FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Propuesta de Sistema de Gestión de Seguridad de la Información para garantizar la Seguridad de la Información en la Sub Gerencia de Tecnología de la Información del Gobierno Regional de La Libertad

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
Ingeniero de Sistemas

AUTORES:

Cornejo Miranda, Alex Jhonatan (ORCID: 0000-0001-8723-6355)

Lezama Calvo, Arturo Ramón (ORCID: 0000-0002-9593-8426)

ASESOR:

Dr. Pacheco Torres, Juan Francisco (ORCID: 0000-0002-8674-3782)

LÍNEA DE INVESTIGACIÓN:

Auditoria de Sistemas y Seguridad de la Información

Trujillo – Perú

2022

DEDICATORIA

A Dios por ser nuestro creador, nuestro amor incondicional; nuestros logros son parte de su gratitud y por la ayuda que nos brinda día a día.

A nuestros padres, pues son la fortaleza de los pasos de nuestra vida, inculcando en nosotros el respeto, la responsabilidad y anhelo de superación; logrando en nosotros las personas que somos actualmente, todos nuestros logros se los debemos a ustedes implicando este.

Cornejo Miranda, Alex Jhonatan

Lezama Calvo, Arturo Ramón

AGRADECIMIENTO

A nuestros docentes, que nos han permitido llegar al camino de nuestra enseñanza, por los buenos consejos y el gran conocimiento que han implantado en nosotros para poder llegar a donde estamos ahora.

A nuestros asesores, por habernos ayudado a completar con éxito esta gran tesis con sus apoyos y sus grandes conocimientos.

Cornejo Miranda, Alex Jhonatan

Lezama Calvo, Arturo Ramón

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE FIGURAS

RESUMEN

La presente investigación tiene como objetivo general Garantizar la Seguridad de la Información en la Subgerencia de TI del GRLL con la Implementación de un sistema de gestión de seguridad basado en NTP-ISO/IEC 27001, se utilizó el diseño de investigación experimental y del tipo preexperimental, la población en estudio fueron los 11 trabajadores del área de tecnologías de información y se utilizó la prueba de normalidad de Shapiro Wilk; además se utilizó la norma técnica peruana ISO 27001 para la realización de la investigación, finalmente se concluye que el nivel de integridad de la información con respecto a la seguridad de la información con el sistema actual se obtuvo una puntuación de 1.80 puntos, mientras con la implementación del sistema propuesto es de 4.33 puntos, obteniendo un incremento del 50.60% sobre el nivel de integridad de la información sobre el personal del área tecnologías de información; en el segundo indicador se concluye que el nivel de confidencialidad de la información con respecto a la seguridad de la información con el sistema actual se obtuvo una puntuación de 1.82 puntos, mientras con la implementación del sistema propuesto es de 4.49 puntos, obteniendo un incremento del 53.40% sobre el nivel de confidencialidad de la información sobre el personal del área tecnologías de información; y por último se cuenta una escala del 1 al 5 para medir el nivel de uso de nuevas políticas de seguridad, se obtuvo con el sistema actual de 1.80 puntos y con la implementación propuesta sobre el nivel de uso de nuevas políticas de seguridad es de 4.76 puntos, alcanzando un incremento de 2.96 puntos equivalente al porcentaje de 59.20%.

Palabras clave: Sistema de Gestión de Seguridad, Norma Técnica Peruana, Seguridad de la Información.

ABSTRACT

The general objective of this research is to guarantee Information Security in the IT Sub-Office of the GRLL with the implementation of a security management system based on NTP-ISO / IEC 27001, the design of experimental research and the pre-experimental type was used , the population under study was the 11 workers in the information technology area and the Shapiro Wilk normality test was used; In addition, the Peruvian technical standard ISO 27001 was used for the realization of the investigation, finally it is concluded that the level of information integrity with respect to the information security with the current system was obtained a score of 1.80 points, while with the implementation of the proposed system is 4.33 points, obtaining an increase of 50.60% on the level of integrity of the information on the personnel of the information technologies area; in the second indicator it is concluded that the level of confidentiality of information with respect to information security with the current system was scored 1.82 points, while with the implementation of the proposed system is 4.49 points, obtaining an increase of 53.40% on the level of confidentiality of information about personnel in the information technology area; and finally, a scale of 1 to 5 is used to measure the level of use of new security policies, was obtained with the current system of 1.80 points and with the proposed implementation on the level of use of new security policies is 4.76 points, reaching an increase of 2.96 points equivalent to the percentage of 59.20%.

Keywords: Security Management System, Peruvian Technical Standard, Information Security

I. INTRODUCCIÓN

La ISO es una organización independiente y no ligado a ningún gobierno, con una cantidad de miembros de 162 organismos nacionales de normalización. Reúne un conjunto de expertos los cuales comparten amplia información para desarrollar conocimiento y normas que den soluciones mundiales, encontrándose su secretaria general en ginebra (Suiza). En 1946 cuando 25 países enviaron a sus delegados, se congregaron en el colegio de ingenieros civiles en Londres y acordaron la creación de una organización internacional, el 23 de febrero de 1947(ISO, 2015).

La norma ISO 27001 permite que se certifiquen las empresas, buscan que las empresas cumplan con los 130 parámetros que establece la norma. Existen 8 pasos para conseguirla: 1) Tener compromiso de los niveles de alta directivos, 2) Participación Colectiva, 3) Comparar el sistema de seguridad actual con el de la norma ISO27001, 4) pedir explicaciones de los Proveedores o clientes sobre la seguridad de la información, 5) Definir un equipo de trabajo para adaptar el sistema de gestión de Seguridad de información, 6) La implantación por sí sola no Basta, 7) Compartir los Conocimientos con los trabajadores, 8) Revisión periódica del Sistema de Gestión de Seguridad de la Información (SGSI, 2016)

La Dirección de normalización, siendo la encargada de aprobar Normas Técnicas Peruanas y siendo miembro de la Organización internacional de Normalización (ISO), la cual representa al país y es parte del Codex , el Instituto Nacional de la Calidad (INACAL) aprueba en los sectores económicos y de diversas actividades, generando así el NTP-ISO/IEC 27001 con el sistema 1, durante los meses de junio del 2014, la NTP-ISO/IEC 27001 la cual se realizó gracias a la participación del comité técnico para la normalización, codificación y distribución de datos, para su confección se usó como ejemplo la norma ISO/IEC 27001:2013 los encargados de la elaboración presentaron a la Comisión de Normalización y a la vez de Fiscalización de Barreras Comerciales no Arancelarias(CNB) en la fecha 2014-08-19, siendo en Discusión Pública el 2014-10-18 (INACAL, 2020)

Siendo oficializada como (NTP, 2014). En la actualidad el Gobierno Regional la Libertad no cuenta con un Sistema de Gestión de Seguridad de la Información, encontrándose la información desprotegida previamente se identificaron los siguientes problemas específicos en el GRLL los cuales son:

La facilidad de acceso a la información, se debe al poco control en el acceso de usuarios debido a políticas incompletas, lo que pone en riesgo de manipulación de la información por parte del personal o de terceros.

La facilidad al acceder a la información, debido al poco control en el acceso de los usuarios debido a las políticas de seguridad incompletas deja saber que existen riesgos de manipulación de la información por parte del personal o de terceros.

Acceso no autorizado de la información, debido a que la información estando disponible al personal que, rota a otras áreas, esto genera que un riesgo de divulgación de la información.

Se genera una demora al realizar la petición para acceder a la información por no estar disponible y estar desactualizada.

No tener políticas de seguridad para la información alineadas a la **RM N° 004** (PCM, 2016)**; y que a la letra indica …"se admite el uso obligado de la NTP ISO/IEC 27001:2014** en todas las instituciones del Sistema Nacional de Informática"; acarrea una fuerte debilidad en el sistema de seguridad.

Según el autor (QUINTANA, 2008), planear el problema es perfeccionar y organizar acertadamente la idea de investigación. En este contexto, se planteó el problema siguiente: ¿De qué manera la Implementación de un sistema de gestión de seguridad basado en NTP-ISO/IEC 27001 influyó en la Seguridad de la Información en la Subgerencia de TI del GRLL en el periodo 2021?

La justificación de la investigación (BERNAL, 2018), se justifica ya que en la Sub Gerencia de la Tecnología de la Información del Gobierno Regional la Libertad no tiene un Sistema de Gestión de Seguridad de la Información eficiente, este sistema le facilitará conseguir un estudio de los procesos que se dan en el manejo de la información crítica, para ello se debe tener presente las normas vigentes para dichos procesos. Cuando se implemente dicho sistema permitirá que la institución está protegida para el manejo de la información.

Se debe tener en consideración los peligros en que pueden estar expuestos la información de las instituciones, otro peligro latente son los continuos cambios de la normativa de carácter obligatorio para todas las instituciones públicas y privadas que deban hacer uso de cierta información privada de estos procesos, para ellos se plantea la implementación de un SGSI lo que permite tener una visión clara de los lineamientos y procedimientos que van a ser necesarios para reconocer y evaluar las posibles amenazas y riesgos en la información que deben estar alineadas por un SGSI que plantea las especificaciones que se requiere en la legislación actual: según la **Resolución ministerial N°004-2016/PCM: que define el uso obligatorio de la NTP ISO/IEC 27001:2014** las instituciones públicas y privadas del Sistema Nacional de Informática.

Por otro lado, el objetivo general, *se enuncia para resumir y detallar trabajos a efectuar por el investigado* (GONZÁLEZ, 2011)*,* se tiene como propósito de garantizar la seguridad de toda la información en la subgerencia de TI del GRLL con la Implementación de un sistema de gestión de seguridad basado en NTP-ISO/IEC 27001; asimismo, los objetivos específicos fueron: a) Incrementar el nivel de Integridad de la información; b) incrementar el nivel de confidencialidad de la información de manera controlada; c) incrementar el nivel de disponibilidad de la información d) incrementar el nivel del uso de nuevas Políticas de Seguridad aplicando la NTP ISO/IEC 27001:2014.

La hipótesis, es una idea que puede no ser positiva, basada en información previa (Espinosa, 2018), se menciona la Implementación de un sistema de gestión de seguridad basado en NTP-ISO/IEC 27001 garantizó significativamente la Seguridad de la Información en la Subgerencia de TI del GRLL.

II. MARCO TEÓRICO

Como antecedente, en el ámbito **Internacional,** AGUIRRE y ARISTIZÁBAL, (2014), quienes plantearon su estudio frente al aumento del número de atacantes virtuales a las redes y los sistemas de instituciones públicas y privadas, un 46% de clientes u usuarios consigna haber recibido un email fraudulento que proviene de servicios de correo electrónico seguros ejemplo de esos servicios son Microsoft y Gmail. Las redes sociales con un 45%, los bancos 44% y tiendas en línea 37%. Otras organizaciones y los juegos de pc o móviles se sitúan en las últimas posiciones con 27% y 25% respectivamente, por otro lado, se presentan ataques internos las estadísticas afirman que entre el 70% y 80 % de los ataques virtuales a una red son de la misma institución, datos que se obtiene de la última encuesta hecho por ESET Latinoamérica. Los administradores consumen muchas horas de trabajo para impedir dichos ataques internos puesto que es muy complicado proteger la red desde dentro en comparación a cuando se tiene que defenderla de ataque que provienen de afuera de la red. Se concluyó que es importante salvaguardar la seguridad de la información frente a los ataques frecuentes que ocurren en la red.

A nivel **Nacional,** ALCÁNTARA, (2015), la investigación tiene como objetivo elaborar una guía de implementación para la seguridad tomando como base para su elaboración a las normas ISO/IEC 27001, con lo cual se garantice la seguridad en los sistemas para la información de una institución policial. Para obtener la información se tomó en cuenta el uso de diferentes técnicas de recolección de los datos como son las entrevistas, fichas de observación, encuestas, para extraer la información requerida y luego su análisis e interpretación y de tal forma que se pueda medir con la realidad problemática que se basa en el uso de las Normas ISO/IEC 27001, con lo cual se determinas cuáles son las deficiencias y luego incrementar la seguridad y confiabilidad del sistema de información de la organización policial. Con los resultados que se han obtenido se ha podido determinar que después de implementar la guía basada en la norma ISO/IEC 27001 se incrementó un 68% en los procesos que se han utilizados en favor de la organización policial lo cual permitió la detección oportuna de las anomalías en la seguridad de la información, lo cual permitió realizar diferentes mecanismos

de seguridad para protegerlas de distintos ataques tanto desde dentro como afuera de la red.

Con la ejecución del plan de riesgos, se logró una disminución significativa de los niveles de riesgos de la información de la organización policial, se consideraron diferentes amenazas y vulnerabilidades con las cuales se tiene que afrontar la institución, esta guía es una referencia para la realización de un plan con lo cual se pueda contratacar y tomar ciertas precauciones que disminuyen o anulen los impactos de estos ataques digitales a la información. Para finalizar debemos obtener con el plan de capacitación y concienciación se logró el aumento en los niveles de conocimiento del personal en temas que se orientan en las políticas y estrategias de seguridad que puedan beneficiar a los miembros de la organización policial.

Para una correcta implementación de la guía que se está elaborando en la presente investigación lo cual logrará el aumento en el porcentaje de la seguridad en los sistemas informáticos de la organización policial, esto se manifiesta en las políticas de seguridad que benefician a la organización y permiten el incremento de los niveles de seguridad de las mismas.

En el plano **Local,** YAN (2015), tuvo como objetivo la creación de un plan de mejora de la seguridad para la información y continuidad para el centro de datos de la institución y luego reportar los resultados que se han obtenido para la auditoria de sistemas, se utilizó la metodología de sistema MAIGTI, también se utilizó los lineamientos de las normas ISO 27001 y COBIT 4.0. Primero se da la revisión de la situación de cómo se encuentra el centro de datos del GRELL, luego se procede a la selección de los diversos procesos para el control que son los más indicados según la norma ISO 27001 y COBIT 4.0 que se deben ajustar a las diferentes situaciones que se presentan en el centro de datos, es en donde se evaluará y se darán las recomendaciones necesarias. Posteriormente se darán a conocer los resultados de la auditoria con un informe técnico de las situaciones encontradas y luego se entregarán las conclusiones necesarias por cada proceso que fue evaluado. A continuación, se procede a una mejora de los planes de seguridad como es la implementación y ejecución de un sistema de gestión para la información y a la vez de tener un plan de continuidad de negocio

con fases y un plan de normalización. Como resultado de la investigación se tiene que ayudó a comprender la implementación de una estrategia de la seguridad en la información.

Para ZAVALETA (2016), cuyo objetivo fue el de garantizar mediante la implementación de un sistema de gestión la seguridad de la información en el sector hospitalario en base a los requerimientos NTP ISIEC 27001:2014 con lo cual se logrará el desarrollo de un informe actualizado de los procesos más importantes que están involucrados en el manejo de la información crítica y el análisis y diseño de un SGSI de cualquier institución del sector hospitalario, se debe tener en consideración el cumplimiento efectivo de las distintas normas vigentes que se aplican en estos casos críticos. La investigación tuvo una forma proyectiva, su diseño es no experimental, holístico y mixto. Para la recolección de datos se utilizó la técnica de la entrevista y como instrumentos se usó la encuesta, la cual se aplicó a 15 trabajadores de la Oficina de admisión e informática. Como resultado se comprobó que hay una gran disposición para la implementación del sistema con un 93.33%, con lo cual se indica que existe un porcentaje alto para la implementación y ejecución del SGSI.

Según De La Cruz (2016), cuyo objetivo principal fue proponer propuestas políticas que se basen en buenas prácticas de gestión de seguridad para la información en una Municipalidad provincial. La investigación tuvo un tipo y diseño de investigación no experimental, descriptivo, con un corte transversal cuantitativo, la muestra de estudio estuvo conformada por 152 empleados se utilizó para la obtención de la información se aplicó un cuestionario y la encuesta conformado por 10 items. Los resultados obtenidos son un 72.37% de los trabajadores municipales comentan que Sí están propensos y expuestos a ciertos riesgos y amenazas, otro resultado de vital importancia es que el 100% de los trabajadores municipales que fueron encuestados comentaron que No hay controles adecuados de seguridad de la información. Se concluye que la Municipalidad no cuenta con políticas y controles eficientes con lo cual se demuestra que se debe implementar un sistema que permita reducir o eliminar en su totalidad la perdida de la información.

Las teorías relaciones con las variables de investigación como el Sistema de Gestión de la Seguridad de la Información está basado en procedimientos, políticas, directrices, actividades y recursos que son organizados y gestionados en forma grupal por una institución que desea proteger la información de su institución. Podemos definir a un SGSI (INACAL, 2020) como un enfoque sistemático que sirve para establecer, monitorear, ejecutar, implementar, mantener, supervisar, mejorar y evaluar la seguridad de la información de las instituciones que permitan el logro de las metas y objetivos de su negocio. Las SGSI se basan en el análisis y la evaluación de los riesgos y la aceptación de dichos riesgos de las instituciones con porcentajes diseñados para su tratamiento y gestión de manera eficiente y efectiva. Es fundamental el análisis de los requisitos para una adecuada protección de la información y a la vez la ejecución de controles que sean los más indicados para garantizar la protección de dichos datos, con lo cual se de una implementación exitosa de un SGSI.

En este sentido, la norma internacional ISO 31000 brinda los principios y guía sobre la gestión de riesgos. (EALDE, 2017) Es una Norma de carácter Internacional que debe ser utilizado en todas las organizaciones públicas o privadas, dicha norma no es específica para cualquier institución de los diferentes sectores productivos.

La presente Norma podrá ser ejecutada durante todo el ciclo de vida de una institución y a la vez poder ser usada en distintas actividades operaciones, procesos, estrategias, decisiones, funciones, proyectos, activos, servicios o productos, también es aplicable a cualquier tipo de riesgo. A pesar que la Norma proporciona una guía genérica, no debe promover la uniformidad de los riesgos de la gestión en las instituciones, más bien se aplicará para lograr una armonía en los procesos de gestión de los riesgos vigentes y las que pueden surgir en un futuro. Por último, debe facilitar un determinado enfoque común de apoyo a las normas que tienen que ver con los riesgos que son específicos a determinados sectores y no deben usarse para sustituir a las normas NTP-ISO/IEC 27001 :2014 NTP-ISO :2011.

Por otra parte, la NTP-ISO/IEC 27001:2014 fue diseñado por un Comité Técnico de Normalización de Codificación e intercambio electrónico de datos, en base al

Sistema 1 o conocido también como de Adopción, que fue realizado en los meses de abril a junio del año 2014, para su realización se usó como precedente a la norma ISO/IEC 27001:2013.

En ese sentido, la estrategia de las elipses identifica los activos de información con que se cuenta en la institución. La elipse concéntrica se determina los subprocesos que componen el alcance, en la elipse externa se encuentran aquellas instituciones extrínsecas de la empresa que cuenta con cierto tipo de

se identifican aquellas organizaciones extrínsecas a la empresa que tienen cierto tipo de acción con los subprocesos que son encontrados en la elipse concéntrica. Las flechas señalan la interacción entre los subprocesos y los grupos de interés (Bernardo, 2018).

Por otro lado, el análisis FODA permite realizar una evaluación de los distintos fortalezas y debilidades que se encuentran dentro de las instituciones y las oportunidades y amenazas que se encuentran fuera de estas, son en su conjunto los que permiten hacer un diagnóstico de la situación interna y externa de una institución, también es una herramienta que puede ser considerada sencilla que nos permite tener una perspectiva global de la situación estratégica una institución. Para (Thompson y Strikland, 1998) el análisis FODA es una evaluación que va a estimar el efecto que una técnica o estrategia puede conseguir un equilibrio o ajuste entre la capacidad interna y externa.

En la gestión pública el valor de la transparencia es un principio fundamental de la democracia, para que dicha transparencia exista se debe difundir todos los actos y resultados de las instituciones estatales, esto se debe dar a través de varios medios o canales de difusión con el fin de que cualquier ciudadano pueda ser partícipe de la administración pública.

La transparencia, en tal sentido, es un instrumento que mejora la relación entre el Estado y la sociedad debido a que obstaculiza los casos de corrupción y, a la vez, actúa como un incentivo para conseguir la eficacia en conjunto con la eficiencia de la función gubernamental. El Decreto Supremo N.º 063-2014-PCM

Por tanto, el acceso a la Información que es de carácter público es imponderable, ya que la información que pertenece al Estado es de índole público es un grupo de información que es administrada por las entidades estatales, incluyendo a gobiernos locales y regionales. Por lo general es la documentación que está anexada al presupuesto fiscal, actas de reuniones de trabajo oficiales, dictámenes, presupuestos de obras, informes técnicos, normas internas, entre otros. (SGP, 2014).

Con excepción de los asuntos de naturaleza secreta, reservada o confidencial, el resto de los manejados por el Estado deberían encontrarse al alcance de cualquier peruano o peruana que desee conocerlos. Se debe considerar que el acceso a la información pública es derecho de todos los individuos dentro de un Estado, se considera un requisito importante de una sociedad democrática.

En el marco legal que sostiene este proceso se tiene la (Ley N° 27806, 2014): Ley de Transparencia y Acceso a la Información Pública, cuyo fin es el de promover la claridad de todos los actos que se realizan en el Estado y es el que regula el derecho primordial del acceso a toda información que según el numeral 5 del artículo 2 de nuestra Constitución. El derecho fundamental de acceso a la información que tenemos de los miembros del poder Legislativo se norma de acuerdo al Reglamento del Congreso y la Constitución Política de nuestro país.

Por otro lado, mediante la Resolución Ministerial (N° 004 - PCM, 2016): Donde se aprueba la obligatoriedad del uso de la NTP ISO/IEC 27001:2014. Que es el preservar sobre todo la confidencialidad, la integridad y sobre todo la disponibilidad de la información, así como de aquellos sistemas implicados en el tratamiento de una organización.

Asimismo, la Resolución Gerencial (N° 2219-GRLL-GOB, 2016), Norma General Regional que regula el procedimiento para la publicación y actualización de la información en el Portal de Transparencia del Gobierno Regional La Libertad, cuya finalidad es mantener actualizada la información de transparencia en los portales de las Unidades Ejecutoras del Gobierno Regional de La Libertad.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

3.1.1. Tipo de investigación: Aplicada.

Se determina porque busca la aplicación o manejo de los conocimientos conseguidos durante la implementación del sistema (Vargas, 2009).

3.1.2. Diseño de investigación: Pre Experimental.

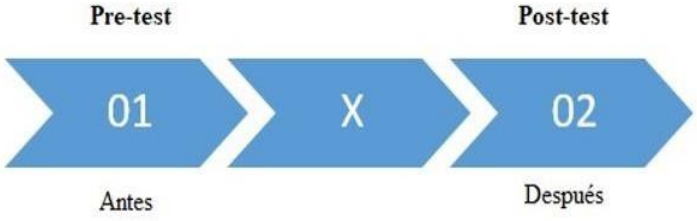


Figura 1. Diseño de investigación

Dónde:

O1: Garantizar la Seguridad de la Información.

X: SGSI basado en NTP-ISO/IEC 27001.

O2: Garantizar la Seguridad de la Información.

3.2. Variables de Operacionalización

- **Variable Independiente:** SGSI basado en NTP-ISO/IEC 27001.
- **Variable Dependiente:** Garantizar la Seguridad de la Información.

El cuadro de operacionalización de variables se encuentra en anexos (Ver Anexo 01)

3.3. Población, muestra, muestreo y unidad de análisis

Según la información que se obtuvo por parte de la GRLL, la cantidad de personas que trabajan dentro del área de TI es de 11 personas por tal motivo la muestra es la misma que la población. El muestreo que se utilizó es de tipo probabilístico y se usó el muestreo aleatorio simple (Guadalupe, 2016).

3.4. Técnicas e instrumentos de recolección de datos

La principal técnica de recolección de datos es la observación directa mediante las comprobaciones de la medición de los tiempos. Según (Orellana, 2006), es el elemento básico que debe percibir toda investigación que tiene relación directo con el objeto a investigar.

Tabla 1. Técnicas e instrumentos de recolección de datos

Técnica	Instrumento	Fuente	Informante
Entrevista	Cuestionario	Área administrativa	Personal de TI

Valides y confiabilidad: Para validar la encuesta realizada en la investigación actual, tuvo que ser validada y aceptada por tres expertos profesionales en la materia, las cuales después de haber revisado juiciosamente la presente encuesta, dieron su opinión aprobando y dando el visto bueno del instrumento.

Para la confiabilidad del instrumento se utilizarán fórmulas para calcular coeficientes de confiabilidad, basados en la consistencia interna, las fórmulas son las siguientes:

Alfa de Cronbach 1951: El coeficiente alfa (α) es un indicador de la fiabilidad de un test basado en su grado de consistencia interna. Indica el grado en que los ítems de un test covarían.

Coeficientes de Kuder-Richardson: Se trata de dos fórmulas aplicables a sendos casos particulares de alfa. KR20 se aplica en el caso en que los ítems del test sean dicotómicos, y KR21, en el caso de que además de ser dicotómicos, tengan la misma dificultad.

Una vez hecho la confiabilidad con las fórmulas mencionadas y haber aprobada el instrumento, se prosiguió a encuestar a los trabajadores del Subgerencia de TI del Gobierno Regional la Libertad (GRLL).

3.5. Procedimientos

Realizamos una reunión mediante llamada telefónica con el Sub-Gerente de Tecnologías del Gobierno Regional de La Libertad, ingeniero Carlos Chunga M. quien nos permitió conocer de una manera muy clara la realidad actual en la cual se encuentra la Oficina de la Sub Gerencia de Tecnologías de la Información.

En primer plano con el conocimiento de las funciones de los responsables principales del área los cuales son un aproximado de 11 trabajadores del área en la que se enfocará el tipo de investigación experimental y preexperimental utilizando la prueba de normalidad Shapiro Wilk, en todos los activos de información como servidores, equipos de cómputo, procesos, información en los cuales estará situada nuestra investigación identificando la problemática para poder darle solución mediante la propuesta de un Sistema de Gestión de Seguridad de la Información (SGSI) el cual está basado en el estándar internacional ISO 27001, la cual ha sido adaptada al estado peruano mediante el Instituto Nacional De La Calidad (INACAL), resultando oficialmente la Norma técnica peruana: NTP-ISO/IEC 27001:2014.

Basado en dicha norma, la cual está enfocada en la gestión de la seguridad de la información, procedimos a la identificación de la problemática, para lo cual mostramos las causas y sus consecuencias en la Tabla 1: Relación casusa – efecto, se realizará un tratamiento de los riesgos identificados que pueden afectar a los activos de información, proponemos la implementación de un SGSI en el área enfocado en los procesos de actualización y publicación del portal de transparencia, para mantener la **Integridad, Confidencialidad y Disponibilidad de la Información** en estos procesos, con el cual no se cuenta actualmente en el área.

Para finalizar, se estableció la influencia que asumió la propuesta de SGSI para garantizarla seguridad de la información en la sub gerencia

de TI del GRLL, utilizando el análisis estadístico mediante la prueba de hipótesis.

3.6. Método de análisis de datos

Para el contraste de las hipótesis de investigación se debe determinar su aceptación o rechazo, el análisis del antes y después de las variables que fueron expuestas a determinada estimulo, con lo que se efectuará la prueba de distribución Z que se usa para aquellas investigaciones donde las muestras son mayores a 30 (BRUNETT, 2019) y **t Student** para aquellos donde las muestras son iguales a 30 (Lorenzo, 2019):

3.7. Aspectos éticos.

Los investigadores en todo momento existen el compromiso de respetar la veracidad en los cuales infieren los resultados, así mismo la confiabilidad de los datos obtenidos y a guardar la identidad de los individuos participantes en la encuesta que abrió la presente investigación.

IV. RESULTADOS

4.1. Indicador 01: Nivel de integridad de la información.

- ✓ **Análisis descriptivo**

  Se compara los resultados (pretest), antes de la propuesta SGSI (Postest) y después de haberlo implementado (Posada, 2016).

Estadísticos descriptivos

	N	Mínimo	Máximo	Suma	Media	Desviación estándar
NIIa	5	1,09	2,36	8,99	1,7980	,47257
NIIp	5	4,00	4,82	21,64	4,3280	,35703
N válido (por lista)	5					

Figura 2. Analisis descriptivo 01

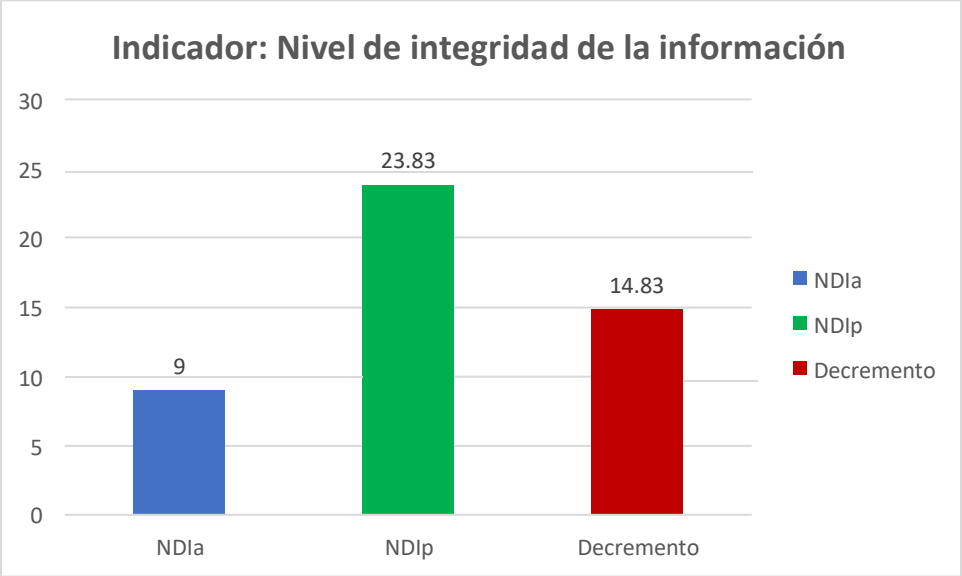


Gráfico 1. Media del indicador 01

Se detalla los puntajes del nivel de integridad de la información antes de la propuesta 8.99 puntos, mediante la implementación de la propuesta se tuvo una puntuación de 21.64 puntos, obteniendo un decremento de 12.65 puntos.

✓ **Análisis inferencial**

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
NIIa	,185	5	,200*	,970	5	,877
NIIp	,221	5	,200*	,901	5	,415

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Figura 3. Análisis inferencial 01

Los resultados de la prueba de normalidad, se obtiene una sig. Superior a 0.05, lo cual representa una distribución normal (Gómez, 2005).

✓ **Prueba de Hipótesis**

- **Definición de variables**

  NIIa = Nivel de integridad de la información con el sistema actual.

  NIId = Nivel de integridad de la información con el sistema propuesto.

- **Hipótesis estadística**

  Hipótesis Ho = El Nivel de integridad de la información con el sistema actual es mayor o igual que el Nivel de integridad de la información con el sistema propuesto.

$$\boldsymbol{H_0 = NII_a - NII_d \geq 0}$$

  Hipótesis Ha = El Nivel de integridad de la información con el sistema actual es menor que El Nivel de integridad de la información con el sistema propuesto.

$$\boldsymbol{H_0 = NII_a - NII_d < 0}$$

- **Nivel de significancia**

  Se define como confiabilidad 95% ($1 - \alpha = 0.95$), con un nivel de significancia del 5% ($\alpha = 0.05$).

- **Región de rechazo**

N = 5 siendo el grado de libertad (N – 1) = 4 tomando como valor critico ($t_{\infty-0.05} = 2.1318$). Entonces la región de rechazo consiste en todos los valores comprendidos que sean menores de t siendo el valor de este 2.1318 (Hernández, 2020).

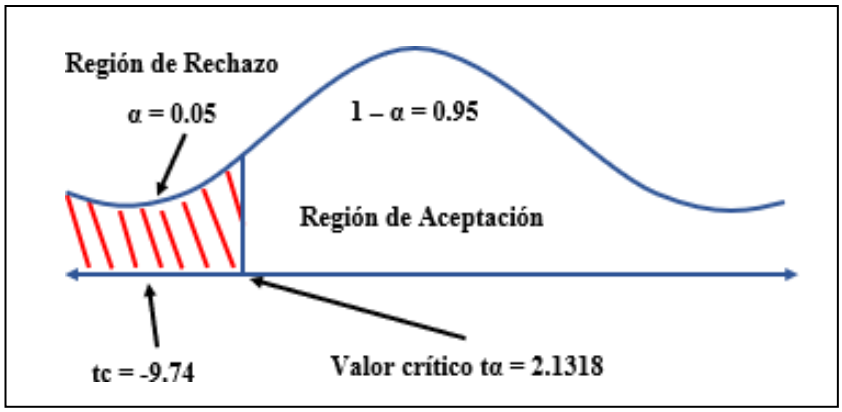


Figura 4. Región de rechazo 01

Puesto que tc = -9.74 y tα = 2.1318, el valor se encuentra en la zona de rechazo concluyendo que se rechaza la Ho el nivel de integridad de la información con el sistema actual y se acepta la Ha el nivel de integridad de la información con el sistema propuesto.

Prueba de muestras emparejadas

		Diferencias emparejadas					t	gl	Sig. (bilateral)
		Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia Inferior	Superior			
Par 1	PreTest - PosTest	-2,52800	,58187	,26022	-3,25048	-1,80552	-9,715	4	,001

Figura 5. Pruebas de muestra emparejadas 01

4.2. Indicador 02: Nivel de confidencialidad de la información.

- ✓ **Análisis descriptivo**

  Se compara los resultados (pretest), antes de la propuesta SGSI (Postest) y después de haberlo implementado.

Estadísticos descriptivos

	N	Mínimo	Máximo	Suma	Media	Desviación estándar
NCIa	5	1,00	2,45	9,09	1,8180	,54002
NCIp	5	4,09	5,00	22,45	4,4900	,37928
N válido (por lista)	5					

Figura 6. Análisis descriptivo 02

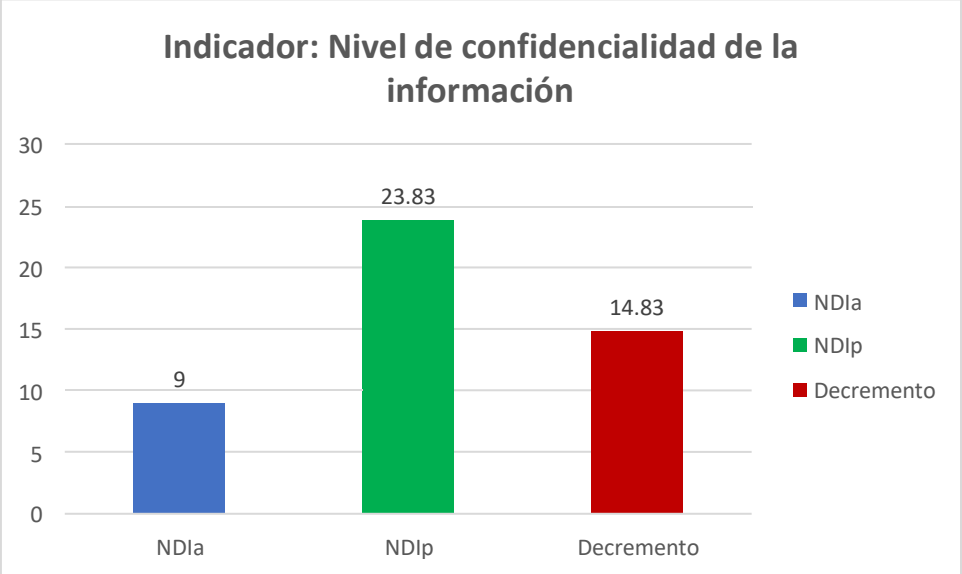


Gráfico 2. Media del indicador 02

Se detalla los puntajes del nivel de confiabilidad de la información antes de la propuesta 9.09 puntos, mediante la implementación de la propuesta se tuvo una puntuación de 22.45 puntos, obteniendo un decremento de 13.36 puntos.

- ✓ **Análisis inferencial**

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
NCIa	,232	5	,200*	,946	5	,710
NCIp	,193	5	,200*	,945	5	,705

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Figura 7. Análisis inferencial 02

Los resultados de la prueba de normalidad, se obtiene una sig. Superior a 0.05, lo cual representa una distribución normal.

- ✓ **Prueba de Hipótesis**

- **Definición de variables**

NCIa = Nivel de confiabilidad de la información con el sistema actual.

NCId = Nivel de confiabilidad de la información con el sistema propuesto.

- **Hipótesis estadística**

Hipótesis Ho = El Nivel de confiabilidad de la información con el sistema actual es mayor o igual que el Nivel de confiabilidad de la información con el sistema propuesto.

$$\boldsymbol{H_0 = NCI_a - NCI_d \geq 0}$$

Hipótesis Ha = El Nivel de confiabilidad de la información con el sistema actual es menor que El Nivel de confiabilidad de la información con el sistema propuesto.

$$\boldsymbol{H_0 = NCI_a - NCI_d < 0}$$

- **Nivel de significancia**

  Se define como confiabilidad 95% (1 – α = 0.95), con un nivel de significancia del 5% ($\alpha = 0.05$).

- **Región de rechazo**

  N = 5 siendo el grado de libertad (N – 1) = 4 tomando como valor critico ($t_{\infty-0.05} = 2.1318$). Entonces la región de rechazo consiste en todos los valores comprendidos que sean menores de t siendo el valor de este 2.1318.

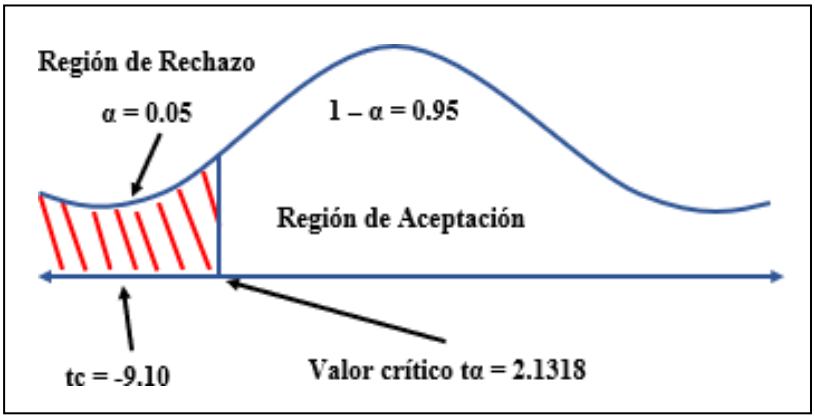


Figura 8. Región de rechazo 02

Puesto que tc = -9.07 y tα = 2.1318, el valor se encuentra en la zona de rechazo concluyendo que se rechaza la Ho el nivel de confiabilidad de la información con el sistema actual y se acepta la Ha el nivel de integridad de la información con el sistema propuesto.

	Diferencias emparejadas					t	gl	Sig. (bilateral)
	Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
				Inferior	Superior			
Par 1 NCIa - NCIp	-2,67200	,65842	,29446	-3,48954	-1,85446	-9,074	4	,001

Figura 9. Pruebas de muestra emparejadas 02

4.3. Indicador 03: Nivel de disponibilidad de la información.

- ✓ **Análisis descriptivo**

  Se compara los resultados (pretest), antes de la propuesta SGSI (Postest) y después de haberlo implementado.

Estadísticos descriptivos

	N	Mínimo	Máximo	Suma	Media	Desviación estándar
NDIa	5	1,00	2,55	9,18	1,8360	,61297
NDIp	5	4,27	5,00	24,18	4,8360	,31879
N válido (por lista)	5					

Figura 10. Análisis descriptivo 03

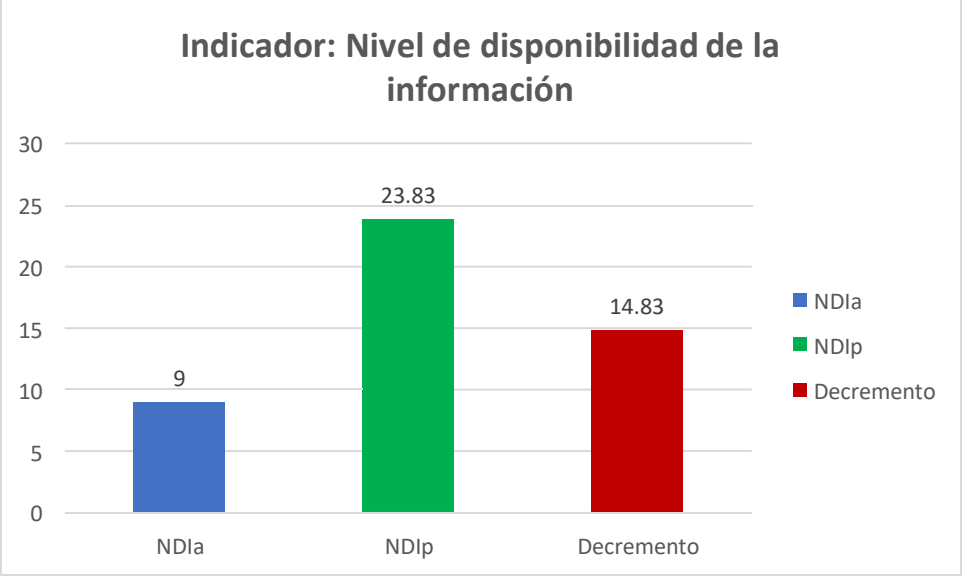


Gráfico 3. Media del indicador 03

Se detalla los puntajes del nivel de disponibilidad de la información antes de la propuesta 9.18 puntos, mediante la implementación de la propuesta se tuvo una puntuación de 24.18 puntos, obteniendo un decremento de 15 puntos.

✓ **Análisis inferencial**

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
NDIa	,205	5	,200*	,968	5	,865
NDIp	,392	5	,012	,632	5	,002

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Figura 11. Análisis inferencial 03

Los resultados de la prueba de normalidad, se obtiene una sig. 0.865 superior a 0.05, lo cual representa una distribución normal.

✓ **Prueba de Hipótesis**

- **Definición de variables**

  NDIa = Nivel de disponibilidad de la información con el sistema actual.

  NDId = Nivel de disponibilidad de la información con el sistema propuesto.

- **Hipótesis estadística**

  Hipótesis Ho = El Nivel de disponibilidad de la información con el sistema actual es mayor o igual que el Nivel de disponibilidad de la información con el sistema propuesto.

$$\boldsymbol{H_0 = NDI_a - NDI_d \geq 0}$$

  Hipótesis Ha = El Nivel de disponibilidad de la información con el sistema actual es menor que El Nivel de disponibilidad de la información con el sistema propuesto.

$$\boldsymbol{H_0 = NDI_a - NDI_d < 0}$$

- **Nivel de significancia**

  Se define como confiabilidad 95% (1 – α = 0.95), con un nivel de significancia del 5% ($\alpha = 0.05$).

- **Región de rechazo**

  N = 5 siendo el grado de libertad (N – 1) = 4 tomando como valor critico ($t_{\infty-0.05} = 2.1318$). Entonces la región de rechazo consiste en todos los valores comprendidos que sean menores de t siendo el valor de este 2.1318.

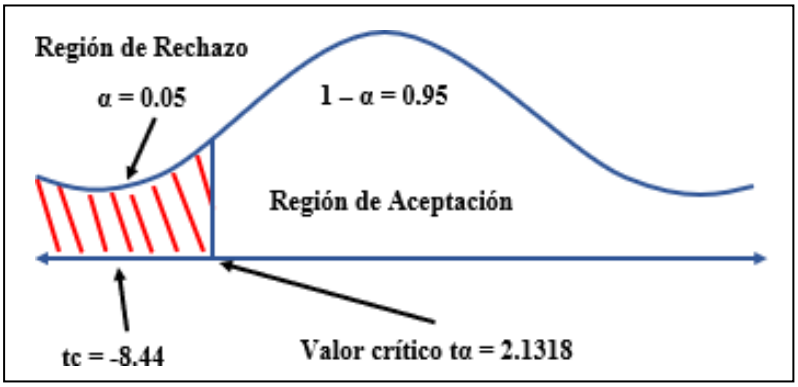


Figura 12. Región de rechazo 03

Puesto que tc = -8.44 y tα = 2.1318, el valor se encuentra en la zona de rechazo concluyendo que se rechaza la Ho el nivel de disponibilidad de la información con el sistema actual y se acepta la Ha el nivel de disponibilidad de la información con el sistema propuesto.

		Diferencias emparejadas					t	gl	Sig. (bilateral)
		Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
					Inferior	Superior			
Par 1	NCIa - NCIp	-2,67200	,65842	,29446	-3,48954	-1,85446	-9,074	4	,001

Figura 13. Pruebas de muestra emparejadas 03

4.4. Indicador 04: Nivel del uso de nuevas políticas de seguridad.

- ✓ **Análisis descriptivo**

  Se compara los resultados (pretest), antes de la propuesta SGSI (Postest) y después de haberlo implementado.

Estadísticos descriptivos

	N	Mínimo	Máximo	Suma	Media	Desviación estándar
NPSa	5	1,45	2,00	9,00	1,8000	,22793
NPSp	5	4,36	5,00	23,82	4,7640	,27070
N válido (por lista)	5					

Figura 14. Análisis descriptivo 04

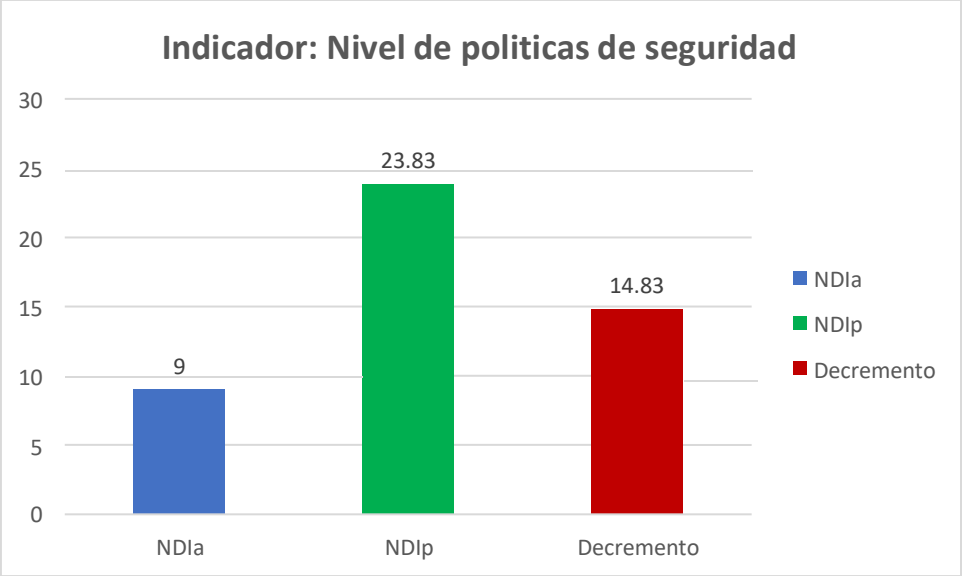


Gráfico 4. Media del indicador 04

Se detalla los puntajes del nivel de uso de políticas de seguridad de la información antes de la propuesta 9 puntos, mediante la implementación de la propuesta se tuvo una puntuación de 23.83 puntos, obteniendo un decremento de 14.83 puntos.

✓ **Análisis inferencial**

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
NPSa	,210	5	,200*	,893	5	,371
NPSp	,208	5	,200*	,895	5	,384

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Figura 15. Análisis inferencial 04

Los resultados de la prueba de normalidad, se obtiene una sig. 0.371 superior a 0.05, lo cual representa una distribución normal.

✓ **Prueba de Hipótesis**

- **Definición de variables**

NUPa = Nivel de uso de nuevas políticas de seguridad con el sistema actual.

NUPd = Nivel de uso de nuevas políticas de seguridad con el sistema propuesto.

- **Hipótesis estadística**

Hipótesis Ho = El Nivel de uso de nuevas políticas de seguridad con el sistema actual es mayor o igual que el Nivel de uso de nuevas políticas de seguridad con el sistema propuesto.

$$\boldsymbol{H_0 = NUP_a - NUP_d \geq 0}$$

Hipótesis Ha = El Nivel de uso de nuevas políticas de seguridad con el sistema actual es menor que El Nivel de uso de nuevas políticas de seguridad con el sistema propuesto.

$$\boldsymbol{H_0 = NUP_a - NUP_d < 0}$$

- **Nivel de significancia**

  Se define como confiabilidad 95% (1 – α = 0.95), con un nivel de significancia del 5% ($\alpha = 0.05$).

- **Región de rechazo**

  N = 5 siendo el grado de libertad (N – 1) = 4 tomando como valor critico ($t_{\infty-0.05} = 2.1318$). Entonces la región de rechazo consiste en todos los valores comprendidos que sean menores de t siendo el valor de este 2.1318.

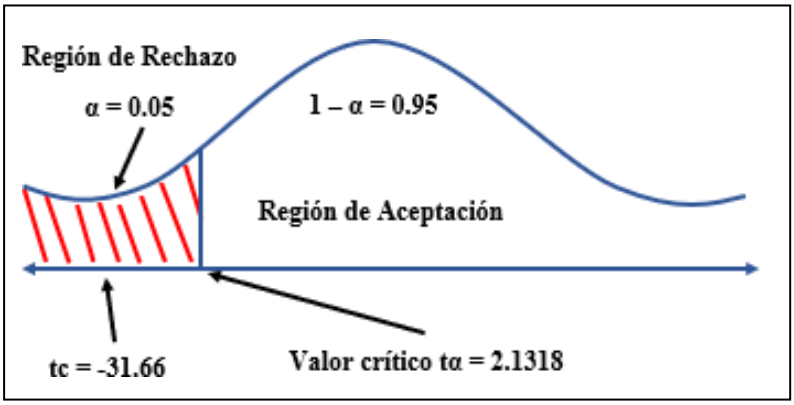


Figura 16. Región de rechazo 04

Puesto que tc = -31.66 y tα = 2.1318, el valor se encuentra en la zona de rechazo concluyendo que se rechaza la Ho el nivel de uso de pláticas de seguridad de la información con el sistema actual y se acepta la Ha el nivel de políticas de seguridad de la información con el sistema propuesto.

Prueba de muestras emparejadas

		Diferencias emparejadas					t	gl	Sig. (bilateral)
		Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
					Inferior	Superior			
Par 1	Pretest - Postest	-2,96400	,20720	,09266	-3,22127	-2,70673	-31,988	4	,000

Figura 17. Pruebas de muestra emparejadas 04

V. DISCUSIÓN

En el primer indicador el nivel de integridad de la información en la gerencia de Tecnologías de información, se realizó mediante encuestas para determinar el pretest y postest, utilizando la escala de Likert donde se consideró una puntuación del 1 al 5, donde se obtuvo el nivel de integridad de la información con el sistema actual una puntuación de 1.80 puntos equivalente a un 36%, y con la implementación del sistema de gestión de seguridad se obtuvo una puntuación de 4.33 puntos; donde se obtiene un incremento de 2.53 puntos equivalente a 50.60%. Estos resultados tienen similitud (ALCÁNTARA, 2015), en su trabajo de investigación que logró incrementar en un 68% los procedimientos utilizados en favor de la Institución permitiéndole la detección de anomalías en la seguridad de la información, reflejado en distintos mecanismos de seguridad para salvaguardarla.

En el segundo indicador el nivel de confidencialidad de la información en la gerencia de Tecnologías de información, se realizó mediante encuestas para determinar el pretest y postest, utilizando la escala de Likert donde se consideró una puntuación del 1 al 5, donde se obtuvo el nivel de confidencialidad de la información con el sistema actual una puntuación de 1.82 puntos equivalente a un 36.40%, y con la implementación del sistema de gestión de seguridad basado en las norma técnica peruana 27001 se obtuvo una puntuación de 4.49 puntos; donde se obtiene un incremento de 2.67 puntos equivalente a 53.40%. Estos resultados tienen comparación al del autor (ZAVALETA, 2016), en su trabajo de investigación manifiesta que se demostró que existen gran disposición para la implementación, de 15 encuestados, 14 usuarios (93.33%), señalan que existe un nivel alto para la implementación del SGSI. Este trabajo ayudó a la implementación de un Sistema de Gestión de Seguridad de la Información aplicando NTP ISO/IEC 27001:2014.

En el tercer indicador el nivel de disponibilidad de la información en la gerencia de Tecnologías de información, se realizó mediante encuestas para determinar el pretest y postest, utilizando la escala de Likert donde se consideró una puntuación del 1 al 5, donde se obtuvo el nivel de disponibilidad de la información con el sistema actual una puntuación de 1.84 puntos equivalente a un 36.80%, y con la implementación del sistema de gestión de seguridad basado en las norma técnica peruana 27001 se obtuvo una puntuación de 4.84 puntos; donde se obtiene un incremento de 3.00 puntos equivalente a 60.00%

Estos resultados tienen comparación al del autor (De La Cruz, 2016), en su trabajo de investigación manifiesta que el 72.37% se tiene la disponibilidad de la información pertinentes en cuanto a la seguridad de la información.

Y por último tenemos el nivel de uso de nuevas políticas de seguridad en la gerencia de Tecnologías de información, se realizó mediante encuestas para determinar el pretest y postest, utilizando la escala de Likert donde se consideró una puntuación del 1 al 5, donde se obtuvo el nivel de uso de nuevas políticas de seguridad con el sistema actual una puntuación de 1.80 puntos equivalente a un 36.00%, y con la implementación del sistema de gestión de seguridad basado en las normas técnica peruana 27001 se obtuvo una puntuación de 4.76 puntos; donde se obtiene un incremento de 2.96 puntos equivalente a 59.20%.

Finalmente, los resultados confirman que se garantiza la seguridad informática en la subgerencia de tecnologías de información del gobierno regional la libertad, debido que se logró incrementar una diferencia significativa entre el pretest y postest, garantizando significativamente la seguridad de la información.

VI. CONCLUSIONES

- ✓ Con la implementación de un sistema de gestión de seguridad basado en la norma técnica peruana ISO/27001 se garantizó significativamente la seguridad de la información en la subgerencia de tecnologías de información del gobierno regional de la libertad.

- ✓ Para determinar el nivel de integridad de la información con respecto a la seguridad de la información con el sistema actual se obtuvo una puntuación de 1.80 puntos, mientras con la implementación del sistema propuesto es de 4.33 puntos, obteniendo un incremento del 50.60% sobre el nivel de integridad de la información sobre el personal del área tecnologías de información.

- ✓ Se concluye que el nivel de confidencialidad de la información con respecto a la seguridad de la información con el sistema actual se obtuvo una puntuación de 1.82 puntos, mientras con la implementación del sistema propuesto es de 4.49 puntos, obteniendo un incremento del 53.40% sobre el nivel de confidencialidad de la información sobre el personal del área tecnologías de información.

- ✓ Se concluye que el nivel de disponibilidad de la información con respecto a la seguridad de la información con el sistema actual se obtuvo una puntuación de 1.84 puntos, mientras con la implementación del sistema propuesto es de 4.84 puntos, obteniendo un incremento del 60.00 % sobre el nivel de disponibilidad de la información sobre el personal del área tecnologías de información.

- ✓ Tomando en cuenta una escala del 1 al 5 para medir el nivel de uso de nuevas políticas de seguridad, se obtuvo con el sistema actual de 1.80 puntos y con la implementación propuesta sobre el nivel de uso de nuevas políticas de seguridad es de 4.76 puntos, alcanzando un incremento de 2.96 puntos equivalente al porcentaje de 59.20%.

VII. RECOMENDACIONES

- ✓ Se recomienda a la Sub Gerencia de TI del GRLL implementar esta norma, que dicho sea de paso cada vez se vuelve más mundialmente aceptada, debe primero capacitar a su personal, empezando por un comité, y luego con toda la organización.
- ✓ Se recomienda a la Sub Gerencia de TI del GRLL realizar un inventario de todos los activos de información con los que cuenta la institución y clasificarlos, para tener muy claro el papel que juegan en el manejo de la información.
- ✓ Se recomienda a la Sub Gerencia de TI del GRLL realizar las tareas más importantes de la norma: Identificar, Analizar y evaluación de los riesgos; y finalmente elaboración de un plan de trabajo o implementación de medidas de control, lo que conllevará a un proyecto, el mismo que podría ser llevado por el Gerente de Proyectos de la institución.
- ✓ Se recomienda a la Sub Gerencia de TI del GRLL a un nivel de madurez de tratamiento de la información con buenas prácticas de seguridad y cuidado de sus activos de información con medidas de control muy detalladas y haciendo seguimiento de su efectividad a través de un sistema de gestión de incidencias.

REFERENCIAS

AGUIRRE CARDONA, O. y ARISTIZÁBAL BETANCOURT, C., 2014. *DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL GRUPO EMPRESARIAL LA OFRENDA* [en línea]. S.l.: UNIVERSIDAD TECNOLÓGICA DE PEREIRA - COLOMBIA. Disponible en: https://docplayer.es/3719230-Diseno-del-sistema-de-gestion-de-seguridad-de-la-informacion-para-el-grupo-empresarial-la-ofrenda-juan-david-aguirre-cardona.html.

ALCÁNTARA FLORES, J., 2015. *Guía de implementación de la seguridad basado en la norma ISO/IEC27001, para apoyar la seguridad en los sistemas informáticos de la Comisaria del Norte P.N.P. en la ciudad de Chiclayo*. Universidad Católica Santo Toribio de Mogrovejo: s.n.

BERNAL, C., 2018. *Justificación de Estudio* [en línea]. 2018. S.l.: s.n. Disponible en: https://leo-yac.wixsite.com/tallerinvestigacion/justificacin-libro.

BERNARDO, A., 2018. *Evaluación de Riesgos* [en línea]. 2018. S.l.: s.n. Disponible en: http://www.iso27000.es/download/Evaluacion_Riesgo_iso27001.pdf.

BRUNETT ZARZA, K., 2019. *DISTRIBUCIÓN NORMAL* [en línea]. 2019. S.l.: s.n. Disponible en: http://ri.uaemex.mx/bitstream/handle/20.500.11799/106113/Distribuci%C3%B3n%20Normal.pdf?sequence=1&isAllowed=y.

DE LA CRUZ VARGAS, R., 2016. *Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la municipalidad provincial de Paita; 2016*. S.l.: Universidad Católica Los Ángeles de Chimbote.

EALDE, 2017. *GESTIÓN DE RIESGOS* [en línea]. 2017. S.l.: s.n. Disponible en: https://www.ealde.es/iso-31000-para-que-sirve/.

ESPINOSA FREIRE, 2018. *La hipótesis en la investigación* [en línea]. 2018. S.l.: s.n. Disponible en: http://scielo.sld.cu/pdf/men/v16n1/1815-7696-men-16-01-122.pdf.

GÓMEZ VILLEGAS, M., 2005. *INFERENCIA ESTADÍSTICA* [en línea]. 2005. S.l.: s.n. Disponible en: https://webcache.googleusercontent.com/search?q=cache:RiSP17hOOBoJ:https://www.editdiazdesantos.com/wwwdat/pdf/9788479786878.pdf+&cd=16&hl=es&ct=clnk&gl=pe.

GONZÁLEZ, T., 2011. *Objetivos de la Investigación* [en línea]. 2011. S.l.: s.n. Disponible en: https://webcache.googleusercontent.com/search?q=cache:ExTQ_DFjWdUJ:https://bib.us.es/educacion/sites/bib3.us.es.educacion/files/poat2016_2_3_2_objetivos_de_investigacion.pdf+&cd=1&hl=es&ct=clnk&gl=pe.

GUADALUPE MIRANDA, M., 2016. *El protocolo de investigación III: la población de estudio* [en línea]. 2016. S.l.: s.n. Disponible en: https://www.redalyc.org/pdf/4867/486755023011.pdf.

HERNÁNDEZ RODRÍGUEZ, R., 2020. *PRUEBA DE HIPÓTESIS ESTADÍSTICA* [en línea]. 2020. S.l.: s.n. Disponible en: http://cucea.udg.mx/include/publicaciones/coorinv/pdf/Libro-Prueba-de-hipotesis.pdf.

INACAL, 2020. *Dirección de Normalización* [en línea]. 2020. S.l.: s.n. Disponible en: https://cdn.www.gob.pe/uploads/document/file/562691/25_Brochure_Normalizacion_2020.pdf.

ISO, 2015. *Organismos Nacionales de Normalización en Países en Desarrollo* [en línea]. 2015. S.l.: s.n. Disponible en: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/fast_forward-es.pdf.

LEY N° 27806, 2014. *Ley de Transparencia y Acceso a la Información Pública*. 2014. S.l.: s.n.

LORENZO, J., 2019. *Introducción a la Prueba t de Student y el Análisis de la Varianza* [en línea]. 2019. S.l.: s.n. Disponible en: https://ansenuza.unc.edu.ar/comunidades/bitstream/handle/11086.1/1348/Prueba%20t%20y%20ANOVA.pdf?sequence=1.

N° 004 - PCM, 2016. *Resolución Ministerial N° 004* [en línea]. 2016. S.l.: s.n. Disponible en: https://www.gob.pe/institucion/pcm/normas-legales/292578-004-2016-pcm.

N° 2219-GRLL-GOB, 2016. *Resolución Ejecutiva Regional N° 2219-2016-GRLL-GOB* [en línea]. 2016. S.l.: s.n. Disponible en: https://www.gob.pe/institucion/regionlalibertad/normas-legales/823291-2219-2016-grll-gob.

NTP, 2014. *TECNOLOGÍA DE LA INFORMACIÓN: Técnicas de seguridad. Sistemas de Gestión de seguridad de la información* [en línea]. 2014. S.l.: s.n. Disponible en: https://cdn.www.gob.pe/uploads/document/file/358700/doc03775920190906151659_compressed.pdf.

ORELLANA LÓPEZ, D., 2006. *TÉCNICAS DE RECOLECCIÓN DE DATOS EN ENTORNOS VIRTUALES MÁS USADAS EN LA INVESTIGACIÓN CUALITATIVA*. 2006. S.l.: s.n.

PCM, 2014. *Programa de fortalecimiento de capacidades en materia de Gobierno Abierto dirigido a gobiernos regionales y locales* [en línea]. 2014. S.l.: s.n. Disponible en: https://sgp.pcm.gob.pe/wp-content/uploads/2015/01/Fasciculo-1-Transparencia.pdf.

PCM, 2016. *Resolución Ministerial N° 004-2016-PCM* [en línea]. 2016. S.l.: s.n. Disponible en: https://www.gob.pe/institucion/pcm/normas-legales/292578-004-2016-pcm.

PONCE TALANCON, 2015. *Análisis FODA* [en línea]. 2015. S.l.: s.n. Disponible en: https://www.cneip.org/documentos/revista/CNEIP_12-1/Ponce_Talancon.pdf.

POSADA HERNÁNDEZ, G., 2016. *ELEMENTOS BÁSICOS DE ESTADÍSTICA DESCRIPTIVA para el análisis de datos* [en línea]. 2016. S.l.: s.n. Disponible en: https://www.funlam.edu.co/uploads/fondoeditorial/120_Ebook-elementos_basicos.pdf.

QUINTANA, A., 2008. *PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN* [en línea]. Lima - Perú: s.n. ISBN 1609 - 7475. Disponible en: https://webcache.googleusercontent.com/search?q=cache:0o_DClplj YAJ:https://dialnet.unirioja.es/descarga/articulo/2747363.pdf+&cd=1 &hl=es&ct=clnk&gl=pe.

SGP, 2014. *Acceso a la información pública* [en línea]. 2014. S.l.: s.n. Disponible en: https://sgp.pcm.gob.pe/wp-content/uploads/2015/06/F2-Acceso-a-la-Informacion-Publica.pdf.

SGSI, 2016. *Sistemas de Gestión de Seguridad de la Información* [en línea]. 2016. S.l.: s.n. Disponible en: https://www.pmg-ssi.com/2016/04/8-pasos-implantacion-de-la-norma-iso-27001/.

VARGAS CORDERO, Z., 2009. *LA INVESTIGACIÓN APLICADA: UNA FORMA DE CONOCER LAS REALIDADES CON EVIDENCIA CIENTÍFICA* [en línea]. 2009. S.l.: s.n. Disponible en: https://www.redalyc.org/pdf/440/44015082010.pdf.

YAN CARRANZA, F., 2015. *Plan de mejora de la seguridad de información y continuidad del centro de datos de la Gerencia Regional de Educación La Libertad aplicando lineamientos ISO 27001 y buenas prácticas COBIT* [en línea]. Universidad Privada Antenor Orrego - UPAO: s.n. Disponible en: https://repositorio.upao.edu.pe/handle/20.500.12759/645.

ZAVALETA, O., 2016. *Implementación De Un Sistema De Gestión De Seguridad De La Información Aplicando NTP ISO/IEC 27001:2014 En El Sector Hospitalario, 2016* [en línea]. Lima - Perú: Universidad Winner. Disponible en: https://repositorio.uss.edu.pe/handle/20.500.12802/3205?show=ful.

Anexo 3. Carta de Aceptación de la empresa

GOBIERNO REGIONAL LA LIBERTAD
FIRMA DIGITAL

SUB GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN

Año del Bicentenario del Perú: 200 años de Independencia

Trujillo, 29 de Noviembre del 2021

CARTA N° 000003-2021-GRLL-GGR-GRA-SGTI

A : Dr. Juan Francisco Pacheco Torres
Director de la Escuela Profesional de Ingenieria de Sistemas.
Universidad Cesar Vallejo S.A.C

Asunto : **CARTA DE ACEPTACIÓN PARA EL DESARROLLO DE INVESTIGACIÓN.**

De mi especial consideración;

Es grato dirigirme a Usted, para saludarlo cordialmente y a la vez manifestarle que la Sub Gerencia de Tecnologías de la Información, **ACEPTA** el desarrollo del Proyecto de Investigación **"Propuesta de SGSSI para garantizar la Seguridad de la información en la Sub Gerencia de TI del Gobierno Regional La Libertad"** realizado por el Sr. Alex Jhonatan Cornejo Miranda identificado con DNI 46153964 y el Sr. Arturo Ramón Lezama Calvo identificado con DNI 45942291, estudiantes del X ciclo de la escuela profesional de Ingenieria de Sistemas de la Universidad Cesar Vallejo, habiendo realizado un aporte en mejorar de nuestra Institución.

Se expide la presente carta a solicitud de la parte interesada para los fines que convengan

Atentamente,

Documento firmado digitalmente por
CARLOS ENRIQUE CHUNGA MONTERO
SUB GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN
GOBIERNO REGIONAL LA LIBERTAD

BICENTENARIO PERÚ LA LIBERTAD 2021

Juntos por la Prosperidad

Anexo 4. Matriz de operacionalización e indicadores de variables

Anexo 4.1: Matriz de operacionalización de variables

Tabla 2. Matriz de operacionalización de variables

Variables	**Definición Conceptual**	**Definición Operacional**	**Indicadores**	**Escala de Medición**
Seguridad de la Información	"El principal fin de La Seguridad de la información es protegerla de ataques y manipulación de los datos considerados como activos primordiales para una organización. (Alberto G. Alexander, 2018)	Permitirá mantener la información de una manera más accesible y segura para un buen funcionamiento del proceso	Nivel de Integridad de la Información	De razón
			Nivel de confidencialidad de la Información	
			Nivel de disponibilidad de la información	
			Nivel del uso de nuevas políticas de seguridad	
Sistema de Gestión de Seguridad de la Información	"Los sistemas de gestión de seguridad de la información, en primera instancia es una herramienta de la que se dispone para dirigir y controlar un determinado ámbito de un proceso, en este caso la seguridad de la información" (ISO_27001, 2005)	El sistema de gestión de la seguridad de la información ayudara a establecer políticas y procedimientos en relación al proceso.	Gestionar los procesos	De razón
			Poner en marcha el SGSI	

FUENTE: 2.2 Variables

Elaboración: Propia (Microsoft Office Word 2016)

Tabla 3. Indicadores de variables

N°	INDICADOR	DESCRIPCIÓN	OBJETIVO	TÉCNICA / INSTRUMENTO	TIEMPO EMPLEADO	MODO DE CÁLCULO
1	Nivel de Integridad de la Información (NII).	Identificar los activos importantes para la organización	Incrementar el nivel de Integridad de la Información	Encuestas	Semanal	$NII = \frac{\sum_{i=1}^{n}(II)_i}{n}$ NII = Nivel de integridad de la información. II = Integridad de la información. n = Número de información
2	Nivel de confidencialidad de la Información (NCI)	Determinar cuáles son los Riesgos para poder monitorear y revisar en el SGSI	Determinar el Nivel de confidencialidad de la Información	Encuestas	Semanal	$NCI = \frac{\sum_{i=1}^{n}(CI)_i}{n}$ NCI = Nivel de confiabilidad de la información. CI = Confiabilidad de la información. n = Numero información
3	Nivel de disponibilidad de la información (NDI).	El Plan de Tratamiento de riesgos permitirá a los usuarios tener un mejor control de ellos en GRLL	Incrementar el Nivel de disponibilidad de la información	Encuestas	Semanal	$NDI = \frac{\sum_{i=1}^{n}(DI)_i}{n}$ NDI = Nivel de disponibilidad de la información DI = Disponibilidad de la información. n = Número de información.
4	Nivel del uso de nuevas políticas de seguridad (IPS)	Políticas establecidas para la mitigación de riesgos	Incrementar el Nivel del uso de nuevas políticas de seguridad	Encuestas	semanal	$NUNPS = \frac{\sum_{i=1}^{n}(NPS)_i}{n}$ NUNPS= Nivel del uso de nuevas políticas de seguridad NPS = Uso de nuevas políticas de seguridad n = Número de información

Anexo 5. Contexto Interno y Externo de la Institución

- **Descripción del Proceso**

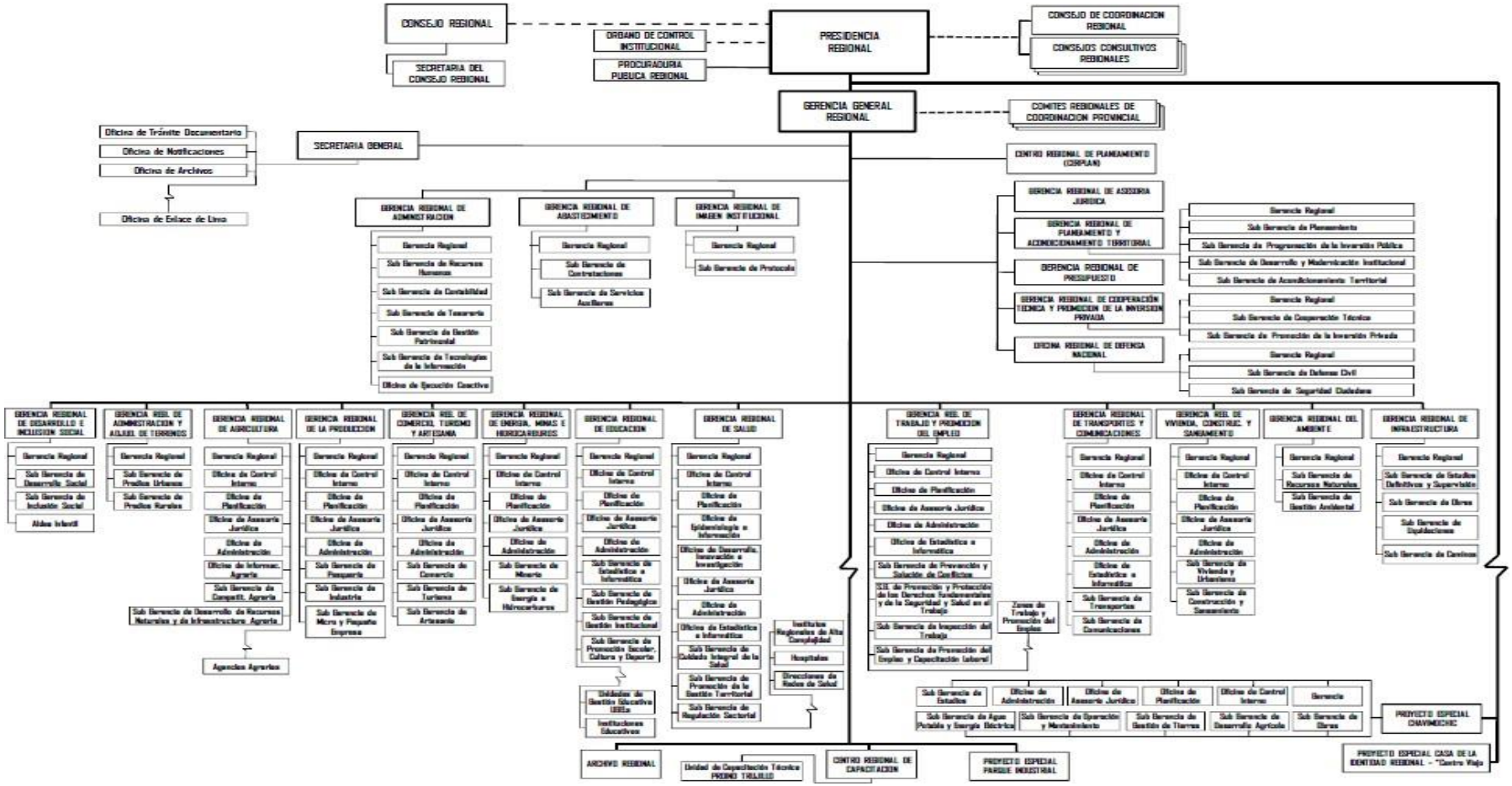
Respecto al proceso sobre el cual plasmaremos el trabajo será el proceso de publicar y mantener actualizada la información de transparencia en los portales de las Unidades Ejecutoras del Gobierno Regional La Libertad, crear y/o dar alojamiento de portales web para las ejecutoras que las soliciten.

Sub Procesos:

- ✓ Designar responsable, coordinadores y creación de usuario (Sugerir implementar procedimiento de entrega de claves)
- ✓ Actualización y publicación de información del portal de transparencia. (Manual del portal de transparencia)
- ✓ Seguimiento y monitoreo de la actualización y publicación de información en los portales de transparencia

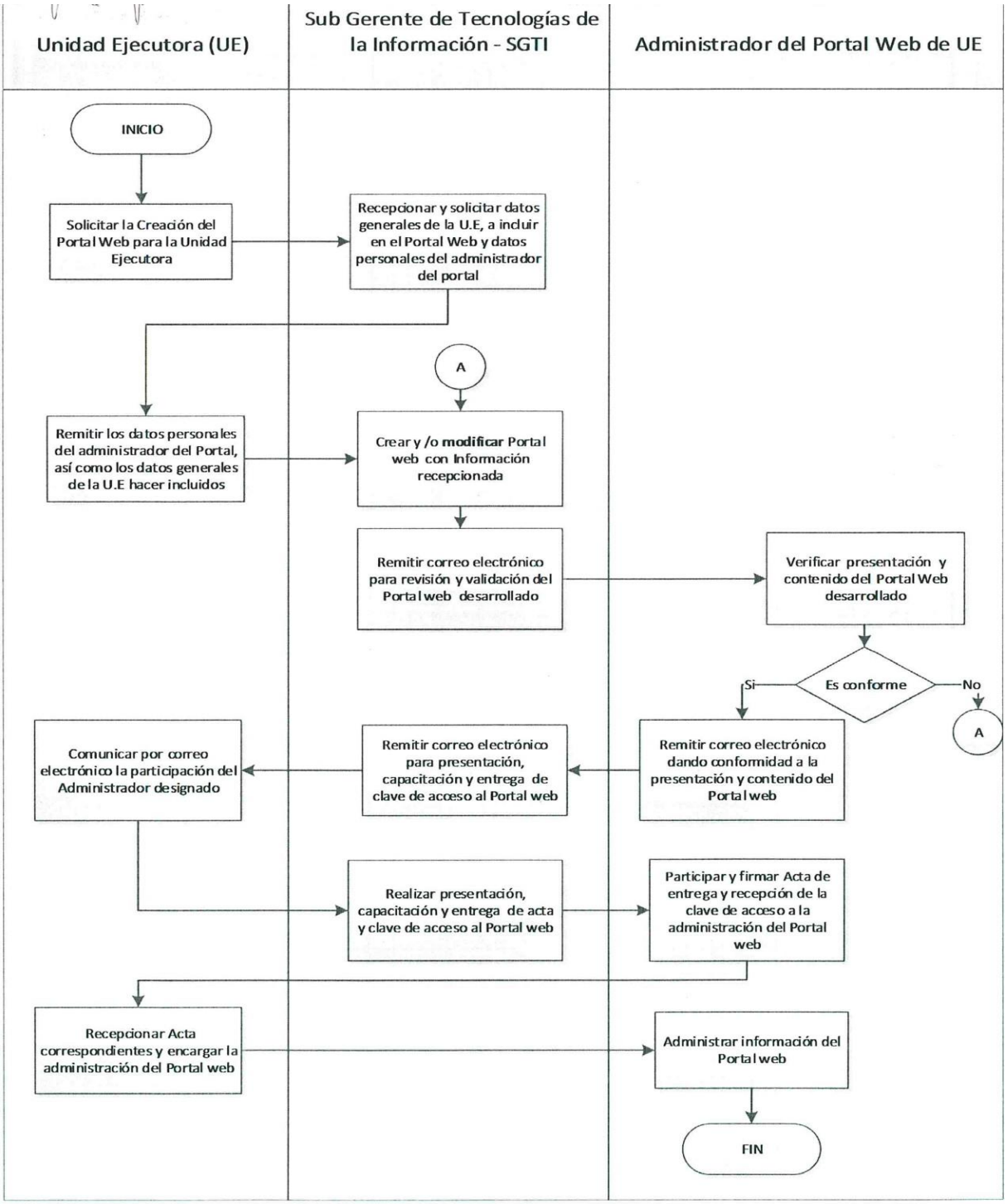
Anexo 6. Organigrama

Figura 18. Organigrama del Gobierno Regional la Libertad



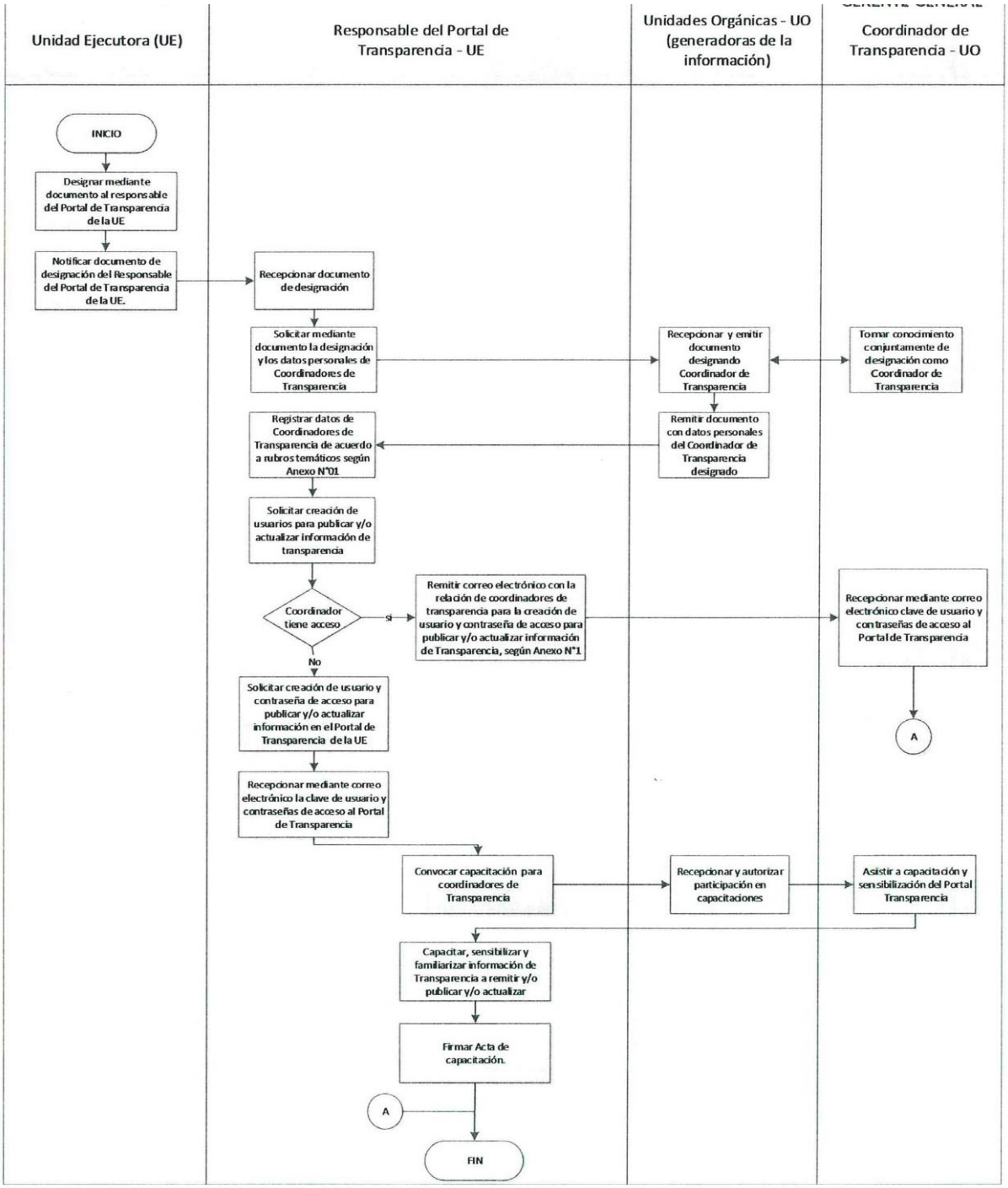
Anexo 7. Diagrama de Procesos de Actualización y Publicación de los Portales de Transparencia

Figura 19. Diagrama de Sub Proceso de Creación de Portales Web



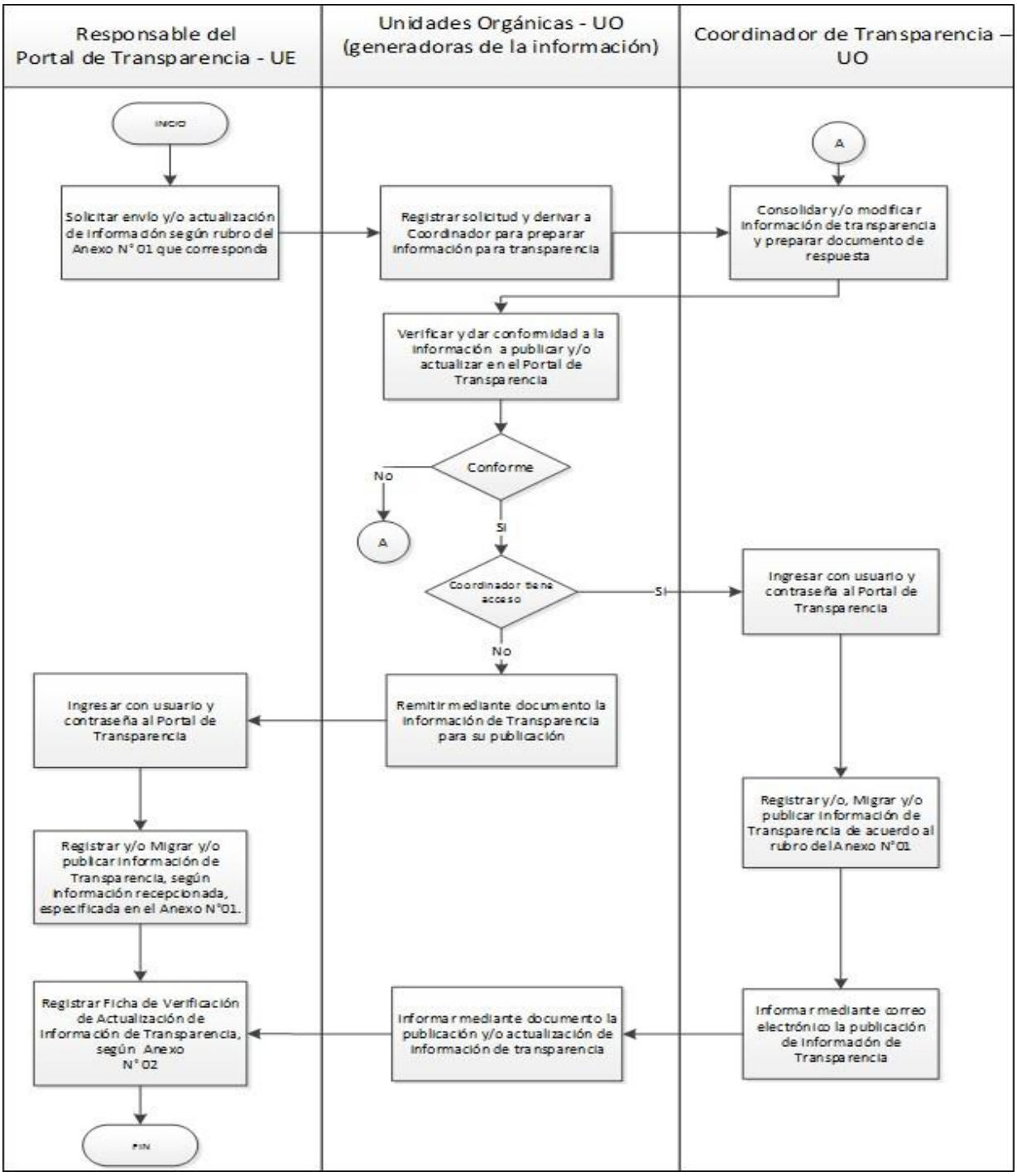
Anexo 8. Diagrama de Sub Proceso de Asignación de responsable

Figura 20. Diagrama de Sub Proceso de Asignación de Responsables



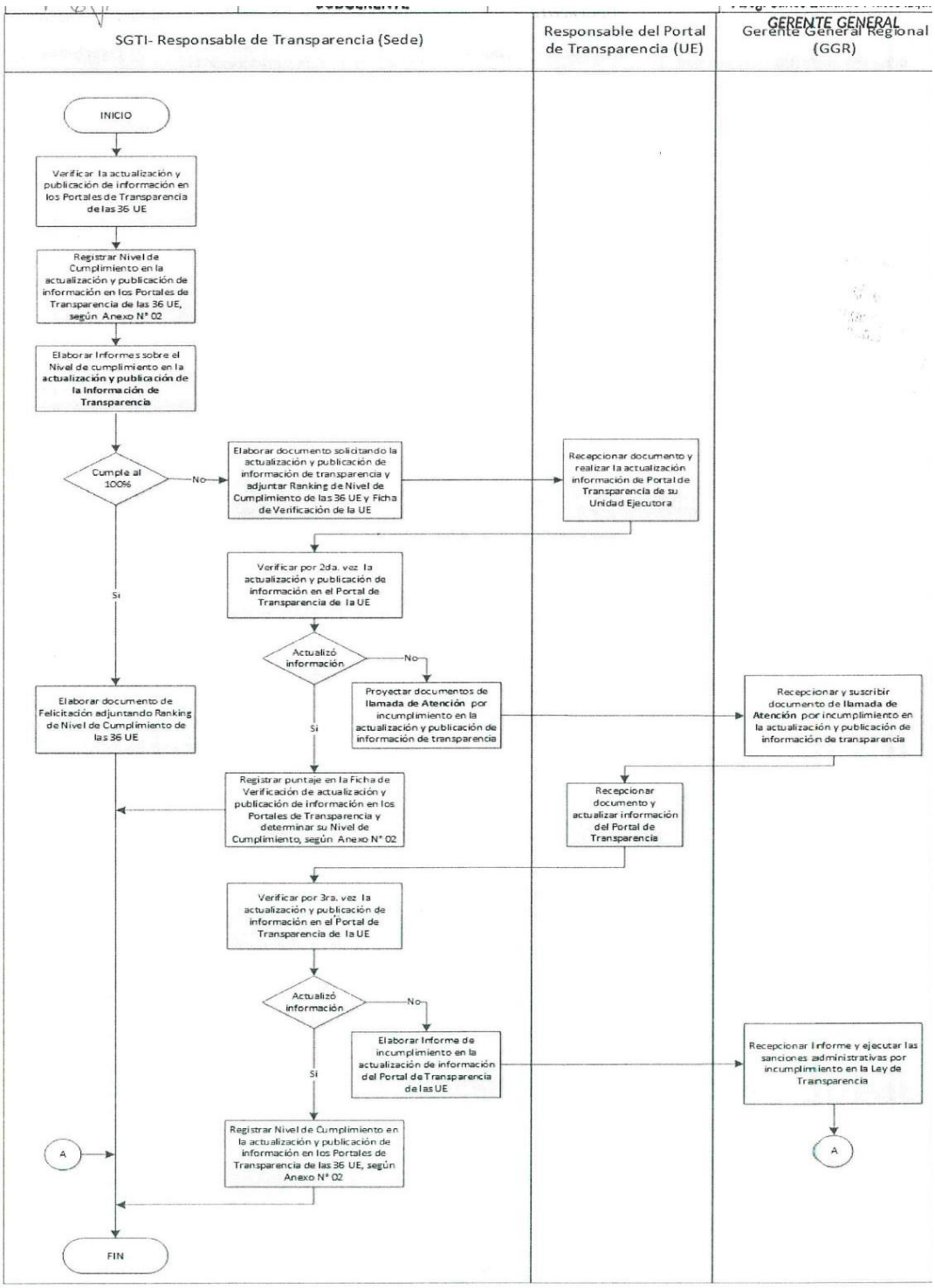
Anexo 9. Diagrama de Sub Proceso de Actualización de Información Institucional

Figura 21. Diagrama de Sub Proceso de Actualización de Información Institucional



Anexo 10. Diagrama de Sub Proceso de Seguimiento y Monitoreo

Figura 22. Diagrama de Sub Proceso de Seguimiento y Monitoreo



Anexo 11. FODA para la implementación del Sistema de Gestión de Seguridad de la Información

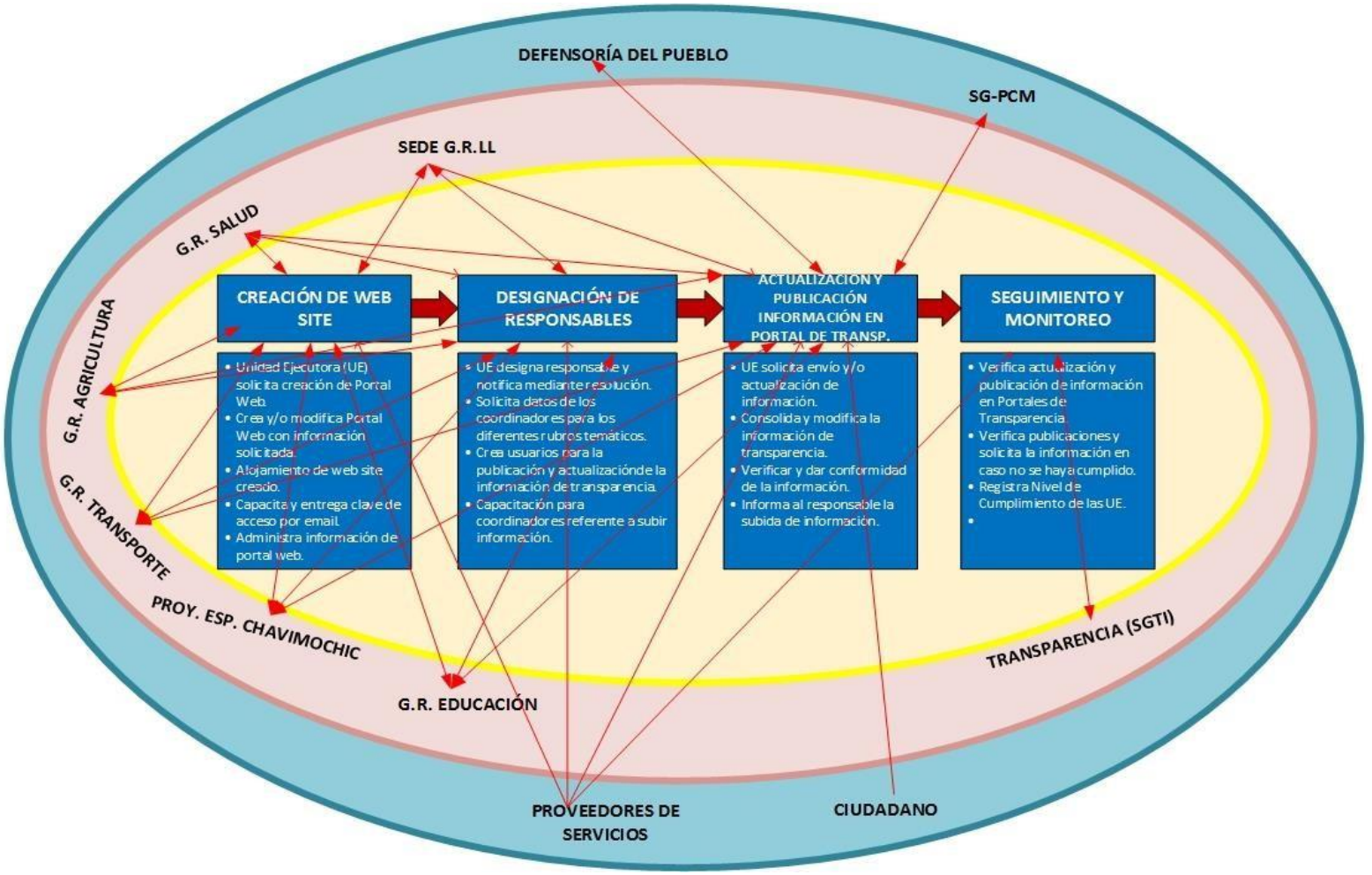
Tabla 4. Análisis FODA

FORTALEZAS	DEBILIDADES
Apoyo institucional para modernizar el Gobierno Regional la Libertad con el fin de integrar todas las Unidades Orgánicas y Ejecutoras regionales.	Inadecuada infraestructura física y tecnológica de la Subgerencia de Tecnologías de la Información.
Dirección con disponibilidad al trabajo en equipo; integrando y delegando funciones y apoyo en su cumplimiento.	Insuficiente partida presupuestal para la Subgerencia de Tecnologías de la Información.
Existencia de un buen clima laboral entre colaboradores de la Subgerencia de Tecnologías de la Información.	Insuficientes planes, políticas y directivas para garantizar el uso adecuado de los equipos y sistemas informáticos.
Procedimientos alineados a la Gestión de Transparencia.	Inadecuada Estructura Jerárquica Orgánica de Tecnologías de la Información con injerencia a nivel regional.
Personal con conocimiento en los procedimientos de gestión pública.	Limitada comunicación entre colaboradores.
	Insuficiente capacitación técnica al personal en temas específicos en tecnologías de última generación
	Falta de cumplimiento y control de las políticas y procedimientos existentes

OPORTUNIDADES	**AMENAZAS**
Convenios de cooperación interinstitucional entre Gobiernos Regionales y proyectos de apoyo para la gestión gubernamental.	Fenómenos naturales y ocurrencia de siniestros que pueden incrementar los costos operativos de TI.
Existencia de nuevas tecnologías de información que permiten una sólida gestión de TI.	Potenciales cambios en la política y gestión del Presupuesto del Sector Público.
Existencia de aplicaciones gubernamentales desarrolladas en Open Source que permiten integrar los procesos de la institución.	Poca predisposición de tendencia al cambio tecnológico por parte del usuario final.
Predisposición de las Unidades Ejecutoras en buscar la integración de las tecnologías de la información	Costos elevados de licenciamiento de Software.
Existencia de políticas y lineamientos establecidos por los entes gubernamentales superiores.	

Anexo 12. Determinación del Alcance

Figura 23. Diagrama de las Elipses



Anexo 13. Activos de Información

Activos de información

- **Información**
- Documentos de Gestión
- **Servicios**
- Internet
- Energía eléctrica
- Correo electrónico Institucional
- **Personas**
- Responsable de transparencia de la Sub Gerencia de TI
- Responsable de transparencia de cada Unidad ejecutora.
- Coordinadores.
- **Software**
- Sistema de Gestor de Contenidos.
- Sistema Operativos.
- Gestor de Base de datos
- **Hardware**
- Servidor web.
- Servidor de archivos.
- Servidor de base de datos (Los usuarios e información que van a subir)
- Equipos de Comunicación. (Switches)
- Central telefónica.
- Desktop
- **Intangible**
- Prestigio de la institución
- Información

Anexo 14. Identificación de Riesgos

Tabla 5. Identificación de Riesgos

N°	Riesgo	Origen(es)	Áreas de impacto	Sucesos	Causas	Consecuencias potenciales	Propietario
R1	Pérdida total o parcial de los activos de información	Inundación	Toda la Sede	Inundación del sector de la localidad donde está ubicada la Sede.	Fenómeno del Niño (lluvias intensas).	Integridad y disponibilidad	Seguridad
R2	Pérdida total o parcial de los activos de información	Sismo	Toda o parte de la Sede	Derrumbe de edificios e infraestructura en general en zona afectada.	Desplazamiento de placas de la corteza terrestre	Integridad y disponibilidad	Seguridad
R3	Pérdida total o parcial de los activos de información	Fuego/Explosión	Toda o parte de la Sede	Incineración de todo o parte de la infraestructura	Cercanía a Grifo con materiales altamente inflamables.	Integridad y disponibilidad	Seguridad
R4	Pérdida total o parcial de los activos de información	Vandalismo	Toda o parte de la Sede	Destrucción de la propiedad privada	Factores sociales	Disponibilidad	Seguridad

R5	No contar con acceso a los activos de información digitales	Caída de energía	Todos los grupos de interés	Apagado de los equipos informáticos	Incumplimiento del proveedor	Integridad y disponibilidad	Logística
R6	No contar con acceso a los activos de información digitales	Caída de energía	Todos o algunos de los grupos de interés	Apagado de los equipos informáticos	Sobrecarga de energía que sobrepasa la potencia contratada	Disponibilidad	Logística
R7	No contar con acceso a los activos de información digitales	Falla de hardware	Tecnología	Error de acceso a la data	Antigüedad de los equipos	Disponibilidad	SGTI
R8	No contar con acceso a los activos de información digitales	Falla de hardware	Tecnología	Error de acceso a la data	Falta de mantenimiento	Disponibilidad	SGTI
R9	No contar con acceso a los activos de información digitales	Falla de red interna	Tecnología	Degradación y/o posible caída de la red de datos.	Gestión de red inadecuada	Disponibilidad	SGTI
R10	Pérdida de acceso a la plataforma de transparencia de la sede.	Falla en el acceso a internet	Unidades Ejecutoras con portales alojados en	Pérdida del acceso a la red externa (internet) en la sede	Incumplimiento en el proveedor de internet	Disponibilidad	Logística

			sede, Coordinación de Transparencia de SGTI				
R11	No contar con acceso a los activos de información digitales	Hackeo	Tecnología	Ataque a la plataforma de de CMS	Falta de actualización de la plataforma CMS	Disponibilidad	SGTI
R12	Gestión ineficiente de los procesos durante la curva de aprendizaje del nuevo personal.	Pérdida de personal	Coordinación de Transparencia SGTI y UE	El Coordinador de Transparencia de la SGTI deja la institución.	Mejores oportunidades en el mercado laboral	Disponibilidad	SGRH
R13	Gestión ineficiente de los procesos durante la curva de aprendizaje del nuevo personal	Pérdida de personal	Coordinación de Transparencia SGTI	El Coordinador de Transparencia de la SGTI deja la institución.	Despido	Disponibilidad	SGRH
R14	Impedimento de ingreso del personal a	Huelgas	Unidades orgánicas de sede	Paro de labores	Descontento de los empleados	Disponibilidad	Seguridad

	laborar con normalidad						
R15	Pérdida de información	Hackeo	Tecnología	Ataque a la infraestructura tecnológica	Falla en la seguridad perimetral	Disponibilidad	SGTI
R16	Pérdida de información	Hackeo	Tecnología	Ataque a la infraestructura tecnológica	Falla en la seguridad interna	Disponibilidad	SGTI
R17	Robo de información	Acceso a la información física	Unidad Orgánica propietaria	Sustracción de documentos	Empleado descontento	Disponibilidad	Seguridad, Propietario Activo
R18	Robo de información	Acceso a la información digital	Tecnología, UE	Suplantación de Identidad	Falta de política de entrega de de credenciales	Confidencialidad	SGTI
R19	Pérdida de información	Hurto	Unidad Orgánica propietaria	Sustracción de documentos	Sabotaje	Disponibilidad	Seguridad
R20	Pérdida de información	Falla de hardware	Unidad Orgánica propietaria	Error en los dispositivos de almacenamiento	Antigüedad	Disponibilidad	SGTI

R21	Pérdida de información	Virus	Tecnología	Virus infecta la infraestructura tecnológica	Falta de una cultura de uso consciente de las herramientas de TI.	Disponibilidad	SGTI

Anexo 15. Análisis y Evaluación de los Riesgos

- ✓ **Criterios de Probabilidad**

Tabla 6. Criterios de Probabilidad

Nivel de probabilidad de ocurrencia	**1**	**2**	**3**	**4**	**5**
	Muy Bajo	**Bajo**	**Medio**	**Alto**	**Muy Alto**
Nivel de frecuencia	1 vez cada 2 o más años	1 vez al año	2 o 3 veces al año	4 o 5 veces al año	De 6 a más
Nivel de vulnerabilidad	Muy Bajo	Bajo	Media	Alta	Muy Alto
Nivel de controles actuales	81-100%	61-80%	41-60%	21-40%	0-20 %

✓ **Criterios de Impacto**

Tabla 7. Criterios de Impacto

Nivel de impacto	**1**	**2**	**3**	**4**	**5**
	Muy Bajo	**Bajo**	**Medio**	**Alto**	**Muy Alto**
Tiempo de recuperación	Inmediata	Entre 1 y 3 Horas	Entre 3 y 6 Horas	Entre 6 y 9 horas	más de 9 horas
Pérdida de imagen	Descrédito mínimo	Descrédito parcial y recuperable	Descredito parcial y Permanente	Descredito total pero recuperable	Descredito total y permanente
Afectación a la operatividad de los procesos	Afecta una actividad	Afecta más de una actividad	Afecta un proceso	Afecta más de un proceso	Afecta a toda la organización

✓ **Matriz Probabilidad de Ocurrencia e impacto**

Tabla 8. Matriz Probabilidad de Ocurrencia e impacto

Probabilidad de Ocurrencia	**Muy Alto**	**5**	Moderado (5)	Importante (10)	Importante (15)	Inaceptable (20)	Inaceptable (25)
	Alto	**4**	Tolerable (4)	Moderado (8)	Importante (12)	Importante (16)	Inaceptable (20)
	Medio	**3**	Tolerable (3)	Moderado (6)	Moderado (9)	Importante (12)	Importante (15)
	Bajo	**2**	Aceptable (2)	Tolerable (4)	Moderado (6)	Moderado (8)	Importante (10)
	Muy Bajo	**1**	Aceptable (1)	Aceptable (2)	Tolerable (3)	Tolerable (4)	Moderado (5)
Nivel de riesgo (probabilidad de ocurrencia x impacto)			**1**	**2**	**3**	**4**	**5**
			Muy Bajo	**Bajo**	**Medio**	**Alto**	**Muy Alto**
			Impacto				

Anexo 16. Evaluación de Riesgos

- ✓ **Impacto**

Tabla 9. Evaluación de Riesgos-Impacto

Riesgos		Causas	Análisis de Riesgo															
			Posibilidad de Ocurrencia															
			Pérdida de Imagen					Tiempo de Recuperación					Operatividad					Valor del impacto
			AYP	YPM	JCHC	LCNC	PROM	AYP	YPM	JCHC	LCNC	PROM	AYP	YPM	JCHC	LCNC	PROM	
R1	Pérdida total o parcial de los activos de información	Fenómeno del Niño (lluvias intensas, huaicos)	2	2	1	3	2	5	5	5	4	4,75	5	5	5	5	5	3,916666667
R2	Pérdida total o parcial de los activos de información	Desplazamiento de placas	2	2	1	3	2	5	5	5	4	4,75	5	5	5	5	5	3,916666667

		de la corteza terrestre																
R 3	Pérdida total o parcial de los activos de información	Cercanía a Grifo con materiales altamente inflamables.	2	2	2	2	2	5	5	5	4	4,75	5	5	5	5	5	3,916666667
R 4	Pérdida total o parcial de los activos de información	Factores sociales	2	2	2	2	2	5	5	5	4	4,75	5	5	5	5	5	3,916666667
R 5	Pérdida de acceso a los activos de información digitales	Incumplimiento del proveedor de energía	3	4	4	4	3,75	1	1	1	1	1	5	5	5	5	5	3,25

R 6	Pérdida con acceso a los activos de información digitales	Sobrecarga de energía que sobrepasa la potencia contratada	4	4	4	5	4,25	1	1	2	1	1,25	5	5	4	5	4,75	3,416666667
R 7	Pérdida de acceso a los activos de información digitales	Antigüedad de los equipos	4	4	4	5	4,25	3	4	3	3	3,25	3	3	4	4	3,5	3,666666667
R 8	Pérdida de acceso a los activos de información digitales	Falta de mantenimiento	4	4	4	5	4,25	3	4	3	3	3,25	3	3	4	4	3,5	3,666666667
R 9	Pérdida de acceso a los activos de	Gestión de red	4	4	4	5	4,25	1	2	2	2	1,75	2	2	2	2	2	2,666666667

	información digitales	inadecuada																
R 10	Pérdida de acceso a la plataforma de transparencia de la sede.	Incumplimiento en el proveedor de internet	4	4	4	5	4,25	1	1	1	1	1	4	4	4	4	4	3,083333333
R 11	Pérdida de Acceso acceso a los activos de información digitales	Falta de actualización de la plataforma CMS	4	5	4	5	4,5	1	1	2	2	1,5	4	4	5	4	4,25	3,416666667
R 12	Gestión ineficiente de los procesos durante la curva de aprendizaje del nuevo personal	Mejores oportunidades en el mercado laboral	1	2	1	2	1,5	1	1	1	1	1	1	1	1	1	1	1,166666667

R 13	Gestión ineficiente de los procesos durante la curva de aprendizaje del nuevo personal	Despido	1	2	1	2	1,5	1	1	1	1	1	1	1	1	1	1	1,166666667
R 14	Impedimento de ingreso del personal a laborar con normalidad	Descontento de los empleados	3	3	3	3	3	1	1	1	1	1	1	1	1	1	1	1,666666667
R 15	Pérdida de información	Falla en la seguridad perimetral	4	4	5	4	4,25	2	2	3	2	2,25	4	4	5	4	4,25	3,583333333
R 16	Pérdida de información	Falla en la	3	2	3	3	2,75	2	2	2	2	2	2	1	4	3	2,5	2,416666667

		seguridad interna																
R 17	Robo de información	Empleado descontento	4	4	4	3	3,75	1	1	1	1	1	1	1	1	1	1	1,916666667
R 18	Robo de información	Falta de política de entrega de de credenciales	4	4	4	3	3,75	1	1	1	1	1	1	1	1	1	1	1,916666667
R 19	Pérdida de información	Sabotaje	4	4	4	3	3,75	2	2	2	2	2	1	2	1	2	1,5	2,416666667
R 20	Pérdida de información	Antigüedad	4	4	5	4	4,25	3	4	4	3	3,5	4	4	5	4	4,25	4
R 21	Pérdida de información	Falta de una cultura de uso	4	4	4	4	4	1	2	1	2	1,5	1	2	1	2	1,5	2,333333333

		consciente de las herramientas de TI.																

- ✓ **Posibilidad de Ocurrencia**

Tabla 10. Evaluación de Riesgos - Posibilidad de Ocurrencia

Riesgo		**Origenes**	**Area de impacto**	**Sucesos**	**Causas**	**Analisis de Riesgo**																		**Evaluación de Riesgo**	
						Posibilidad de Ocurrencia																			
						AYP	**YPM**	**JCHC**	**LCNC**	**PROM**	**AYP**	**YPM**	**JCHC**	**LCNC**	**PROM**	**AYP**	**YPM**	**JCHC**	**LCNC**	**PROM**	**Prom. De la Prob ab.**	**Valor del impacto**	**Valor Final de Análisis del Riesgo**	**Severidad del Riesgo (*)**	**Priorización del Riesgo**
R1	Pérdida total o parci	Inundación	Toda la Sede	Inundación del sector	Fenómeno del Niño	1	1	1	1	1	1	1	1	1	1	3	2	1	2	2	1,33	3,92	5,22	Aceptable	1

	al de los activos de información			de la localidad donde está ubicada la Sede.	(lluvias intensas, huaicos)																				
R2	Pérdida total o parcial de los activos de información	Sismo	Toda o parte de la Sede	Derrumbe de edificios e infraestructura en general en zona afectada.	Desplazamiento de placas de la corteza terrestre	1	1	1	1	1	5	5	5	5	5	2	3	2	2	2,25	2,75	3,92	10,77	Importante	12

R3	Pérdida total o parcial de los activos de información	Fuego/ Explosión	Toda o parte de la Sede	Incineración de todo o parte de la infraestructura	Cercanía a Grifo con materiales altamente inflamables.	1	1	1	1	1	1	1	1	1	1	3	3	2	2	2,5	1,50	3,92	5,88	Moderado	8
R4	Pérdida total o parcial de los activos de información	Vandalismo	Toda o parte de la Sede	Destrucción de la propiedad privada	Factores sociales	1	1	1	1	1	3	4	3	3	3,25	3	3	3	3	3	2,42	3,92	9,47	Importante	12

R5	Pérdida de acceso a los activos de información digitales	Caída de energía	Todos los grupos de interés	Apagado de los equipos informáticos	Incumplimiento del proveedor de energía	3	3	3	3	3	5	4	4	4	4,25	2	2	2	2	2	3,08	3,25	10,02	Importante	16
R6	Pérdida con acceso a los activos de infor	Caída de energía	Todos o algunos de los grupos de interés	Apagado de los equipos informáticos	Sobrecarga de energía que sobrepasa la potencia	4	4	4	4	4	5	4	4	4	4,25	1	2	2	2	1,75	3,33	3,42	11,39	Importante	16

	mación digitales				contratada																				
R7	Pérdida de acceso a los activos de información digitales	Falla de hardware	Tecnología	Error de acceso a la data	Antigüedad de los equipos	3	2	2	3	2,5	3	3	3	3	3	2	2	2	2	2	2,50	3,67	9,17	Importante	12
R8	Pérdida de acceso a los	Falla de hardware	Tecnología	Error de acceso a la data	Falta de mantenimiento	2	3	1	3	2,25	4	4	4	4	4	2	2	2	2	2	2,75	3,67	10,08	Importante	12

	activos de información digitales																							
R9	Pérdida de acceso a los activos de información digitales	Falla de red interna	Tecnología	Degradación y/o posible caída de la red de datos.	Gestión de red inadecuada	1	2	1	2	1,5	3	4	3	3	3,25	2	2	2	2	2	2,25	2,67	6,00	Moderado	9

R10	Pérdida de acceso a la plataforma de transparencia de la sede.	Falla en el acceso a internet	Unidades Ejecutoras con portales alojados en sede, Coordinación de Transparencia de SGTI	Pérdida del acceso a la red externa (internet) en la sede	Incumplimiento en el proveedor de internet	1	2	1	1	1,25	4	4	4	4	4	1	1	1	1	1	2,08	3,08	6,42	Importante	12
R11	Pérdida de Acceso acces	Hackeo	Tecnología	Ataque a la plataforma de CMS	Falta de actualización de la	1	1	1	1	1	4	4	3	4	3,75	2	2	2	2	2	2,25	3,42	7,69	Importante	12

	o a los activos de información digitales				plataforma CMS																				
R12	Gestión ineficiente de los procesos durante la curva de apren	Pérdida de personal	Coordinación de Transparencia SGTI y UE	El Coordinador de Transparencia de la SGTI deja la institución.	Mejores oportunidades en el mercado laboral	3	2	2	2	2,25	3	3	3	3	3	3	2	2	2	2,25	2,50	1,17	2,92	Moderado	6

	dizaje del nuevo personal																							
R13	Gestión ineficiente de los procesos durante la curva de aprendizaje del nuevo	Pérdida de personal	Coordinación de Transparencia SGTI	El Coordinador de Transparencia de la SGTI deja la institución.	Despido	1	1	1	2	1,25	2	2	2	2	2	3	2	3	3	2,75	2,00	1,17	2,33	Tolerable	4

	personal																								
R14	Impedimento de ingreso del personal a laborar con normalidad	Huelgas	Unidades orgánicas de sede	Paro de labores	Descontento de los empleados	2	2	2	2	2	4	3	4	3	3,5	3	3	3	3	3	2,83	1,67	4,72	Moderado	6
R15	Pérdida de información	Hackeo	Tecnología	Ataque a la infraestructura	Falla en la seguridad	2	2	2	2	2	1	1	1	1	1	5	4	5	5	4,75	2,58	3,58	9,26	Importante	12

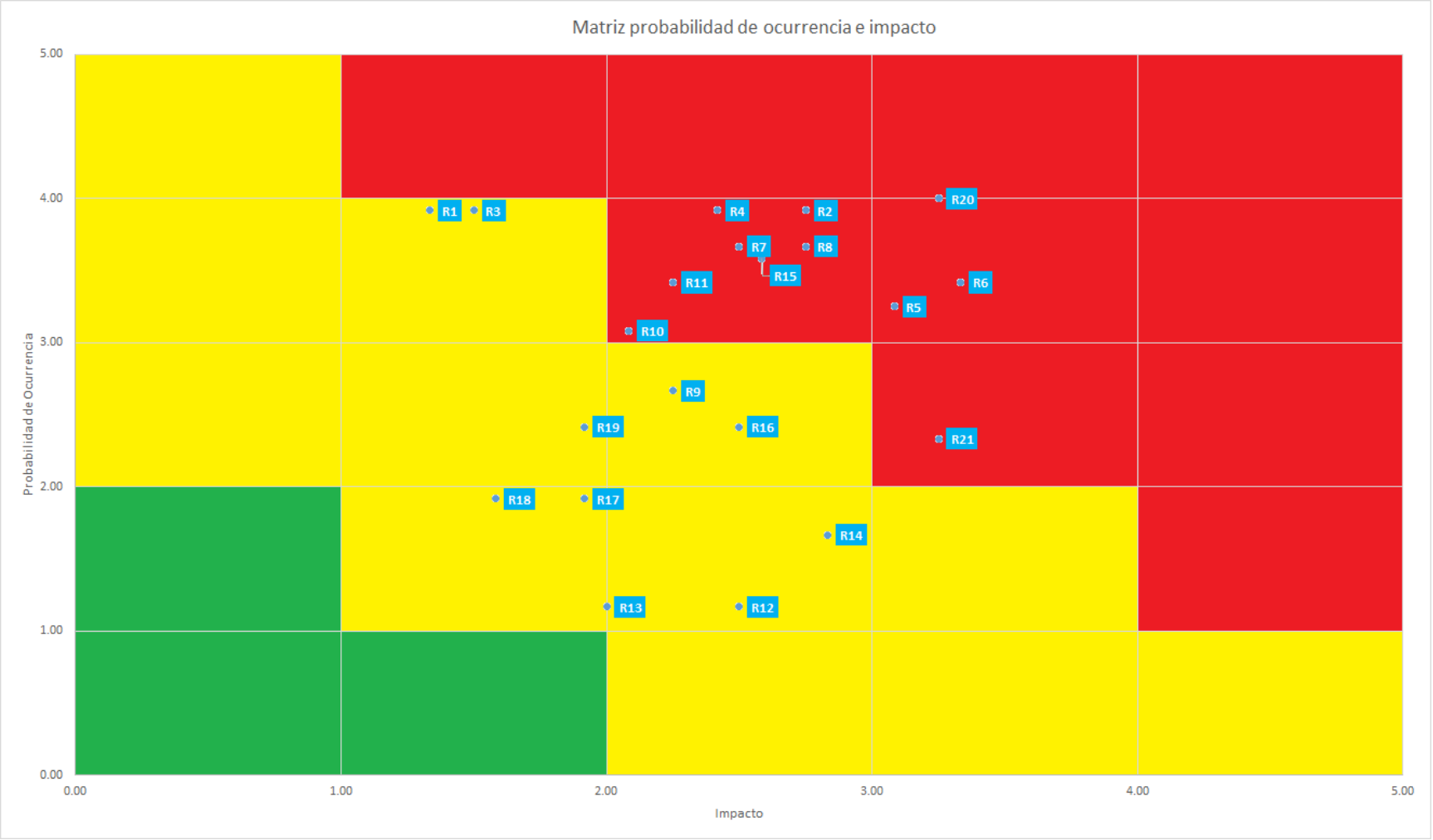
				tecnológica	perimetral																			
R16	Pérdida de información	Hackeo	Tecnología	Ataque a la infraestructura tecnológica	Falla en la seguridad interna	3	3	3	3	3	2	2	4	2	2,5	2	2	2	2	2	2,50	2,42	6,04	Moderado	9
R17	Robo de información	Acceso a la información física	Unidad Orgánica propietaria	Sustracción de documentos	Empleado descontento	1	2	1	2	1,5	3	3	4	3	3,25	1	1	1	1	1	1,92	1,92	3,67	Tolerable	4
R18	Robo de información	Acceso a la información digital	Tecnología, UE	Suplantación de Identidad	Suplantación de Identidad	1	1	1	1	1	2	3	3	3	2,75	1	1	1	1	1	1,58	1,92	3,03	Tolerable	4

R19	Pérdida de información	Hurto	Unidad Orgánica propietaria	Sustracción de documentos	Sabotaje	1	1	1	1	1	3	3	4	3	3,25	1	2	1	2	1,5	1,92	2,42	4,63	Moderado	6
R20	Pérdida de información	Falla de hardware	Unidad Orgánica propietaria	Error en los dispositivos de almacenamiento	Antigüedad de los equipos	3	3	4	4	3,5	3	4	3	4	3,5	3	3	2	3	2,75	3,25	4,00	13,00	Importante	16
R21	Pérdida de información	Virus	Tecnología	Virus infecta la infraestructura	Falta de una cultura de uso consciente de las	4	4	4	4	4	2	3	2	3	2,5	3	3	3	4	3,25	3,25	2,33	7,58	Importante	12

				tecnológica	herramientas de TI.																				

- ✓ **Mapa de Calor**

Figura 24. Mapa de Calor



✓ **Estrategia de respuesta a los riesgos**

Tabla 11. Estrategia de Respuesta a Riesgos

Riesgo		Origen	Suceso	Causas	Evaluación de Riesgo		Respuesta al riesgo						Identificación de activos			
					Severidad del Riesgo	Priorización del Riesgo	Estrategia de respuesta	Control ISO 27001:2013		Medida de respuesta o contrl	Responsable del riesgo	Responsable de la implementación de la medida de respuesta o control	Nombre del activo	Propietario del activo	Controles actuales	Vulnerabilidades
								Código	Detalle							
R6	Pérdida de Acceso acces	Caída de energía	Apagado de los equipos	Sobrecarga de energía que	Importante	16	Mitigar	A.11.2.2	Los equipos deben ser protegidos contra fallas de	Adquisición sub estación	Logística	Logística	Servidores y equipos de	Usuarios Finales		Existencia de equipos que sobrep

	o a los activos de información digitales	eléctrica	informáticos	sobrepasa la potencia contratada				electricidad y otras alteraciones causadas por fallas en los servicios de suministros.	eléctrica			comunicación			asan la potencia de energía contratada
R11	Pérdida de Acceso a los activos de información	Hackeo	Ataque a la plataforma de de CMS	Falta de actualización de la plataforma CMS	Importante	12	Mitigar	A.12.5.1	Procedimientos deben ser implementados para controlar la instalación de software en sistemas operacionales.	Se deberá contar con un manual de procedimientos para la actuali	Administrador de Infraestructura	Administrador de Infraestructura	Gestor de Contenidos	Responsable de Transparencia de SGTI		No este actualizado el CMS

	digitales									zación del CMS						
								A.12.2.1	Controles de detección, prevención y recuperación para proteger contra códigos maliciosos deben ser implementadas, en combinación con una concientización	Adquirir con un UTM que tenga visibilidad hasta la capa de aplicación de los paquetes entran	Administrador de Infraestructura	Administrador de Infraestructura	Gestor de Contenidos	Responsable de Transparencia de SGTI	Firewall Perimetral (Antivirus,Filtrado web)	No este actualizado el CMS

									apropiada de los usuarios.	tes a la red.						
								A.12.4.1	Registros (logs) de eventos de actividades de usuarios,excepciones,fallas y eventos de seguridad de la información deben ser producidos, mantenidos y regularmen	Instalar un SisLog	Administrador de Infraestructura	Administrador de Infraestructura	Servidores (Gestor de Contenidos, Equipos de Comunicación)	Responsable de Transparencia de SGTI	Registro de eventos de cada servidor	No este actualizado el CMS

									te revisados.							
R10	Pérdida de acceso a la plataforma de transparencia de la sede.	Falla en el acceso a internet	Pérdida del acceso a la red externa (internet) en la sede	Incumplimiento en el proveedor de internet	Importante	12	Mitigar	A17.2.1	Las instalaciones de procesamiento de la información deben ser implementadas con redundancia suficiente para cumplir con los requisitos de disponibilidad.	Contar con una solución de Router en alta disponibilidad Contratar una Línea Respaldo con un proveedor	Logística	SGTI	Administrador de contenidos (CMS)	Responsable de Transparencia de la región		Tener un único punto de acceso a Internet

									diferente						
R20	Pérdida de información	Falla de hardware	Error en los dispositivos de almacenamiento	Antigüedad de los equipos	Importante	16	Mitigar	A.12.3.1	Respaldo de información	Adquisición de una Librería Robótica	SGTI	Infraestructura tecnológica	Base de datos de visitas	Administrador de Base de datos	Backups	No se tiene copia respaldo
R21	Pérdida de información	Virus	Virus infecta la infraestructura tecnológica	Falta de una cultura de uso consciente de las herramient	Importante	12	Mitigar	A.7.2.2	Todos los empleados de la organización y cuando fuera relevante, los contratistas deben recibir	Sensibilización, Charlas y capacitación	SGTI	Gerencia Planificación y modernización	Servidores	Empleados y Proveedores	Antivirus en los equipos.	Falta de Concientización del personal

				as de TI.					educación y educación sobre la conciencia de la seguridad de la información, así como actualizaciones regulables sobre políticas y procedimientos de la organización, según sea relevante para la función del								

									trabajo que cumplen.							
								A.8.3.1	Se debe implementar procedimientos para la gestión de medios removibles en concordancia con el esquema de clasificación adoptado por la	Denegar permisos de lectura escritura en dispositivos extraíbles	SGTI	Administrador de Infraestructura	Servidores (Gestor de Contenidos, Equipos de Comunicación)	Empleados y Proveedores		Falta de política de control de medios extraíbles

									organización.							
								A.9.1.2	Los usuarios deben tener acceso solamente a la red y a servicios de red que hayan sido especialmente autorizados a usar.	Creación de una política de control de acceso por perfiles de usuario	SGTI	SGTI	Servidores (Gestor de Contenidos, Equipos de Comunicación,PCs)	Empleados y Proveedores	Firewall Perimetral (Antivirus, Filtrado web)	Falta de política de control de acceso por perfiles de usuarios.

- ✓ **Plan de Tratamiento de Drogas**

Tabla 12. Plan de tratamiento de riesgos

Código	Riesgo	Responsable del riesgo	Activo asociado al riesgo	Medida de respuesta o control	Responsable de la implementación de la medida de respuesta o control	Recursos requeridos				Cronograma de implementación																	
						Cantidad	Descripción del recurso	Monto	Presupuesto total	E	F	M	A	M	J	J	A	S	O	N	D	E	F	M	A	M	J
R6	Pérdida de Acceso a los activos de información	Logística	Servidores y equipos de comunicación	Adquisición sub estación eléctrica	Logística	1	Adquisición de una sub estación eléctrica,	S/. 120.000,00	S/. 120.000,00																		

	digitales						Trifásica																				
R11	Pérdida de Acceso a los activos de información digitales	Administrador de Infraestructura	Gestor de Contenidos	Se deberá contar con un manual de procedimientos para la actualización del CMS	Administrador de Infraestructura	1	Personal	S/. 1.045,00	S/. 1.045,00																		
		Administrador de Infraestructura	Gestor de Contenidos	Adquirir UTM	Administrador de Infraestructura	1	Adquirir UTM que tenga visibilidad hasta	S/. 300.000,00	S/. 300.000,00																		

							la capa de aplicación de los paquetes entrantes a la red.																									
		Administrador de Infraestructura	Servidores (Gestor de Contenidos, Equipos de Comunicación)	Instalar SisLog	Administrador de Infraestructura	1	Personal	S/. 40,00	S/. 40,00																						
R10	Pérdida de acceso a la	Logística	Administrador de contenidos (CMS)	Contar con solución de	SGTI	1	Router Cisco Serie 1800	S/. 39.240,00	S/. 39.240,00																						

	plataforma de transparencia de la sede.			Router en alta disponibilidad																							
				Contratar una Línea Respaldo con un proveedor diferente		1	Línea de Respaldo	S/. 6.000,00	S/. 6.000,00																		
R20	Pérdida de información	SGTI	Base de datos de visitas	Adquisición de Librería Robótica	Infraestructura tecnológica	1	Librería robótica, MSL2024 HP	S/. 33.000,00	S/. 33.000,00																		
R21	Pérdida de	SGTI	Servidores	Sensibilización, Charlas	Gerencia Planificación y	1	Personal	S/. 2.300,00	S/. 2.300,00																		

	informa ción			y capacita ción	moderniz ación																								
		SGTI	Servidores (Gestor de Contenido s, Equipos de Comunicac ión)	Denegar permiso s de lectura escritura en dispositi vos extraíble s a través active Director y	Administr ador de Infraestru ctura	1	Person al	S/. 2.300, 00	S/. 2.300,0 0																				
		SGTI	Servidores (Gestor de Contenido s, Equipos	Creació n de una política de	SGTI	1	Person al	S/. 3.500, 00	S/. 3.500,0 0																				

			de Comunicación,PCs)	control de acceso a la red por perfiles de usuario																							
Inversión								S/. 507.425,00	S/. 507.425,00																		

Anexo 17. Plantilla Modelo

TITULO DEL DOCUMENTO

Código:	SGSI-001
Versión:	0.1
Fecha de la versión:	17/04/2018
Creado por:	Alex Cornejo
Aprobado por:	Sub Gerencia de TI GRLL
Nombre del archivo:	Sgsi-000.docx
Nivel de confidencialidad:	Baja

Historial de Revisiones

Fecha	Versión		Modificado/Creado por	Descripción de la modificación
26/11/2014	0.1		xxxxxxxxxxxxxxx	Creación del primer documento

Aprobación

Fecha	Nombre	Cargo	Sello y Firma

Mejora Continua

Fecha	Revisor/Auditor	Resumen Observaciones

Tabla de contenido

Anexo 18. Plantilla Modelo Ejemplo

Plan del Proyecto

PLAN DEL PROYECTO PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Código:	SGSI-001
Versión:	0.1
Fecha de la versión:	26/11/2014
Creado por:	xxxxxxxxxxxxxxxxx
Aprobado por:	yyyyyyyyyyyyyyyy
Nombre del archivo:	SGSI-001 - Plan del Proyecto.docx
Nivel de confidencialidad:	Baja

Historial de Revisiones

26/11/2014	0.1	xxxxxxxxxxxxxx	Creación del primer documento

Distribución

Aprobación

Mejora Continua
