Facultad de Ingeniería

Ingeniería de Sistemas e Informática

Programa Especial de Titulación

Implementación de una infraestructura de seguridad tecnológica para controlar el tráfico de red durante el proceso de transmisión de resultados de una entidad pública en la ciudad de Lima - 2021

Raúl Octavio Contreras Capcha

Para optar el Título Profesional de

Ingeniero de Sistemas e Informática

Asesor: Pedro Angel Molina Velarde

Lima – Perú

2021

Dedicatoria

El trabajo se lo dedico a mi familia, a quien le debo, el haber podido tener esta oportunidad, en diferentes sentidos, compresión, apoyo moral y mucha fe en mi persona.

Agradecimiento

Agradezco a mi asesor el Ing. Molina, la perspicacia y la objetividad de evaluar el presente trabajo, asimismo al equipo técnico que dirigí donde como equipo se desarrolló y se implementó el presente proyecto, en distintas etapas.

Resumen

La infraestructura de seguridad tecnológica se mantiene actualmente en toda organización publica o privada, así como de estructurar el proceso de diseño, implementación y operación de un sistema de gestión de seguridad informática, y que estén orientados al establecimiento, implementación, seguimiento, revisión, mantenimiento y mejora de un sistema de seguridad en una entidad pública. Es por ello, que el objetivo de la presente investigación es implementar una infraestructura de seguridad tecnológica con la finalidad de mejorar la seguridad y los activos institucional en una entidad pública. Por lo cual, se empleó el NTP –ISO/IEC 27001:2014, teniendo como resultado la seguridad del proceso de transmisión de datos (resultados) desde las oficinas remotas hacia los centros de datos, así mismo se elaboró el diseño de la infraestructura de seguridad tecnológica para controlar el tráfico de red durante el proceso de transmisión de resultados, alineado a la NTP –ISO/IEC 27001:2014 e implementado una infraestructura de seguridad tecnológica para controlar el tráfico de red durante el proceso de transmisión de resultados.

Palabras clave: Infraestructura, ISO 20071, análisis de riesgos, gestión de la seguridad de la información

Abstract

The technological security infrastructure is currently maintained in every public or private organization, as well as structuring the process of design, implementation and operation of a computer security management system, and that are oriented to the establishment, implementation, monitoring, review, maintenance and improvement of a security system in a public entity. That is why the objective of this research is to implement a technological security infrastructure in order to improve security and institutional assets in a public entity. Therefore, the NTP -ISO / IEC 27001: 2014 was used, resulting in the security of the data transmission process (results) from the remote offices to the data centers, and the design of the infrastructure of technological security to control network traffic during the results transmission process, aligned with the NTP –ISO / IEC 27001: 2014 and implemented a technological security infrastructure to control network traffic during the results transmission process.

Keywords: Infrastructure, ISO 20071, risk analysis, information security management

Tabla de contenido

Índice de Tablas

Índices de Figuras

Introducción

En los últimos años, con el desarrollo de las tecnologías de información y su relación directa con los objetivos de las organizaciones, el universo de amenazas y vulnerabilidades crece, por lo tanto es necesario proteger uno de los activos más importantes de la organización, la información, garantizando siempre la disponibilidad, confidencialidad e integridad de la misma. Debido a que actualmente existen diversos escenarios de amenazas, tales como: la fuga de información o un ataque de ingeniería social, que en cualquier momento pueden manifestarse, con el fin de obtener información confidencial y hacer colapsar a la empresa; es necesario que el negocio cuente con una estrategia de continuidad de negocio, claramente definida por cada escenario de amenaza identificado para así poder reanudar las operaciones rápidamente. La forma más adecuada para proteger los activos de información, es mediante una correcta gestión del riesgo, para así identificar y focalizar esfuerzos hacia aquellos elementos que se encuentran más expuestos. El presente proyecto de titulación reúne la información necesaria para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001:2005, para asegurar la protección de los activos de información y otorgar confianza a los usuarios de una entidad pública. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI.

Capítulo I: Aspectos Generales

1.1 Definición del Problema

1.1.1 Descripcion del problema.

El presente trabajo de investigación, parte de un análisis a la problemática de una entidad estatal del gobierno peruano, la cual tiene que habilitar una cantidad 94 oficinas remotas a nivel nacional para el procesamiento de datos de un evento particular, los cuales generaran información de manera simultánea en todas las oficinas remotas, la información mencionada será generada a través las soluciones de software coyunturales de la institución, sin embargo, no se escapan de los requerimientos de transporte de los datos y la seguridad aplicada a estos, dentro de la unidad de trabajo de la Subgerencia Infraestructura y Seguridad Tecnológica se encarga de brindar facilidades a los requerimientos tecnológicos de las soluciones de software designadas para el procesamiento de los datos durante el evento, por lo que se requiere se implemente una infraestructura de seguridad tecnológica para controlar el tráfico de red, de las oficinas remotas que serán desplegadas, con la finalidad que estas se puedan interconectar con dos centros de datos, al mismo tiempo la disponibilidad, confidencialidad e integridad de las comunicaciones es de suma importancia para la institución, además la implementación debe pasar una evaluación de seguridad informáticas por un servicio contratado y veedores de organismos internacionales.

1.1.2 Formulacion del problema.

1.1.2.1 Problema General.

Actualmente la entidad no cuenta con una infraestructura de seguridad tecnológica para la transmisión de resultados de 94 oficinas remotas hacia los dos centros de datos.

1.1.2.2 Problemas especificos.

Actualmente se recurre a la experiencia del personal con más antigüedad de los eventos similares donde se implementó una cantidad de oficinas de la misma magnitud.

No se cuenta con la documentación de los controles de seguridad informática implementados anteriormente.

La normativa de la institución requiere que la infraestructura de seguridad tecnologica para la transmisión de datos a implementar, deben estar alineados a la NTP –ISO/IEC 27001:2014.

1.2 Definición de Objetivos

1.2.1 Objetivo General

Implementar una infraestructura de seguridad tecnológica para controlar el tráfico de red durante el proceso de transmisión de resultados de una entidad del gobierno peruano.

1.2.2 Obejtivo Especificos

Analizar requerimientos de la operación y de seguridad del proceso de transmisión de datos (resultados) desde las oficinas remotas hacia los centros de datos.

Elaborar el diseño de la infraestructura de seguridad tecnológica para controlar el tráfico de red durante el proceso de transmisión de resultados, alineado a la NTP –ISO/IEC 27001:2014.

Elaborar el plan de implementación de la infraestructura de seguridad tecnológica para controlar el tráfico de red durante el proceso de transmisión de resultados.

1.3 Alcance y limitaciones.

1.3.1 Alcance.

La labor de la investigación tiene como alcance elaborar el diseño e implementación de la infraestructura de seguridad tecnológica para proteger y controlar el tráfico de red de las oficinas remotas hacia los centros de datos de la institución, para el proceso de transmisión de datos, que serán registrados en cada oficina remota de manera simultánea en una fecha preestablecida inamovible.

El diseño de la infraestructura de seguridad tecnológica para proteger y controlar el tráfico de red, estará alineado a la NTP-ISO/IEC 27001, para cumplir con la normativa de la entidad, asimismo transparentar los niveles de disponibilidad, integridad, confidencial de los datos y de la información, también los sistemas que se ejecutan.

1.3.2 Limitaciones.

Para el diseño y la implementación de una infraestructura de seguridad tecnología para el control de tráfico de red para la transmisión de resultados para una institución pública del gobierno peruano, se han determinado las siguientes restricciones.

Se tiene identificado que el personal para las sedes remotas no pueda ser contratados oportunamente, ya que está a cargo de otra unidad orgánica.

Las ubicaciones de las sedes remotas pudrían representar un riesgo por la lejanía de la cobertura de los servicios, representando un incremento en el costo.

Se tiene una restricción de ejecución del plan de implementación, ya que las fechas de los eventos principales no son flexibles.

Riesgo por el tiempo de importación del equipamiento informático a adquirir.

1.4 Justificación.

Este trabajo de investigación recomienda la elaboración de un diseño y un plan de implementación de una infraestructura de seguridad tecnológica para la transmisión de datos. La importancia de utilizar un diseño y un plan de implementación, facilita en entendimiento, facilita la identificación de errores o debilidades, reducción el retrabajo de las áreas involucradas, una estimación más acertada de los recursos necesarios, permite la trazabilidad de las actividades, así como también un punto de base para la mejora continua.

De continuar con la implementación de la infraestructura de red de la forma tradicional, podría abrir brechas de seguridad informática, errores de dimensionamiento o sobredimensionamiento, la trazabilidad podría ser reducida, representando una observación ante lo auditores o veedores internacionales.

Mediante esta propuesta, con el personal de Subgerencia de Infraestructura y Seguridad Tecnológica, se levantará la información de las áreas clave, con la finalidad de establecer los requerimientos, el diseño de la red y los controles adecuados de seguridad informática, alineados a la NTP-ISO/IEC 27001.

1.4.1 Teoría.

La entidad cuenta con el personal calificado para desarrollar el proyecto de diseño e implementación de una infraestructura de seguridad tecnológica para controlar el tráfico de red durante el proceso de transmisión de resultados de una entidad del gobierno peruano.

1.4.2 Practica.

La institución tiene misión el velar por la obtención de la fiel y libre expresión de la voluntad popular de los ciudadanos, organizaciones políticas, instituciones públicas, privadas y de la sociedad civil, en todos los procesos electorales, de referéndum y otros tipos de consulta popular de manera oportuna, transparente con un enfoque intercultural e inclusivo

1.4.3 Metodología

La institución cuenta con recursos internos como equipamiento de computo, seguridad y de comunicaciones, sin embargo, por la envergadura del proyecto es necesarios la contratación de los servicios externos para complementar los recursos adicionales necesarios para su implementación, como por ejemplo enlaces de comunicación, equipamiento de computo, comunicaciones, seguridad adicional y licenciamiento.

Capítulo II: Marco Teórico.

2.1. Fundamento Teórico.

2.1.1. Estado del Arte

A continuación, se presentan las soluciones más importantes con respecto a Seguridad de la información y la Norma ISO/IEC 27001 para la presente investigación.

Menciona Quinteros, F. (2017) expone en su trabajo de investigación "Elaboración de las políticas de seguridad de la información para el Consejo Nacional Electoral del Ecuador" dicha investigación valora las medidas de seguridad de la Información del Consejo Nacional Electoral del Ecuador (CNE) con el objetivo de mejorar sus niveles de seguridad en los procesos electorales y no electorales. Esta entidad tiene la responsabilidad de "… vigilar y garantizar, de manera transparente, los procesos electorales…" (Asamblea Nacional Constituyente, 2008, p. sn), por lo que es urgente implementar políticas de seguridad de la información, las cuales admitirán el contar con normativas que favorezcan la gestión de manera eficaz la seguridad de la información, de tal manera de que se consiga contrarrestar: amenazas, evaluar riesgos, e incrementar controles que permitan "garantizar la confidencialidad, integridad y disponibilidad de la información de la cual es responsable el Consejo Nacional Electoral". (p. 2) Dicho trabajo intenta crear las Políticas de Seguridad de la Información para el Consejo Nacional Electoral del Ecuador usando como base la normativa ISO/IEC 27001:2013, "estas políticas propenden la protección de los datos desde la parte informática, su acceso físico y restricciones de uso, responsabilidad de los servidores y servidoras que forma parte del CNE, entre otros" (p. 2).

Por otro lado, refiere Piña, G. (2017) en su trabajo de investigación denominado "Implementación de Seguridad en la Infraestructura de red para la difusión del Programa de resultados electorales preliminares 2017 en el estado de México bajo la Norma ISO/IEC 27001:2013" (p. 1). Dicha investigación "detalla una descripción general de todo el transcurso de producción de los resultados electorales y del Programa de Resultados Electorales Iniciales del Instituto Electoral del Estado de México realizado el 4 de junio de 2017 hacia la elección de Gobernador en el Estado de México" (p. 5).

En específico se explica el cómo se implementó seguridad en la Infraestructura que se usó para la difusión de los resultados electorales. Así mismo, se especifica la infraestructura que operó para la difusión del PREP, la cual estaba "compuesta del hosteo del servicio web en un centro de datos que cuenta con el nivel Tier IV e International Computer Room Expert Association (ICREA) nivel 5" (p. 1). De igual forma, en las pruebas se insertó un ataque de Denial

of Service (DoS), para monitorear el consumo del ancho de banda, con ello se incrementó el tiempo de espera de la página web, aunque siempre estuvo en línea. Este fenómeno tuvo presencia el día de la Jornada Electoral.

También Pérez, D (2017) expuso en su proyecto de "Diseño de una Infraestructura de red a gran escala con Tecnologías avanzadas de Seguridad aplicadas a Sistemas de Voto Telemático" tiene como propósito el brindar una solución a la problemática de res y seguridad existente, a partir de eso se ha definido la Arquitectura del sistema que satisfaga los requerimientos de seguridad planteadas y que pueda hacer una gestión correcta de los involucrados en el proceso electoral. Así también, se propone la creación de distintos niveles de competencia con objetivos específicos, siendo estos: Infraestructura para e voto, red y Proveedores de servicio. Cabe resaltar, que se hace énfasis en la problemática actual a partir de la cual se propone una solución apoyada en equipamiento y mecanismos de apoyo.

Igualmente, Vargas, A. , Rasilla, R. , Salas, A. , Ormeño, A. y Nuñez, R. (2018) señalan en su trabajo de investigación denominado "Adecuación de la Infraestructura de red para dar Soporte a las Unidades Orgánicas del JNE" cuyo propósito es analizar los servicios clave que ofrece a la Infraestructura TO del Jurado Nacional de Elecciones a partir de ello se plantea un esquema de solución que contempla los siguientes componentes: Instalación de switches, instalación de Plataforma de Gestión de Infraestructura de red, configuración de red de datos e implementación de VLANs, migración de políticas, roles y configuración de switches, entre otros. Cabe resaltar que "no se aplica ninguna Metodología ya que es una infraestructura de red" (p. 41). Finalmente, la propuesta de solución que incluye "la renovación de la Infraestructura de red la cual contempla el cambio de switch (Core/Borde), Cableado de red a Fibra ótica y una nueva Plataforma de monitoreo en el local de Lampa" (p. 48).

Así pues, Baldeón, V. y Zambrano, J. (2018) en su trabajo de investigación titulado "Implementación de un Prototipo de una Red descentralizada Blockchain para el voto electrónico en la Universidad de Guayaquil" destacan que la seguridad en las redes de datos es vital como herramienta y mecanismo de protección para salvaguardar la integridad de los datos. Para dar solución a esta problemática proponen la aplicación de la tecnología Blockchain cuyo significado en español es cadena de bloques que hace que el sistema informático sea seguro. "Esta tecnología permite realizar las transacciones sin intermediarios" (p. 20) dicho de otra forma, la forma descentralizada lo cual proporciona seguridad, esta tecnología ofrece un gran número de posibilidades para ser implementado y una de ellas es el voto electrónico. En la actualidad, muchos países a nivel mundial han optado y apostado por el voto electrónico, pero

a pesar de ello se ha identificado una gran debilidad en el sistema informático, el cual es blanco fácil para los hackers, esta tecnología es capaz de dar solución a este tipo de problemas haciendo para ello que las identidades de los votantes estén cifradas, protegidas y por ende que dichos votos no puedan ser manipulados o adulterados, garantizando así la integridad de dicha información.

Por último, refieren Angarita, J. y Bautista C. (2014), en su trabajo de investigación titulado "Diseño de un Sistema de Gestión de la Seguridad de la Información ISO 27001 para la alcaldía de Floridablanca y Plan de acción para su implementación según la guía PMBOK" (p. 1). Dicha investigación plantea un diseño de un SGSI basado en los principales procesos de la organización, y que posteriormente realiza el proceso de "gestión del proyecto enfocado en la guía PMBOK, lo que permitirá tener a la entidad un mejor control sobre sus principales activos de información y lograr el mejoramiento continuo de los controles implementados" (págs. 7 -8).

2.1.2. Base Teórica

2.1.2.1. Conceptos relacionados al Negocio.

Oficina Nacional de Procesos Electorales – ONPE.

Es un organismo electoral constitucional autónomo conforma parte del Estado Peruano. Así mismo representa "la autoridad máxima que se encarga de organizar y ejecutar distintos procesos electorales, de referéndum y otros tipos de consulta popular. Nuestro fin es velar por que se obtenga la fiel y libre expresión de la voluntad popular, manifestada a través de los procesos electorales que se llevan a cabo. Con relación a las organizaciones políticas, nos encargamos de la verificación de firmas de adherentes de los partidos políticos en proceso de inscripción; la verificación y control externos de la actividad económico-financiera, así como brindar asistencia técnico-electoral en los procesos de democracia interna" (ONPE, 2020).

Figura 1 Instalaciones ONPE

Fuente: https://www.onpe.gob.pe/nosotros/nuestra-historia/

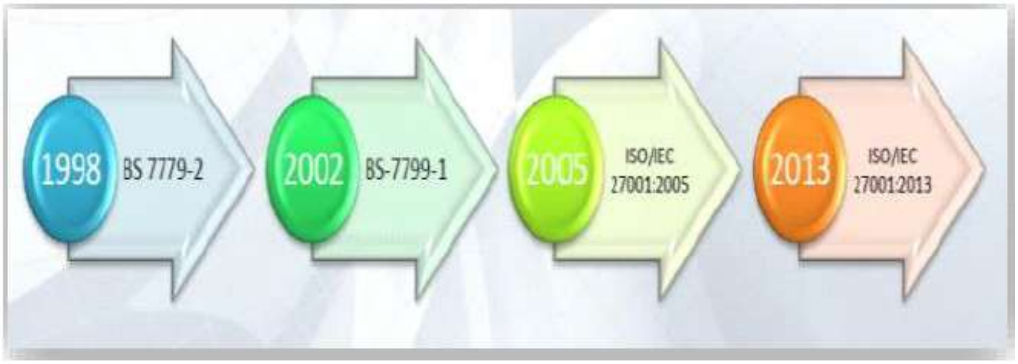
2.1.2.2. Conceptos relacionados a la Tecnología.

Norma ISO IEC 27001.

La presente norma se toma en cuenta dentro del marco regulatorio porque la seguridad de información es el enfoque del gobierno de TI. Es una norma cuya última versión fue publicada en octubre del 2013. Forma parte de la familia 27000 y cubre todo tipo de organizaciones. Es una norma que "ha sido preparada para brindar los requisitos para establecer, implementar, mantener y mejorar de manera continua un-Sistema de Gestión de Seguridad de la Información (SGSI)" (ISO 27001:2013).

Cabe mencionar que la ISO 27001 no se encarga de definir lo que es riesgo u otros aspectos relacionados, sino se enfoca en definir las actividades que guardan relación con el riesgo y mostrar como alinearlas políticas de gestión de seguridad de información con el contexto de gestión estratégica de riesgos. (Calder y Watkins, 2010).

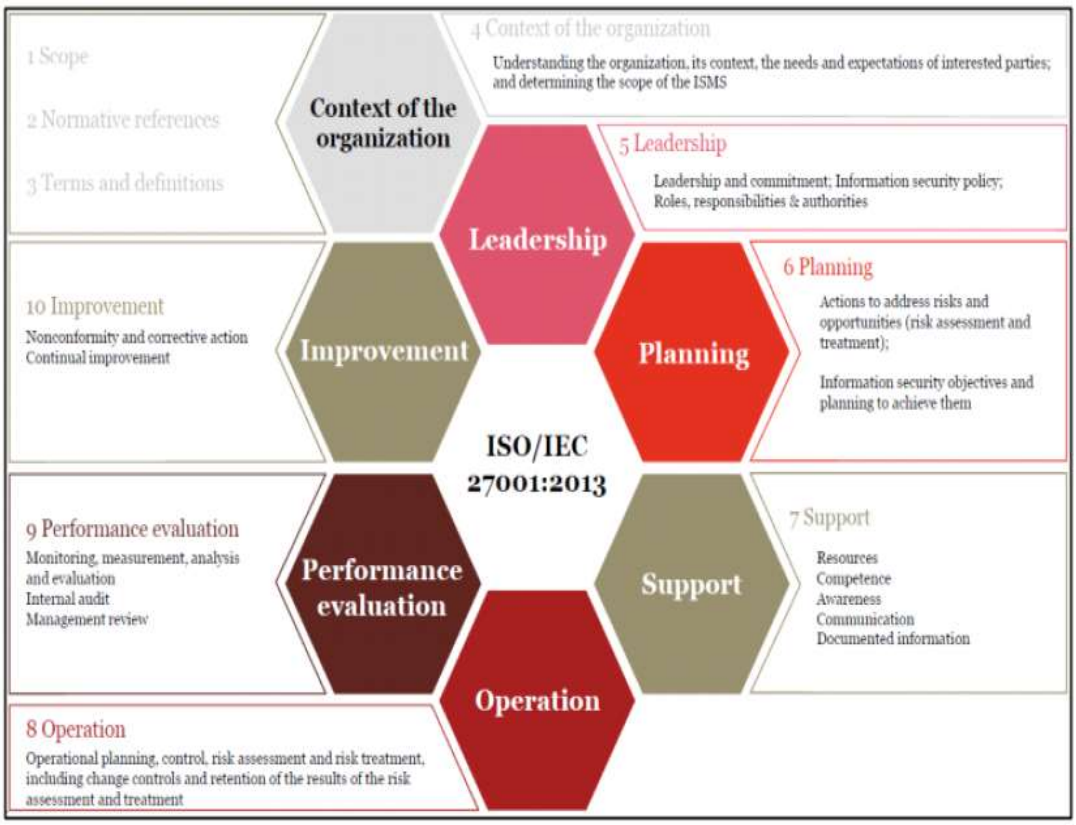
Figura 2 Origen y evolución de la norma ISO/IEC 27001



Fuente: Adaptado de https://www.pmg-ssi.com/2013/08/la-nch-iso-27001-origen-y-evolucion/

La ISO/IEC 27001:2013 está compuesta por diez (10) cláusulas más el Anexo A, de las cuales las tres primeras son introductorias y muestran el contexto de la norma; y los siete restantes, presentan los requisitos para la implementación del SGSI.

Figura 3 Cláusulas de la Norma ISO/IEC 27001:2013



Fuente: Adaptado de ISO/IEC 27001

Norma ISO IEC 27002.

La presente norma se encuentra dentro del marco regulatorio debido a que está vinculada con la norma ISO 27001, pues esta indica cómo debe de aplicarse., su fecha de publicación proviene de octubre del 2013 y se basa en la anterior norma ISO/IEC 27002:2005. Establece las directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de información en una organización. Los objetivos señalados es el de proporcionar una orientación general sobre las metas comúnmente aceptadas de gestión de seguridad de información. (ISO 27002, 2013). Así también, ha sido publicada por la Organización Internacional de Normalización (ISO) así como la Comisión Electrotécnica Internacional (IEC) como ISO/IEC 17799, la cual que tiene su origen en el British Standard BS 7799-1 publicada en el año 1995. Ya en el año 2002 la publicaron como ISO/IEC 17799:2000 y luego de un periodo de revisión y actualización se publicó en el año 2005 la ISO/IEC 17799:2005 hasta el año 2007,

donde se actualizó el nombre a ISO/IEC 27002:2005, y en la actualidad contamos con la última versión ISO/IEC 27002:2013. Esta norma, está compuesta de 14 (catorce) cláusulas de control de seguridad, que a su vez tienen un total de 35 (treinta y cinco) objetivos de control y ciento catorce (114) controles.

Figura 4 Dominios de la ISO 27002

Fuente: ISO 27001, ISO 27002

Norma ISO IEC 27003.

ISO 27003 es un estándar internacional que conforma una guía para la implantación de un SGSI. Además, es una adaptación tanto para los que quieren lanzarse a implantar un SGSI como para los consultores en su trabajo diario, debido a que da solución ciertas controversias que venían escaseando de un criterio normalizado. Así también, esta norma focaliza su atención en los puntos que se requieren para un diseño exitoso y una buena implementación del Sistema de Gestión de Seguridad de la Información – SGSI – según el estándar ISO 27001.

Cabe resaltar que un documento básico e integral que ofrece orientación para todos los requisitos de ISO / IEC 27001, pero no cuenta con descripciones específicas sobre "monitoreo, medición, análisis y evaluación" ni "gestión de riesgos de seguridad de la información". ISO / IEC 27004 e ISO / IEC 27005 se centran en contenidos específicos y brindan una guía más detallada sobre “monitoreo, medición, análisis y evaluación” y "gestión de riesgos de seguridad de la información" (Tecnologías de la información y Consultoría, 2020).

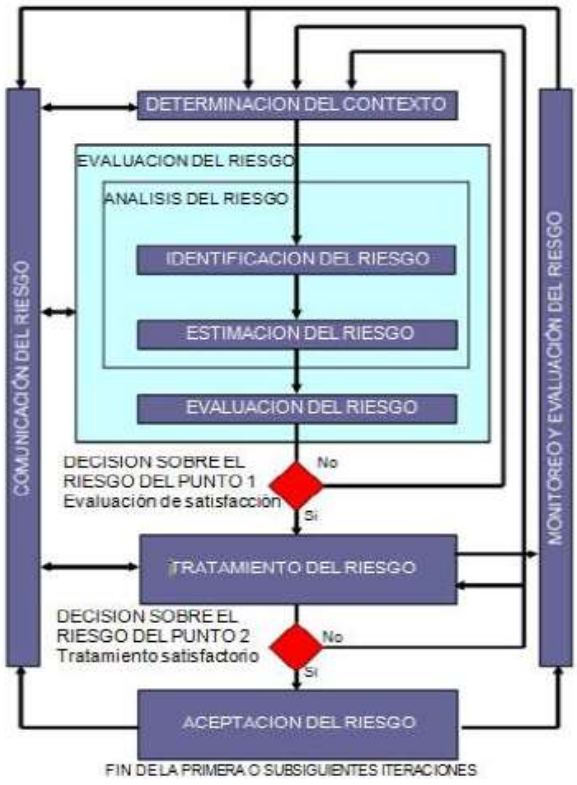
Figura 5 ISO 207003

Fuente: NORMA ISO -27003 by Elena Rangel

Norma ISO IEC 27005.

Según la NTP-ISO/IEC 27005 (2009), "el proceso de gestión del riesgo en seguridad de la información consiste en establecer el contexto, evaluar el riesgo, tratar el riesgo, aceptar el riesgo, comunicar el riesgo y monitorear y revisar el riesgo". (Hanson, J. y Escobar, P., 2005)

Figura 6 Proceso de gestión del riesgo de seguridad de la información



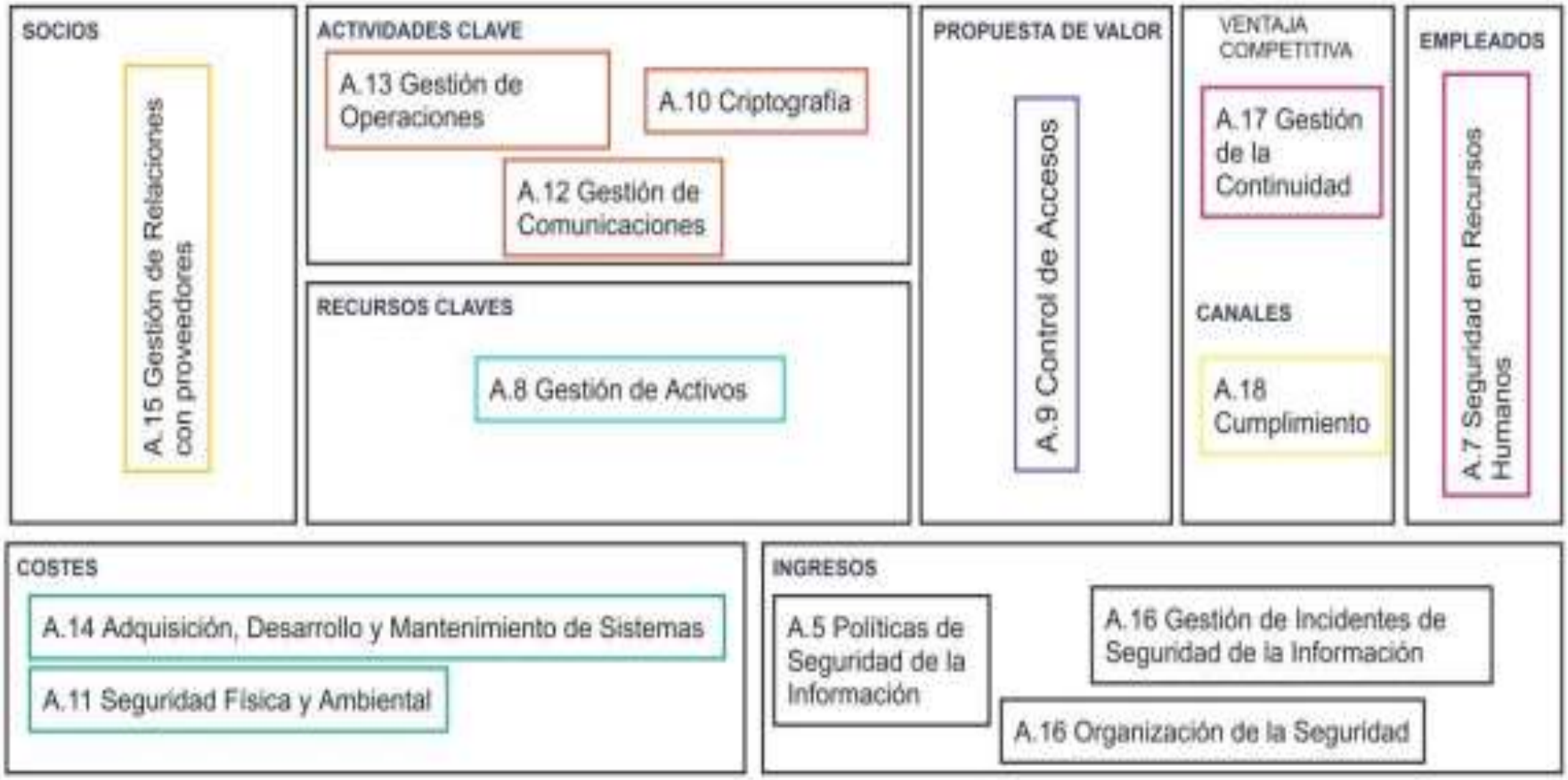
Fuente: (NTP-ISO/IEC 27005, 2009)

Norma Técnica Peruana NTP ISO/IEC 27001.

Es una norma hecha por el Comité Técnico Permanente de Codificación e Intercambio Electrónico de Datos, fue publicada en el año 2009 e instaurada como de uso obligatorio a través de la Resolución Ministerial N° 129-2012-PCM el año 2012, se encuentra trazada al estándar ISO/IEC 27001 - estándar internacional publicado en el año 2005 que ofrece un modelo a seguir para establecer y mantener un SGSI. El objetivo principal de esta norma es instaurar los requisitos que deben cumplirse para poder implementar el SGSI usando un enfoque a procesos, lo cual necesita que se tenga disponible la mayor cantidad de documentación respecto a los mismos.

La versión que corresponde al año 2013 presenta una nueva estructura de acuerdo al estándar determinado por ISO/IEC para todas las normas referentes a sistemas de gestión, facilitando la integración y trabajo compuesto entre los distintos estándares de gestión publicados por dicha institución. Este estándar es de uso crítico en los proyectos de análisis y diseño de SGSI's, dado que constituye concretamente los pasos que se implican en este proceso. Así también, con la Resolución N° 129-2014/CNB-INDECOPI de la comisión de normalización y de fiscalización de barreras comerciales no arancelarias se aprueba como Norma técnica peruana (NTP), entre otras, la NTP-ISO/IEC 27001:2014 TECNIOLOGÍA DE LA INFORMACIÓN Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. 2a Edición. De igual forma, la Norma Técnica Peruana ISO/IEC 27001:2014 brinda 14 dominios, 35 objetivos de control y 114 controles, organizados de la siguiente forma:

Figura 7 Controles de la NTP ISO/IEC 27001:2014



Fuente: Adaptado de Seguridad en el Dialecto del jefe - Incibe (2016).

Gestión de riesgos.

La gestión de riesgos es una pieza clave dentro de la implementación de un Sistema de Gestión de Seguridad de la Información. La gestión de riesgos es un proceso que busca establecer un equilibrio entre lo que la empresa "quiere ganar" frente a lo que "está dispuesta a sufrir": ganancias enfrentadas a las vulnerabilidades y pérdidas que pueda por efecto de las amenazas a sus recursos más críticos. En este caso específico, los recursos de información (Tupia, 2010, p.50).

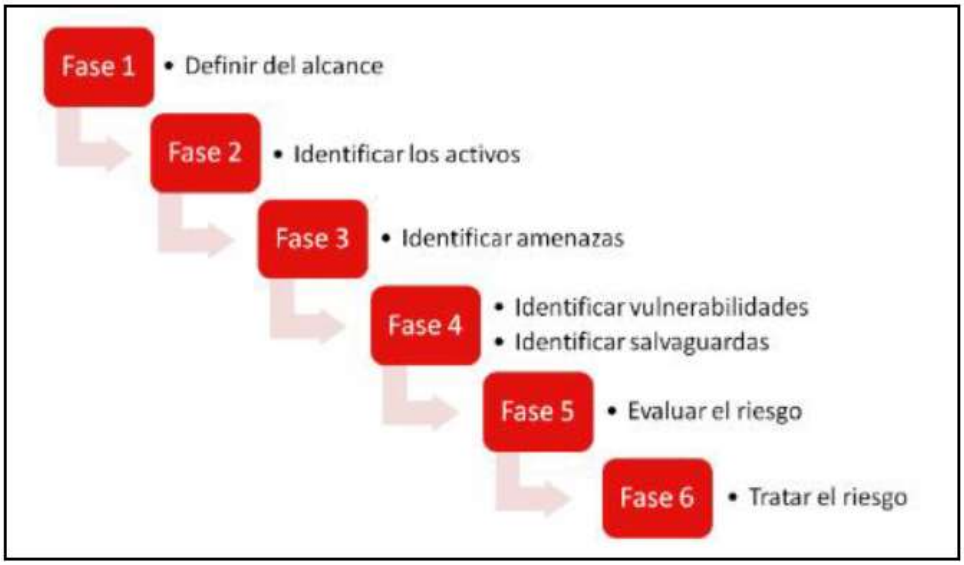
Figura 8 Gestión del Riesgo

Fuente: https://advisera.com/27001academy/es/que-es-iso-27001/

Análisis de Riesgos

Cabe mencionar que las fases o etapas que componen un análisis de riesgo dependen de la metodología seleccionada, sin embargo, vamos a utilizar las fases más comunes de la mayoría de las metodologías para el análisis de riesgo.

Figura 9 Fases que componen el análisis de riesgo

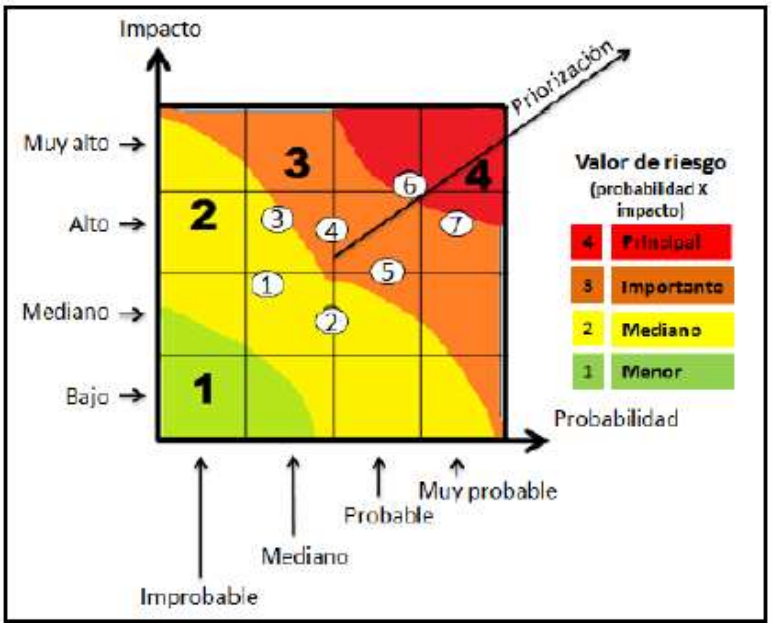


Fuente: Adaptado de INCIBE, 2017.

Priorización de Riesgos.

Se puede afirmar que "el riesgo cero no existe, pero es posible definir un umbral por debajo del cual es aceptable no hacer nada para reducir el riesgo. En el otro extremo de la escala, hay un umbral más allá del cual es riesgo inaceptable, entonces se debe hacer todo lo posible para eliminar su fuente, o reducir los riesgos de forma fiable" (PECB.2016, p. 96).

Figura 10 Priorización de riesgos



Fuente: Adaptado de PECB, 2016.

2.2. Marco Conceptual

2.2.1. El PMBOK

Es la norma de Gerencia de Proyectos principal del PMI. Admitida dentro del conjunto de normas ANSI, Concentra normas internacionales para delimitar los procesos precisos para gestionar proyectos. La información se encuentra organizada en 05 grupos de proceso. Actualmente estamos en la sexta edición del PMBOK, publicada en el año 2017.

1. Los procesos de iniciación. Estos procesos se realizan para especificar un nuevo proyecto o una nueva fase ya existente, para ello se requiere la autorización para iniciar el proyecto o fase.

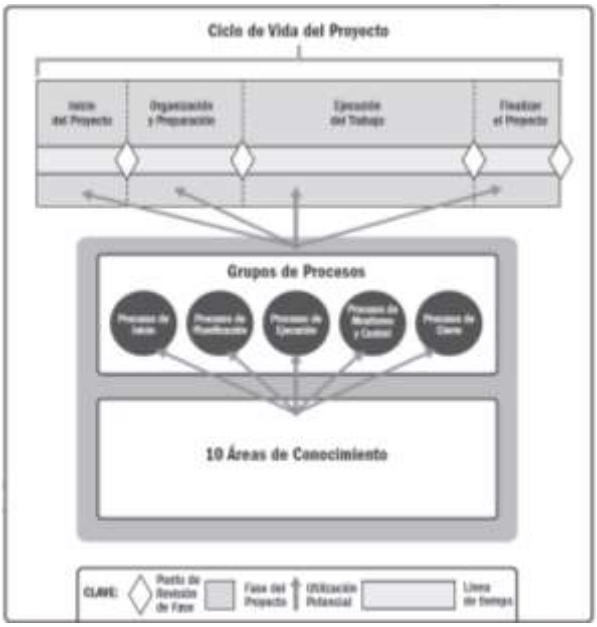
2. El proceso de planificación. Son procesos necesarios para constituir la trayectoria del proyecto, afinar los metas y limitar el recorrido de ejecución obligatoriamente para lograr los objetivos para cuyo logro se inició el proyecto.

3. Los procesos de ejecución. Son procesos ejecutados para culminar la tarea definida en el método para la trayectoria del proyecto a fin de culminar los detalles del mismo.

4. Los procesos de seguimiento y control. Son procesos demandados para facilitar el rastreo, examinar y conocer el avance de los proyectos, para nivelar áreas en las que el plan requiera permutas y para iniciar los ajustes necesarios.

5. Los procesos de cierre. Son procesos ejecutados para culminar cada una de las etapas a través de los procesos, a fin de culminar explícitamente el proyecto o una fase del mismo.

Figura 17 Ciclo de Vida del Proyecto



2.2.2. Activo de información

Los activos son los recursos que tienen valor para la organización, sus operaciones de negocio y su continuidad, requeridos para que esta funcione y logre los objetivos que sugiere su dirección "… algo a lo que una organización directamente le asigna un valor y, por lo tanto, la organización debe proteger" (novasec, 2019).

De la definición de la ISO/IEC 17799:2005 Código para práctica de la gestión de la seguridad de la información, un activo de información es "algo a lo que una organización directamente le asignan un valor y, por lo tanto, la organización debe proteger" (novasec, 2019). Otra definición relevante es "aquel bien o servicio tangible o intangible, que genera, procesa o almacena información al cual una organización directamente le atribuye valor y por tanto requiere una adecuada protección y cuidado" (Seminario, 2015).

Figura 11 Activos de la información

Fuente: https://docplayer.es/11304445-Ntp-iso-iec-27001-2008.html

2.2.3. Infraestructura de Red Tecnológica

El servicio que proporciona "el conjunto de dispositivos y aplicaciones necesarios para una empresa, es conocido como infraestructura IT. Este sistema se gestiona a través de la

monitorización mediante el despliegue de los equipos suficientes, máquinas y software para el cliente" (clavei, 2020).

Figura 12 Componentes de la Infraestructura TI

Fuente: https://www.slideshare.net/Akirepaho/presentacion-infraestructura-ti/5

En principio, el contar con este tipo de infraestructura posibilita que podamos trabajar con un gran volumen cantidad de datos, almacenados en la nube con una gran seguridad, pero con maneras sencillas para su acceso. Así mismo, la infraestructura IT proporciona soporte en un contexto de tecnologías disruptivas en una sociedad conectada a nivel mundial conectada, teniendo en cuenta un ecosistema que visualiza, según Gartner, a más de 25 billones de los más diversos dispositivos y cosas conectadas para 2020. En todo ese proceso de cambios, contar con la infraestructura tecnológica IT ideal, será un factor determinante para la competitividad de los negocios y el éxito de la transformación digital.

"La arquitectura tecnológica del sistema de transmisión de datos permite garantizar la transmisión de la información a la sede principal (centro de datos principal) y sede de contingencia (centro de datos de contingencia). Se precisa que estas sedes son los puntos de recepción de la información, los cuales se encuentran geográficamente separados, cuya comunicación es mediante una conexión de tipo Fibra Óptica dedicada". (RESOLUCION GERENCIAL N° 000003-2020-GITE/ONPE, 2018, p. 20)

Figura 13 Arquitectura Tecnológica

Fuente: RESOLUCION GERENCIAL N° 000003-2020-GITE/ONPE

2.2.4. Proceso Electoral

Cada proceso electoral organizado y ejecutado por la ONPE ha representado una exhaustiva labor y un tratamiento diferente de acuerdo al contexto de la elección convocada. Aun así, la característica similar en todos ellos ha sido la transparencia y la eficiencia.

Durante la organización de un proceso electoral," como son las elecciones regionales y municipales, las ORC brindan apoyo a las ODPE para el éxito de los comicios" (Guía Elecciones Regionales y Municipales, 2008, p. 20). Para este proceso electoral, "el financiamiento público indirecto busca beneficiar a las organizaciones políticas con inscripción definitiva de sus candidaturas a gobernador y vicegobernador y/o listas de consejeros regionales con espacios gratuitos en radio y televisión". (Guía Elecciones Regionales y Municipales, 2008, p. 16)

2.2.5. Sincronización de Tramas

El Sincronizador de tramas es una herramienta tecnológica que se usa en los servidores de la sede central de la ONPE, para transformar las tramas transmitidas en datos para la integración con la Suite de Cómputo de Resultados Electorales. Este proceso se realiza a través de la "ejecución de tareas programadas desde un servidor sin acceso a Internet, las cuales procesan las tramas transmitidas, las convierten en datos y los insertan en las tablas correspondientes en el formato requerido por el S-CORE para que sean procesadas con los

documentos físicos recibidos en los centros de cómputo" (Plan de Acción para implementación del SEA, 2020, p. 13).

2.2.6. Seguridad de la información

Conocido como SGSI o ISMS – Information Security Management System. "Es un conjunto de procesos que permiten establecer, implementar, mantener y mejorar de manera continua la seguridad de la información, tomando como base para ello los riesgos a los que se enfrenta la organización" (Gómez & Fernández, 2015, p. 11).

La enciclopedia de seguridad informática lo define como "… aquella parte del sistema general de gestión que comprende la política, la estructura organizativa, los recursos necesarios, los procedimientos y los procesos necesarios para implementar la gestión de seguridad de la información en una organización" (Gómez, 2011, p. 52).

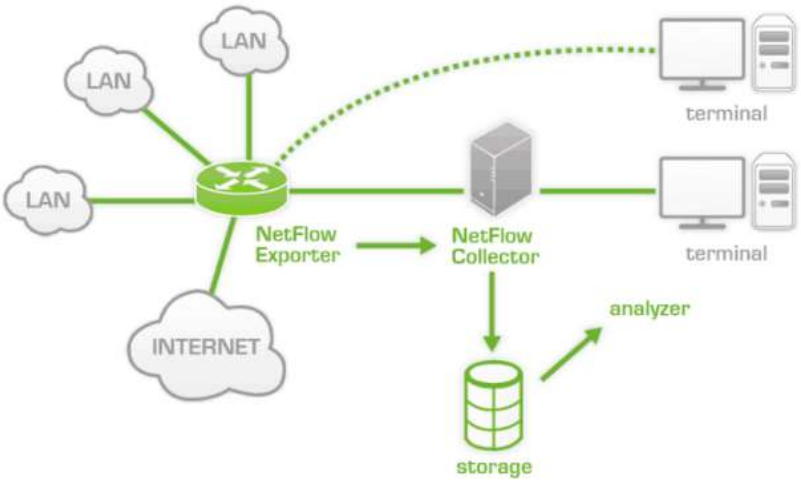
Figura 14 Base de la Seguridad de la información

Fuente:www.recursostic.educacion.es

2.2.7. Trafico de red

El tráfico de red (también llamado tráfico o tráfico de datos) "hace referencia a los datos que se desplazan por una red en un momento determinado. Los datos de la red están compuestos por paquetes, que son las unidades fundamentales más pequeñas de datos que se transmiten por una red". (solarwinds, sf)

Figura 15 Análisis de Tráfico de red



Fuente: www.pamdorafms.com

2.3. Marco Metodológico

Para la implementación vamos a utilizar los lineamientos del PMBOK para conducción del proyecto, el cual contempla un marco de trabajo de 49 procesos, 10 áreas de conocimiento y 05 grupos de proceso, así mismo se hará uso de la ISO 27001 hacia la confección de inspecciones de seguridad de la información para la infraestructura a diseñar.

2.3.1. La Norma Técnica Peruana NTP ISO/IEC 27001:2014

Dentro de la fuente original de base de la norma tenemos la siguiente recomendación, acerca de las fases de aplicación. Así mismo, en esta sección se describe la metodología propuesta que servirá de guía para la implementación del Sistema de Gestión de Seguridad de la Información para la Transmisión de datos de los resultados electorales, el establecer una metodología para la implementación de un SGSI, se ha generado la necesidad de instaurar un modelo propuesto para la implementación de lo establecido en la Norma Técnica Peruana NTP-ISO/IEC 27001:2014, tomando como referencia los siguientes marcos normativos.

Task Mode	WE	Task Name	Duration	Start	Finish	Predecessors
	0	IMPLEMENTACION DE UNA INFRAESTRUCTURA DE SEGURIDAD TECNOLÓGICA PARA CONTROLAR EL TRÁFICO DE RED DURANTE EL PROCESO DE TRANSMISIÓN DE RESULTADOS DE UNA ENTIDAD DEL GOBIERNO PERUANO	91 days?	Thu 10/10/19	Fri 14/02/20	
	1	Gestion de Proyecto	1 day?	Thu 10/10/19	Fri 11/10/19	
	1.1	Acta de constitucion	1 day?	Thu 10/10/19	Fri 11/10/19	
	1.2	Implementacion	1 day?	Fri 20/12/19	Mon 23/12/19	41
	1.3	Seguimiento	29 days	Fri 20/12/19	Thu 30/01/20	41
	1.4	Cierre del Proyecto	30 days	Fri 3/01/20	Fri 14/02/20	49
	2	Levantameinto de Informacion	2 days	Thu 10/10/19	Mon 14/10/19	
	3	Elaboracion del diseño	23 days?	Mon 14/10/19	Thu 14/11/19	6
	3.1	Identificacion de Zonas de Red	8 days?	Mon 14/10/19	Thu 24/10/19	
	3.1.1	Zona de Gestion	4 days	Mon 14/10/19	Fri 18/10/19	
	3.1.2	Zonas de Servidores y Servicios	4 days?	Fri 18/10/19	Thu 24/10/19	13
	3.2	Definicion de topologia de Red	4 days	Thu 24/10/19	Wed 30/10/19	12
	3.2.1	Definicion de topologia fisica de red	2 days	Thu 24/10/19	Mon 28/10/19	
	3.2.2	Definicion de topologia logica de red	2 days	Mon 28/10/19	Wed 30/10/19	24
	3.3	Definicion de servicio de telecomunicaciones	1 day	Wed 30/10/19	Thu 31/10/19	23
	3.3.1	Definicion de capa de transporte	1 day	Wed 30/10/19	Thu 31/10/19	
	3.3.2	Definicion de enlaces seguros	1 day	Wed 30/10/19	Thu 31/10/19	
	3.4	Definicion controles de seguridad	3 days?	Thu 31/10/19	Tue 5/11/19	30
	3.5	Definicion de cumplimiento normativo	5 days	Thu 31/10/19	Thu 7/11/19	30
	3.6	Definicion de cronograma y requerimientos	5 days	Thu 7/11/19	Thu 14/11/19	37
	3.6.1	Definicion de requerimientos	5 days	Thu 7/11/19	Thu 14/11/19	
	3.6.2	Definicion de cronograma de crontatacion de servicios	1 day	Thu 7/11/19	Fri 8/11/19	
	4	implementacion y control de calidad	34 days?	Thu 14/11/19	Wed 1/01/20	11

Fuente: Elaboración propia cronograma de desarrollo del proyecto.

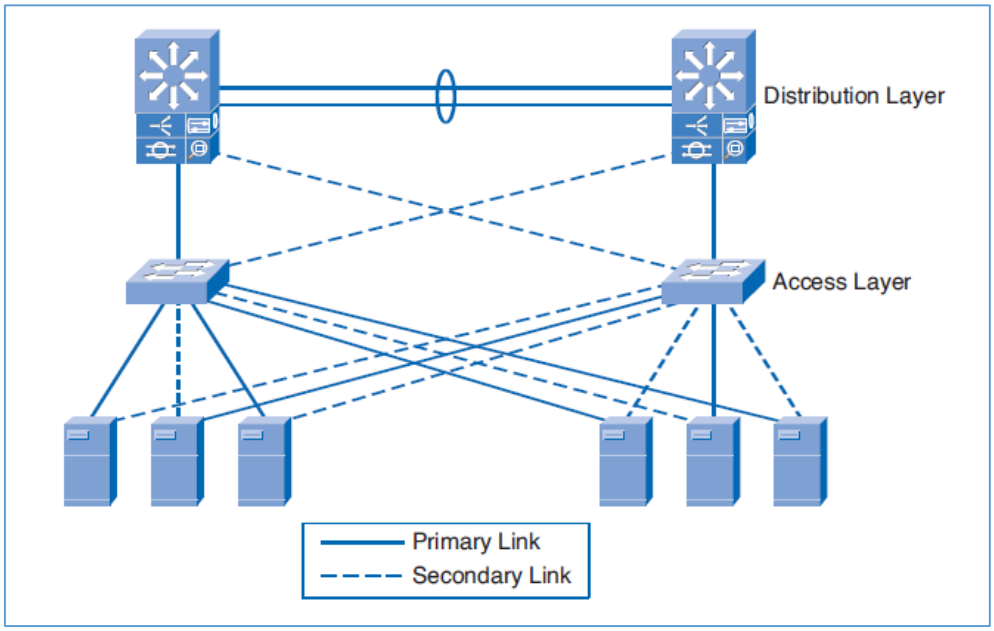
Capítulo III: Desarrollo de la Solución

3.1. Levantamiento de informacion.

3.1.1. Infraestructura prexistente

Dentro de la reunión para el levantamiento de información con el área de infraestructura de seguridad, no había un proceso electoral en curso por lo cual solo tenía una imagen de representación de la red que se toma como modelo para la implementación durante el uso dentro de un proceso electoral.

Figura 22 Diagrama de referencia



Fuente:

3.1.2. Reunión con el área usuaria

Dentro de la reunión del área usuaria que utiliza los recursos tecnológicos y de cómputo, hicieron referencia al último procedimiento aproado por su la ONPE para la transmisión de datos electorales. Así mismo nos compartieron este procedimiento donde se señala el periodo que se contempla para el uso como transmisión de datos.

3.1.3. Visita a los centros de datos

Si bien no tenía un proceso electoral ejecutándose, los ambientes que utilizan para este fin se encontraban disponible, poseían cámaras de seguridad y controles biométricos, en la entrada y en la exclusa.

3.1.3.1 Centro de Datos Principal**.**

- ✓ Servidor de transmisión de colas principal
- ✓ Servidor de transmisión de colas de calidad
- ✓ Servidor de base de datos nación principal

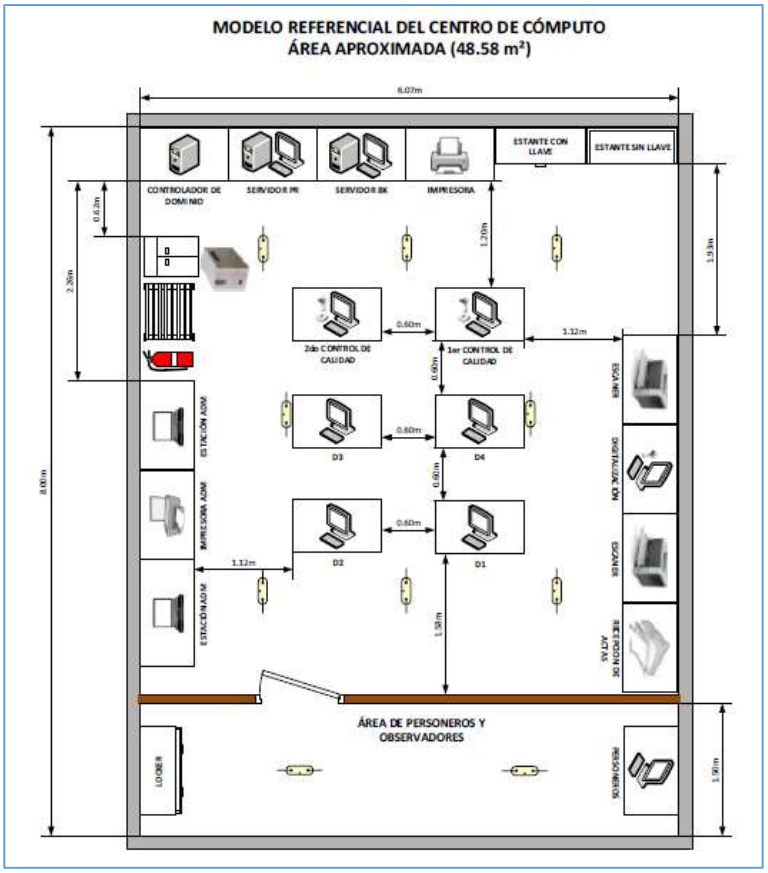
3.1.3.2 Centro de Datos Contingencia.

- ✓ Servidor de transmisión de colas de contingencia
- ✓ Servidor de base de datos nación principal.

3.1.4. Visita a una sede ODPE

Se muestra el diseño de la ODPE modelo para la implementación de una ODPE, en el momento del levantamiento de información, no se contaba con un local ODPE disponible, sin embargo, a nivel de procesos se encuentran definidos las ubicaciones por una línea producción y se tiene estructurado los sistemas a utilizar. Asimismo, se definieron los requerimientos base de seguridad.

Figura 25 Diagrama de distribución de estaciones de trabajo de una ODPE.



Se pudo identificar los siguientes elementos de intervienen dentro del proceso de transmisión de resultados, lo cuales se pueden agrupar en dos grupos.

3.1.5. Solución de procesamiento de transmisión de resultados – ODPE.

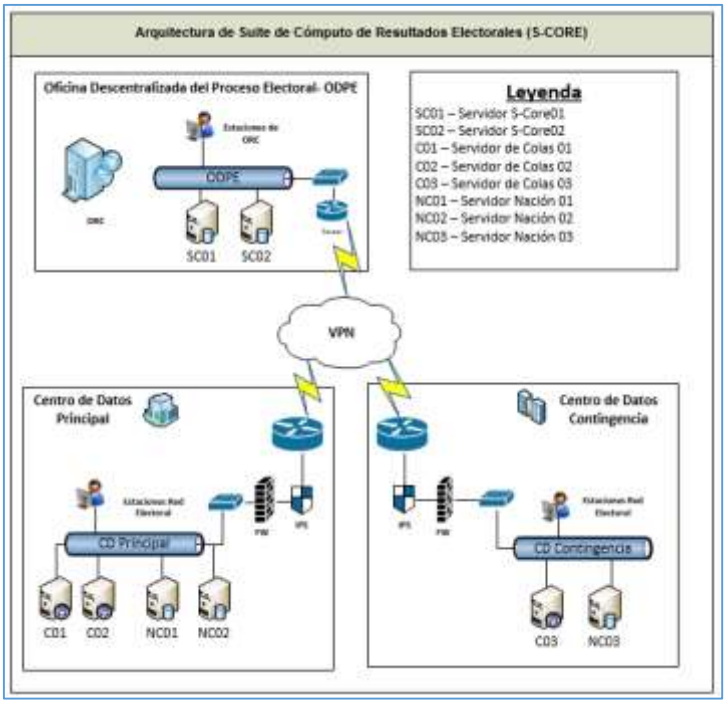
Los elementos que componen esta sección son soluciones de software desarrolladas a medida para el procesamiento y transmisión de resultados (S-CORE), los cuales se componen de los siguiente.

- ✓ Sistema de digitación de actas.
- ✓ Sistemas de control de calidad de actas digitadas
- ✓ Sistema de digitalización de actas.
- ✓ Sistema de control de calidad de digitalización.
- ✓ Sistema de transmisión de actas procesadas.

3.1.6. Infraestructura que brinda soporte al procesamiento y transmisión de resultados - ODPE.

- ✓ Estaciones de digitación
- ✓ Estaciones de digitalizaciones
- ✓ Estaciones de control de calidad
- ✓ Servidores de procesamiento y transmisión
- ✓ Equipos de comunicación:

Figura 24 Diagrama de representación de interconexión del sistema S-CORE



3.1.7. Elaborar acta de levantamiento de requerimientos funcionales de seguridad

Dentro los requerimientos funcionales de seguridad, estuvo la separación por zonas de seguridad y trabajos exclusivos. Así mismo presentaron la necesidad de mantener los registros de los eventos con una retención mínima de 2 años y exportable para cualquier auditoria que pudiera presentarse.

Zonas identificadas:

- ✓ Zonas de servidores de colas
- ✓ Zonas de servidores de base de datos.
- ✓ Zonas de control o infraestructura.

3.1.7.1 Elaborar acta de levantamiento de requisitos no funcionales de seguridad

Dentro los requerimientos no funcionales inherentes al proceso de transmisión de resultado, se detecta que de una necesidad de otro proceso que se ejecuta dentro de la ODPE, se requiere una autorización bajo los lineamientos del proceso de transmisión de microformas se realice un respaldo desde la misma ODPE, preservando las restricciones implementadas para el proceso de transmisión, es decir una exención dentro del proceso en paralelo.

Zonas de red identificadas no funcionales:

- ✓ Zona de monitores de red.
- ✓ Zona de monitoreo de base datos.
- ✓ Zona de Centro de comando.
- ✓ Zona de Auditorio.
- ✓ Zona de Personeros.

3.2. Elaboración del diseño.

Para el diseño creado se definieron dos grupos de zonas de red principales la Zonas de Red LAN y Zonas de Red WAN, cada una ópera en una zona distinta, pero a la vez dependiente de otra ya que sin ellas no habría procesamiento o comunicación entre sí para la transmisión de datos, asimismo se ha considerado controles de seguridad para el aseguramiento de la transmisión de los resultados electorales, así como también el monitoreo que se realiza durante el proceso.

Se identificó tres tipos de locaciones: Se precisa que se tiene una constante en la Sede Principal y Contingencia para todos los procesos electorales, sin embargo, para la ODPE, es

variable ya que el número de ODPE depende del alcance de la elección, es decir si es la elección es nacional, por lo cual el tamaño es variable.

- ✓ Sede Principal (01).
  - Centro de Datos Principal.
- ✓ Sede Contingencia (01).
  - Centro de Datos de Contingencia.
- ✓ Oficina Descentralizada del Proceso Electoral – ODPE.

El diseño elaborado se ha dividió en tres secciones.

- ✓ Definición de Zonas de Red.
- ✓ Diseño de topología de Red.
- ✓ Diseño de Controles de Seguridad.

3.2.1. Definición de Zonas de Red

Las definiciones de zonas de red, se ha divido en dos grupos Zonas de Red LAN y Zonas de Red WAN, los cuales tiene como principio definir los ámbitos de acción y los propósitos de cada una de estas, para ser utilizadas en la elaboración de la topología de Red.

Tabla 13 Cuadro de aplicabilidad de las zonas de red por sede identificada.

. Zonas de Red	Sedes		
	Principal	Contingencia	Sedes Remotas
A - Zonas de Red - LAN:	X	X	---
a) Zonas de Procesamiento Electoral	X	X	---
Zona de Recepción de Tramas:	X	X	---
Zona de Base de Datos:	X	X	---
b) Zonas de Gestión de Infraestructura:	X	X	---
Zona de Infraestructura de Virtualización:	X	X	---
Zona de Telecomunicaciones:	X	X	X
Zona de Monitoreo de Servicios e Infraestructura:	X	X	---
Zona de Monitores de Red:	X	X	---
Zona de Monitores de BD:	X	X	---
c) Zonas de Gestión de Proceso Electoral:	X	X	---

Zona de Centro de Comando:	X	X	---
Zona de Auditorio:	X	---	---
Zona de Personeros:	X	---	X
d) Zona de Acopio Procesamiento Electoral - ODPE:	---	---	X
B - Zonas de Red - WAN:	X	X	X
a) Zona de servicios de telecomunicaciones:	X	X	X
b) Zonas de encapsulación y cifrado:	X	X	X

Fuente: Elaboración Propia

3.2.1.1 Zonas de Red – LAN.

Como parte del diseño propuesto se ha dispuesto la siguiente distribución lógica con la finalidad de atender los requerimientos identificados, la cual se detalla a continuación.

Zonas de Procesamiento Electoral: las zonas del proceso electoral tienen como finalidad, alojar lo servicios informáticos usados para el proceso electoral en la sede central y contingencia.

- ✓ Zona de Recepción de Tramas: Zona definida para para recepción de tramas de datos de las ODPE que contienen los avances del acopio de actas electorales.
- ✓ Zona de Base de Datos: Zona definida para alojar los servidores base de datos que reciben las tramas procesadas para ser ingresada como datos.
- ✓ Zona de Centro de Comando:
- ✓ Zona definida que contiene a los operadores del proceso electoral y monitoreo del avance de la transmisión de resultados desde las ODPE.

Zonas de Gestión de Infraestructura:

Las zonas de gestión tienen como finalidad establecer una zona de control aislada de cualquier otro punto de comunicación, independiente de la infraestructura tecnológica, así como también sin intervenir en el proceso electoral directamente.

- ✓ Zona de Infraestructura de Virtualización: Zona definida para la gestión de la infraestructura de virtualización, donde se desplegarán los servidores para el procesamiento de datos.

- ✓ Zona de Telecomunicaciones: Zona definida para la gestión de los dispositivos de telecomunicaciones.
- ✓ Zona de Monitoreo de Servicios e Infraestructura: Zona definida para albergar los distintos servicios de monitoreo para la red y los servicios informáticos.
- ✓ Zona de Monitores de Red: Zona que alberga las estaciones de los operadores y monitoreo de red e infraestructura.
- ✓ Zona de Monitores de BD: Zona de monitoreo del servicio de base de datos.

Zonas de Gestión de Proceso Electoral: las zonas del proceso electoral tienen como finalidad, alojar lo servicios informáticos usados para el proceso electoral en la sede central y contingencia.

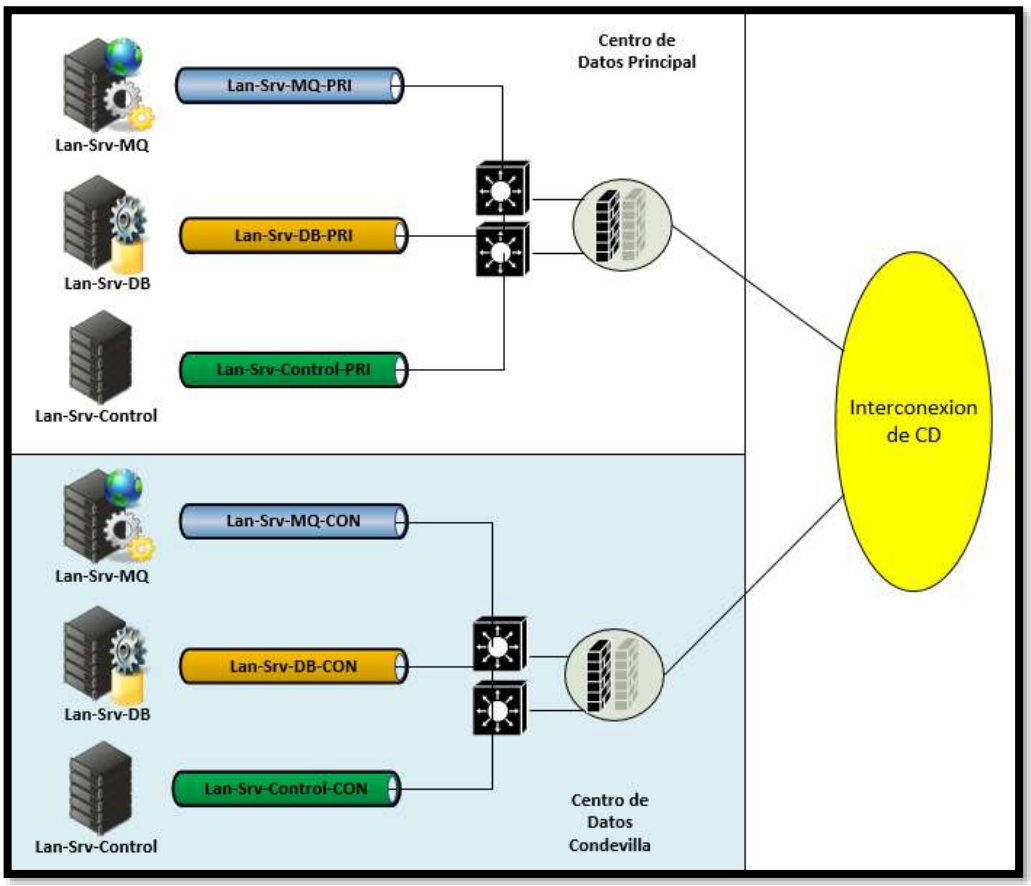
- ✓ Zona de Centro de Comando: Zona definida que contiene a los operadores del proceso electoral y monitoreo del avance de la transmisión de resultados desde las ODPE.
- ✓ Zona de Auditorio: Zona definida para realizar los actos públicos, tales como por ejemplo la limpieza de contadores del proceso electoral, dando inicio a este, conocidos como puesta cero.
- ✓ Zona de Personeros: Zona definida para las estaciones donde los personeros de los partidos políticos puedan visualizar el avance del proceso electoral.

Zona de Acopio y Procesamiento Electoral - ODPE: las zonas del proceso electoral tienen como finalidad, alojar estaciones de trabajo usados para el proceso acopio y el procesamiento de actas electorales en las oficinas descentralizadas del proceso electoral - ODPE.

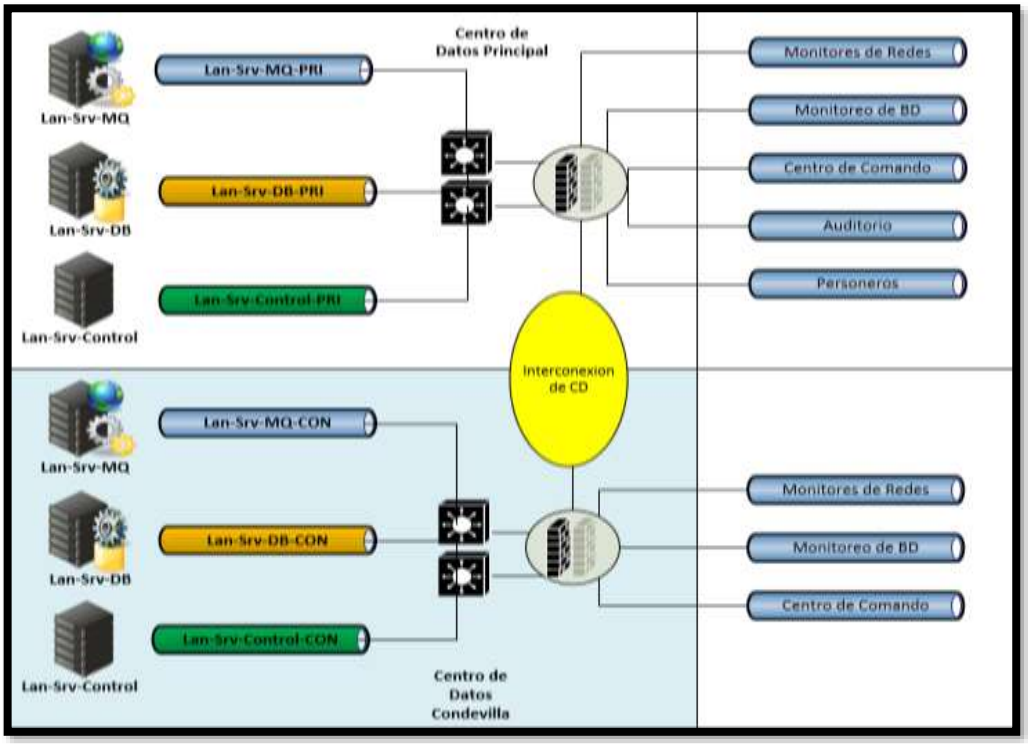
3.2.1.2 Zonas de Red - WAN:

Se define las zonas de interconexión, con la finalidad de ser flexible para cualquier proveedor de telecomunicaciones y servicios de comunicación.

- ✓ Zona de servicios de telecomunicaciones: Zona definida para que el proveedor de telecomunicaciones implemente su nube MPLS.
- ✓ Zonas de encapsulación y cifrado: Zona definidas para la encapsulación y cifrado de la información que se transmitirá entre los centros de datos y las ODPE.



Elaboración propia: Diagrama de servicios de los centros de datos.



Elaboración propia: Diagrama de servicios de los centros de datos para servicios internos.

3.2.2. Diseño de Topología de Red

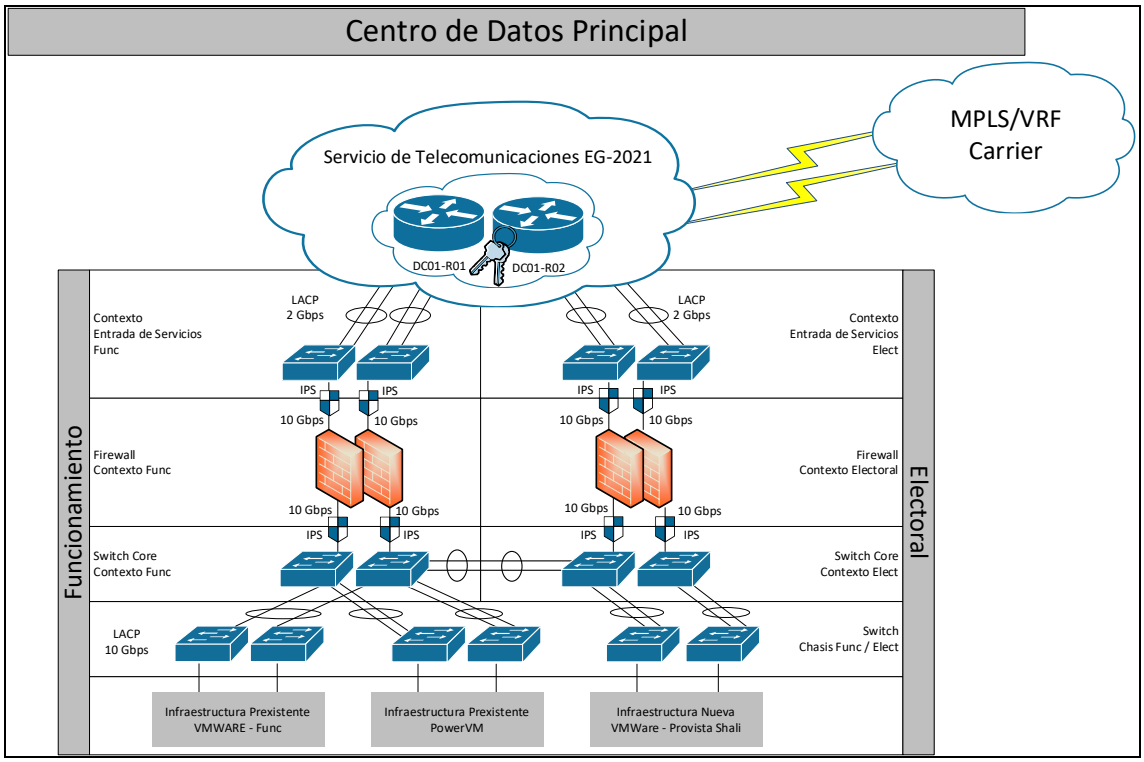
Para la definición de la topología de red se ha considerado tres topologías LAN y una Topología LAN.

3.2.2.1 Definicion de topologia fisica.

3.2.2.1.1. Definicion de topologia de red - Centro de Datos Principal

La topología LAN diseñada tiene la finalidad de brindar un esquema de alta disponibilidad ante la pérdida de un elemento de red definido dentro de la topología. Se describe a continuación los elementos.

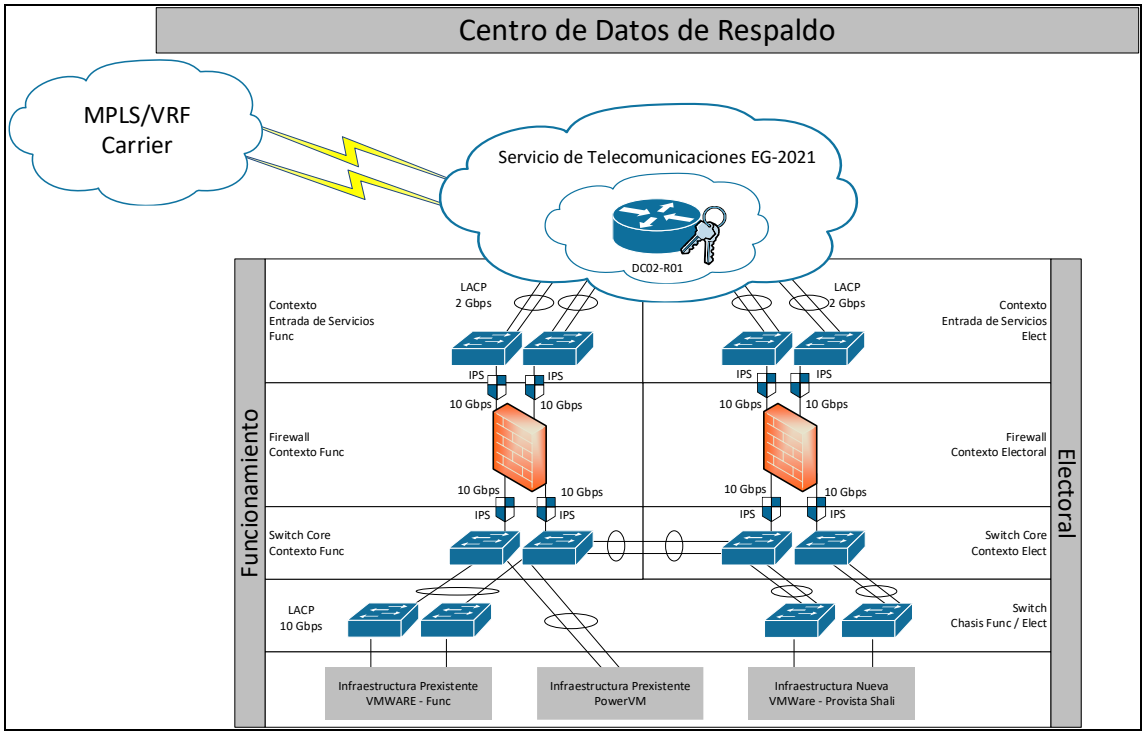
Elaboración Propia – Definición de servicios a nivel de centro de datos



Elaboración Propia – Diagrama de topología física de centro de datos de principal

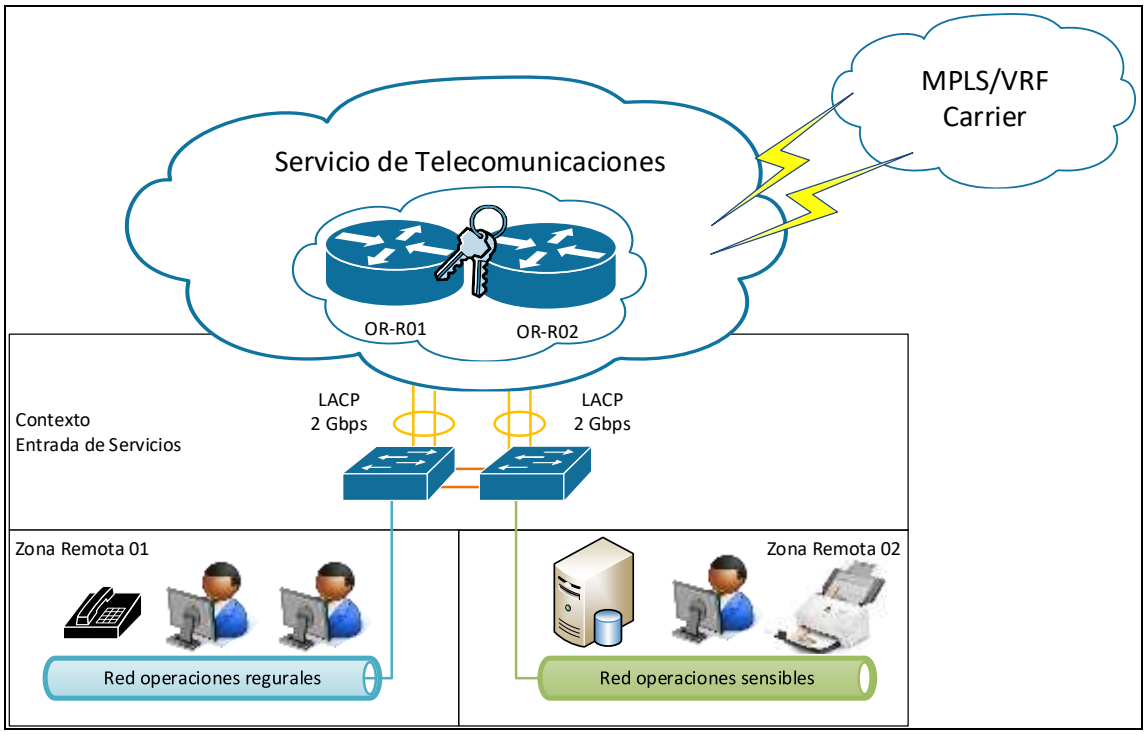
3.2.2.1.2. Definicion de topologia de red - Centro de Datos de Respaldo

La topología LAN diseñada tiene la finalidad de brindar un esquema de alta disponibilidad ante la pérdida de un elemento de red definido dentro de la topología. Se describe a continuación los elementos.



Elaboración Propia – Diagrama de topología física de centro de datos de respaldo

3.2.2.1.3. Topologia fisica de red para las sedes remotas.



Elaboración Propia – Diagrama de topología física de las sedes remotas

3.2.2.2 Topologia de red logica.

3.2.2.2.1. Direccionamiento de red de los centros de datos.

Centro de de Datos Principal

N°	Sementos CD Principal	VLAN	Zona	DIRECCION DE RED	GW de Destino	Costo o Prioridad
1	SERVIDORES01 - Func	221	Func - Principal	10.2.1.0/24	10.21.0.1	22
2	SERVIDORES02 - Func	221	Func - Principal	172.15.0.0/16	10.21.0.1	22
3	SERVIDORES03 - Func	221	Func - Principal	10.40.0.0/16	10.21.0.1	22
4	SERVIDORES04 - Func	221	Func - Principal	10.30.0.0/16	10.21.0.1	22
5	Internet - Func	221	Func - Principal	0.0.0.0/0	10.21.0.1	22
9	Telefonia	222	Telefonia - Principal	172.15.160.0/24	10.22.0.1	23
10	Telefonia	222	Telefonia - Principal	10.60.0.0/16	10.22.0.1	23
11	Telefonia	222	Telefonia - Principal	10.50.0.0/16	10.22.0.1	23
6	SERVIDORES01 - Electoral	223	Electoral - Principal	172.11.0.0/16	10.23.0.1	24
7	SERVIDORES02 - Electoral	223	Electoral - Principal	10.91.0.0/16	10.23.0.1	24

Centro de de Datos Contingencia

N°	Sementos CD Contingencia	VLAN	Zona	DIRECCION DE RED	GW de Destino	Costo o Prioridad
1	SERVIDORES01 - Func	224	Func - Contingencia	10.30.29.0/24	10.131.0.1	25
2	SERVIDORES02 - Func	224	Func - Contingencia	10.30.28.0/24	10.131.0.1	25
3	SERVIDORES03 - Func	224	Func - Contingencia	10.40.29.0/24	10.131.0.1	25
4	SERVIDORES04 - Func	224	Func - Contingencia	10.40.28.0/24	10.131.0.1	25
5	Internet - Func	224	Func - Contingencia	0.0.0.0/0	10.131.0.1	25
8	Telefonia	225	Telefonia - Contingencia	10.50.29.0/24	10.132.0.1	26
9	Telefonia	225	Telefonia - Contingencia	10.50.28.0/24	10.132.0.1	26
9	Telefonia	225	Telefonia - Contingencia	172.15.160.0/24	10.132.0.1	26
6	SERVIDORES01 - Electoral	226	Electoral - Contingencia	10.92.0.0/16	10.133.0.1	27
7	SERVIDORES02 - Electoral	226	Electoral - Contingencia	172.12.0.0/16	10.133.0.1	27

3.2.2.2.2. Direccionamiento de red de las sedes remotas.

N°	ODPE	DIRECCION DE RED MGM	MASCARA /24	DIRECCION DE RED Administrativa	MASCARA /24	DIRECCION DE RED Telefonia	MASCARA /24	DIRECCION DE RED Electoral	MASCARA /26
		VLAN 230 / UNTAGED IP Router 10.160.XX.(1 * float) 2 - 3		VLAN 231 / TAGED IP Router 10.170.XX.(1 * float) 2 - 3		VLAN 232 / TAGED IP Router 10.180.XX.(1 * float) 2 - 3		VLAN 233 / TAGED IP Router 10.190.XX.(1 * float) 2 - 3	
1	CHACHAPOYAS	10.160.1.0	255.255.255.0	10.170.1.0	255.255.255.0	10.180.1.0	255.255.255.0	10.190.1.0	255.255.255.192
2	BONGARA	10.160.2.0	255.255.255.0	10.170.2.0	255.255.255.0	10.180.2.0	255.255.255.0	10.190.2.0	255.255.255.192
3	BAGUA	10.160.3.0	255.255.255.0	10.170.3.0	255.255.255.0	10.180.3.0	255.255.255.0	10.190.3.0	255.255.255.192
4	HUARAZ	10.160.4.0	255.255.255.0	10.170.4.0	255.255.255.0	10.180.4.0	255.255.255.0	10.190.4.0	255.255.255.192
5	RECUAY	10.160.5.0	255.255.255.0	10.170.5.0	255.255.255.0	10.180.5.0	255.255.255.0	10.190.5.0	255.255.255.192
6	HUAYLAS	10.160.6.0	255.255.255.0	10.170.6.0	255.255.255.0	10.180.6.0	255.255.255.0	10.190.6.0	255.255.255.192
7	BOLOGNESI	10.160.7.0	255.255.255.0	10.170.7.0	255.255.255.0	10.180.7.0	255.255.255.0	10.190.7.0	255.255.255.192

3.2.3. Definicion de servicio de telecomunicaciones

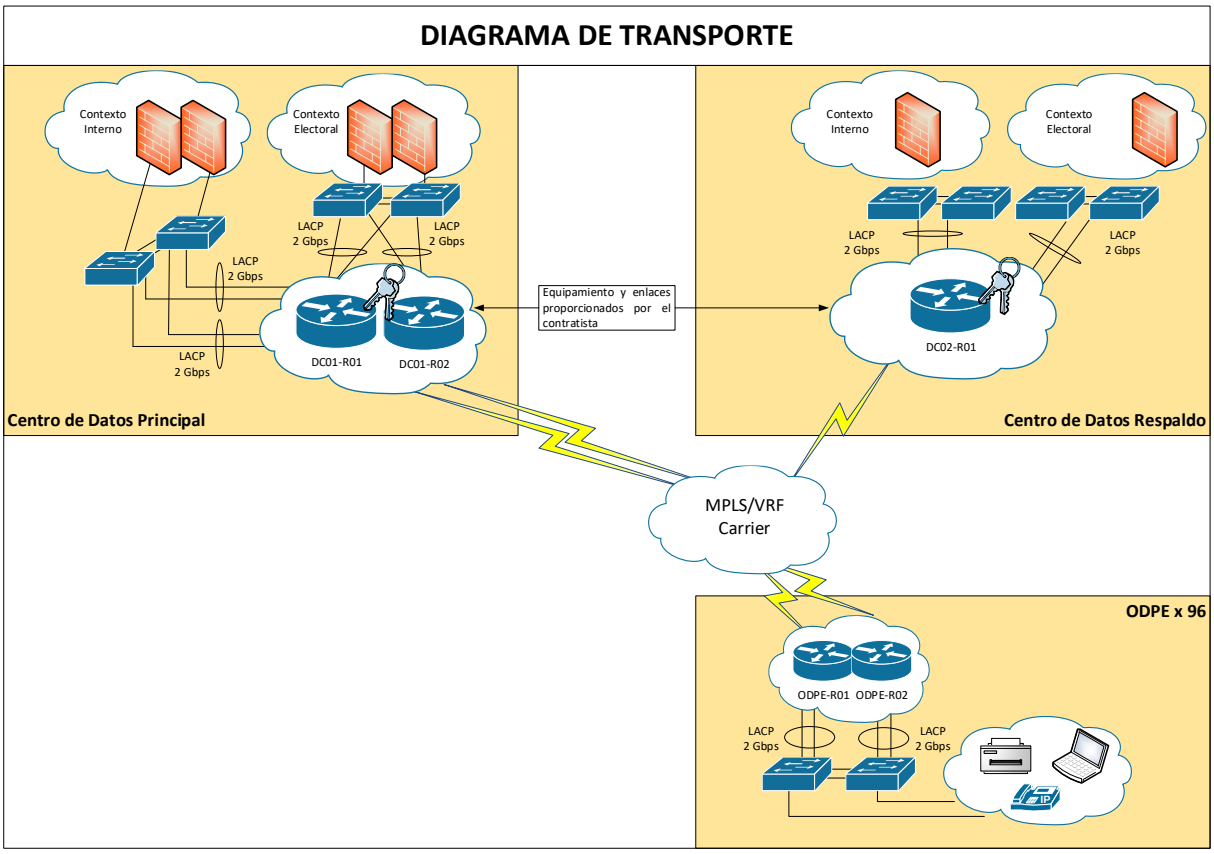
La topología WAN diseñada estaba basada en el modelo de estrella con la finalidad de control del flujo de datos, y se considera un esquema de basado en protocolo de enrutamiento BGP y OSPF para la detección de perdida de algún enlace o para la conmutación total de centro de datos.

3.2.3.1 Definición de topología de transporte

3.2.3.1.1. Zona de servicio de enrutamiento.

Zona de tipo WAN que conecta entre los centros de datos y las ODPE contra la nube (MPLS) del proveedor de servicio de telecomunicaciones.

Figura 26 Diagrama WAN de topología estrella para a interconexión de los Centros de Datos y las ODPE



Fuente: Elaboración Propia – Diagrama de interconexión de los centros de datos y las oficinas remotas a nivel de transporte.

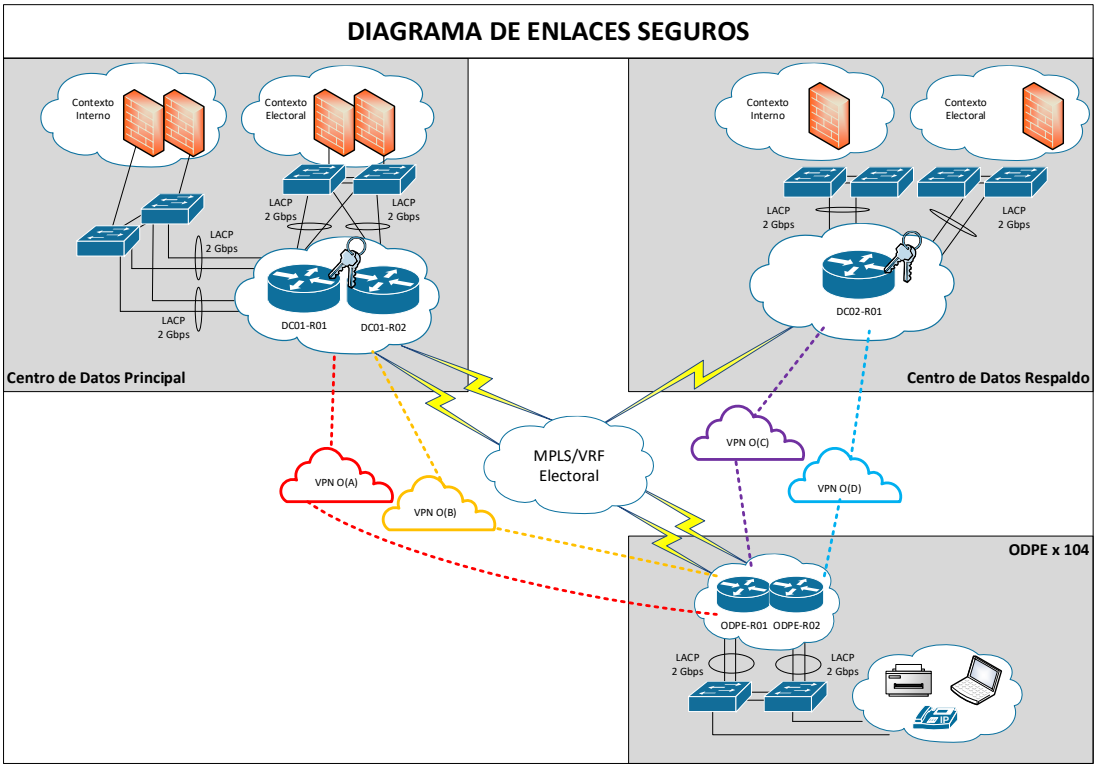
Nivel IP o Layer 3.

Para el ingreso de servicios a la red se considera la conexión a un dispositivo de capa 3, el cual se configurará el protocolo OSPF y la configuración BGP hacia una interface virtual para la detección de corte o perdida de conexión de algún enlace con la sede principal o contingencia, los números de área serán definidos durante la implementación.

3.2.3.2 Definición de topología enlaces seguros.

3.2.3.2.1. Zona de servicio de datos encriptados (VPN):

Zona de tipo WAN que conecta entre los Centros de Datos y las ODPE contra la nube privada dinámica generada entre los centros de datos de la ONPE.



Fuente: Elaboración Propia – Diagrama de interconexión de los centros de datos y las oficinas remotas a través túneles lógicos (enlaces seguros).

Encapsulado y Cifrado:

Este esquema de conexión se utiliza dispositivos de seguridad perimetral, conocidos como firewall el propósito de usar estos dispositivos es establecer enlaces seguros y controlados, incluyendo flexibilidad en la implementación e independiente del proveedor de servicio.

Para el funcionamiento de la solución de encapsulado y cifrado de información se componen de los siguientes elementos:

- ✓ Controlador VPN o Firewall (Data Center): Estos equipos son dedicados y debe considerarse uno por cada centro de datos, el funcionamiento permite administrar los túneles VPN.

- ✓ Firewall Remoto (ODPE): Este equipo es dedicado para establecer la comunicación de la oficina remita y sobre el medio que ya se ha establecido comunicación se crea un túnel de datos cifrado.
- ✓ Alta Disponibilidad: El funcionamiento del túnel dinámico, asocia los todos caminos disponibles hacia los destinos declarados, con la finalidad si se perdiera un enlace, se reestablece el túnel VPN, se precisa que para la detección de la pérdida de un enlace se utiliza el protocolo BGP y OSPF, así mismo la priorización del enlace principal sobre el enlace de respaldo.
- ✓ Administración centralizada: Este equipo permite administrar de manera centralizada el total de sedes remotas, facilitando la gestión y el monitoreo de una sola consola.

3.2.4. Diseño de controles de seguridad de red y monitoreo:

3.2.4.1 Definicion de controles de seguridad.

Se ha definido cinco (5) niveles de seguridad, los cuales se encuentran enmarcados en los principales servicios que se brindan dentro del proceso electoral.

- Nivel 1: Seguridad a nivel de red de datos (Canal de comunicación)
- Nivel 2: Seguridad a nivel de equipos de comunicaciones (switches, Routers)
- Nivel 3: Seguridad a nivel de servidores de aplicaciones
- Nivel 4: Seguridad a nivel de servidores de base de datos (sede central y sedes remotas)
- Nivel 5: Seguridad a nivel de estaciones de trabajo

3.2.4.1.1. Nivel 1: Seguridad a nivel de red de datos (Canal de comunicación)

- Los centros de cómputos se conectan al centro de datos principal y centro de datos de contingencia a través de enlaces privados.
- La transmisión desde los centros de cómputos se realizará por un canal seguro a los centros de datos principal y centro de datos de contingencia.
- Los enlaces de transmisión de datos entre los centros de cómputo y los centros de datos principal y contingencia son cifrados.

- El centro de cómputo de contingencia realizará la transmisión del procesamiento de las actas electorales mediante una comunicación segura (cifrada) hacia los centros de datos principal y contingencia.

3.2.4.1.2. Nivel 2: Seguridad a nivel de equipos de comunicaciones (switches, Routers)

- Los equipos de comunicaciones (Router) son administrados por el proveedor externo, quienes son los responsables del monitoreo de dicho equipo, cumpliendo con las políticas de seguridad establecidas por la ONPE.

- Los switch cuentan con usuarios locales con privilegios de administrador, para su monitoreo y administración.

- Los puertos de los switch están restringidos, con la finalidad de que solo los equipos registrados en el mismo puedan tener acceso a la red

- La gestión del equipamiento se realiza por canales cifrados

3.2.4.1.3. Nivel 3: Seguridad a nivel de servidores de aplicaciones

- La ONPE cuenta con los siguientes mecanismos de protección de seguridad para las aplicaciones internas, transmisión de resultados, y aplicaciones de acceso al público (página web y publicación de resultados), los cuales se mencionan a continuación:

  - Web Application Firewall (WAF)
  - IPS (Sistema de prevención de intrusos)
  - Firewall basado en análisis completo de paquetes
  - Monitoreo de seguridad de correlación de eventos

3.2.4.1.4. Nivel 4: Seguridad a nivel de servidores de base de datos (sede central y centros de cómputo)

- Los siguientes mecanismos de protección de seguridad para los servidores de base de datos, los cuales se mencionan a continuación.

  - IPS (Sistema de prevención de intrusos)
  - Firewall basado en análisis completo de paquetes
  - Monitoreo de seguridad de correlación de eventos

3.2.4.1.5. Nivel 5: Seguridad a nivel de estaciones de trabajo (Oficinas Remotas – Computadoras y Laptops)

- **Hardware**

- El acceso al BIOS de cada uno de los equipos informáticos (estaciones, laptop y servidores) está protegido por una contraseña.

- Se deshabilitará en el BIOS, el arranque del sistema por medios extraíbles o de red en todas las estaciones y servidores.

- **Software**

- Los usuarios con perfil de administrador, son los únicos autorizados de poder realizar cambios en la configuración de los equipos.

- Implementación de políticas a nivel local y de servicio de Directorio Activo según el perfil del usuario.

- Se tiene instalado en todos los equipos del centro de cómputo de la red electoral, un programa antivirus que es actualizado regularmente.

3.2.4.2 Elementos de seguridad de red y monitoreo.

Para el diseño de los controles de seguridad se tuvo que dividir en las siguientes secciones.

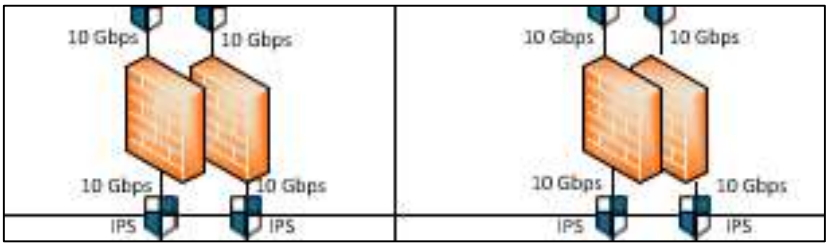
3.2.4.2.1. Protección de accesos no autorizados (Contrafuegos - Firewall):

La protección perimetral contra accesos no autorizados, tiene como objetivo solo permitir el tráfico de red declarado como permitido, es decir esta solución restringe los accesos a nivel de red solo permitiendo bajo reglas definida de entrada y salida, este control está basado en el principio de packet filtering, es decir L3 y L4, asimismo incluye el análisis de aplicaciones L7, detectado no solo el tráfico de red si no, las aplicaciones se encuentran autorizadas. La importancia del equipo se puede dividir en tres grupos.

El equipamiento tiene la característica de alta disponibilidad, está configurado en pares de equipos, por lo cual soporta a perdida de una miembro del clúster configurado.

La solución propuesta también es un equipo UTM, que permite asignar roles de trabajo, tales como Antivirus, DDoS, NLB, IPS y otros que no se atañes a la implementación descrita.

Figura 30 Protección de accesos no autorizados (Contrafuegos - Firewall):



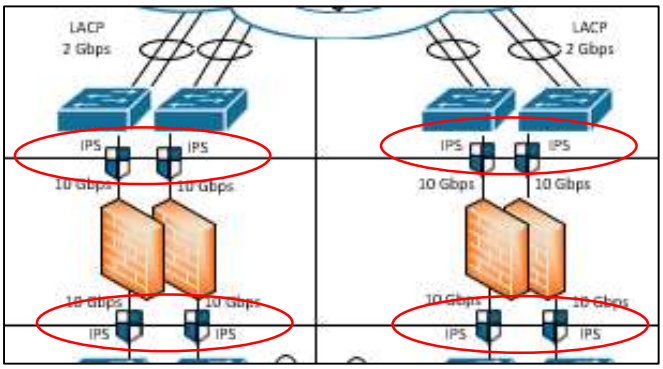
Fuente: Elaboración propia.

3.2.4.2.2. Prevención de Intrusos (IPS):

Equipo de seguridad que permite analizar el tráfico de red basado en firmas y patrones de comportamiento de tráfico, detectando el tráfico anómalo de la red.

El equipo preventor de intrusos tiene como finalidad detener los ataques basados en firmas y en el comportamiento del tráfico de red, así como también incluye un módulo de GTI que permite identificación temprana del tráfico anómalo, gracias al procesamiento.

Figura 31 Diagrama de Prevención de Intrusos (IPS)

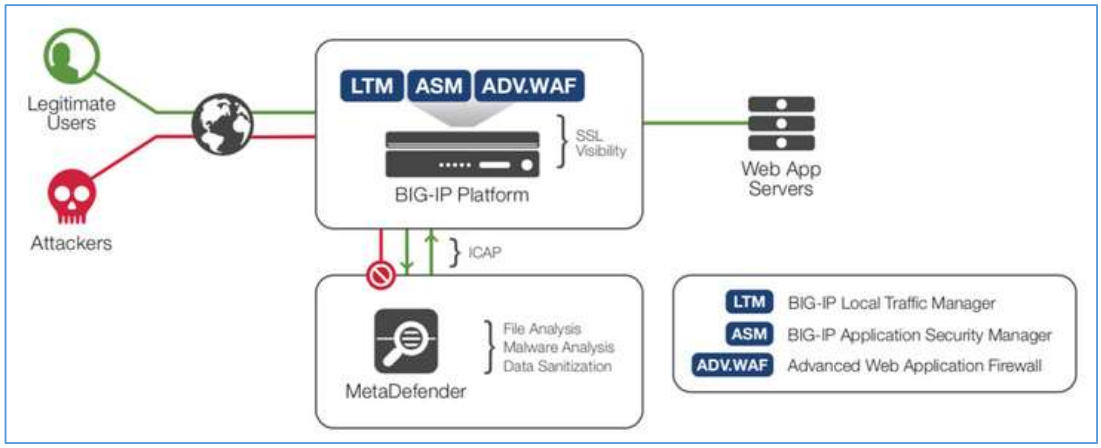


Fuente:

3.2.4.2.3. Protección de Aplicaciones Web (WAF):

El equipo protección de aplicaciones web tiene como finalidad la protección de las aplicaciones web, esto objetivo es alcanzado definiendo reglas de uso y de comportamiento de los estados y métodos utilizados por el protocolo HTTP, tales como los métodos GET, POST entre otros que se deben autorizar, asimismo como también la longitud de las de las URI, tamaño de las cadena de para recibir y enviar, también incluye la protección basadas en firmas conocidas de ataques a servidores web, tales como SQL Injection o Cross Site Scripting.

Figura 32 Diagrama de representación de trabajo del equipamiento de protección de aplicaciones web

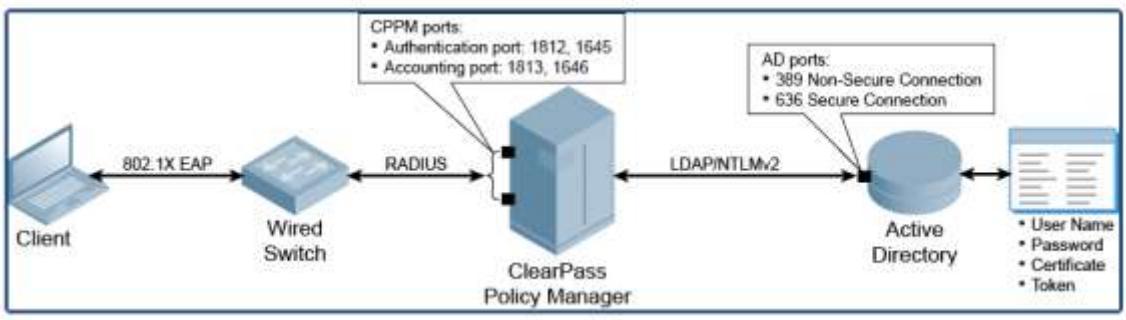


Fuente:

3.2.4.2.4. Protección de Control de Acceso a la Red (NAC):

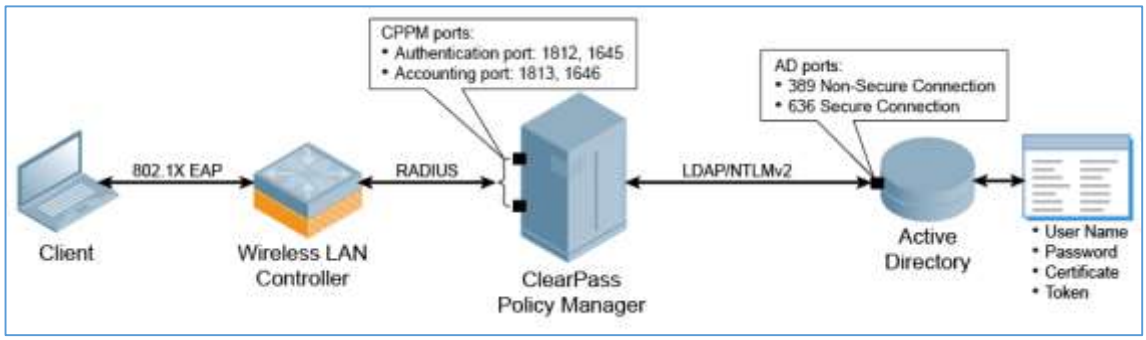
La solución de control de acceso a la red tiene como propósito el control de los puntos finales de conexión, agregando perfiles de validación para validar la autenticidad de las estaciones que serán conectadas a la red, asimismo de validar la integridad de la fiabilidad de la máquina, validando lo recursos de protección tales como los últimos updates desplegados.

Figura 33 Diagrama de representación del proceso de validación del medio de comunicación cableado contra el acceso el servicio NAC



Fuente:

Figura 34 Diagrama de representación del proceso de validación del medio de comunicación inalámbrico contra el acceso el servicio NAC.



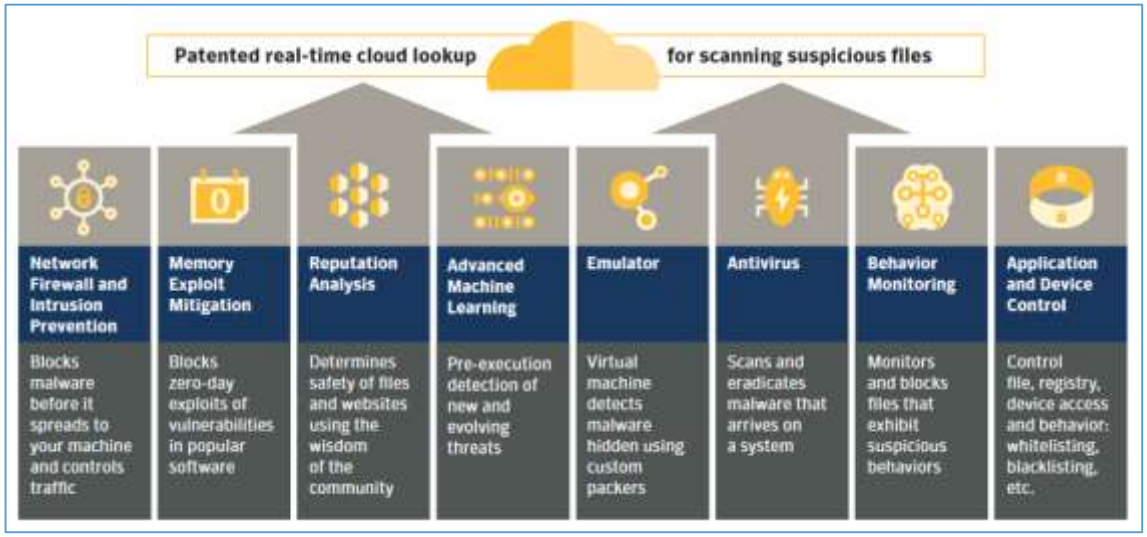
Fuente:

3.2.4.2.5. Herramienta de protección de código malicioso y control de dispositivos

Esta herramienta distribuida y de gestión centralizada, más conocida como antivirus de gestión centralizada, protege contra malware, troyanos y comportamiento anómalo de trafico de red para los dispositivos finales, es decir las estaciones de trabajo del personal y para los servidores.

El software de antivirus ahora también incluye el control de dispositivos, con la finalidad de prevenir infecciones no deseadas, por tal motivo incluyen este control, donde se registra los id de cada dispositivo para que se habilite.

Figura 35 Herramienta de Protección de Código malicioso y Control de Dispositivos



Fuente: https://www.broadcom.com/products/cyber-security

3.2.4.2.6. Correlacionador de Eventos (SIEM):

Esta herramienta tiene como finalidad recibir flujos de datos de log, donde se registra de manera centralizada de distintos puntos y/o dispositivos, con la finalidad no solo reportear los eventos, sino de hacer una análisis y predicción de comportamiento

Figura 36 Correlacionador de Eventos (SIEM).

Fuente: https://www.mcafee.com/enterprise/es-mx/products/enterprise-security-manager.html

Como parte del diseño propuesto se ha dispuesto la siguiente distribución Física y lógica con la finalidad de atender los requerimientos identificados, la cual se detalla a continuación para interconexión de los Centros de Datos y la ODPE.

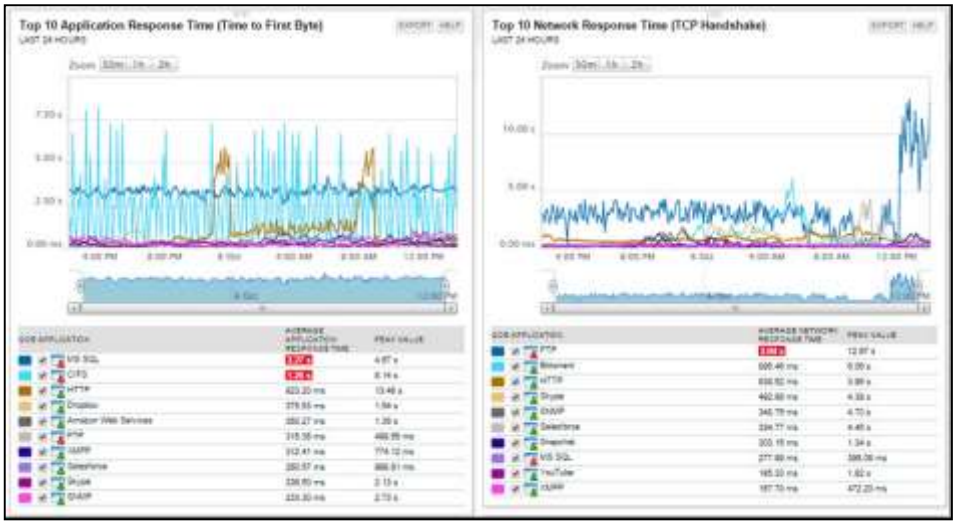
3.2.4.2.7. Monitoreo de dispositivos y aplicaciones (APM y NPM)

Esta herramienta permite el monitoreo del estado de salud de los dispositivos y su rendimiento, asimismo permite visualizar el rendimiento de las aplicaciones y sus dependencias con la finalidad de alertar oportunamente ante la variación del rendimiento o la ausencia de algún componente.

Figura 39 Diagrama de monitoreo de aplicaciones y sus dependencias

Fuente: https://www.solarwinds.com

Figura 40 Gráfico de monitoreo y estado de salud de los enlaces y la disponibilidad del dispositivo



Fuente: https://www.solarwinds.com

3.3. Gestión de riesgos SGSI

La gestión de riesgos permitirá a la alta dirección a tomar decisiones ante factores de riesgos que se puedan presentar, con la finalidad de cumplir los objetivos de la institución en base a los controles implantados. En tal sentido se debe efectuar la revisión y/o actualización de la metodología de gestión de riesgos aprobada por la institución.

3.3.1. Inventario de activos:

Se realiza un inventario de los activos de información involucrados en el desarrollo de la presente solución tecnológica. Éstos deberán ser clasificados y valorados (crítico, alto, medio, bajo). El inventario de activos se debe realizar haciendo uso de los formatos establecidos y aprobados por la institución.

3.3.2. Análisis de riesgos:

Nos sirve para conocer las consecuencias y la probabilidad de que algún riesgo se produzca, sin perder de vista los controles implantados. Estos parámetros nos servirán para establecer el nivel del riesgo.

3.3.3. Plan de tratamiento de riesgos:

Es una herramienta que proporciona las pautas necesarias para el adecuado tratamiento de los riesgos a los que están expuestos los activos de información, el cual permita

una adecuada toma de decisiones para disminuir la probabilidad que se materialice una amenaza.

3.3.4. Plan de monitoreo de riesgos:

Es una herramienta que se utiliza para gestionar activamente los riesgos de las soluciones tecnológicas implementadas o a implementar, las cuales pueden mermar su capacidad de alcanzar los resultados que la institución tiene planificado.

3.3.5. Enunciado de aplicabilidad:

Elaboración del informe de aplicabilidad alineado con la norma NTP-ISO/IEC 27001:2014 en el cual se detallarán los controles implementados o a implementar, así como las justificaciones de aquellos controles que no sean implementados.

3.4. Definicion de requerimientos y contratación de servicios.

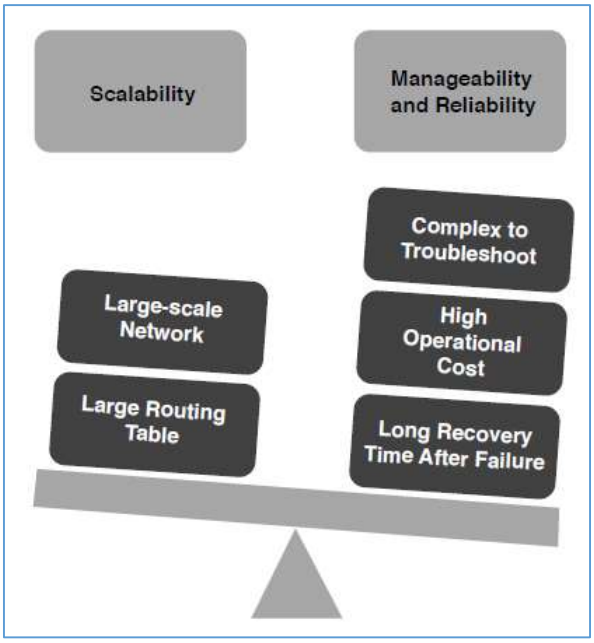
3.4.1. Definicion de requerimientos de equipamiento y servicios.

3.4.1.1 Selección de la Solución.

Dentro de los fabricantes evaluados, existía dos vertientes una era continuar con el modelo tradicional de equipamiento aislado o converger las tecnologías, por ello optamos por una solución convergente, permitiendo unir dos mundos de la simplificación en la gestión y la seguridad. Los fabricantes seguridad y comunicación, han utilizado este concepto de redes definidas por software para simplificar la gestión, de múltiples equipamientos, agregando valor a la detección temprana y fortaleciendo la infraestructura de seguridad tecnológica.

Como un punto dentro de la evaluación se tomaron documentos de referencia para el diseño de una red, el siguiente grafico mostro un resumen de la ponderación de la complejidad y la administración simplificada.

Figura 18 Representación de escalabilidad vs administración con fiabilidad



Fuente:

3.4.1.2 Network Fabric – SDN y SDWAN

De acuerdo a la evaluación de costo y beneficio de las características y permitiendo la pluralidad de postores, se encontró que la marca Fortinet, Cisco y otras soluciones combinadas, contemplan una solución orquestada que permite asegurar desde el punto del usuario final hasta la comunicación con el servidor, permitiendo asegurar las líneas de comunicación y brindando una flexibilidad entre múltiples medios de comunicación haciéndola redundante.

Para lograr este objetivo y ensamblar un Fabric Fortinet se compone de los siguientes elementos base para la interacción con el resto de los equipamientos.

Figura 19 Elementos de interacción necesarios para aplicación de una Fabric Fortinet.

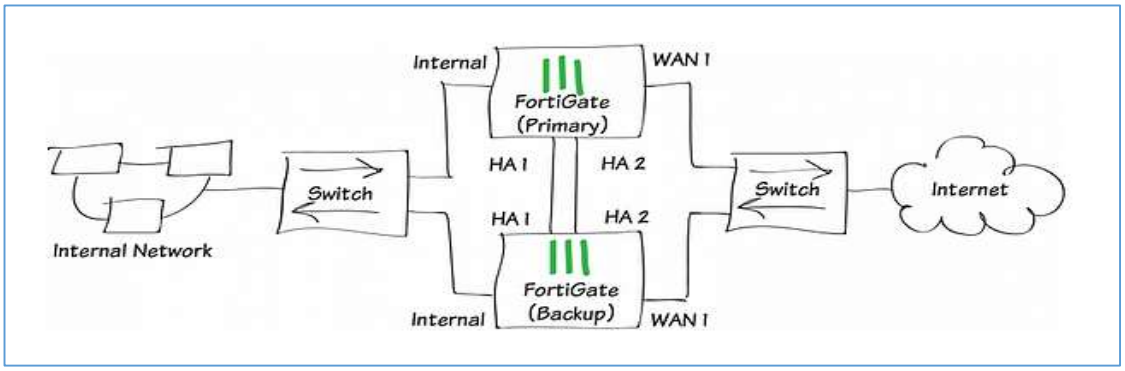
Fuente: https://www.fortinet.com

3.4.1.3 Solución de protección de perímetros (Next Generation UTM - Firewall)

Es un firewall con capacidad de análisis de Capa 7 – Aplicaciones, el modelo evaluado de acuerdo a capacidades históricas de trafico de red y considerando el peor escenario de full inspection, se consideró el modelo Fortigate 1500E para los centros de datos y para cada ODPE el modelo Fortigate 60E.

Dentro de sus características más resaltantes podemos decir que permite concentrar más de una funcionalidad requerida dentro del diseño a proponer en un solo equipo, así mismo la virtualización de instalación de firewall, propone también escenarios de alta disponibilidad. Estas características se desarrollarán dentro de la propuesta de la solución final.

Figura 20 Esquema de alta disponibilidad del Firewall



Fuente: https://www.fortinet.com

3.4.1.4 Fabric Switch

Los desafíos que enfrentan las LAN Ethernet existentes actualmente son más evidentes en la capa de acceso. Estos incluyen un crecimiento exponencial en el número de dispositivos y aplicaciones habilitados para la red, la innovación en LAN inalámbricas que requieren un mayor rendimiento y un diseño de LAN heredado que ha obligado a complejas implementaciones de seguridad "atornilladas". Este desafío se siente en pequeñas y medianas empresas, empresas distribuidas, sucursales y oficinas en el hogar. Los conmutadores FortiSwitch Secure Access Series ofrecen seguridad, rendimiento y capacidad de administración superiores en una amplia cartera de conmutadores de capa de acceso Ethernet seguros, simples y escalables.

3.4.2. Recursos necesarios

3.4.2.1 Cuadro de requerimiento de personal

Tabla 5 Recursos necesarios

Personal	
Rol	Cantidad
Jefe de Proyecto	1
Administrador de Red	2
Monitor de Red	4
Monitor de Firewall UTM	2

Fuente: Elaboración Propia

3.4.2.2 Cuadro de sedes a implementar

Tabla 6 Sedes a Implementar

Sedes	
Centro de Datos	2
Oficinas remotas (ODPE)	90

Fuente: Elaboración Propia

3.4.2.3 Cuadro de equipamiento requerido para los centros de datos (Principal y Contingencia)

Tabla 7 Cuadro de Equipamiento Requerido

Equipamiento Centros de Datos (Principal y Contingencia)			
Equipamiento	Cantidad	Nro. Sede	Cantidad x Sede
Fabric Manager (Capa de Orquestación)	1	2	2
Firewall Data Center - UTM	2	2	4
Switch Data Center (Core)	2	2	4
Switch Data Center (Distribución)	2	2	4
FortiAnalyzer	1	2	2
FortiSiem	1	2	2

Fuente: Elaboración Propia

3.4.2.4 Cuadro de requerimiento de equipamiento para las oficinas remotas

Tabla 8 Cuadro de Requerimiento de Equipamiento

Equipamiento Oficina Remota (ODPE)				
Equipamiento	Cantidad	Sede	Nro. Sede	Cantidad x Sede
Firewall Oficina Remota - UTM	2	Oficina Remota	90	180
Switch Borde (Acceso)	2	Oficina Remota	90	180

Fuente: Elaboración Propia

3.4.2.5 Cuadro de requerimiento de enlaces de comunicación para la interconexión con las sedes.

Tabla 9 Cuadro de Equipamiento Requerido

Líneas Dedicada - MPLS			
Sede	Nro. Sedes	Nro. Enlaces	MBPS
Data Center (Principal)	1	2	360 Mbps
Data Center (Contingencia)	1	1	360 Mbps
Oficina Remota	90	180	4 Mbps

Fuente: Elaboración Propia

3.4.2.6 Requisitos complementarios

- ✓ Licenciamiento del equipamiento a desplegar.
- ✓ Habilitación de las líneas de comunicación de los centros de datos y sedes remotas.
- ✓ Habilitación del cableado interno de red de datos en las oficinas remotas.
- ✓ Habilitación del cableado interno en los centros de datos.

3.4.2.7 Herramientas de control y de seguridad de red**:**

- ✓ Correlacionador de eventos de múltiples dispositivos, dentro y fuera del fabric.
- ✓ Fabric Manager LAN o SDN Controller: Capa de interacción de administración y cli.
- ✓ Fabric Manager WAN o SDWAN Controller: Capa de interacción de administración y cli.

Conclusiones

- Los analices de requerimientos de la operación y de seguridad del proceso de transmisión de datos dieron como resultados óptimos desde las oficinas remotas hacia los centros de datos.
- Se elaboró un diseño de la infraestructura de seguridad tecnológica el cual controlo todo el tráfico de red durante el proceso de transmisión de resultados, las cuales fueron alineados a la NTP –ISO/IEC 27001:2014.
- Se elaboró el plan de implementación de la infraestructura de seguridad tecnológica para controlar el tráfico de red durante el proceso de transmisión de resultados.

Referencias Bibliográficas

Arévalo, E. K. (2019). *Aplicación de las directivas de la NTP ISO/IEC 27001:2014 para la implementación de un sistema de gestión de seguridad de la información en el Centro de Gestión Tributaria de Chiclayo.* Lima.

Baldeón, M., & Zambrano, J. (2018). *IMPLEMENTACIÒN DE UN PROTOTIPO DE UNA RED DESCENTRALIZADA BLOCKCHAIN PARA EL VOTO ELECTRÓNICO EN LA UNIVERSIDAD DE GUAYAQUIL.* Guayaquil.

Bravo, S. (2013). *Tesis doctorales y trabajos de investigacion cientifica: Metodología general de su elaboración y documentación.* Madrid: Paraninfo, Décima edición.

Carballo, M., Guelmes, E. . (2016). Algunas consideraciones acerca de las variables en las investigaciones que se desarrollan en educación. *SciELO* , (p. 6).

Carrasco, L. (2009). *Metodoligía de investigación científica.* Lima: Editorial San Marcos.

Castro Siguas, J. J. (2018). *IMPLEMENTACIÓN DE LA NTP ISO/IEC 27001:2014 PARA MEJORAR LA GESTIÓN DE LA SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN DE LA AUTORIDAD PORTUARIA NACIONAL, CALLAO - 2017.* Lima.

Constitución Política del Perú. (2017). Lima: Congreso de la República.

Espinoza, E. (2018). *La Hipótesis en la investigación.* Machala: Universidad Técnica de Machala.

Espinoza, E. (05 de ABRIL de 2018). LAS VARIABLES Y SU OPERACIONALIZACIÓN EN LA INVESTIGACIÓN EDUCATIVA. *CONRADO, Revista pedagógica de la Universidad de Cienfuegos*.

Espinoza, F. (2018). *La hipótesis en la investigación. d*isponible en http://mendive.upr.edu.cu/index.php/MendiveUPR/article/view/1197.

Fariza, A. (2016). *Computer Hoy.* Obtenido de https://computerhoy.com/noticias/internet/metadatos-fotografia-que-son-datos-exif-38347

Feirherd, G. et al. (2002). *Una aproximación a los requerimientos del software de voto elecxtrónico de Argentina.* Argentina: Instituto de Investigación Informática LIDI.

Grau, R., et al. . (2004). *Metodología de la investigación.* Ibagué: Universidad de Ibagué.

Hernández, R. Fernández, C. y Baptista, L. (2014). *Metodología de la Investigación.* México: Mc Graw Hill.

Oficina Nacional de Procesos Electorales. (2012). *Historia del voto electrónico, Perú 2005-2012.* Lima: P. 124.

Oficina Nacional de Procesos Electorales, O. (01 de mayo de 2017). *Voto electrónico*. Obtenido de www.ONPE.com: www.ONPE.com

Palella, M. (2016). *Metodología de la investigación cualitativa.* Caracas: FEDEUPEL.

Pesado, P., et al. (S/F). *E-Goverment: El voto electrónico sobre internet. .* México: Instituto de Investigación en Informática.

Pesado, P., Feirerhhd, G., y Pasini, A., . (S/F). *Especificcaión de requerimientos para sistema del voto electrónico.* Instituto de Investigación Informática LIDI.

Picasso, M., Prado, L. (03 de enero de 2012). *Ciencias de la comunicación*. Recuperado el 03 de septiembre de 2018, de Aldea Global: www.cienciasdelacominicación.com

Piña, G. (2013). *Implementación de seguridad en la infraestructura de red para la difusión del Programa de resultados electorales preliminares 2017 en el estado de Máxico bajo la norma ISSO/IEC 27001:2013.* México: Universidad Autónoma del Estado de México.

Plethora. (2018). Obtenido de http://consulta-psicologica.com/diccionario-de-psicologia/206-comportamiento.html

Prince, A. ((S/F)). Consideraciónes, aportes y experiencias para el voto electrónico en Argentina. *Investigación periodistica Enrique Garabetyan*.

Quintero, J. (2017). *Elaboración de las políticas de seguridad de la información para el Consejo Nacional Electtoral de Ecuador.* Ecuador: Universidad de Cuenca.

Quintero, J., y Poz, J., . (2017). Beneficioes de la palicación de normas internacional ISSO en procesos electorales. . *Revista de Derecho Electoral*, 1-18.

Reniu, J. (2008). Ocho dudas razonables sobre la necesidad del voto electrónico . *Revista de internet Derecho y Política* , 32-44.

Revista Urvio. (2015). Comparativo histórico del sicariato en América Latina. *Revista Latinoamericana de Seguridad Ciudadana URVIO*, 7-167.

Reza, L., et al. . (2018). El TDAH y su repercusión en el rendimiento académico. *Revista Atlante: Cuadernos de Educación y Desarrollo*, EUMED.

Sabino, C. (2014). *El proceso dela investigación.* Guatemala: Editorial Episteme.

Thompson, J. (2009). La experiencia reciente del voto electrónico en América Latina: Avances y perspectivas. (P. 1-35).

Tobón, R. M. (2018). *Citizen security in Latin America: Facts and Figures.* Rio de Janeiro: Igarapé Institute. Obtenido de https://igarape.org.br/wp-content/uploads/2018/04/Citizen-Security-in-Latin-America-Facts-and-Figures.pdf

Velaverde, C. (2016). *Implementación del voto electrónico en Perú: algunas reflexiones para su viabilidad.* Perú.