con ella.	Garantizar la autenticidad de las comunicaciones electrónicas, el contenido de las mismas y la responsabilidad de las personas que las envían	Planta PKI – GRCD	'GRCD	GRCD	'SGGBD	8	5	5	6	IMPORTANTE
	58	Servicio de correo electrónico	Servicio que permite enviar mensajería electrónica para el personal	Remitir correos electrónicos para la atención de requerimientos y/o distribución de información solicitada por el personal de la Institución y/u otros.	Sede Administrativa, Piso 28	'SGOT	SGOT, SGSTO	'SGGBD	5	5	10	7	IMPORTANTE
	59	Soporte de Líneas de Producción	Atender los requerimientos solicitados por la SGIS.	Establecer los lineamientos para la atención de los requerimientos los cuales aseguran la administración y control de los cambios realizados sobre la Base de Datos Institucional.	Sede San Borja, Piso 1	'SGGBD	'SGGBD	'SGIS, SGGBD	5	5	10	7	IMPORTANTE

GESTIÓN DEL RIESGO														
IDENTIFICACIÓN DE ACTIVOS						RESPONSABILIDAD			VALORIZACIÓN DEL ACTIVO				DESCRIPCIÓN
									C	I	D		
CLASIFICACIÓN	N°	NOMBRE DEL ACTIVO	DESCRIPCIÓN	FUNCIÓN	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO DEL ACTIVO	USUARIO DEL ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DEL ACTIVO	
PROCESOS DE NEGOCIO Y SERVICIOS	60	Configuración de Servidores	Atención de los requerimientos solicitado por las UU.OO los cuales son: Pase a Producción, Atención DML/DDL, Atención DCL, Libro Discoverer, Carga de Servidores Biométricos, Backup SIGA, Carga Omisos, Fiscalización Posterior, Actualizar Servidores Master, Clonación de Servidores de Agencias, Revisar Servidores de Agencias.	Establecer los lineamientos para la atención de los requerimientos los cuales aseguran la administración y control de los cambios realizados sobre la Base de Datos Institucional.	Sede San Borja, Piso 1	SGGBD	SGGBD	'AGENCIAS RENIEC	5	5	5	5	IMPORTANTE
	61	Generación de Padrón Electoral	El Padrón Electoral es la relación de ciudadanos hábiles que pueden ejercer su derecho a voto en un determinado proceso electoral.	Generar la información electoral de los ciudadanos hábiles al voto correspondiente a los comisios electorales a celebrarse de acuerdo a lo solicitado por el ente electoral.	Sede San Borja, Piso 1	SGGBD	SGGBD	'RENIEC, ONPE y JNE	10	10	50	9	CRITICO
	62	Generación de Lista de Ciudadanos para JEE	La Lista de Ciudadanos del Jurado Electoral Especial es la relación de 25 candidatos para ser elegido como jurado electoral especial, el cual se encargará de monitorear el proceso electoral vigente.	Generar la relación de las Listas de Ciudadanos candidatos a conformar el Jurado Electoral Especial (JEE)	Sede San Borja, Piso 1	SGGBD	SGGBD	'RENIEC y JNE	10	10	5	9	CRITICO
	63	Generación de Reportes de los Sistemas de Información	La información generada por las diversas UU.OO, consiste en la extracción de la información almacenada en las bases de datos institucionales en base a los filtros y criterios indicados por las UU.OO para su posterior análisis y mejora de sus procesos internos.	Generar la información a demanda según los criterios otorgados por las diversas UU.OO de la institución con el propósito de sacar conclusiones sobre la información obtenida.	Sede San Borja, Piso 1	SGGBD	SGGBD	'RENIEC	5	5	5	5	IMPORTANTE

GESTIÓN DEL RIESGO														
IDENTIFICACIÓN DE ACTIVOS						RESPONSABILIDAD			VALORIZACIÓN DEL ACTIVO				DESCRIPCIÓN
									C	I	D		
CLASIFICACIÓN	N°	NOMBRE DEL ACTIVO	DESCRIPCIÓN	FUNCIÓN	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO DEL ACTIVO	USUARIO DEL ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DEL ACTIVO	
PROCESOS DE NEGOCIO Y SERVICIOS	64	Servicios en Línea Vía Internet	Proceso que permite el acceso a las consultas de los ciudadanos a través de las aplicaciones del RENIEC.	Validar los datos de los ciudadanos para su correcta y completa identificación orientados a las entidades públicas y privadas que tienen un convenio suscrito con el RENIEC.	Sede San Borja, Piso 1	SGGBD	SGGBD	'Entidades externas	8	10	10	10	CRITICO
	65	Registro de Convenio	Proceso donde se registra los convenios suscritos con el RENIEC:	Verificar la información completa y correcta de los formatos, los datos, niveles de acceso de las entidades que van a suscribir un convenio, para el VºBº de la GTI y el registro de convenios.	Sede San Borja, Piso 1	SGGBD	SGGBD	'Oficina de Convenios / SGEN	5	5	5	5	IMPORTANTE
	66	Administración de usuarios	Este proceso permite realizar modificaciones en la Base de Datos de los usuarios, efectuando Altas o Bajas en el sistema.	Llevar el control de las personas que utilizara el servicio y que son autorizadas por los coordinadores o representantes legales de las entidades que han suscrito un convenio con el RENIEC.	Sede San Borja, Piso 1	SGGBD	SGGBD	'SGGBD / CEL	5	5	5	5	IMPORTANTE
	67	Consolidado de Facturación	Procesos donde se consolida la información para la facturación.	Verificar la cantidad de consultas realizadas por las entidades que utilizan el servicio, y el equivalente en soles. Se envía a la Sub Gerencia de Tesorería para la recaudación correspondiente.	Sede San Borja, Piso 1	SGGBD	SGGBD	'Entidades externas	8	10	5	8	CRITICO

GESTIÓN DEL RIESGO														
IDENTIFICACIÓN DE ACTIVOS						RESPONSABILIDAD			VALORIZACIÓN DEL ACTIVO				DESCRIPCIÓN
									C	I	D		
CLASIFICACIÓN	N°	NOMBRE DEL ACTIVO	DESCRIPCIÓN	FUNCIÓN	UBICACIÓN	PROPIETARIO DEL ACTIVO	CUSTODIO DEL ACTIVO	USUARIO DEL ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DEL ACTIVO	
PROCESOS DE NEGOCIO Y SERVICIOS	68	Cotejo Masivo	Validación de DNIs, apellidos y nombres entregado por una entidad pública y/o privada que es comparada con la información que se tiene almacenada en el RUIPN.	Obtener la información validada de los ciudadanos registrados en el Registro Único de Identificación de Personas Naturales (RUIPN)	Sede San Borja, Piso 1	SGGBD	SGGBD	'Entidades Externas	8	5	5	6	IMPORTANTE
	69	Monitoreo de Seguridad de BD	La seguridad en las bases de datos es un mecanismo fundamental con el fin de no exponer la información a cualquier tipo de amenaza que de alguna u otra manera causan perdida de confidencialidad y/o información	Establecer los lineamientos para la seguridad de la información almacenada en las Bases de Datos institucionales.	Sede San Borja, Piso 1	SGGBD	SGGBD	'SGGBD	5	5	5	5	IMPORTANTE
	70	Monitoreo y Administración de Base de Datos	Mejorar el desempeño y rendimiento de las bases de datos institucionales y garantizar la disponibilidad de los servicios.	Mantener la continuidad del negocio	Sede San Borja, Piso 1	AGGBD	SGGBD	'SGGBD	8	5	10	8	CRITICO

1.3.2. EVALUACIÓN DE RIESGOS

Acciones para tratar los riesgos y las oportunidades

El RENIEC, a través de la Oficina de Seguridad y Defensa Nacional, mediante la Directiva DI-372-OSDN/006 "Gestión de Riesgos de Seguridad de la Información" e Instructivo INS-208-OSDN-001 "Gestión de Riesgos de Seguridad de la Información", establece los lineamientos para identificar, analizar, evaluar, y tratar los riesgos de seguridad de la información a los que se encuentra expuesto, hasta obtener un nivel aceptable del riesgo y garantizar la seguridad de la información en las áreas que cuenten o implementen un Sistema de Gestión de Seguridad de la Información.

Valoración del Riesgo de Seguridad de la Información

Las actividades de identificación, análisis, evaluación y tratamiento de riesgos de seguridad de la información se encuentran definidas en la Directiva DI-372-OSDN/006 "Gestión de Riesgos de Seguridad de la Información" e Instructivo INS-208-OSDN-001 "Gestión de Riesgos de Seguridad de la Información" de la Oficina de Seguridad y Defensa Nacional, que establece los criterios contra los cuales se evalúan los riesgos de seguridad de la información, los lineamientos para identificar, analizar, evaluar, y tratar los riesgos de seguridad de la información a los que se encuentran expuestos los productos y servicios que presta la Gerencia de Registro Electoral, hasta obtener un nivel aceptable del riesgo y garantizar la seguridad de la Información en las áreas que cuenten o implementen un Sistema de Gestión de Seguridad de la Información.

El Dueño de Proceso Padrón Electoral, a través de los Gestores Operativos y Gestor Líder de Seguridad de la Información, con el asesoramiento de la Oficina de Seguridad y Defensa Nacional, identifica las amenazas y oportunidades, generando así un "Plan de Tratamiento de Riesgos y Oportunidades de Seguridad de la Información" bajo los criterios de disponibilidad, confidencialidad e integridad de la información. Se mantiene información documentada de este proceso.

Tratamiento del Riesgo de Seguridad de la Información

Los lineamientos para identificar, analizar, evaluar y tratar los riesgos del Sistema de Seguridad de la Información se encuentran definidos en la Directiva DI-372-OSDN/006 “Gestión de Riesgos de Seguridad de la Información” e Instructivo INS-208-OSDN-001 “Gestión de Riesgos de Seguridad de la Información” de la Oficina de Seguridad y Defensa Nacional, para lo cual el Dueño del Proceso, la Sub Gerencia de Verificación de Firmas y Apoyo Técnico Electoral y la Sub Gerencia de Verificación Domiciliaria y Procesamiento, establecen estrategias, responsables y tiempo estimado, para el tratamiento del riesgo, seleccionando los controles e impulsores que sean necesarios hasta obtener un nivel aceptable del riesgo.

Se han establecido controles e impulsores necesarios para el Sistema de Gestión de Seguridad de la Información del proceso Monitoreo y Seguridad de la Base de Datos, los mismos que se encuentran expresados en la Declaración de Aplicabilidad, que incluye la justificación de las inclusiones, ya sea que se implementen o no, así como la justificación de excluir controles del Anexo A de la Norma Técnica Peruana NTP ISO/IEC 27001:2014.

IDENTIFICACIÓN Y ANÁLISIS DEL RIESGO Y OPORTUNIDAD										
N°	VULNERABILIDAD / FORTALEZA	CAUSAS	AMENAZA / OPORTUNIDAD	EFECTO (POSITIVO O NEGATIVO)	ACTIVOS DE INFORMACIÓN RELACIONADOS	CONTROLES / IMPULSOR ACTUALES	EFECTIVIDAD DE CONTROLES / IMPULSORES	CALIFICACIÓN		CÁLCULO DEL NIVEL DE RIESGO
								PROBABILIDAD	IMPACTO	
1	Accesos de consulta a la BD de producción por personal de desarrollo	Tecnológico	Fuga de información	Daño a la imagen de la institución.	Bases de Datos Institucionales	'- Registro de accesos a base de datos de sólo lectura - Restricción de accesos a las tablas críticas y de usuarios	CEPC	2	2	4
2	La información de datos de prueba no se encuentra disociada (enmascarada)	Tecnológico	Fuga de información	Daño a la imagen de la institución.	Bases de Datos Institucionales		NEC	4	4	16
3	Falta de definición de un sitio alterno para continuar con las actividades	Medioambientales	Sismos Fuego	Interrupción de las actividades del personal	Personal	'- Los DBAS Senior tienen asignados privilegios para trabajar remotamente.	CEPC	2	2	4
4	Falta de documento normativo de responsabilidad de entrega del Padrón Electoral	Procesos	Robo de información	Daño a la imagen de la institución.	' - Padrón Electoral	'- Generación de contraseñas en sobre lacrado -Instructivo de entrega de Padrón Electoral	CNE	3	5	15
5	Falta de infraestructura para implementar el ambiente de pruebas de BD y aplicaciones	Tecnológico	Cambios no intencionados en el software o en la información	Problemas operacionales	Bases de Datos Institucionales	'- Ambiente de desarrollo con espacio limitado para creación y modificación de objetos y nuevas funcionalidades de los aplicativos	CNE	2	5	10
6	Falta de infraestructura para implementar el ambiente de pruebas de BD y aplicaciones	Tecnológico	Accesos no autorizados a los datos o software de producción	Problemas operacionales	Bases de Datos Institucionales	'- Registro de accesos a base de datos de sólo lectura - Restricción de accesos a las tablas críticas y de usuarios	CEPC	2	5	10
7	Transferencia inadecuada de los datos del padrón electoral	Procesos	Accesos no autorizados a los datos Divulgación de la información del ciudadano	Daño a la imagen de la institución.	Padrón Electoral	'- Tabla con los datos del Padrón encriptada - Envío de sobre lacrado con la contraseña de acceso a la tabla	CEPCC	2	5	10
8	Ubicación insegura del archivo maestro de las claves de acceso a las BD institucionales	Tecnológico	Robo de información	Indisponibilidad de las Bases de Datos Manipulación de la información de las BD Destrucción o pérdida.	Bases de Datos Institucionales	'- Archivo maestro de las claves de acceso con contraseña	CEPCC	2	5	10

IDENTIFICACIÓN Y ANÁLISIS DEL RIESGO Y OPORTUNIDAD										
N°	VULNERABILIDAD / FORTALEZA	CAUSAS	AMENAZA / OPORTUNIDAD	EFECTO (POSITIVO O NEGATIVO)	ACTIVOS DE INFORMACIÓN RELACIONADOS	CONTROLES / IMPULSOR ACTUALES	EFECTIVIDAD DE CONTROLES / IMPULSORES	CALIFICACIÓN		CÁLCULO DEL NIVEL DE RIESGO
								PROBABILIDAD	IMPACTO	
9	Uso de privilegios de Súper-usuarios	Recursos humanos	Abuso de información privilegiada Operaciones no autorizadas	Daño o perjuicio en la información a la que tiene acceso	Administrador de Base de Datos Senior	' - Activación de la pista de auditoria '-Verificación de los permisos asignados al personal de la SGGBD	CNE	2	5	10
10	El contrato del servicio es básico (en línea, no presencial)	Tecnológico	Indisponibilidad del servicio	No atención a los usuarios por no tener disponibilidad del servicio	Servicio Soporte Técnico ORACLE		NEC	2	5	10
11	Falla de las medidas de seguridad informática	Tecnológico	Hacking en BD	'- Daño a la imagen de la institución. - Pérdida y/o acceso no autorizado de la información.	Bases de Datos Institucionales	'- Procedimiento para el registro de conexiones de los usuarios de la base de datos	CEPC	2	5	10
12	Falta de monitoreo del Equipo que contiene el RUIPN - Ubicación insegura del Equipo	Tecnológico	Robo de equipos	Pérdida de información	Bases de Datos de Agencias	'- El RUIPN se encuentra encriptado - Servicio de Vigilancia Monitoreo de cámaras	CEPC	3	3	9
13	Falta actualización de los estándares de BD	Tecnológico	Fallos en los sistemas informáticos	Desarrollo de software o sistemas inseguros que puedan introducir vulnerabilidades al entorno de la organización	Documentos normativos	'- Revisión periódica de los documentos normativos	CEPC	3	3	9
14	Uso no autorizado del equipo para el copiado cualquier clase de información	Tecnológico	Fuga de información	Pérdida de información	Reproductor grabador de DVD - DVD grabador	'- Ubicación segura solo de acceso al Subgerente, secretaria	CEPC	2	4	8
15	Media rotación del personal	Recursos humanos	Fuga de información (conocimiento)	'- Lentitud en la atención de requerimientos. -Sobrecarga de trabajo	Personal	'-Procedimientos claves documentados - Inducción básica de los procedimientos principales	CEPC	2	4	8
16	Personal no conforme	Recursos humanos	Boicot de la información a la que tiene acceso	Daño o perjuicio en la información a la que tiene acceso	Personal	'- Los DBAS tienen accesos restringidos dependiendo de la naturaleza de su función	CEPC	2	4	8
17	Falta de conciencia al utilizar los accesos privilegiados	Tecnológico	Abuso de información privilegiada	Manipulación de la información de las BD	Personal de la SGGBD	'- Cada colaborador de la SGGBD posee Los privilegios necesarios de acuerdos a sus funciones	CEPC	2	4	8

IDENTIFICACIÓN Y ANÁLISIS DEL RIESGO Y OPORTUNIDAD										
N°	VULNERABILIDAD / FORTALEZA	CAUSAS	AMENAZA / OPORTUNIDAD	EFECTO (POSITIVO O NEGATIVO)	ACTIVOS DE INFORMACIÓN RELACIONADOS	CONTROLES / IMPULSOR ACTUALES	EFECTIVIDAD DE CONTROLES / IMPULSORES	CALIFICACIÓN		CÁLCULO DEL NIVEL DE RIESGO
								PROBABILIDAD	IMPACTO	
18	Insuficiencia de licencias de base de datos para el despliegue de nuevos proyectos	Tecnológico	Incumplimiento de plazos o de responsabilidades	Incumplimiento de los nuevos proyectos	Oracle Enterprise Edition / Cluster Enterprise Edition	'- Contrato de adquisición de licencias	CEPC	1	5	5
19	Falta de armario para guardar información o equipos	Infraestructura	Robo de información	Exista una pérdida de la información	Documentos administrativos	'- Armarios para guarda la documentación correspondiente de la SGGBD	CNE	3	2	6
20	Uso no controlado del papel reciclado	Procesos	Fuga de información	Daño a la imagen de la institución.	Documentos administrativos	'- Triturador de papeles	CNE	3	2	6
21	Falta de cámaras de video vigilancia	Infraestructura	Robo de información Robo de equipos	Interrupción de las actividades del personal	Documentos administrativos Equipos tecnológicos		NEC	3	2	6
22	Falta de mantenimiento de los equipos de luces de emergencia	Infraestructura	Sismos Fuego	Incapacidad de acción inmediata ante un incidente	Entorno	'- Mantenimiento periódico de los dispositivos	CNE	3	2	6
23	Falla del sistema de detección de humo	Infraestructura	Fuego	Interrupción del funcionamiento de los equipos	Entorno	'- Mantenimiento periódico de los dispositivos	CEPC	3	2	6
24	Falta de medidas de seguridad durante el traslado del equipo	Tecnológico	Robo de equipos	Pérdida de información	' - Bases de Datos de Agencias - Computadora personal portátil - LAPTOP	'- Orden de salida de control Patrimonial - Las equipos portátiles se conectan a los sistemas mediante usuario y contraseña	CEPC	3	2	6
25	Falta de medidas de seguridad para las estaciones de trabajo de los administradores de BD	Tecnológico	Robo de información / equipos	Interrupción de las actividades de la SGGBD	Estaciones de trabajo - DBAS Senior	'- El acceso a las PC se realiza mediante un usuario y contraseña de dominio de la red - Cada Sede de la Institución cuenta con personal de vigilancia	CEPC	2	3	6

N°	VULNERABILIDAD / FORTALEZA	EVALUACIÓN DEL RIESGO / OPORTUNIDAD			EVALUACIÓN DEL RIESGO RESIDUAL			
		EVALUACIÓN DEL RIESGO	DESCRIPCIÓN DEL RIESGO / OPORTUNIDAD	TIPO DE RIESGO / OPORTUNIDAD	CALIFICACIÓN		CÁLCULO DEL NIVEL DE RIESGO RESIDUAL	EVALUACIÓN DEL RIESGO RESIDUAL
					PROBABILIDAD	IMPACTO		
1	Accesos de consulta a la BD de producción por personal de desarrollo	TOLERADO	Riesgo TOLERADO que pueda ocurrir fuga de información debido a los accesos de consulta a la BD de producción por personal de desarrollo, produciendo que daño a la imagen de la institución.	Riesgo de Imagen	2	2	4	TOLERADO
2	La información de datos de prueba no se encuentra disociada (enmascarada)	IMPORTANTE	Riesgo IMPORTANTE que pueda ocurrir fuga de información debido a la información de datos de prueba no se encuentra disociada (enmascarada), produciendo daño a la imagen institución.	Riesgo de Imagen	1	1	2	NO SIGNIFICATIVO
3	Falta de definición de un sitio alterno para continuar con las actividades	TOLERADO	Riesgo TOLERADO de que pueda ocurrir sismos Fuego debido a la falta de definición de un sitio alterno para continuar con las actividades, produciendo interrupción de las actividades del personal	Riesgo Operativo	2	2	4	TOLERADO
4	Falta de documento normativo de responsabilidad de entrega del Padrón Electoral	IMPORTANTE	Riesgo IMPORTANTE que pueda ocurrir robo de información debido a la falta de documento normativo de responsabilidad de entrega del Padrón Electoral, produciendo daño a la imagen de la institución.	Riesgo de Imagen	1	1	1	NO SIGNIFICATIVO
5	Falta de infraestructura para implementar el ambiente de pruebas de BD y aplicaciones	MODERADO	Riesgo MODERADO que pueda ocurrir cambios no intencionados en el software o en la información debido a la falta de infraestructura para implementar el ambiente de pruebas de la BD y aplicaciones, produciendo problemas operacionales.	Riesgo Operativo	2	5	10	MODERADO
6	Falta de infraestructura para implementar el ambiente de pruebas de BD y aplicaciones	MODERADO	Riesgo MODERADO que pueda ocurrir accesos no autorizados a los datos o software de producción debido a la falta de infraestructura para implementar el ambiente de pruebas de la BD y aplicaciones	Riesgo Operativo	2	5	10	MODERADO
7	Transferencia inadecuada de los datos del padrón electoral	MODERADO	Riesgo MODERADO que pueda ocurrir accesos no autorizados a los datos divulgación de la información del ciudadano debido a la transferencia inadecuada de los datos del Padrón Electoral, produciendo daño a la institución.	Riesgo de Imagen	2	5	10	MODERADO

N°	VULNERABILIDAD / FORTALEZA	EVALUACIÓN DEL RIESGO / OPORTUNIDAD			EVALUACIÓN DEL RIESGO RESIDUAL			
		EVALUACION DEL RIESGO	DESCRIPCIÓN DEL RIESGO / OPORTUNIDAD	TIPO DE RIESGO / OPORTUNIDAD	CALIFICACIÓN		CÁLCULO DEL NIVEL DE RIESGO RESIDUAL	EVALUACIÓN DEL RIESGO RESIDUAL
					PROBABILIDAD	IMPACTO		
8	Ubicación insegura del archivo maestro de las claves de acceso a las BD institucionales	MODERADO	Riesgo MODERADO que pueda ocurrir robo de información debido a la ubicación insegura del archivo maestro de las claves de acceso a las BD institucionales, produciendo la indisponibilidad de las BD por manipulación de la información las BD, destrucción o pérdida de las BD.	Riesgo de Operativo	2	5	10	MODERADO
9	Uso de privilegios de Súper-usuarios	MODERADO	Riesgo MODERADO de que pueda ocurrir abuso de información privilegiada a operaciones no autorizadas debido al uso de privilegios de súper-usuarios, produciendo daño o perjuicio a la información a la que se tiene acceso.	Riesgo de Operativo	2	5	10	MODERADO
10	El contrato del servicio es básico (en línea, no presencial)	MODERADO	Riesgo MODERADO que pueda ocurrir indisponibilidad del servicio debido al contrato del servicio es básico (en línea no presencial), produciendo la no atención de los usuarios por no tener disponibilidad del servicio.	Riesgo de Imagen	2	5	10	MODERADO
11	Falla de las medidas de seguridad informática	MODERADO	Riesgo MODERADO que pueda ocurrir HACKING en BD debido a las falta de medida de seguridad informática, produciendo daño a la imagen de la institución.	Riesgo de Imagen	2	5	10	MODERADO
12	Falta de monitoreo del Equipo que contiene el RUIPN - Ubicación insegura del Equipo	MODERADO	Riesgo MODERADO que pueda ocurrir robo de equipos debido a la falta de monitoreo del equipo que contiene el RUIPN, ubicación insegura del equipo, produciendo pérdida de información.	Riesgo Operativo	3	3	9	MODERADO
13	Falta actualización de los estándares de BD	MODERADO	Riesgo MODERADO que pueda ocurrir fallos en los sistemas informáticos debido a la falta de actualización de los estándares de BD, produciendo que el desarrollo de software o sistemas inseguros que puedan introducir vulnerabilidades al entorno de la organización.	Riesgo de Tecnología	3	3	9	MODERADO
14	Uso no autorizado del equipo para el copiado cualquier clase de información	MODERADO	Riesgo MODERADO que pueda ocurrir fuga de información debido al uso no autorizado del equipo para el copiado de cualquier clase de información, produciendo perdida de información	Riesgo de Operativo	2	4	8	MODERADO

N°	VULNERABILIDAD / FORTALEZA	EVALUACIÓN DEL RIESGO / OPORTUNIDAD			EVALUACIÓN DEL RIESGO RESIDUAL			
		EVALUACIÓN DEL RIESGO	DESCRIPCIÓN DEL RIESGO / OPORTUNIDAD	TIPO DE RIESGO / OPORTUNIDAD	CALIFICACIÓN		CÁLCULO DEL NIVEL DE RIESGO RESIDUAL	EVALUACIÓN DEL RIESGO RESIDUAL
					PROBABILIDAD	IMPACTO		
15	Media rotación del personal	MODERADO	Riesgo MODERADO que pueda ocurrir fuga de información (conocimiento) debido a la media rotación del personal, produciendo la lentitud en la atención de requerimientos, sobrecarga de trabajos	Riesgo Operativo	2	4	8	MODERADO
16	Personal no conforme	MODERADO	Riesgo MODERADO de que pueda ocurrir BOICOT de la información a la que se tiene acceso debido al personal no conforme produciendo daño.	Riesgo Operativo	2	4	8	MODERADO
17	Falta de conciencia al utilizar los accesos privilegiados	MODERADO	Riesgo MODERADO de que pueda ocurrir abuso de información privilegiada debido a la falta de conciencia al utilizar los accesos privilegiados, produciendo la manipulación de la información de las BD.	Riesgo Operativo	2	4	8	MODERADO
18	Insuficiencia de licencias de base de datos para el despliegue de nuevos proyectos	MODERADO	Riesgo MODERADO que pueda ocurrir incumplimiento de plazos o de responsabilidades debido a la insuficiencia de licencias de base de datos para el despliegue de nuevos proyectos, produciendo el incumplimiento de los mismos.	Riesgo Operativo	1	5	5	MODERADO
19	Falta de armario para guardar información o equipos	TOLERADO	Riesgo TOLERADO de que pueda ocurrir robo de información debido a la falta de armario para guardar información o equipos, produciendo que exista perdida de la información.	Riesgo Operativo	3	2	6	TOLERADO
20	Uso no controlado del papel reciclado	TOLERADO	Riesgo TOELRADO que pueda ocurrir fuga de información debido al uso no controlado de papel reciclado, produciendo daño a la imagen de la institución.	Riesgo de Imagen	3	2	6	TOLERADO
21	Falta de cámaras de video vigilancia	TOLERADO	Riesgo TOLERADO de que pueda ocurrir robo de información, robo de equipos debido a la falta de cámaras de video vigilancia, produciendo interrupción en las actividades del personal.	Riesgo de	3	2	6	TOLERADO
22	Falta de mantenimiento de los equipos de luces de emergencia	TOLERADO	Riesgo TOLERADO que pueda ocurrir sismos, fuego debido a la falta de mantenimiento de los equipos de luces de emergencias.	Riesgo Operativo	3	2	6	TOLERADO

N°	VULNERABILIDAD / FORTALEZA	EVALUACIÓN DEL RIESGO / OPORTUNIDAD			EVALUACIÓN DEL RIESGO RESIDUAL			
		EVALUACIÓN DEL RIESGO	DESCRIPCIÓN DEL RIESGO / OPORTUNIDAD	TIPO DE RIESGO / OPORTUNIDAD	CALIFICACIÓN		CÁLCULO DEL NIVEL DE RIESGO RESIDUAL	EVALUACIÓN DEL RIESGO RESIDUAL
					PROBABILIDAD	IMPACTO		
22	Falta de mantenimiento de los equipos de luces de emergencia	TOLERADO	Riesgo TOLERADO que pueda ocurrir sismos, fuego debido a la falta de mantenimiento de los equipos de luces de emergencias, produciendo la incapacidad de acción inmediata ante un incidente.	Riesgo Operativo	3	2	6	TOLERADO
23	Falla del sistema de detección de humo	TOLERADO	Riesgo TOLERADO que pueda ocurrir fuego debido a la falla del sistema de detección de humo, produciendo la interrupción del funcionamiento de los equipos.	Riesgo Operativo	3	2	6	TOLERADO
24	Falta de medidas de seguridad durante el traslado del equipo	TOLERADO	Riesgo TOLERADO de que pueda ocurrir robo de equipos debido a la falta de medidas de seguridad durante el traslado del equipo, produciendo la perdida de información.	Riesgo Operativo	3	2	6	TOLERADO
25	Falta de medidas de seguridad para las estaciones de trabajo de los administradores de BD	TOLERADO	Riesgo TOLERADO que pueda ocurrir robo de información/equipos debido a la falta de medidas de seguridad para las estaciones de trabajo de los administradores de BD, produciendo la interrupción de las actividades en la SGGBD.	Riesgo Operativo	2	3	6	TOLERADO

1.4. COMPROBAR (CHECK)

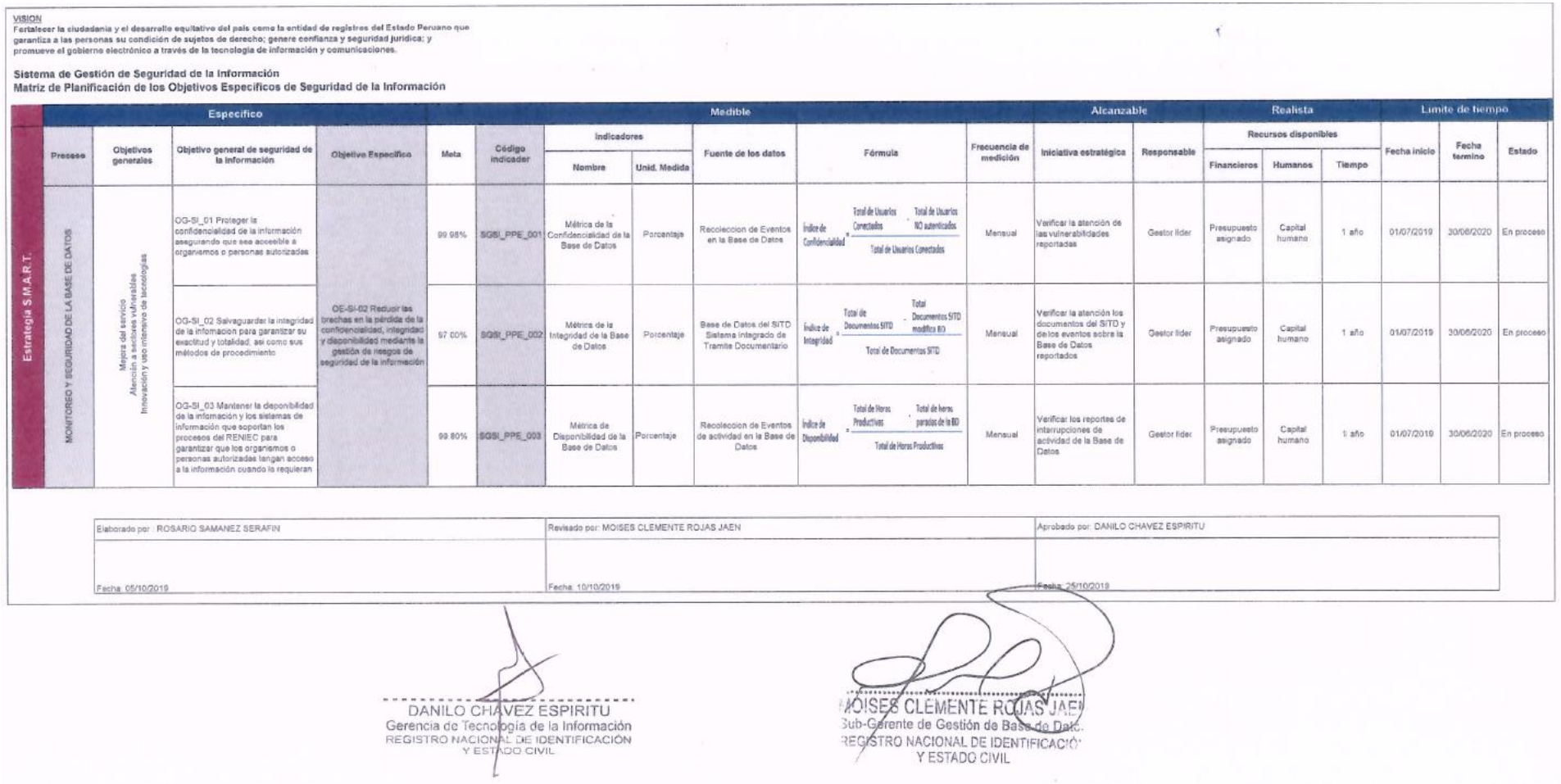
1.4.1. MONITOREO DE LOS PROCESOS DE LA IMPLANTACIÓN DE LA NTP ISO/IEC 27001:2014

Dominio	Objetivo del Control	Evidencia del Cumplimiento	Ubicación	Quien va a medir	Que se va a medir	Resultados
4 CONTEXTO DE LA ORGANIZACIÓN	4.1 Comprender la organización y su contexto	Informe Técnico de Implantación ISO 27001	File Server	Gestores de Seguridad	Cumplimiento con los Requisitos de la ISO 27001	100%
	4.2 Comprender las necesidades y expectativas de las partes interesadas	Identificación de las Partes Interesadas			Cumplimiento con los Requisitos de la ISO 27001	100%
	4.3 Determinar el alcance del sistema de gestión de seguridad de la información	Informe Técnico de Implantación ISO 27001			Cumplimiento con los Requisitos de la ISO 27001	100%
	4.4 Sistema de gestión de la seguridad de la información	Lista Maestra de Documentos			Cumplimiento con los Requisitos de la ISO 27001	100%
5. LIDERAZGO	5.1 Liderazgo y Compromiso	Política de Seguridad de Información			Cumplimiento de Objetivos Control A.5.1.1 y A.5.1.2	100%
		Informe Técnico de Implantación ISO 27001				100%
		Plan de Capacitación				100%
		Manual de Organización y Funciones				100%
	5.2 Política	Política de Seguridad de la Información			Cumplimiento de Objetivos Control A.5.1.1 y A.5.1.2	100%
	5.3 Roles organizacionales, responsabilidades y autoridades	MAN.GER.001 Manual de Organización y Funciones del SGSI			Validar que considere todas las áreas del alcance	100%

Dominio	Objetivo del Control	Evidencia del Cumplimiento	Ubicación	Quien va a medir	Que se va a medir	Resultados
4 CONTEXTO DE LA ORGANIZACIÓN	6.1 Acciones para abordar los riesgos y las oportunidades	Objetivos de la Implantación de la NTP ISO/IEC 27001	File Server	Gestores de Seguridad	Validar el Avance del Cronograma de los Riesgos y Oportunidades de las áreas del alcance	100%
	6.1.1 General	Informe Técnico de Implantación ISO 27001				100%
		Gestión de Riesgos y Oportunidades				100%
	6.1.2 Evaluación de Riesgo de la Seguridad de la Información	Informe Técnico de Implantación ISO 27001			Análisis y Evaluación de riesgos y oportunidades de las áreas del alcance	100%
	6.1.3 Tratamiento de Riesgos de la seguridad de la Información	Informe Técnico de Implantación ISO 27001			Riesgos aceptados formalmente	100%
	6.2 Objetivos de la Seguridad de la Información	Objetivos de la Implantación de la NTP ISO/IEC 27001			Objetivos alineados a la política de seguridad y a los objetivos estratégicos	100%
7. APOYO	7.1 Recursos	Comité de SGSI				100%
	7.2 Competencias	Manual de Organización y Funciones			Ejecución de Comités del SGSI	100%

	Objetivo del Control	Evidencia del Cumplimiento	Ubicación	Quien va a medir	Que se va a medir	Resultados
8. OPERACIÓN	8.1 Control y planificación operacional	Medición de los Controles de la Implantación	File Server	Gestores de Seguridad	Cumplimiento	100%
	8.2 Evaluación de riesgo de la seguridad de la información	Gestión de Cambios			Cronograma y registro de Evaluación de riesgos	100%
	8.3 Tratamiento de riesgo de la seguridad de la información	Plan de Tratamiento de Riesgos			Cronograma y registro de Evaluación de riesgos	100%
9. EVALUACIÓN DEL DESEMPEÑO	9.1 Monitoreo, medición, análisis y evaluación	Medición de los Controles de la Implantación			Revisión del Monitoreo del SGSI	100%
	9.2 Auditoría Interna	Auditoría Interna			Ejecución de Auditorías internas en las áreas del alcance	100%
	9.3 Revisión de gestión	Informe de los Gestores de Seguridad			Validar que se traten todos los puntos indicados en la Norma	100%
10. MEJORA	10.1 No Conformidades y acciones correctivas	Acciones Correctivas y Preventivas			Avance del tratamiento de No Conformidades	100%
	10.2 Mejora continua	Informe de los Gestores de Seguridad			Implementación de proyectos de mejora	100%

1.4.2. MONITOREO DE LOS CONTROLES



VISION

Fortalecer la ciudadanía y el desarrollo equitativo del país como la entidad de registros del Estado Peruano que garantiza a las personas su condición de sujetos de derecho; genere confianza y seguridad jurídica; y promueve el gobierno electrónico a través de la tecnología de información y comunicaciones.

Sistema de Gestión de Seguridad de la Información

Matriz de Planificación de los Objetivos Específicos de Seguridad de la Información

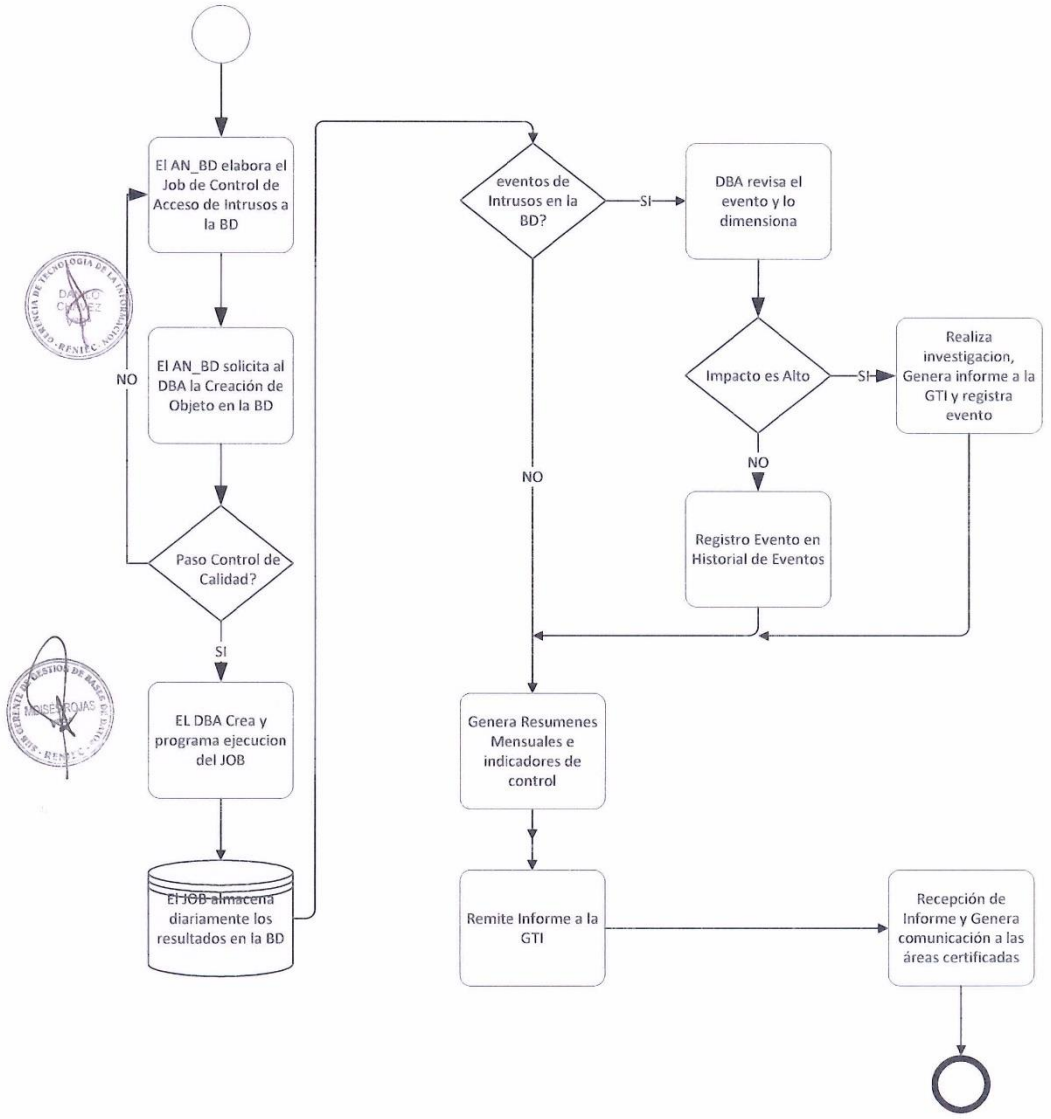
	Específico				Medible							Alcanzable		Realista			Límite de tiempo		
	Proceso	Objetivos generales	Objetivo general de seguridad de la información	Objetivo Específico	Meta	Código indicador	Indicadores		Fuente de los datos	Fórmula	Frecuencia de medición	Iniciativa estratégica	Responsable	Recursos disponibles			Fecha inicio	Fecha termino	Estado
							Nombre	Unid. Medida						Financieros	Humanos	Tiempo			
Estrategia S.M.A.R.T.	MONITOREO Y SEGURIDAD DE LA BASE DE DATOS	Mejora del servicio Atención a servicios vulnerables Innovación y uso intensivo de tecnologías	OG-SI_01 Proteger la confidencialidad de la información asegurando que sea accesible a organismos o personas autorizadas	OE-SI-02 Reducir las brechas en la pérdida de la confidencialidad, integridad y disponibilidad mediante la gestión de riesgos de seguridad de la información	99.98%	SGSI_PPE_001	Métrica de la Confidencialidad de la Base de Datos	Porcentaje	Recoleccion de Eventos en la Base de Datos	Índice de Confidencialidad = (Total de Usuarios Conectados − Total de Usuarios NO autenticados) / Total de Usuarios Conectados	Mensual	Verificar la atención de las vulnerabilidades reportadas	Gestor líder	Presupuesto asignado	Capital humano	1 año	01/07/2019	30/06/2020	En proceso
			OG-SI_02 Salvaguardar la integridad de la infomacion para garantizar su exactitud y totalidad, así como sus métodos de procedimiento		97.00%	SGSI_PPE_002	Métrica de la Integridad de la Base de Datos	Porcentaje	Base de Datos del SITD Sistema integrado de Tramite Documentario	Índice de Integridad = (Total de Documentos SITD − Total Documentos SITD modifica BD) / Total de Documentos SITD	Mensual	Verificar la atención los documentos del SITD y de los eventos sobre la Base de Datos reportados	Gestor líder	Presupuesto asignado	Capital humano	1 año	01/07/2019	30/06/2020	En proceso
			OG-SI_03 Mantener la deponibilidad de la información y los sistemas de información que soportan los procesos del RENIEC para garantizar que los organismos o personas autorizadas tengan acceso a la información cuando lo requieran		99.80%	SGSI_PPE_003	Métrica de Disponibilidad de la Base de Datos	Porcentaje	Recoleccion de Eventos de actividad en la Base de Datos	Índice de Disponibilidad = (Total de Horas Productivas − Total de horas paradas de la BD) / Total de Horas Productivas	Mensual	Verificar los reportes de interrupciones de actividad de la Base de Datos	Gestor líder	Presupuesto asignado	Capital humano	1 año	01/07/2019	30/06/2020	En proceso

Elaborado por : ROSARIO SAMANEZ SERAFIN	Revisado por: MOISES CLEMENTE ROJAS JAEN	Aprobado por: DANILO CHAVEZ ESPIRITU
Fecha: 05/10/2019	Fecha: 10/10/2019	Fecha: 25/10/2019

DANILO CHAVEZ ESPIRITU
Gerencia de Tecnología de la Información
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

MOISES CLEMENTE ROJAS JAEN
Sub-Gerente de Gestión de Base de Datos
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

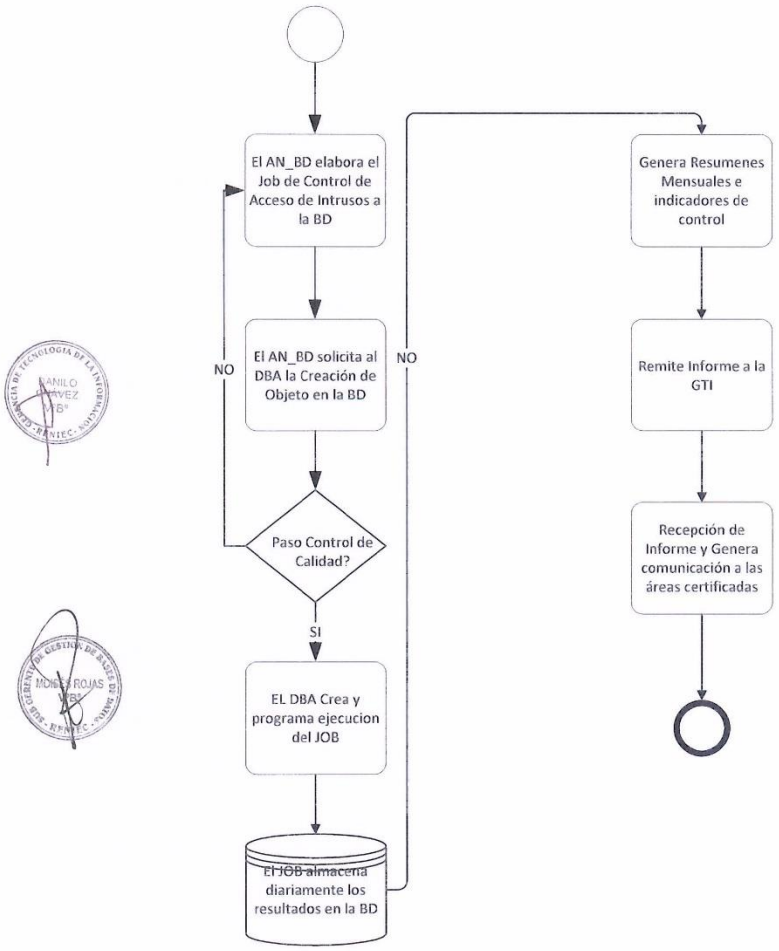
FLUJO DEL PROCESO DE LA ELABORACION Y GENERACION DE LA INFORMACION PARA EL INDICADOR DE CONFIDENCIALIDAD DE LA BASE DE DATOS



PARTICIPANTES	FECHA DE APROBACIÓN
Elaborado : MOISES CLEMENTE ROJAS JAEN	12/09/2019
Revisado : ROSARIO SAMANEZ SERAFIN	13/09/2019
APROBADO : DANILO CHAVEZ ESPIRITU	15/09/2019

AN_BD Analista de Base de Datos
BD Base de Datos
DBA Administrador de Base de Datos
JOB Proceso programado que se ejecuta en batch
SGSTO Sub Gerencia de Soporte Técnico Operativo
SGOT Sub Gerencia de Operaciones Telemáticas

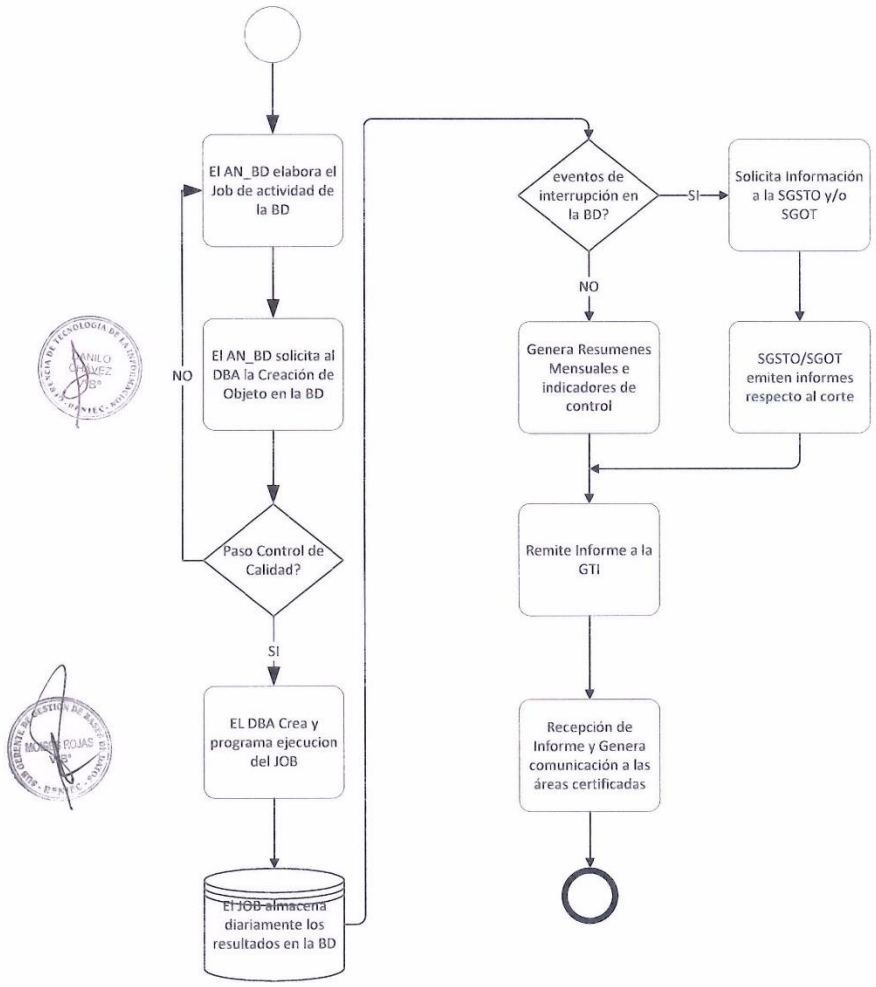
FLUJO DEL PROCESO DE LA ELABORACION Y GENERACION DE LA INFORMACION PARA EL INDICADOR DE INTEGRIDAD DE LA BASE DE DATOS



PARTICIPANTES	FECHA DE APROBACIÓN
Elaborado : MOISES CLEMENTE ROJAS JAEN	12/09/2019
Revisado : ROSARIO SAMANEZ SERAFIN	13/09/2019
APROBADO : DANILO CHAVEZ ESPIRITU	15/09/2019

AN_BD Analista de Base de Datos
BD Base de Datos
DBA Administrador de Base de Datos
JOB Proceso programado que se ejecuta en batch
SGSTO Sub Gerencia de Soporte Técnico Operativo
SGOT Sub Gerencia de Operaciones Telemáticas

FLUJO DEL PROCESO DE LA ELABORACION Y GENERACION DE LA INFORMACION PARA EL INDICADOR DE DISPONIBILIDAD DE LA BASE DE DATOS



PARTICIPANTES	FECHA DE APROBACIÓN
Elaborado : MOISES CLEMENTE ROJAS JAEN	12/09/2019
Revisado : ROSARIO SAMANEZ SERAFIN	13/09/2019
APROBADO : DANILO CHAVEZ ESPIRITU	15/09/2019

AN_BD Analista de Base de Datos
BD Base de Datos
DBA Administrador de Base de Datos
JOB Proceso programado que se ejecuta en batch
SGSTO Sub Gerencia de Soporte Técnico Operativo
SGOT Sub Gerencia de Operaciones Telemáticas

1.4.3. COMPETENCIAS

Recursos

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implantación, mantenimiento y mejora continua del sistema de gestión de Seguridad de la Información.

Competencias

La organización debe:

Determinar las competencias necesarias de las personas que trabajan bajo su control que afecta su desempeño en seguridad de la información.

Asegurar que estas personas son competentes sobre la base de la educación, capacitación, o experiencias adecuados.

Cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la efectividad de las acciones tomadas.

Retener información documentada apropiada como evidencia de competencia.

REQUISITOS DE COMPETENCIAS PARA LOS ROLES DE LOS SISTEMAS DE GESTIÓN

Objetivo	Determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta al desempeño de los Sistemas de Gestión de Seguridad de la Información
Alcance	Personal con vínculo laboral con RENIEC y que se encuentre laborando en el proceso de **Administración de la Base de Datos**

Versión	1.0
Fecha de Aprobación del documento	18/12/2019

N°	TIPO DE SISTEMA	ROL	CONOCIMIENTOS OBLIGATORIOS PARA EL ROL	COMPETENCIAS SERVIR	COMPETENCIA 1	COMPETENCIA 2	EXPERIENCIA EN EL ROL (AÑOS)	CONOCIMIENTOS PARA LA MEJORA DEL ROL
1	***SGSI/SGC***	*Responsable del proceso (Sub Gerente)*	*1. Conocimientos de las normativas vigentes de la entidad*	*CT1. Orientación a los Resultados. CT2. Trabajo en Equipo. CT3. Vocación de Servicio*	***Liderazgo***	***Capacidad de Análisis***	***[4-5]***	*Conocimiento sobre Cyberseguridad*
2	***Sistema de Gestión de Calidad***	*Gestor Operativo*	*1. Interpretación y Formación de Auditor Interno en la Norma ISO 27001:2014. 2. Conocimiento en lenguaje SQL 3. Conocimientos en base de datos Oracle 4. Conocimiento de Sistema Operativo UNIX*	*CT1. Orientación a los Resultados. CT2. Trabajo en Equipo. CT3. Vocación de Servicio*	***Liderazgo***	***Capacidad de Análisis***	***[1-3]***	*Conocimiento sobre Cyberseguridad*
3	***Sistema de Gestión de Seguridad de la Información***	*DBA Senior*	*1. Interpretación de la norma ISO 27001 2. Conocimiento en lenguaje SQL 3. Conocimientos en motor de base de datos Oracle 4. Conocimiento de Sistema Operativo UNIX*	*CT1. Orientación a los Resultados. CT2. Trabajo en Equipo. CT3. Vocación de Servicio*	***Capacidad de Análisis***	***Discrecionalidad y Ética***	***[1-3]***	*Conocimiento sobre Cyberseguridad*

ELABORADO POR: Eliana Irene Zapata Quiñones	REVISADO POR: Carolina Armas Vela	APROBADO POR: Moisés Clemente Rojas Jaén
Rol: Gestor Operativo de Seguridad de la Información	Rol: Gestor Líder SGSI	Rol: Responsable del Proceso de Administración de Base de Datos
Fecha: 18/12/2019	Fecha: 18/12/2019	Fecha: 18/12/2019

REQUISITOS DE COMPETENCIAS PARA LOS ROLES DE LOS SISTEMAS DE GESTIÓN

Objetivo	Determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta al desempeño de los Sistemas de Gestión de Seguridad de la Información
Alcance	Personal con vínculo laboral con RENIEC y que se encuentre laborando en el proceso de **Soporte y Control de los Objetos de Base de Datos**

Versión	1.0
Fecha de Aprobación del documento	18/12/2019

N°	TIPO DE SISTEMA	ROL	CONOCIMIENTOS OBLIGATORIOS PARA EL ROL	COMPETENCIAS SERVIR	COMPETENCIA 1	COMPETENCIA 2	EXPERIENCIA EN EL ROL (AÑOS)	CONOCIMIENTOS PARA LA MEJORA DEL ROL
1	SGSI/SGC	Responsable del proceso (Sub Gerente)	1. Conocimientos de las normativas vigentes de la entidad	CT1. Orientación a los Resultados. CT2. Trabajo en Equipo. CT3. Vocación de Servicio	Liderazgo	Capacidad de Análisis	[4-5]	Conocimiento sobre Ciberseguridad
2	Sistema de Gestión de Calidad	Gestor Operativo	1. Interpretación y Formación de Auditor Interno en la Norma ISO 27001:2014. 2. Conocimiento en lenguaje SQL 3. Conocimientos en base de datos Oracle 4. Conocimiento de Sistema Operativo UNIX	CT1. Orientación a los Resultados. CT2. Trabajo en Equipo. CT3. Vocación de Servicio	Liderazgo	Capacidad de Análisis	[1-3]	Conocimiento sobre Ciberseguridad
3	Sistema de Gestión de Seguridad de la Información	DBA Senior	1. Interpretación de la norma ISO 27001 2. Conocimiento en lenguaje SQL 3. Conocimientos en motor de base de datos Oracle 4. Conocimiento de Sistema Operativo UNIX	CT1. Orientación a los Resultados. CT2. Trabajo en Equipo. CT3. Vocación de Servicio	Capacidad de Análisis	Discrecionalidad y Ética	[1-3]	Conocimiento sobre Ciberseguridad
4	Sistema de Gestión de Seguridad de la Información	Analista de Base de Datos	1. Conocimiento en lenguaje SQL 2. Conocimientos en motor de base de datos Oracle	CT1. Orientación a los Resultados. CT2. Trabajo en Equipo. CT3. Vocación de Servicio	Capacidad de Análisis	Innovación	[1-3]	
5	Sistema de Gestión de Seguridad de la Información	Operador de Base de datos	1. Conocimiento en lenguaje SQL 2. Conocimientos en motor de base de datos Oracle	CT1. Orientación a los Resultados. CT2. Trabajo en Equipo. CT3. Vocación de Servicio	Capacidad de Análisis	Innovación	[1-3]	
6	Sistema de Gestión de Seguridad de la Información	Asistente administrativo de base de datos	1. Conocimiento sobre elaboración de documentos normativos	CT1. Orientación a los Resultados. CT2. Trabajo en Equipo. CT3. Vocación de Servicio	Capacidad de Análisis	Comunicación	[1-3]	

ELABORADO POR: Eliana Irene Zapata Quiñones	REVISADO POR: Carolina Armas Vela	APROBADO POR: Moisés Clemente Rojas Jaén
Rol: Gestor Operativo de Seguridad de la Información	Rol: Gestor Líder SGSI	Rol: Responsable del Proceso de Soporte y Control de los Objetos de Base de Datos
Fecha: 18/12/2019	Fecha: 18/12/2019	Fecha: 18/12/2019

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

SEGUIMIENTO DE COMPETENCIAS DE LOS ROLES DE LOS SISTEMAS DE GESTIÓN

Objetivo	Determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta al desempeño de los Sistemas de Gestión de Seguridad de la Información
Alcance	Personal con vínculo laboral con RENIEC y que se encuentre laborando en el proceso de **Generación del Padrón Electoral**

						PRE GRADO			POST GRADO		
N°	TIPO DE SISTEMA	ROL	PERSONAL ASIGNADO	DNI	PUESTO	NOMBRE DE LA FORMACIÓN	NIVEL EDUCATIVO	SITUACIÓN ACADÉMICA	FORMACIÓN	GRADO-SITUACIÓN	OTROS ESTUDIOS
1	**Sistema de Gestión de Seguridad de la Información**	Dueño del Proceso	MOISÉS CLEMENTE ROJAS JAÉN		Sub Gerente		**Técnica Superior**	**Titulado**			1.- Interpretación y Formación de Auditor Interno ISO 9001:2015
2	**Sistema de Gestión de Seguridad de la Información**	Gestor Líder	CAROLINA MILENA ARMAS VELA	08160655	DBA Senior	Ingeniería de Sistemas e Informática	**Universitario**	**Titulado**	**Maestría en Administración de Negocios**	-	1. Curso: Interpretación y Formación de Auditor Interno en la Norma ISO 9001:2015 2. Curso: Gestión integral de riesgo
3	**Sistema de Gestión de Seguridad de la Información**	DBA Senior	ROSARIO CLAUDIA SAMANEZ SERAFIN	46338879	DBA Senior	Ingeniería de Sistemas	**Universitario**	**Titulado**	-	-	1. Curso: Interpretación y Formación de Auditor Interno en la Norma ISO 9001:2015 2. Curso: Gestión integral de riesgo
4	**Sistema de Gestión de Seguridad de la Información**	Analista de Base de Datos	ELIANA IRENE ZAPATA QUIÑONES	45470818	Analista de Base de Datos	Ingeniería de Sistemas e Informática	**Universitario**	**Bachiller**	**Maestría en Administración de Negocios**	**Maestría en curso**	1.- Curso: Sistema de Gestión de la Seguridad de la Información 2. Curso: Gestión por proceso y mejora continua
5	**Sistema de Gestión de Seguridad de la Información**	Asistente administrativo de base de datos	TERESA AMAO	10006301	Asistente administrativo de base de datos		**Universitario**	**Titulado**			

Leyenda:
1.- Para el caso del rol Publicador todo el personal cumple con las competencias.
2.- Para el rol de Supervisor de Actividades Electorales, todo el personal cumple con las competencias.
3.- Para el rol de Empadronador Electoral, todo el personal cumple con las competencias.

1.4.4. AUDITORÍA INTERNA

Proceso que permite verificar en forma objetiva el cumplimiento y efectividad de todos los procesos que conforman el sistema de gestión de seguridad de la información.

Los lineamientos para la realización de la auditoría interna son los siguientes;

La auditoría interna podrá ser ejecutada por un auditor y/o equipo auditor externo de acuerdo con los requisitos que establezca la organización y debe contar con los siguientes perfiles:

a) Debe ser liderada por un Líder Auditor y el equipo auditor que deben de ser Auditores Internos certificados en el Sistema de Gestión que se auditará.

b) Demostrar habilidades y conocimientos suficientes, relacionados con la disciplina y la aplicación de métodos, técnicas, procesos y prácticas específicos del sistema de gestión a examinar, permitiéndole generar hallazgos y conclusiones apropiados. (Lo cual se evidenciará a través de certificados de cursos especializados correspondientes al Sistema de Gestión que será Auditado).

c) Tener experiencia del auditor en auditorías internas de procesos (evidencia en horas).

Toda la información generada en el proceso deberá almacenarse en el repositorio correspondiente

Los hallazgos que figuran en los informes deben cumplir con losiguiente:

a) Deben redactarse de tal forma que sean entendidos fácilmente por el auditado y que posteriormente el área responsable del tratamiento pueda analizar y plantear soluciones acertadas al problema.

b) Las notas deben de ser: objetivas, claras, concretas, concisas, precisas y útiles para el auditado.

c) Deben de contar con la evidencia objetiva específica según sea el caso (código y nombre de documento, ubicación, fecha, etc.)

d) Los informes finales deberán enviarse al área como máximo 7 días después de finalizada la auditoria.

e) La Gerencia o Área responsable auditada debe asegurarse de que se establece el tratamiento para los hallazgos, es decir: se designa un responsable, se realizan las correcciones y se establecen las acciones correctivas necesarias para eliminar las no conformidades y sus causas.

JUAN HERNÁN GUTIERREZ CALDERÓN
Gerente de Calidad e Innovación
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: GUTIERREZ CALDERON Juan Hernan FAU 20295613620 soft
Motivo: Soy el autor del documento
Fecha: 07/11/2019 14:50:15-0500

"DECENIO DE LA IGUALDAD DE OPORTUNIDADES PARA MUJERES Y HOMBRES"
"AÑO DE LA LUCHA CONTRA LA CORRUPCION Y LA IMPUNIDAD"

Lima, 07 de Noviembre del 2019

MEMORANDO MULTIPLE N° 000104-2019/GCI/RENIEC

A :

ROA QUINTANA MIGUEL ANGEL
Gerente de Registro Electoral(e)

TINOCO REYNOSO JUAN PABLO
Gerente de Talento Humano(e)

GUIBOVICH ARTEAGA OTTO NAPOLEON
Jefe de Oficina de Seguridad y Defensa Nacional

PEREZ DUHARTE JOSE ALFREDO
Escuela Registral

CHAVEZ ESPIRITU DANILO ALBERTO
Gerente de Tecnología de la Información

PALOMINO CASANOVA GILBERTO ARMANDO
Gerente de Administración

HERRERA COMBE MARIO EDUARDO
Gerente de Operaciones Registrales(e)

PUCH PARDO FIGUEROA JORGE ANTONIO
Gerente de Registros Civiles

SARAVIA BONIFACIO CELIA ANTONIA
Gerente de Registros de Identificación

De : **JUAN HERNAN GUTIERREZ CALDERON**
Gerente de Calidad e Innovación

Asunto : DIFUSIÓN DEL PLAN DE AUDITORIA INTERNA AL SGSI_PROCESO DEL SERVICIO ELECTORAL - ISO 27001

Referencia : INFORME Nº 000127-2019/GCI/SGC/RENIEC (07NOV2019)

Me dirijo a sus despachos para saludarlos cordialmente y remitirles adjunto al presente, el INFORME Nº 000127-2019/GCI/SGC/RENIEC de la Sub Gerencia de Calidad que hago mio, en relacion a la Difusion del Plan de Auditoria Interna del Sistema de Gestion de Seguridad de la Informacion (SGSI) del Proceso de Gestión del Servicio Electoral, bajo la norma ISO 27001, a realizarse los días 13, 14 y 15 de noviembre del presente.

Sin otro particular, es propicia la oportunidad para expresarle los sentimientos de mi especial consideración y estima personal.

DANILO ALBERTO CHAVEZ ESPÍRITU
Gerente de Tecnología de la Información
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: CHAVEZ ESPIRITU Danilo Alberto FAU 20295613820 soft
Motivo: Soy el autor del documento
Fecha: 07/11/2019 17:15:05-0500

Fecha : 07/11/2019
Hora : 17:14:53

GERENCIA DE TECNOLOGIA DE LA INFORMACION

PROVEIDO N° 007402-2019/GTI/RENIEC

DIA	MES	AÑO
07	11	2019

REGISTRO : **10709**

ASUNTO : DIFUSIÓN DEL PLAN DE AUDITORIA INTERNA AL SGSI_PROCESO DEL SERVICIO ELECTORAL - ISO 27001

Atender en 1 días

REFERENCIA : MEMORANDO MULTIPLE N° 000104-2019/ DIFUSIÓN DEL PLAN DE AUDITORIA INTERNA AL SGSI_PROCESO DEL SERVICIO ELECTORAL - ISO 27001

DEPENDENCIA DESTINO	TRAMITE	PRIORIDAD	INDICACIONES
SUB GERENCIA DE INGENIERIA DE SOFTWARE	GESTION CORRESPONDIENTE	NORMAL	PARTICIPAR DE AUDITORIA, DE ACUERDO AL CRONOGRAMA ADJUNTO.
SUB GERENCIA DE SOPORTE TECNICO OPERATIVO	GESTION CORRESPONDIENTE	NORMAL	PARTICIPAR DE AUDITORIA, DE ACUERDO AL CRONOGRAMA ADJUNTO.
SUB GERENCIA DE GESTION DE BASE DE DATOS	GESTION CORRESPONDIENTE	NORMAL	PARTICIPAR DE AUDITORIA, DE ACUERDO AL CRONOGRAMA ADJUNTO.
SUB GERENCIA DE OPERACIONES TELEMATICAS	GESTION CORRESPONDIENTE	NORMAL	PARTICIPAR DE AUDITORIA, DE ACUERDO AL CRONOGRAMA ADJUNTO.
SUB GERENCIA DE GESTION DE SERVICIOS DE INFORMACION	GESTION CORRESPONDIENTE	NORMAL	PARTICIPAR DE AUDITORIA, DE ACUERDO AL CRONOGRAMA ADJUNTO.
GTI/ESPECIALISTAS - MONROY MIRANDA ARIEL LUDWING	GESTION CORRESPONDIENTE	NORMAL	PARTICIPAR DE AUDITORIA, DE ACUERDO AL CRONOGRAMA ADJUNTO.
GTI/REQUERIMIENTO INFORMATICO	CONOCIMIENTO	NORMAL	

DANILO ALBERTO CHAVEZ ESPIRITU
GERENTE

ANEXO N°01

TABLA DE CONTROLES AUDITADOS - ISO 27001

CONTROLES – NORMA ISO 27001		AUDITADO (si / no)	ESTADO (conforme / con hallazgo)
A.5 Políticas de seguridad			
A.5.1 Directrices de gestión de la seguridad de la información			
A.5.1.1	Políticas para la seguridad de la información	SI	
A.5.1.2	Revisión de las políticas de seguridad de la información	SI	
A.6 Organización de la seguridad de la información			
A.6.1 Organización interna			
A.6.1.1	Roles y responsabilidades en seguridad de la información	SI	
A.6.1.2	Segregación de tareas	SI	
A.6.1.3	Contacto con las autoridades	SI	
A.6.1.4	Contacto con grupos de interés especial	SI	
A.6.1.5	Seguridad de la información en la gestión de proyectos	SI	
A.6.2 Los dispositivos móviles y el teletrabajo			
A.6.2.1	Política de dispositivos móviles	SI	
A.6.2.2	Teletrabajo	NO	
A.7 Seguridad relativa a los recursos humanos			
A.7.1 Antes del empleo			
A.7.1.1	Investigación de antecedentes	SI	
A.7.1.2	Términos y condiciones del empleo	SI	
A.7.2 Durante el empleo			
A.7.2.1	Responsabilidades de gestión	SI	
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	SI	
A.7.2.3	Proceso disciplinario	SI	
A.7.3 Finalización del empleo o cambio en el puesto de trabajo			
A.7.3.1	Responsabilidades ante la finalización o cambio	SI	
A.8 Gestión de activos			
A.8.1 Responsabilidad sobre los activos			
A.8.1.1	Inventario de activos	SI	
A.8.1.2	Propiedad de los activos	SI	
A.8.1.3	Uso aceptable de los activos	SI	
A.8.1.4	Devolución de activos	SI	
A.8.2 Clasificación de la información			
A.8.2.1	Clasificación de la información	SI	
A.8.2.2	Etiquetado de la información	SI	
A.8.2.3	Manipulado de la información	SI	
A.8.3 Manipulación de los soportes			
A.8.3.1	Gestión de soportes extraíbles	SI	
A.8.3.2	Eliminación de soportes	SI	
A.8.3.3	Soportes físicos en tránsito	SI	
A.9 Control de acceso			
A.9.1 Requisitos de negocio para el control de acceso			
A.9.1.1	Política de control de acceso	SI	
A.9.1.2	Acceso a las redes y a los servicios de red	SI	
A.9.2 Gestión de acceso de usuario			
A.9.2.1	Registro y baja de usuario	SI	
A.9.2.2	Provisión de acceso de los usuarios	SI	
A.9.2.3	Gestión de privilegios de acceso	SI	
A.9.2.4	Gestión de la información secreta de autentificación de los usuarios	SI	
A.9.2.5	Revisión de los derechos de acceso de usuario	SI	
A.9.2.6	Retirada o reajuste de los derechos de acceso	SI	
A.9.3 Responsabilidades del usuario			
A.9.3.1	Uso de la información secreta de autenticación	SI	
A.9.4 Control de acceso a sistemas y aplicaciones			
A.9.4.1	Restricción del acceso a la información	SI	
A.9.4.2	Procedimientos seguros de inicio de sesión	SI	
A.9.4.3	Sistema de gestión de contraseñas	SI	
A.9.4.4	Uso de utilidades con privilegios del sistema	SI	
A.9.4.5	Control de acceso al código fuente de los programas	SI	

CONTROLES – NORMA ISO 27001		AUDITADO (si / no)	ESTADO (conforme / con hallazgo)
A.10 Criptografía			
A.10.1 Controles criptográficos			
A.10.1.1	Política de uso de los controles criptográficos	SI	
A.10.1.2	Gestión de claves	SI	
A.11 Seguridad física y del entorno			
A.11.1 Áreas seguras			
A.11.1.1	Perímetro de seguridad física	SI	
A.11.1.2	Controles físicos de entrada	SI	
A.11.1.3	Seguridad de oficinas, despachos y recursos	SI	
A.11.1.4	Protección contra las amenazas externas y ambientales	SI	
A.11.1.5	El trabajo en áreas seguras	SI	
A.11.1.6	Áreas de carga y descarga	SI	
A.11.2 Seguridad de los equipos			
A.11.2.1	Emplazamiento y protección de equipos	SI	
A.11.2.2	Instalaciones de suministro	SI	
A.11.2.3	Seguridad del cableado	SI	
A.11.2.4	Mantenimiento de los equipos	SI	
A.11.2.5	Retirada de materiales propiedad de la empresa	SI	
A.11.2.6	Seguridad de los equipos fuera de las instalaciones	SI	
A.11.2.7	Reutilización o eliminación de equipos	SI	
A.11.2.8	Equipo de usuario desatendido	SI	
A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia	SI	
A.12 Seguridad de las operaciones			
A.12.1 Procedimientos y responsabilidades de operaciones			
A.12.1.1	Documentación de procedimientos de operación	SI	
A.12.1.2	Gestión de cambios	SI	
A.12.1.3	Gestión de capacidades	SI	
A.12.1.4	Separación de los recursos de desarrollo, prueba y operación	SI	
A.12.2 Protección contra software malicioso			
A.12.2.1	Controles contra el código malicioso	SI	
A.12.3	**Copias de seguridad**		
A.12.3.1	Copias de seguridad de la información	SI	
A.12.4	**Registros y supervisión**		
A.12.4.1	Registro de eventos	SI	
A.12.4.1	Protección de Información de registros		
A.12.4.3	Registros de administración y operación	SI	
A.12.4.4	Sincronización del reloj	SI	
A.12.5	**Control del software en explotación**		
A.12.5.1	Instalación del software en explotación	SI	
A.12.6	**Gestión de la vulnerabilidad técnica**		
A.12.6.1	Control de las vulnerabilidades técnicas	SI	
A.12.6.2	Restricción en la instalación de software	SI	
A.12.7	**Consideraciones sobre la auditoria de sistemas de información**		
A.12.7.1	Control de auditoría de sistemas de información	SI	
A.13	**Seguridad de las comunicaciones**		
A.13.1	**Gestión de la seguridad de redes**		
A.13.1.1	Controles de red	SI	
A.13.1.2	Seguridad de los servicios de red	SI	
A.13.1.3	Segregación en redes	SI	
A.13.2	**Intercambio de información**		
A.13.2.1	Políticas y procedimientos de intercambio de información	SI	
A.13.2.2	Acuerdos de intercambio	SI	
A.13.2.3	Mensajes electrónicos	SI	
A.13.2.4	Acuerdos de confidencialidad o no divulgación	SI	
A.14.1	**Requisitos de seguridad de los sistemas de información**		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	SI	

	CONTROLES – NORMA ISO 27001	AUDITADO (si / no)	ESTADO (conforme / con hallazgo)
A.14.1.2	Aseguramiento de servicios de aplicaciones sobre redes públicas	SI	
A.14.1.3	Protección de transacciones en servicios de aplicación	SI	
A.14.2	**Seguridad en los procesos de desarrollo y soporte**		
A.14.2.1	Política de desarrollo seguro	NO	
A.14.2.2	Procedimientos de control de cambio del sistema	NO	
A.14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	NO	
A.14.2.4	Restricciones sobre cambios a los paquetes de software.	NO	
A.14.2.5	Principios de ingeniería de sistemas seguros	NO	
A.14.2.6	Ambiente de desarrollo seguro	NO	
A.14.2.7	Desarrollo contratado externamente	NO	
A.14.2.8	Pruebas de seguridad del sistema	NO	
A.14.2.9	Pruebas de aceptación del sistema	NO	
A.14.3	**Datos de prueba**		
A.14.3.1	Protección de datos de prueba	NO	
A.15.1	**Seguridad de la información en las relaciones con los proveedores**		
A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores	SI	
A.15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	SI	
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	SI	
A.15.2	**Gestión de entrega de servicios del proveedor**		
A.15.2.1	Monitoreo y revisión de servicios de los proveedores.	SI	
A.15.2.2	Gestión de cambios a los servicios de proveedores.	SI	
A.16.1	**Gestión de incidentes y mejoras en la seguridad de la información**		
A.16.1.1	Responsabilidades y procedimientos	SI	
A.16.1.2	Reporte de eventos de seguridad de la información	SI	
A.16.1.3	Reporte de debilidades de seguridad de la información	SI	
A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información.	SI	
A.16.1.5	Respuesta a incidentes de seguridad de la información.	SI	
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	SI	
A.16.1.7	Recolección de evidencia	SI	
A.17.1	**Continuidad de seguridad de la información**		
A.17.1.1	Planificación de continuidad de seguridad de la información.	SI	
A.17.1.2	Implementación de continuidad de seguridad de la información.	SI	
A.17.1.3	Verificación, revisión y evaluación de continuidad de seguridad de la información.	SI	
A.17.2	**Redundancias**		
A.17.2.1	Instalaciones de procesamiento de la información.	SI	
A.18.1	**Cumplimiento con requisitos legales y contractuales**		
A.18.1.1	Identificación de la legislación vigente y los requisitos contractuales	SI	
A.18.1.2	Derechos de propiedad intelectual	SI	
A.18.1.3	Protección de registros	SI	
A.18.1.4	Privacidad y protección de datos personales	SI	
A.18.1.5	Regulación de controles criptográficos	SI	
A.18.2	**Revisiones de seguridad de la información**		
A.18.2.1	Revisión independiente de la seguridad de la información.	SI	
A.18.2.2	Cumplimiento de políticas y normas de seguridad.	SI	
A.18.2.3	Revisión del cumplimiento técnico.	SI	

1.5. ACTUAR (ACT)

1.5.1. NO CONFORMIDADES Y ACCIONES CORRECTIVAS

Se han definido los siguientes escenarios como "No Conformidad":

- **Incumplimiento de algún requisito legal y/o contractual:** Situación donde se evidencia un incumplimiento de algún requisito legal o contractual aplicado al servicio o al Sistema de Gestión de Seguridad de la Información.
- **Incumplimiento de las Políticas y/o normas de seguridad:** Situación donde se evidencia un incumplimiento de las políticas, normas, procedimientos, planes, controles, y similares, definidos dentro del Sistema de Gestión de Seguridad de la Información.
- **Incumplimiento de los objetivos de seguridad:** Situación donde se evidencia que los resultados de medición de los objetivos de seguridad no fueron satisfactorios conforme a las metas establecidas.
- **Resultados de auditorías internas / externas:** No conformidades detectadas por el equipo auditor o auditores en la realización de auditorías internos o externas.
- **Resultados de investigación de incidentes:** Situación donde como resultado de la investigación de incidentes se determine no conformidades en los procesos o actividades definidas dentro del Sistema de Gestión de Seguridad de la Información.
- **Resultados de monitoreo y seguimiento:** Situación donde como resultado del monitoreo se evidencie eventos de seguridad de manera sistemática y con potencialidad de vulnerar las políticas de seguridad de la información.
- **Resultados de la revisión por la Dirección:** Situación donde se determina que existe algún incumplimiento de los requisitos del Sistema de Gestión de Seguridad de la Información.
- **Incumplimiento de acciones establecidas en las solicitudes de acciones correctivas:** Situación donde se evidencie incumplimiento en los plazos o acciones no tomadas, sin justificación, que se definieron en las solicitudes

de acciones correctivas / preventivas.

La Sub Gerencia de Gestión de Base de Datos, participo indirectamente como proceso de soporte en la Auditoría Externa realizada por la empresa AENOR al Proceso Misional PADRON ELECTORAL del 09 al 10 de diciembre del 2019, recibiendo a la Sra. Auditora VICA GALICIA CRUZ en la sede de Javier Prado Este 2392 – Área de la Sub Gerencia de Gestión de Base de Datos, el día 2, 10 de diciembre del 2019, tal como se indica en la página 7 del siguiente Plan de Auditoria:

AENOR

PLAN DE VISITA

REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL - RENIEC

Nº SUBEXPEDIENTE	TIPO DE ACTIVIDAD	NORMA DE APLICACIÓN O REGLAMENTO	FECHA
2014/0728/SI/04	Renovación (AREN)	UNE-ISO/IEC 27001:2014	2019-12-09 al 10

AENOR

ANEXO - MATRIZ ACTIVIDADES DE AUDITORÍA

UNE-ISO/IEC 27001:2014

Sistema de Gestión de Seguridad de la Información

DIA	CENTRO	HORA	AUDITOR	PROCESO/ DEPARTAM/ DOCUMENTO/ ACTIVIDAD	4 CONTEXTO DE LA ORGANIZACION	4.1 Comprensión de la organización y de su contexto	4.2 Comprensión de las necesidades y expectativas de las partes	4.3 Determinación del alcance del sistema de gestión de	4.4 Sistema de gestión de seguridad de la información	5 LIDERAZGO	5.1 Liderazgo y compromiso	5.2 Política	5.3 Roles, responsabilidades y autoridades en la organización	6 PLANIFICACION	6.1 Acciones para tratar los riesgos y oportunidades	6.1.1 Consideraciones Generales	6.1.2 Apreciación de riesgos de seguridad de la información	6.1.3 Tratamiento de los riesgos de seguridad de la información	6.2 Objetivos de seguridad de la información y planificación para	7 SOPORTE	7.1 Recursos	7.2 Competencia	7.3 Concienciación	7.4 Comunicación	7.5 Información Documentada	7.5.1 Consideraciones Generales	7.5.2 Creación y actualización	7.5.3 Control de información documentada	8 OPERACION	8.1 Planificación y Control Operacional	8.2 Apreciación de los riesgos de seguridad de información	8.3 Tratamiento de los riesgos de seguridad de información	9 EVALUACION DEL DESEMPEÑO	9.1 Seguimiento, medición, análisis y evaluación	9.2 Auditoría interna	9.3 Revisión por la Dirección	10 MEJORA	10.1 No conformidad y acciones correctivas	10.2 Mejora Continua
1	1	09:00 – 09:30	PBL/VGC	**REUNION INICIAL**																																		
1	1	09:30 – 10:00	PBL/VGC	**TRASLADO A CENTRO 2**																																		
1	2	10:00 – 10:40	PBL/VGC	Contexto y alcance	X	X	X	X																	X													
1	2	10:40 – 11:30	PBL/VGC	Revisión de hallazgos anteriores	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
1	2	11:30 – 12:30	PBL	Análisis de Riesgos										X	X	X	X								X				X	X	X							
1	2	12:30 – 13:30	PBL	SoA & Plan de Tratamiento										X				X							X				X	X		X						
1	2	11:00 – 13:00	VGC	Revisión de controles																					X				X			X						
1	2	13:00 – 14:30	PBL/VGC	**ALMUERZO**																																		
1	2	14:30 – 15:00	PBL/VGC	**TRASLADO A CENTRO 1**																																		
1	1	15:00 – 16:30	PBL	Competencias																X		X			X													
1	1	16:30 – 18:00	PBL	Auditoria Interna																					X								X			X	X	
1	1	15:00 – 18:00	VGC	Revisión de controles																					X				X			X						

AENOR

ANEXO – MATRIZ ACTIVIDADES DE AUDITORÍA

UNE-ISO/IEC 27001:2014 (GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN) (Continuación)					A.5 Políticas de seguridad de la información	A.6 Organización de la seguridad de la información	A.7 Seguridad relativa a los recursos humanos	A.8 Gestión de activos	A.9 Control de acceso	A.10 Criptografía	A.11 Seguridad física y del entorno	A.12 Seguridad de las operaciones	A.13 Seguridad de las comunicaciones	A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información	A.15 Relación con proveedores	A.16 Gestión de incidentes de seguridad de la información	A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio	A.18 Cumplimiento
DIA	CENTRO	HORA	AUDITOR	PROCESO/ DEPARTAM/ DOCUMENTO/ ACTIVIDAD														
1	2	11:00-11:30	VGC	Políticas de seguridad	X													
1	2	11:30-12:15	VGC	Gestión de activos				X										
1	2	12:15-13:00	VGC	Cumplimiento														X
1	1	15:00-15:45	VGC	Seguridad en comunicaciones									X					
1	1	15:45-16:30	VGC	Seguridad física							X							
1	1	16:30-17:15	VGC	Seguridad en recursos humanos			X											
1	1	17:15-18:00	VGC	Seguridad en operaciones								X						
2	2	09:00-09:30	PBL	Función de seguridad		X												
2	2	09:00-09:30	VGC	Incidentes de seguridad												X		
2	2	09:30-10:00	PBL	Seguridad en continuidad													X	
2	2	09:30-10:00	VGC	Control de acceso					X									

La auditoría realizada por la Auditora Externa fue sobre los siguientes controles:

- A.6 Organización de la Seguridad de la Información
- A.9 Control de Accesos
- A.16 Gestión de Incidentes de Seguridad de Información
- A.17 Aspectos de Seguridad de la Información para la gestión de la continuidad del negocio.

Consecuencia de esta Auditoría Externa, la Empresa AENOR remite el siguiente Informe de Auditoria, por medidas de seguridad y por ser un documento confidencial, se presentará extractos del mismo.

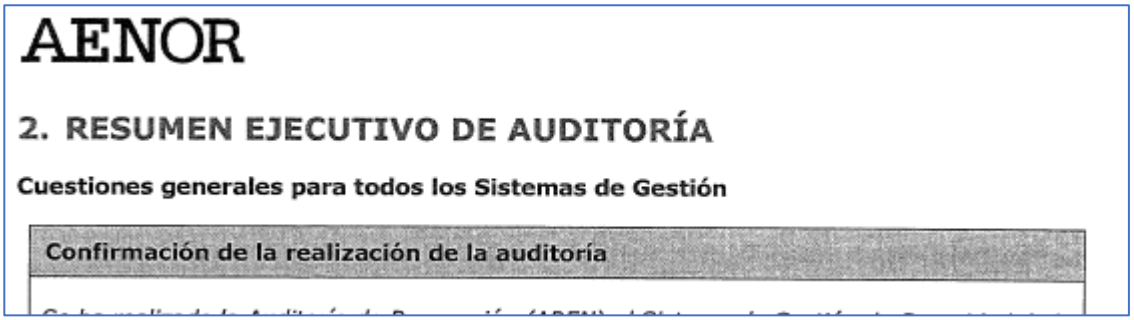
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL – RENIEC

Informe de Auditoría

Nº SUBEXPEDIENTE: **2014/0728/SI/04** NORMA DE APLICACIÓN: **UNE-ISO/IEC 27001:2014**	Nº INFORME: **5** TIPO DE AUDITORÍA: **Renovación** Auditoría: Individual ☒ Combinada ☐ Integrada ☐ Requiere envío de PAC a AENOR INTERNACIONAL S.A.U.: SI ■ NO ☐
Nº SUBEXPEDIENTE: NORMA DE APLICACIÓN:	Nº INFORME: TIPO DE AUDITORÍA: Auditoría: Individual ☐ Combinada ☐ Integrada ☐ Requiere envío de PAC a AENOR INTERNACIONAL S.A.U.: SI ☐ NO ☐
Nº SUBEXPEDIENTE: NORMA DE APLICACIÓN:	Nº INFORME: TIPO DE AUDITORÍA: Auditoría: Individual ☐ Combinada ☐ Integrada ☐ Requiere envío de PAC a AENOR INTERNACIONAL S.A.U.: SI ☐ NO ☐

Fecha de realización de la Auditoría: 2019-12-09 y 10

En la sección de:



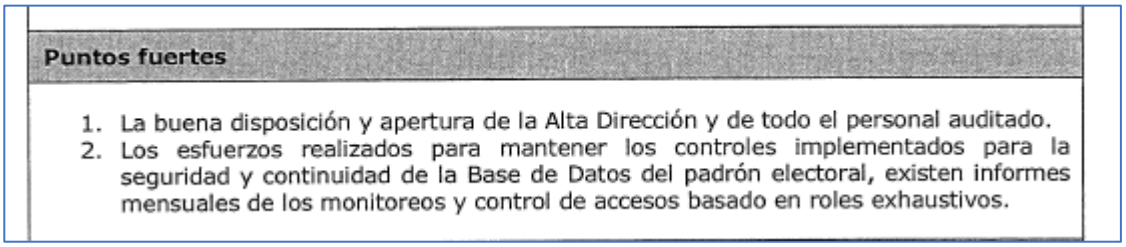
AENOR

2. RESUMEN EJECUTIVO DE AUDITORÍA

Cuestiones generales para todos los Sistemas de Gestión

Confirmación de la realización de la auditoría

Se puede evidenciar que informe de auditoría indica:



Puntos fuertes
1. La buena disposición y apertura de la Alta Dirección y de todo el personal auditado. 2. Los esfuerzos realizados para mantener los controles implementados para la seguridad y continuidad de la Base de Datos del padrón electoral, existen informes mensuales de los monitoreos y control de accesos basado en roles exhaustivos.

La revisión de los controles y los registros y evidencias presentadas en la auditoria, determinan la implantación de la ISO 27001, la cual está preparada para una posterior solicitud de certificación de la Sub Gerencia de Gestión de Base de Datos bajo la ISO/IEC 27001:2014.

ANEXO G: CONSTANCIAS DE AUTORIZACIÓN Y ACTA DE IMPLEMENTACIÓN

DANILO ALBERTO CHAVEZ ESPÍRITU
Gerente de Tecnología de la Información
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: CHAVEZ ESPIRITU Danilo Alberto FAU 20295613820 soft
Motivo: Soy el autor del documento
Fecha: 18/07/2019 17:14:09-0500

"DECENIO DE LA IGUALDAD DE OPORTUNIDADES PARA MUJERES Y HOMBRES"
"AÑO DE LA LUCHA CONTRA LA CORRUPCION Y LA IMPUNIDAD"

Lima, 18 de Julio del 2019

CARTA N° 000044-2019/GTI/RENIEC

Sr(a).
UNIVERSIDAD CESAR VALLEJO
Sede Lima Norte – Escuela Académico Profesional de Ingenieria de Sistemas
Presente .-

Asunto : **CONSTANCIA DE AUTORIZACIÓN**

Referencia : **CARTA N° 000001-2019/GTI/SGGBD/RENIEC**

De nuestra consideración :

Por medio de la presente comunicación y a solicitud de la Sub Gerencia de Gestión de Base de Datos – SGGBD, citada en la referencia, el suscrito, emite constancia que el colaborador MOISES CLEMENTE ROJAS JAEN, identificado con DNI N° 10712325, Sub Gerente de Gestión de Base de Datos de la Gerencia de Tecnología de la Información, se le autoriza el planeamiento y desarrollo del proyecto de Investigación "**SEGURIDAD EN LOS DATOS E IMPLANTANCION DE LA NTP-ISO/IEC 27001:2014 EN LA SUBGERENCIA DE GESTION DE BASE DE DATOS DEL RENIEC**", en dicha Sub Gerencia.

En ese sentido, se informa lo pertinente, para su conocimiento.

Atentamente,

DANILO CHAVEZ ESPIRITU
Gerencia de Tecnología de la Información
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

(DCE/ggo)

DANILO ALBERTO CHAVEZ ESPÍRITU
Gerente de Tecnología de la Información
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: CHAVEZ ESPIRITU Danilo Alberto FAU 20295613620 soft
Motivo: Soy el autor del documento
Fecha: 18/07/2019 17:18:03-0500

"DECENIO DE LA IGUALDAD DE OPORTUNIDADES PARA MUJERES Y HOMBRES"
"AÑO DE LA LUCHA CONTRA LA CORRUPCION Y LA IMPUNIDAD"

Lima, 18 de Julio del 2019

MEMORANDO N° 001413-2019/GTI/RENIEC

A : **ROJAS JAEN MOISES CLEMENTE**
Sub Gerente de Gestión de Base de Datos

De : **DANILO ALBERTO CHAVEZ ESPIRITU**
Gerente de Tecnología de la Información

Asunto : **AUTORIZACIÓN PARA EL PLANEAMIENTO Y DESARROLLO DE PROYECTO DE INVESTIGACIÓN EN LA SUB GERENCIA DE GESTIÓN DE BASE DE DATOS DE LA GTI.**

Referencia : **CARTA Nº 000001-2019/GTI/SGGBD/RENIEC (17JUL2019)**

Es grato dirigirme a Usted, expresándole mi cordial saludo y a la vez referirme acerca del asunto del documento de la referencia, e indicarle que se le autoriza el planeamiento y desarrollo del proyecto de investigación "**SEGURIDAD EN LOS DATOS E IMPLANTANCION DE LA NTP-ISO/IEC 27001:2014 EN LA SUBGERENCIA DE GESTION DE BASE DE DATOS DEL RENIEC**", la cual deberá de ser informada cada fin de mes sobre los avances y los resultados respectivos de dicho proyecto.

Atentamente,

DANILO CHAVEZ ESPIRITU
Gerencia de Tecnología de la Información
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

(DCE/ggo)

DANILO ALBERTO CHAVEZ ESPÍRITU
Gerente de Tecnología de la Información
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: CHAVEZ ESPIRITU Danilo Alberto FAU 20295613620 soft
Motivo: Soy el autor del documento
Fecha: 19/12/2019 11:26:32-0500

"DECENIO DE LA IGUALDAD DE OPORTUNIDADES PARA MUJERES Y HOMBRES"
"AÑO DE LA LUCHA CONTRA LA CORRUPCION Y LA IMPUNIDAD"

Lima, 19 de Diciembre del 2019

MEMORANDO N° 002639-2019/GTI/RENIEC

A : **ROJAS JAEN MOISES CLEMENTE**
Sub Gerente de Gestión de Base de Datos

De : **DANILO ALBERTO CHAVEZ ESPIRITU**
Gerente de Tecnología de la Información

Asunto : **PRESENTACION DEL INFORME TECNICO DEL TERMINO DEL DESARROLLO DE PROYECTO DE INVESTIGACION EN LA SUB GERENCIA DE GESTION DE BASE DE DATOS**

Referencia : **INFORME Nº 000979-2019/GTI/SGGBD/RENIEC (19DIC2019)**

Es grato dirigirme a Usted, expresándole mi cordial saludo y a la vez referirme acerca del asunto indicado en el rubro y en relación al documento de la referencia, en el cual remite el INFORME TECNICO de implantación y culminación del proyecto de investigación "**Seguridad en los Datos e Implantación de la NTP-ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de Datos del RENIEC".**

Vistos y revisados los documentos y sustentos remitidos, se firma y remite el Acta de Implantación producto del proyecto de investigación *"Seguridad en los Datos e Implantación de la NTP-ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de Datos del RENIEC"* y así mismo al confirmar que se ha implantado los controles respectivos de la ISO/IEC 27001:2014, se le autoriza a continuar con los procedimientos y requerimientos necesarios para la certificación de la UNE-ISO/IEC 27001:2014 en los procesos de la Sub Gerencia de Gestión de Base de Datos.

Es propicia la oportunidad para expresarle los sentimientos de mi especial consideración y estima personal.

Atentamente,

DANILO CHAVEZ ESPIRITU
Gerencia de Tecnología de la Información
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

(DCE/ggo)

Lima, 19 de Diciembre de 2019

ACTA DE IMPLANTACION

"Seguridad en los Datos e Implantación de la NTP-ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de Datos del RENIEC"

Mediante la presente acta, se confirma y respalda, que se ha recibido y verificado documentalmente la culminación del proyecto de investigación "**Seguridad en los Datos e Implantación de la NTP-ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de Datos del RENIEC"**, confirmando que se ha implantado la **ISO/IEC 27001:2014**, en el proceso de Monitoreo y Seguridad de la Base de Datos a cargo de la Sub Gerencia de Gestión de Base de Datos, con la finalidad de fortalecer las dimensiones de seguridad de la información, CONFIDENCIALIDAD, INTEGRIDAD y DISPONIBILIDAD, alineadas a los planes estratégico y a las políticas y objetivos institucionales de Seguridad de la Información en el RENIEC.

La Gerencia de Tecnología de la Información, recibe el Informe Técnico de implantación, así como también la evidencia de haber sido auditados indirectamente bajo los anexos y controles de la norma NTP-ISO/IEC 27001:2014, al ser parte del proceso Generación del Padrón Electoral, que recibió la renovación de la certificación el 10/12/2019.

DANILO CHAVEZ ESPIRITU
Gerencia de Tecnología de la Información
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

Mgtr. Danilo Chavez Espiritu
Gerente de Tecnología de la Información

ROSARIO SAMANEZ SERAFIN
Sub Gerencia de Gestión de Base de Datos (e)
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

Ing. Rosario Samanez Serafin
Gestor Líder – DBA Senior ORACLE

MOISES CLEMENTE ROJAS JAEN
Sub-Gerente de Gestión de Base de Datos
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

Moises Clemente Rojas Jaén
Investigador

ANEXO H: GESTIÓN DE EVENTOS RELACIONADOS CON LA INFORMACIÓN EN LA BASE DE DATOS DEL RENIEC

"DECENIO DE LA IGUALDAD DE OPORTUNIDADES PARA MUJERES Y HOMBRES"
"AÑO DE LA LUCHA CONTRA LA CORRUPCION Y LA IMPUNIDAD"

RESOLUCION SECRETARIAL Nº 143 -2019/SGEN/RENIEC

Lima, 19 DIC. 2019

VISTOS:

El Memorando N° 0002369-2019/GTI/RENIEC (22NOV2019) de la Gerencia de Tecnología de la Información, el Informe N° 000792-2019/GTI/SGGBD/RENIEC (14NOV2019) de la Sub Gerencia de Gestión de Base de Datos de la Gerencia de Tecnología de la Información, el Memorando N° 004476-2019/GPP/RENIEC (26NOV2019) de la Gerencia de Planificación y Presupuesto, el Informe N° 000337-2019/GPP/SGRM/RENIEC (26NOV2019) de la Sub Gerencia de Racionalización y Modernización, el Informe Nº 002109-2019/GAJ/SGAJA/RENIEC (03DIC2019) de la Sub Gerencia de Asesoría Jurídica Administrativa de la Gerencia de Asesoría Jurídica y la Hoja de Elevación Nº 000692-2019/GAJ/RENIEC (03DIC2019), de la Gerencia de Asesoría Jurídica; y,

CONSIDERANDO:

Que el Registro Nacional de Identificación y Estado Civil es un organismo constitucionalmente autónomo, encargado de manera exclusiva y excluyente, de las funciones de organizar y actualizar el Registro Único de Identificación de las Personas Naturales, inscribir los hechos y actos relativos a su capacidad y estado civil, asimismo, de emitir los documentos que acreditan la identidad de las personas; para tal fin, desarrollará técnicas y procedimientos automatizados que permitan un manejo integrado y eficaz de la información;

Que la Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, tiene como finalidad la obtención de mayores niveles de eficiencia del aparato estatal, de manera que se logre una mejor atención a la ciudadanía, priorizando y optimizando el uso de los recursos públicos;

Que la Ley N° 28716, Ley de Control Interno de las entidades del Estado, tiene el propósito de cautelar y fortalecer los sistemas administrativos con acciones y actividades de control previo, simultáneo y posterior; en concordancia con la Resolución de Contraloría N° 320-2006-CG, que aprueba las Normas de Control Interno con el objetivo principal de propiciar el fortalecimiento de los sistemas de control interno y mejorar la gestión pública; y, la Resolución de Contraloría N° 0146-2019-CG, que aprueba la Directiva N° 006-2019-CG/INTEG sobre "Implementación del Sistema de Control Interno en las Entidades del Estado", como precepto regulador del procedimiento para implementar el Sistema de Control Interno en las entidades del Estado, así como las normas que dicten los órganos rectores de los sistemas administrativos;

Que los diversos órganos y unidades orgánicas del RENIEC, en su constante compromiso de mejoramiento, vienen revisando su normativa, a efectos de solicitar la aprobación de nuevos documentos normativos o en otros casos, éstos se dejen sin efecto, con la finalidad de mejorar u optimizar las labores de cada una de ellos;

Que en ese sentido, la Gerencia de Tecnología de la Información del RENIEC, propuso el proyecto del documento normativo Directiva DI-442-GTI/006 "Gestión de eventos relacionados con la información en la Base de Datos del RENIEC", Primera

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

Versión, el cual tiene como objetivo establecer los lineamientos para la adecuada gestión de las solicitudes de eventos que están relacionados con la información almacenada en la base de datos institucional, a fin de garantizar su correcta administración, de manera eficaz y eficiente, cumpliendo con los objetivos de seguridad de la información como confidencialidad, integridad y disponibilidad de la información del Registro Nacional de Identificación y Estado Civil – RENIEC;

Que mediante documento de vistos, la Gerencia de Planificación y Presupuesto, sobre la base de lo informado por la Sub Gerencia de Racionalización y Modernización, determinó que el proyecto de documento normativo propuesto se ajusta a los lineamientos dispuestos en la Directiva DI-200-GPP/001 "Lineamientos para la Formulación de los Documentos Normativos del RENIEC", sexta versión, aprobada por Resolución Secretarial N° 55-2017/SGEN/RENIEC (28AGO2017);

Que a través de los documentos de vistos, la Sub Gerencia de Asesoría Jurídica Administrativa de la Gerencia de Asesoría Jurídica, opina que el documento normativo propuesto presenta la consistencia legal pertinente y recomienda su aprobación; y,

Estando a lo opinado por la Gerencia de Asesoría Jurídica y conforme a las facultades delegadas a la Secretaría General del Registro Nacional de Identificación y Estado Civil – RENIEC en mérito a la Resolución Jefatural N° 21-2019-JNAC-RENIEC (12FEB2019) y expresadas en el literal ii) del artículo 26° del Reglamento de Organización y Funciones del RENIEC, aprobado por Resolución Jefatural N° 073-2016-JNAC/RENIEC (01ABR2016) y su modificatoria y a lo dispuesto por la Ley N° 26497, Ley Orgánica del Registro Nacional de Identificación y Estado Civil;

SE RESUELVE:

Artículo Primero.- Aprobar la Directiva DI-442-GTI/006 "Gestión de eventos relacionados con la información en la Base de Datos del RENIEC", Primera Versión, propuesta por la Gerencia de Tecnología de la Información.

Artículo Segundo.- Encargar a la Gerencia de Tecnología de la Información el cumplimiento de lo resuelto en la presente Resolución Secretarial.

Artículo Tercero.- Encargar a la Gerencia de Planificación y Presupuesto la difusión del documento normativo aprobado.

Regístrese, comuníquese y cúmplase.

ABOG. HECTOR MARTIN ROJAS ALIAGA
Secretario General
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

HRA/ltv

RENIEC

RENIEC

DIRECTIVA

GESTIÓN DE EVENTOS RELACIONADOS CON LA INFORMACIÓN EN LA BASE DE DATOS DEL RENIEC

RESOLUCIÓN SECRETARIAL N° 143 -2019/SGEN/RENIEC		
DI-442-GTI/006	VERSIÓN: 01 N° PÁGINAS: 13	FECHA DE APROBACIÓN 19 DIC. 2019

ÍNDICE

I. OBJETIVO

Establecer los lineamientos para la adecuada gestión de las solicitudes de eventos que están relacionados con la información almacenada en la base de datos institucional, a fin de garantizar su correcta administración, de manera eficaz y eficiente, cumpliendo con los objetivos de seguridad de la información como confidencialidad, integridad y disponibilidad de la información del Registro Nacional de Identificación y Estado Civil – RENIEC.

II. ALCANCE

La presente Directiva es administrada por la Gerencia de Tecnología de la Información (GTI), a través de la Sub Gerencia de Gestión de Base de Datos (SGGBD), y es de aplicación por las Líneas de Procesos a cargo de la Gerencia de Registros de Identificación, Gerencia de Registros Civiles y Gerencia de Registro Electoral, y sus unidades orgánicas respectivas.

III. BASE LEGAL

3.1 **Ley Nº 26497**, Ley Orgánica del Registro Nacional de Identificación y Estado Civil, del 12 de julio de 1995 y sus modificatorias.

3.2 **Ley N° 27269**, Ley de Firmas y Certificados Digitales del 28 de mayo de 2000 y sus modificatorias

3.3 **Ley N° 27658,** Ley Marco de Modernización de la Gestión del Estado, del 30 de enero de 2002 y sus modificatorias.

3.4 **Ley Nº 28716,** Ley de Control Interno de las Entidades del Estado, del 18 de abril de 2006, y sus modificatorias.

3.5 **Ley N° 29733**, Protección de Datos Personales, del 03 de julio de 2011, y sus modificatorias.

3.6 **Ley N° 30096**, Ley de Delitos Informáticos, del 22 de octubre de 2013 y sus modificatorias.

3.7 **Decreto Supremo Nº 043-2003-PCM**, aprueba el Texto Único Ordenado de la Ley Nº 27806, Ley de Transparencia y Acceso a la Información Pública, del 24 de abril de 2003 y sus modificatorias.

3.8 **Resolución de Contraloría Nº 320-2006-CG**, aprueban Normas de Control Interno, del 03 de noviembre de 2006.

3.9 **Resolución Ministerial N° 004-2016-PCM,** aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2da. Edición", en todas las Entidades integrantes del Sistema Nacional de Informática, del 14 de Enero de 2016.

3.10 **Resolución Ministerial N° 119-2018-PCM**, que dispone la creación de un Comité de Gobierno Digital en las Entidades de la Administración Pública, del 10 de mayo de 2018.

3.11 **Resolución N° 001-2007/INDECOPI-CTR**, aprueba Normas Técnicas Peruanas, del 22 de enero de 2007.

3.12 **Resolución Jefatural N° 020-2003-JEF/RENIEC**, aprueba el logo del RENIEC, del 01 de febrero de 2003.

3.13 Resolución Jefatural N° 073-2015/JNAC/RENIEC, aprueba la Política de Seguridad de la Información y los Objetivos de Seguridad de la Información del RENIEC, del 30 de Marzo del 2015.

3.14 Resolución Jefatural N° 073-2016/JNAC/RENIEC, aprueba el Reglamento de Organización y Funciones y la Estructura Orgánica del Registro Nacional de Identificación y Estado Civil, del 01 de junio 2016 y su modificatoria.

3.15 Resolución Jefatural N° 069-2017/JNAC/RENIEC, aprueba la reconstitución del Comité de Gestión de Seguridad de la Información del Registro Nacional de Identificación y Estado Civil, del 22 de mayo de 2017.

3.16 Resolución Jefatural N° 021-2019/JNAC/RENIEC, delegan a la Secretaría General la facultad de aprobar documentos normativos, del 12 de febrero de 2019.

3.17 Resolución Jefatural N°107-2019/JNAC/RENIEC, que constituye el Comité de Gobierno Digital del Registro Nacional y Estado Civil, del 22 de julio de 2019.

3.18 Resolución Secretarial N° 055-2017/SGEN/RENIEC, aprueba la Directiva DI-200/GPP/001 "Lineamientos para la Formulación de los Documentos Normativos del RENIEC", del 28 de agosto de 2017 y su modificatoria.

3.19 Resolución Secretarial N° 051-2018/SGEN/RENIEC, aprueba la Directiva DI-423-GTI/005 "Requerimiento de Desarrollo de Software y/o Mantenimiento", del 24 de mayo de 2018.

IV. DEFINICIÓN DE TÉRMINOS

4.1 CA SERVICE DESK

Software de Gestión de Servicios, diseñado para ayudar a los analistas del Service Desk (Mesa de Ayuda) a ofrecer un servicio de atención al usuario cuando exista un requerimiento: solicitud o incidente.

4.2 Dato sensible

Es toda información correspondiente a los datos de identificación de los ciudadanos, tanto en el DNI como de los Hechos Vitales (nacimiento, matrimonio y defunción).

4.3 Dato operativo

Es toda información correspondiente a los datos generados por los sistemas informáticos en las líneas de procesamiento (DNI y Hechos vitales).

4.4 Dependencias

Áreas que dependen directamente de las unidades orgánicas y reportan el cumplimiento de sus funciones.

4.5 Documento Nacional de Identidad - DNI

Es un documento público, personal e intransferible. Constituye la única cédula de identidad personal para todos los actos civiles, comerciales, administrativos, judiciales y en general para todos aquellos casos en que por mandato legal, deba ser presentado. Constituye también el único título de derecho al sufragio de la persona a cuyo favor ha sido otorgado.

4.6 Documentos de sustento

Documentos exigibles que sustenten la modificación o actualización de la información en la Base de Datos, solicitados a través del Anexo N° 01.

4.7 Evento

Ocurrencia o cambio de un conjunto particular de circunstancias. En seguridad de la información está referida a una ocurrencia identificada del estado de un sistema, servicio o red, indicando una posible violación a la política de seguridad de la información, o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad de la información (MGIR-200-GG/OFCR/001).

4.8 Firma digital

Es aquella firma electrónica que cumple con todas las funciones de la firma manuscrita. En particular se trata de aquella firma electrónica basada en la tecnología de criptografía asimétrica. La firma digital permite la identificación del signatario, la integridad del contenido y tiene la misma validez que el uso de una firma manuscrita, siempre y cuando haya sido generada dentro de la Infraestructura Oficial de Firma Electrónica - IOFE. La firma digital está vinculada únicamente al signatario.

4.9 Formato .PDF

Es un formato de almacenamiento para documentos digitales.

4.10 Matriz de casuísticas

Cuadro donde se definen los eventos que conllevan a una enmienda de datos según el tipo de dato, nivel de prioridad y aprobación.

4.11 Matriz master de casuísticas

Es el archivo centralizado de las casuísticas derivadas de los eventos ocurridos en la información tanto sensible u operativa en la SGGBD.

4.12 Norma Técnica Peruana NTP ISO/IEC 27001:2014, Sistemas de gestión de seguridad de la información

El Estado Peruano ha elaborado la Norma Técnica Peruana ISO/IEC 27001, en base a la norma ISO/IEC 27001:2013 de Sistema de Gestión de Seguridad de la Información, para que todos los organismos estatales implanten las políticas y normas necesarias para gestionar la protección de su información, basados en un marco de mejora continua.

4.13 Sistema Integrado de Trámite Documentario - SITD

Sistema informático de alcance institucional a nivel nacional, que permite la gestión del flujo administrativo de la documentación, dependiendo del perfil de acceso que el usuario tiene al sistema (acceso a bandeja personal o total), es decir del grado de autorización delegada, las funciones y responsabilidades en la organización. Toda documentación se encuentra en formato digital, debe conservar la firma digital durante la emisión y lectura del documento.

4.14 Usuarios

Se refiere al personal interno que reporta el cumplimiento de sus funciones a las dependencias del RENIEC; hacen uso de la información del RENIEC con el objeto de poder cumplir con sus funciones correspondientes.

V. RESPONSABILIDADES

5.1. Es responsabilidad del Gerente de la GTI velar por el cumplimiento de la presente Directiva.

5.2. Es responsabilidad del Sub Gerente de la SGGBD supervisar la atención de las solicitudes de eventos relacionados con la información en la Base de Datos, evaluar su aplicación y actualización, estableciendo los controles necesarios que garanticen su integridad en concordancia al sistema de gestión de seguridad de la información dispuesta en la política institucional.

5.3. Es responsabilidad de cada unidad orgánica, remitir las solicitudes de eventos relacionados con la información de la Base de Datos, completando correctamente el formato indicado en el Anexo N° 01, debidamente firmado de manera digital por el funcionario autorizado, y adjuntando los sustentos respectivos, utilizando los medios de comunicación internos (SITD o CA SERVICE DESK) y remitirlos a la SGGBD.

5.4. Es responsabilidad de cada órgano y sus unidades orgánicas y/o Jefaturas Regionales analizar, sustentar, revisar y enviar las solicitudes de eventos, dando la conformidad y aprobación de la ejecución de las acciones que se implementarán a la información de la Base de Datos.

5.5. Es responsabilidad de cada unidad orgánica que utilizará las solicitudes de eventos relacionados a la información de la Base de Datos, respecto a su creación, actualización o desactivación de los ítems de la matriz de casuísticas relacionada a su unidad orgánica, comunicar y remitir en el formato establecido (Anexo N° 02) a la SGGBD para la actualización de la matriz master de casuísticas en la Base de Datos.

5.6. Es responsabilidad de la SGGBD atender las solicitudes de eventos relacionados a la información a la Base de Datos de las distintas dependencias, derivados a través de los medios de comunicación implementados (SITD o CA SERVICE DESK).

5.7. Es responsabilidad de la SGGBD, evaluar, procesar, atender o rechazar las solicitudes de eventos relacionados a la Base de Datos, en los casos que estas tuvieran errores en su creación, faltase firmas de autorización, o no tuvieran una explicación precisa y documentada del evento solicitado.

5.8. Es responsabilidad de la SGGBD remitir un informe mensual a la GTI, con las estadísticas de los eventos atendidos por unidad orgánica, para su gestión y fines correspondientes.

VI. DISPOSICIONES GENERALES

6.1 DE LA GENERACIÓN DE LAS SOLICITUDES DE EVENTOS RELACIONADOS A LA INFORMACIÓN DE LA BASE DE DATOS

6.1.1 Las dependencias de cada órgano y de sus unidades orgánicas y/o Jefaturas Regionales generan las solicitudes de eventos relacionados a la información en la Base de Datos, de acuerdo a sus facultades y funciones establecidas en el ROF institucional, previo análisis, sustento y revisión de las casuísticas relacionadas al evento.

6.1.2 Las solicitudes de eventos relacionados a la información en la Base de Datos, deben completarse correctamente (Anexo N° 01) con los datos requeridos y las firmas digitales correspondientes a la SGGBD.

6.1.3 Es necesario que cada unidad orgánica determine el nivel de prioridad de sus solicitudes.

6.2 DE LAS APROBACIONES Y FIRMAS DIGITALES

6.2.1 Las dependencias que realizan las solicitudes de eventos relacionados a la información de la Base de Datos, deben remitir a su órgano o unidad orgánica correspondiente para su aprobación, de acuerdo a lo determinado en la matriz de casuísticas.

6.2.2 Cada Gerente o Sub Gerente debe firmar digitalmente las solicitudes de eventos relacionados a la información de la Base de Datos, dando la conformidad y aprobación al contenido de la rectificación indicada en el formato de solicitud.

6.3 DE LA ADMINISTRACIÓN DE LA MATRIZ DE CASUÍSTICAS

6.3.1 La SGGBD gestiona y administra la información contenida en la matriz de casuísticas.

6.3.2 La inserción, modificación o desactivación de un registro en la matriz de casuísticas es solicitada por cada unidad orgánica a través del formato de actualización de la matriz de casuísticas con su firma digital correspondiente (Anexo N° 02).

6.3.3 La SGGBD, realiza la actualización de la matriz de casuísticas (Anexo N° 03) y comunica la atención brindada a la unidad orgánica solicitante.

6.4 DEL PROCESAMIENTO DE LAS SOLICITUDES DE EVENTOS RELACIONADOS A LA INFORMACIÓN DE LA BASE DE DATOS

6.4.1 La SGGBD recibe y verifica las solicitudes de eventos relacionados a la información de la Base de Datos, acorde a las facultades y funciones de la unidad orgánica solicitante establecidas en el ROF institucional, así como los requisitos exigibles establecidos en la matriz de casuísticas.

6.4.2. Todas las solicitudes de eventos relacionados a la información de la Base de Datos pasan por una validación interna a nivel de datos y coordinaciones con los analistas de sistemas de la Sub Gerencia de Ingeniería de Software (SGIS).

6.4.3. La SGGBD procesa la solicitud y comunica la atención brindada a la unidad orgánica solicitante.

6.5 DE LA GENERACIÓN DE LOS INFORMES A LAS UNIDADES ORGÁNICAS

6.5.1. La SGGBD genera informes mensuales presentando información consolidada de todas las atenciones a las solicitudes de eventos relacionados con la información de la base de datos.

6.5.2. La información que se consigne en los informes estadísticos debe ser remitida a las unidades orgánicas para que se tomen las medidas correctivas; si están relacionadas a un mantenimiento de software, debe solicitarse a la SGIS según lo dispuesto en la Directiva DI-423-GTI/005 "Requerimiento de Desarrollo de Software y/o Mantenimiento".

6.5.3. La presentación de la información debe ser ordenada, coherente y de fácil utilización e interpretación por parte de los usuarios

VII. DISPOSICIONES ESPECÍFICAS

7.1 DE LA GENERACIÓN DE LAS SOLICITUDES DE EVENTOS RELACIONADOS A LA INFORMACIÓN DE LA BASE DE DATOS

7.1.1. Las solicitudes de eventos relacionados a la información de la Base de Datos, deben ser solicitados a través del SITD o CA SERVICE DESK, adjuntando el Anexo N° 01 en formato PDF, debidamente completado y firmado digitalmente por el Gerente del órgano o el Sub Gerente de la unidad orgánica correspondiente.

7.1.2. Las solicitudes de eventos relacionados a la información en la Base de Datos deben contener los datos del solicitante, la información del evento a modificar relacionado a una o más casuísticas con los sustentos respectivos.

7.1.3. La unidad orgánica debe indicar el nivel de prioridad de atención de sus solicitudes.

7.2 DE LAS APROBACIONES Y FIRMAS DIGITALES

7.2.1 Cuando las solicitudes son de rectificación de datos sensibles, deben ser aprobadas por la Sub Gerencia o Gerencia a través de las firmas digitales.

7.2.2 Cuando las solicitudes son de rectificación de datos operativos, deben ser aprobadas por la Sub Gerencia a través de las firmas digitales.

7.2.3. En el caso de las solicitudes que rectifiquen datos en el RUIPN, en las actas o los datos en los hechos vitales, deben ser aprobadas mediante firma digital del Sub Gerente y/o visto bueno del Gerente del órgano correspondiente.

7.3. DE LA ADMINISTRACIÓN DE LA MATRIZ DE CASUÍSTICAS

7.3.1. La matriz de casuísticas contiene los eventos que están relacionados con la información almacenada en la Base de Datos mediante los sistemas tecnológicos implementados en el RENIEC.

7.3.2. Las solicitudes de actualización de la matriz de casuísticas deben ser realizadas a través del SITD o CA SERVICE DESK, adjuntando el Anexo N° 02 en formato PDF, debidamente completado, y firmado digitalmente por el Gerente del órgano o el Sub Gerente de la unidad orgánica correspondiente.

7.3.3. Las solicitudes de actualización de la matriz de casuísticas deben contener los datos del solicitante y la descripción de la casuística(s) a insertar, modificar o desactivar.

7.3.4. La SGGBD actualiza la matriz de casuísticas (Anexo N° 03) y remite respuesta de atención a la unidad orgánica, adjuntando la solicitud en formato PDF con la firma digital del analista de la SGGBD o del Sub Gerente, a través del SITD o CA SERVICE DESK.

7.4. DEL PROCESAMIENTO DE LAS SOLICITUDES DE EVENTOS RELACIONADOS A LA INFORMACIÓN DE LA BASE DE DATOS

7.4.1. La SGGBD recibe, a través del SITD o CA SERVICE DESK, las solicitudes de eventos relacionados a la información de la Base de Datos.

7.4.2. La SGGBD verifica las solicitudes, conforme a lo establecido en el numeral 5.5 de la presente Directiva, y revisa los controles de la matriz de casuísticas.

7.4.3. Si la solicitud no contiene las firmas digitales de aprobación, no presenta algún control o la validación interna a nivel de datos presenta una inconsistencia, es devuelto a través del SITD o CA SERVICE DESK, para su verificación por la unidad orgánica.

7.4.4. Si la solicitud presenta los controles respectivos y la validación interna a nivel de datos no presenta inconsistencias, se procede con la atención del evento.

7.4.5. La SGGBD remite la respuesta de atención a la unidad orgánica, adjuntando la solicitud en formato PDF con la firma digital del analista de la SGGBD y/o del Sub Gerente, a través del SITD o CA SERVICE DESK.

7.5. DE LA GENERACIÓN DE LOS INFORMES A LAS UNIDADES ORGÁNICAS

7.5.1. La fuente de información para la generación de los informes mensuales son las solicitudes realizadas por las unidades orgánicas.

7.5.2. La información estadística debe ser completa, confiable y oportuna.

7.5.3. La SGGBD, realiza los procedimientos respectivos para la generación de la información estadística.

7.5.4. La SGGBD remite un informe con los reportes estadísticos a la GTI, conforme a lo establecido en el numeral 5.8 de la presente Directiva, para los fines correspondientes.

7.5.5. La GTI debe remitir los cuadros estadísticos a las unidades orgánicas conforme a su competencia funcional, para la evaluación de las medidas correctivas.

7.5.6. Las medidas correctivas que sean determinadas con mantenimiento de software deben ser canalizadas por cada unidad orgánica, debiendo remitir el formato "Requerimiento de Sistema Informático Implementación / Mantenimiento" de la Directiva DI-423-GTI/005, debidamente completado, en coordinación con la SGIS.

VIII. VIGENCIA

Entra en vigencia a partir de su aprobación.

IX. APROBACIÓN

Se aprueba mediante Resolución Secretarial.

X. ANEXOS

ANEXO N° 01

Formato de Solicitud de Eventos Relacionados a la Información de la Base de Datos

FORMATO DE SOLICITUD DE EVENTOS RELACIONADOS A LA INFORMACIÓN EN LA BASE DE DATOS

DEL FORMATO:
CÓDIGO: RE.GE.GE.01
VERSIÓN: 01
EMISIÓN: 00/00/20XX
ACTUAL: 00/00/20XX

Requerimiento Informático: 001-2019/GRO/SGDI/RENIEC

FECHA : 00/00/20XX
N° ACTA.: 001-2019/
N° PAG.: 3

LUGAR:
SEDE: Av. Javier Prado Este N°2382 – San Borja

SOLICITANTE:

Nombres y Apellidos :
DNI :
Cargo :
Unidad Orgánica : Gerencia de Registros Civiles
Area de Procedencia : SGTN - Sub Gerencia Técnica Normativa

IDENTIFICACION DEL EVENTO:

Categoria	☐ Datos sensibles ☐ Datos operativos
Código del Cambio	0001 - ACTUALIZACION DE PRENOMBRE, PRIMER APELLIDO, SEGUNDO APELLIDO DEL TITULAR POR ERROR I 0002 - ACTUALIZACION DE PRENOMBRE, PRIMER APELLIDO, SEGUNDO APELLIDO DEL PADRE POR ERROR D 0003 - ELIMINACION DE ANOTACION MARGINAL POR DUPLICIDAD 0004 - ELIMINACION DE ANOTACION MARGINAL EN ACTA QUE NO CORRESPONDE 0005 - INTEGRAR EL ENLACE NACIMIENTO-MATRIMONIO DE DUPLICADOS 0006 - ACTUALIZAR ESTADO ACTA ARCHIVADA A VIGENTE 0007 - ACTUALIZAR ESTADO ACTA VIGENTE A ARCHIVADA
Descripción	
Motivo	
Nivel de Prioridad	◉ Baja ○ Media ○ Alta

PROCEDIMIENTOS O INSTRUCCIONES A REALIZAR:

Campo	Dice	Debe Decir

Cantidad de registros:

DOCUMENTOS DE SUSTENTO:

ANEXO N° 02

Formato de Actualización de Matriz de Casuísticas

FORMATO DE ACTUALIZACIÓN DE MATRIZ DE CASUÍSTICAS

DEL FORMATO: CÓDIGO: RE.GIE-GIE.13-F VERSION: 01 EMISION: 02/06/2006 ACTUAL: 02/06/2006	Requerimiento Informático: 001-2019/GTI/SGGBD/RENIEC	FECHA : 12/03/2019 N° ACTA : 001-2019/
LUGAR: SGGBD, Av. Javier Prado Este N° 2392 – San Borja	SOLICITANTE: Nombres y Apellidos : DNI : Cargo : Area de Procedencia : (Seleccionar Área de Procedencia) Unidad Orgánica : (Seleccionar Unidad Orgánica)	

ACCIONES:

ITEM	DESCRIPCION DE REQUERIMIENTOS	DATO	Funcionario que los solicita	SUSTENTO	Informe Legal	Informe Tecnico - SGTN	Aprobacion de Gerencia	Aprobacion de la SubGerencia	ACCION
1	ELIMINACION DE ANOTACION MARGINAL POR DUPLICIDAD	S	SGINT	OFICIO DE LA ORDC - (PANTALLA DE AMBAS ANOTACIONES)			X		A
2	ACTUALIZACION DE PRE NOMBRE (INSCRIPCION EXTEMPORANEA MAYOR O MENOR) - JUDICIAL PARA NACIMIENTO	S	SGINT	OFICIO DE ORDC - RESOLUCION JUDICIAL			X	X	M
3	ACTUALIZAR ESTADO ALTA ARCHIVADA A VIGENTE (TEMPORAL PARA GENERAR OP)	O	SGINT						A

ANEXO N° 03

Matriz de Casuísticas

Item	Requerimiento	Tipo de dato	Aprobacion de Gerencia	Aprobacion de la SubGerencia / Jefatura Regional

Ítem: Colocar número correlativo.
Requerimiento: Colocar nombre de la casuística.
Tipo de dato: Colocar el valor "S" si es dato sensible o colocar "O" si es dato operativo.
Aprobación de Gerencia: Colocar "X" si debe tener la firma digital del Gerente de la unidad orgánica.
Aprobación de Sub Gerencia / Jefatura Regional: Colocar "X" si debe tener la firma digital del Sub Gerente de la unidad orgánica o de la Jefatura Regional.

UCV UNIVERSIDAD CÉSAR VALLEJO	ACTA DE APROBACIÓN DE ORIGINALIDAD DE TESIS	Código : F06-PP-PR-02.02 Versión : 10 Fecha : 10-06-2019 Página : 1 de 1

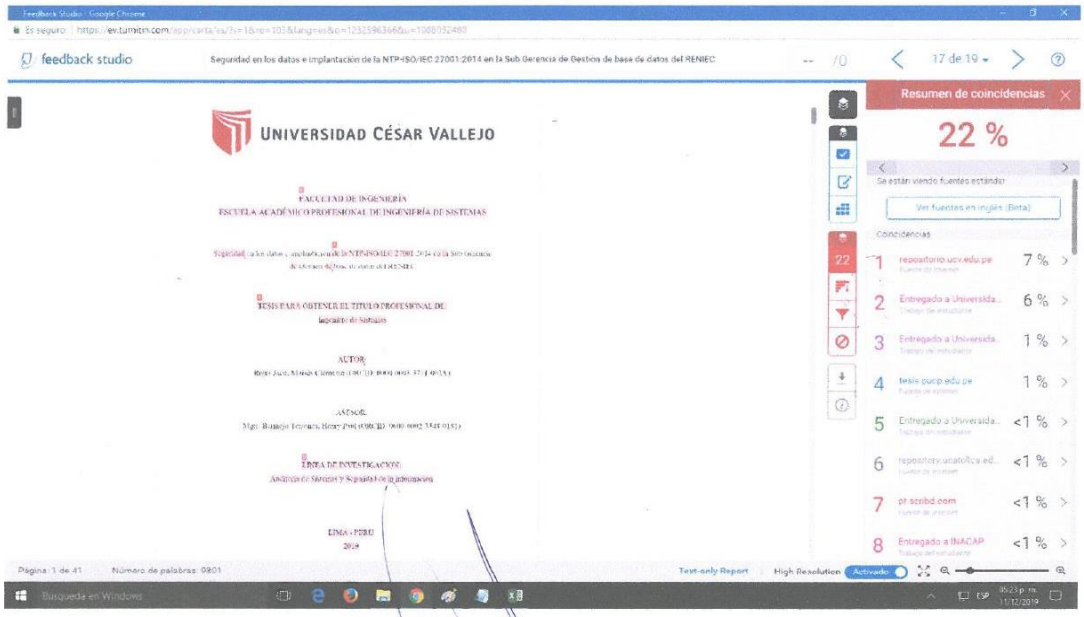
Yo, HENRY PAÚL BERMEJO TERRONES docente de la FACULTAD DE INGENIERÍA y Escuela Profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, revisor(a) de la tesis titulada **"SEGURIDAD EN LOS DATOS E IMPLANTACIÓN DE LA NTP-ISO/IEC 27001:2014 EN LA SUB GERENCIA DE GESTIÓN DE BASE DE DATOS DEL RENIEC"**, del (de la) estudiante MOISES CLEMENTE ROJAS JAEN, constato que la investigación tiene un índice de similitud de 22% verificable en el reporte de originalidad del programa Turnitin.

El/la suscrito (a) analizó dicho reporte y concluyó que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

Lima, 16 de diciembre de 2019

HENRY PAÚL BERMEJO TERRONES
DNI: 18214307

Elaboró	Dirección de investigación	Revisó	Responsable del SGC	Aprobó	Vicerrectorado de Investigación



Henry P. Bermejo Terrones
ING. DE SISTEMAS
R. CIP. 96749

UCV UNIVERSIDAD CÉSAR VALLEJO	AUTORIZACIÓN DE PUBLICACIÓN DE TESIS EN REPOSITORIO INSTITUCIONAL UCV	Código : F08-PP-PR-02.02 Versión : 10 Fecha : 10-06-2019 Página : 1 de 1

Yo ROJAS JAEN MOISES CLEMENTE, identificado con Documento de Identidad N° 10712325 egresado de la Escuela Profesional de INGENIERÍA DE SISTEMAS de la Universidad César Vallejo, autorizo (X), No autorizo ( ) la divulgación y comunicación pública de mi trabajo de investigación titulado **"SEGURIDAD EN LOS DATOS E IMPLANTACIÓN DE LA NTP-ISO/IEC 27001:2014 EN LA SUB GERENCIA DE GESTIÓN DE BASE DE DATOS DEL RENIEC"**; en el Repositorio Institucional de la UCV (http://repositorio.ucv.edu.pe/), según lo estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art. 23 y Art. 33.

Fundamentación en caso de no autorización:

.....

.....

.....

.....

.....

.....

.....

.....

ROJAS JAEN MOISES CLEMENTE
10712325

FECHA: 22 de Diciembre de 2019