UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS
FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Presentado por:

DIEGO MILKER ESCALANTE CORONEL

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BAJO EL ENFOQUE DE LA NTP ISO/IEC 27001 PARA LA DIRECCIÓN DE SALUD VIRGEN DE COCHARCAS – CHINCHEROS

Asesor:

Dr. Julio Cesar Huanca Marín

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

ANDAHUAYLAS - APURÍMAC - PERÚ

2019

APROBACIÓN DEL ASESOR

APROBACION DEL ASESOR

Quién suscribe:
Dr. Julio Cesar Huanca Marín, por la presente:

CERTIFICA,
Que, el Bachiller en Ingeniería de Sistemas, DIEGO MILKER ESCALANTE CORONEL ha culminado satisfactoriamente el informe final de tesis intitulado: "DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION BAJO EL ENFOQUE DE LA NTP ISO/IEC 27001 PARA LA DIRECCION DE SALUD VIRGEN DE COCHARCAS - CHINCHEROS" para optar el Título Profesional de Ingeniero de Sistemas.

Andahuaylas, 13 de setiembre del 2019.

Dr. Julio Cesar Huanca Marín
Asesor

Br. Diego Milker Escalante Coronel
Tesista

APROBACIÓN DEL JURADO DICTAMINADOR

APROBACIÓN DEL JURADO DICTAMINADOR

LA TESIS: "DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BAJO EL ENFOQUE DE LA NTP ISO/IEC 27001 PARA LA DIRECCIÓN DE SALUD VIRGEN DE COCHARCAS - CHINCHEROS"; para optar el Título Profesional de ingeniero de sistemas, ha sido evaluada por el Jurado Dictaminador conformado por:

PRESIDENTE: DRA. CECILIA EDITH GARCÍA RIVAS PLATA
PRIMER MIEMBRO: DR. YALMAR TEMISTOCLES PONCE ATENCIO
SEGUNDO MIEMBRO: MTR. JUAN JOSÉ ORÉ CERRÓN

Habiendo sido aprobado por UNANIMIDAD, en la ciudad de Andahuaylas el día 5 del mes de setiembre de 2019

Andahuaylas, 13 de setiembre de 2019.

DRA. CECILIA EDITH GARCÍA RIVAS PLATA
PRESIDENTE DEL JURADO DICTAMINADOR

DR. YALMAR TEMISTOCLES PONCE ATENCIO
PRIMER MIEMBRO DEL JURADO DICTAMINADOR

MTR. JUAN JOSÉ ORÉ CERRÓN
SEGUNDO MIEMBRO DEL JURADO DICTAMINADOR

DECLARACIÓN JURADA DE AUTENTICIDAD

DECLARACIÓN JURADA DE AUTENTICIDAD

Yo, Diego Milker Escalante Coronel identificado (a) con DNI N° 47416734 de la Escuela Profesional de Ingeniería de Sistemas
Declaro bajo juramento que el Proyecto Titulado: "DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BAJO EL ENFOQUE DE LA NTP ISO/IEC 27001 PARA LA DIRECCIÓN DE SALUD VIRGEN DE COCHARCAS - CHINCHEROS"; Es auténtico y no vulnera los derechos de autor. Además, su contenido es de entera responsabilidad del autor (es) del proyecto, quedando la UNAJMA exenta de toda responsabilidad en caso de atentar contra la Ley de propiedad intelectual y derechos de autor.

Andahuaylas, 13 de setiembre de 2019

.....
Firma
N° DNI: 47416734
E-mail: descalantecoronel@gmail.com
N° Celular: 983614495

ACTA DE SUSTENTACION DE TESIS

Universidad Nacional José María Arguedas

Identidad y Excelencia para el Trabajo Productivo y el Desarrollo

FACULTAD DE INGENIERÍA

ACTA DE SUSTENTACIÓN DE TESIS

En la Av. José María Arguedas del Local Académico SL01 (Ccoyahuacho) en el auditorio de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional José María Arguedas ubicado en el distrito de San Jerónimo de la Provincia de Andahuaylas, siendo las 17:00 horas del día 05 de setiembre del año 2019, se reunieron los docentes: Dra. Cecilia Edith García Rivas Plata, Dr. Yalmar Temístocles Ponce Atencio, Mtr. Juan José Oré Cerrón, en condición de integrantes del Jurado Evaluador del Informe Final de Tesis intitulado: "DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BAJO EL ENFOQUE DE LA NTP ISO/IEC 27001 PARA LA DIRECCIÓN DE SALUD VIRGEN DE COCHARCAS – CHINCHEROS", cuyo autor es el Bachiller en Ingeniería de Sistemas **DIEGO MILKER ESCALANTE CORONEL**, el asesor Dr. Julio César Huanca Marín, con el propósito de proceder a la sustentación y defensa de dicha tesis.

Luego de la sustentación y defensa de la tesis, el Jurado Evaluador **ACORDÓ**: aprobar por unanimidad al Bachiller en Ingeniería de Sistemas **DIEGO MILKER ESCALANTE CORONEL**, obteniendo la siguiente calificación y mención:

Nota escala vigesimal		Mención
Números	Letras	
15	quince	bueno

En señal de conformidad, se procedió a la firma de la presente acta en 03 ejemplares.

.....
Dra. Cecilia Edith García Rivas Plata
Presidente del Jurado Evaluador

.....
Dr. Yalmar Temístocles Ponce Atencio
Primer Miembro del Jurado Evaluador

.....
Mtr. Juan José Oré Cerrón
Segundo Miembro del Jurado Evaluador

DEDICATORIA

A Dios, por regalarme la vida y poner a las personas indicadas en mi camino siempre.

A mis padres, por su compañía, confianza, consejos y solidaridad durante todo el camino transitado; quienes son mi fuente de motivación y ejemplo para ser un gran hombre.

A mis docentes, que con su esfuerzo e insistencia me enseñaron que es posible construir un mundo de excelencia, justicia, libertad, tolerancia, estudio, trabajo y perseverancia.

AGRADECIMIENTO

A Dios por haberme dado la vida.

Al culminar tal vez uno de los retos más complicados que he tenido en mi vida, es justo dar las gracias a un sin número de personas que de una u otra forma han contribuido para que culminar mi carrera sea una realidad.

A mis padres por darme la oportunidad de estudiar y depositar toda la confianza en mi persona, por su ejemplo al demostrarme día a día que no hay otro camino para la felicidad que el trabajo honesto, y apoyo incondicional en los tiempos difíciles.

Agradezco a cada uno de los docentes que fueron parte esencial en mi formación profesional, no solo por ser grandes maestros sino por haberme brindado su amistad, en especial a mi asesor Dr. Julio Cesar Huanca Marín por todo el apoyo a lo largo de la realización de esta tesis.

INDICE

INDICE DE TABLAS

INDICE DE FIGURAS

RESUMEN

En la presente tesis en la Dirección de Salud Virgen de Cocharcas se implementó el "Diseño de un Sistema de Gestión de Seguridad de la Información bajo el enfoque de la NTP ISO/IEC 27001:2014".

La información es un activo valioso para las empresas, instituciones, organizaciones, tanto en el sector público como privado, por lo que buscan diferentes formas de salvaguardar la información de los riesgos ya sea internos como externos.

Debido a la importancia que tiene este activo, la Organización Internacional de Normalización crea una norma específica para la seguridad de la información, la cual es denominada como un Sistema de Gestión de la Seguridad de la Información (SGSI).

A consecuencia de la importancia que le brindan a la información la presente tesis ha realizado una investigación de las normas, estándares y buenas prácticas reconocidas mundialmente, para poder desarrollar cada una de las etapas del SGSI, tomando como enfoque la NTP ISO/IEC 27001:2014, a partir de los cuales en la entidad Dirección de Salud Virgen de Cocharcas, se implementó el "Diseño de un Sistema de Gestión de Seguridad de la Información bajo el enfoque de la NTP ISO/IEC 27001, la cual permitirá que ésta cumpla con las normas de regulación vigente respecto a la seguridad de la información.

La implementación está dividida en tres fases: **Primera fase:** Se realizó el diagnóstico inicial de la DISA V.C. con respecto a la NTP ISO/IEC 27001:2014 y su posibilidad de aceptación, en **Segunda fase**: Se estudió a la organización y su contexto; se identificó el proceso crítico; se definió la política de seguridad, el alcance y se identificó al comité de seguridad de la información de la organización y como **tercera fase:** Siguiendo la metodología de análisis y gestión de riesgos adoptada, se identificó y valoró los activos de información, las amenazas, se realizó el cálculo del impacto y del riesgo, se identificaron las medidas de control necesarias para mitigar los riesgos a un nivel aceptable y finalmente se elaboró un documento denominado declaración de aplicabilidad que contiene la justificación de qué controles del Anexo A de la NTP ISO/IEC 27001:2014 pueden ser implementados en la entidad.

Palabras claves: Seguridad de la información, ISO/IEC 27001:2014, Análisis, Riesgo.

ABSTRACT

In this thesis at the Health Department Virgen de Cocharcas, the "Design of an Information Security Management System under the approach of NTP ISO / IEC 27001: 2014" was implemented.

Information is a valuable asset for companies, institutions, organizations, both in the public and private sectors, so they seek different ways to safeguard information from risks, both internal and external.

Due to the importance of this asset, the International Organization for Standardization creates a specific standard for information security, which is referred to as an Information Security Management System (ISMS).

As a result of the importance they give to the information, this thesis has conducted an investigation of the standards, standards and good practices recognized worldwide, in order to develop each of the stages of the ISMS, taking as an approach the NTP ISO / IEC 27001: 2014, from which in the entity Virgen de Cocharcas Health Directorate, the “Design of an Information Security Management System under the approach of NTP ISO / IEC 27001 was implemented, which will allow it to comply with the regulations in force regarding information security.

The implementation is divided into three phases: **First phase:** The initial diagnosis of DISA V.C. Regarding the NTP ISO / IEC 27001: 2014 and its possibility of acceptance, in the **second phase:** The organization and its context were studied; the critical process was identified; The security policy was defined, the scope and the information security committee of the organization was identified and as a **third phase:** Following the methodology of risk analysis and management adopted, information assets, threats, were identified and assessed. the impact and risk calculation was performed, the control measures necessary to mitigate the risks to an acceptable level were identified and finally a document called declaration of applicability was prepared containing the justification of which controls in Annex A of the NTP ISO / IEC 27001: 2014 can be implemented in the entity.

Keywords: Information security, ISO / IEC 27001: 2014, Analysis, Risk.

CHUMASQA

Kay llamkaymi taqwiriyninpi maskaspa qawachin chay hatun ruraykuna umalliq hampi kamayuq wasi mamacha cocharcas- Chincheros llaqtapi" ruraywan huntachisqanmanta kay "wayrapi awaspa willakuy llamkay allin chaninchasqa kananpaq chay kamachikuypa ukunpi NTP ISO/IEC 27001: 2014".

Willakuy willasqa kananqa ancha allinmi llamkaykuna umalliq wasikunapaq,llapallan huñunasqa ruraykuna kamachikkunapaq, chaynataq suyunchikpi llamkapakuqkunapaq,huk kamachikpa llamkapakuqninhinapas, chaymi maskanku tukuy rikchaq kaqta allin allchasqa -waqaychasqa chay willakuy kananpaq mana hawaman lluqsinanpaq, nitaq ukupi llamkaqkunapas yachananpaq.

Chaypachaqa ancha allin kasqanrayku kay ruraymanta, tiqsimuyuntinpi munaychakuq huñunakuykuna rikurichimurqa huk kamachikuyta lliw willakuykuna allin waqaychasqa kananpaq chaypaqmi sutincharqa wayrapi awaspa willakuy llamkay allin chaninchasqa - waqaychasqa kananpaq (SGSI) nisqawan.

Nisqanmanhina ancha allin kasqanrayku wayrapi awaspa willakuykuna quy, kay yachaykuna taqwiriq llamkaymi qatiparqa kamachikuykunata, huñusqa ruraykunata hinaspa allinkaq ruruyninta lliwpa riqsisqan tiqsimuyuntinpi kasqanta, chaynapi rurarinanpaq wiñasqanmanhina SGSI nisqawan , imakaqta qawarispa chay NTP ISO/IEC .nisqawan 27001:2014, Chaymantapacha hatun ruraykuna umalliq hampi kamayuq wasi mamacha cocharcas, ruraykunawan huntachisqa karqa " wayrapi awaspa willakuy llamkay allin chaninchasqa kananpaq chay kamachikuypa ukunpi NTP ISO/IEC 27001: 2014" chay ruraykuna umalliq hampi kamayuq wasi mamacha cocharcas, - Chincheros llaqtapi", kay ruraykuna yanapanqa allinta puririnanpaq lliw kamachikuykunamanhina allichasqa willakuy kananpaq.

chaymi rakisqa kachkan: Kimsa patachaypi **Punta patachay:** Kaymi rurakurqa qallariyninpi rimariy chuymay DISA V.C. qawarispa NTP ISO/IEC 27001:2014 chaynapi chaskisqa kananpaq. **Iskay patachay**: Yachaywan qatipasqam karqa huñukuynin chaynataq tarikuynin; chaypim tarikurqa puririyninpi huk sasachakuy hina; chaymi chuyanchakurqa allin waqaychasqa, aypasqa kananpaq, hinaspa riqsichisqa karqa huk nanachikuq allin waqaychaq chay willakuykuna huñuqman. **Kimsa patachay**:

Yachaykunata qatispa hinataq hamutaspa ruraykunata hapispa, tarikurqa huk chaninchakuyta chitillaña willakuyta, chaynataq watiqaqkunata, rurakurqa huk yuyaymanariy, maskariy kallpawan chaynataq sasachakuynin, chaymi tarikurqa tupuykuna waqaychanapaq mana llakipi tarikunapaq, tukupayninpi rurakurqa huk qillqa maytu sutichasqa rimariykuna churakunanpaq chaypim tarikun imaynapim rurakurqa kay qillqa taqwiriy NTP ISO/IEC 27001:2014 kanman huntachisqa kay kamachikuq wasikunapi.

Musuq Sutikuna: Seguridad de la información, ISO/IEC 27001:2014, Análisis, Riesgo nisqankuna.

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, que es la información, garantizando siempre la disponibilidad, confidencialidad e integridad de la misma.

Debido a que actualmente existen diversos escenarios de amenazas, tales como: el daño, el robo y/o la fuga de información, que en cualquier momento pueden manifestarse con el fin de obtener información confidencial y hacer colapsar a la Dirección de Salud Virgen de Cocharcas, es necesario que cuente con una estrategia de continuidad de negocio, claramente definida por cada escenario de amenaza identificado para así poder reanudar las operaciones rápidamente.

La presente tesis reúne la información necesaria para el análisis de riesgos e implementar políticas de seguridad de la información bajo el enfoque de la NTP - ISO/IEC 27001:2014 para la Dirección de Salud Virgen de Cocharcas - Chincheros", para asegurar la protección de los activos de información y otorgar confianza a todo el personal. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI.

La presente tesis desarrollada también cuenta con conclusiones que dan respuesta a cada uno de los objetivos planteados, así como las recomendaciones que nos ayudan en un futuro a mejorar el trabajo realizado.

CAPITULO I

1. PLANTEAMIENTO DEL PROBLEMA

1.1. Realidad Problemática

Las organizaciones públicas y privadas día a día generan conocimientos, datos, reportes, actas y material de diferente índole de suma importancia para ellas, lo cual representa toda la información que requieren para su funcionalidad. Esta información en la mayoría de los casos, es almacenada en diferentes medios tanto físicos como electrónicos, además es puesta a disposición del personal que requiere hacer uso de esta información para toma de decisiones, realización de planes, reportes, inventarios, entre otros.

La información, tanto digital como física, cumplen un papel muy importante ya que actúa como activo principal y genera valor económico real para una organización. Si una empresa no administra, protege o asegura adecuadamente su información estará expuesta a riesgos que perjudicarán la continuidad de su negocio. Es por ello, que toda información debe ser protegida para que se encuentre accesible en tiempo y forma o, desde el punto de vista de seguridad de la información, conserve sus características de confidencialidad, integridad y disponibilidad.

El acceso no autorizado a la información se ha tornado más fácil debido a los tantos métodos existentes y nuevos para extraer información, esto ha permitido que sea más fácil salvaguardar la información y sus métodos de transmisión; ya sean estos comunicados verbales, archivos, documentos, base de datos, entre otros.

(Barrantes Porras, 2012), debido al crecimiento de la entidad, la probabilidad de que la información sea interceptada, robada y/o modificada por personas inescrupulosas y sin autorización de acceso a esta, ha aumentado considerablemente. Esto resulta peligroso para la institución, ya que mucha

de la información fundamental es importante para la realización de los procesos críticos del negocio puede ser vulnerada y amenazada ocasionando la interrupción de estos procesos; que conllevan, de esta manera retrasos en la ejecución de proyectos, toma de decisiones, etc.

Para (Héctor, 2003), especialista en Seguridad de la Información en el artículo **¿Qué es la seguridad de la información?** Afirma que la "Seguridad" es una necesidad básica ya que se encuentra implícita en la prevención de la vida y las posesiones, haciéndola tan antigua como estas. Los primeros conceptos de seguridad se evidencian en los inicios de la escritura Sumeria (3000 AC) o el Hammurabi (2000 AC).

La Dirección de Salud Virgen de Cocharcas es una entidad que requiere información oportuna y confiable, para tomar decisiones, para ello se cuenta con la oficina de Estadística que vela por el mantenimiento y adecuado funcionamiento de los sistemas de información con los que cuenta la DISA V.C. pero al igual que en otras entidades tanto públicas como privadas no le dan el interés adecuado al tema de seguridad de la información.

A continuación, se nombra algunas deficiencias en la DISA V.C.:

- Ausencia de una política de seguridad de la información
- Ausencia de un plan de gestión de riesgos.
- Ausencia de un plan de seguridad de la información.
- Inapropiada administración de recursos informáticos.
- Inadecuado control de accesos a la información.
- Inadecuada administración de los incidentes de la seguridad de la información.
- Inadecuado cumplimiento (legal, de estándares y auditorias)

1.2. Formulación del problema

Carencia en la gestión de seguridad de la información en la Dirección de Salud Virgen de Cocharcas.

1.2.1. problema general

¿Cuáles son las características del diseño de un sistema de gestión de la seguridad de la información en la Dirección de Salud Virgen de Cocharcas?

1.2.2. problemas específicos

- ¿Cuál es el alcance del diseño del SGSI para la Dirección de Salud Virgen de Cocharcas?
- ¿Cuáles son los resultados del análisis de riesgos del diseño del SGSI para la Dirección de Salud Virgen de Cocharcas?
- ¿Qué controles de seguridad son aplicables para el diseño del SGSI para la Dirección de Salud Virgen de Cocharcas?

1.3. Justificación

La información es parte de los activos más importantes de toda empresa, y a su vez es uno de los recursos más propenso a vulnerabilidades, siendo necesario protegerlo de amenazas internas y externas. En la actualidad las empresas necesitan que la información que manejan esté siempre disponible, sin alteraciones en sus datos y sea confiable.

Para (Bermudez M & Bailon S, 2015), la norma ISO/IEC 27001: Sistemas de gestión de seguridad de la información, proporcionan un estándar de calidad de seguridad de la información, ayudando a minimizar los riesgos de daño, robo o fuga de información; permitiendo mantener la integridad, confidencialidad y disponibilidad de la información.

Debido a los riesgos a los que están expuestos lo activos de información, el impacto que la interrupción de estos puede causar, es preponderantemente la definición de una metodología y el uso de herramientas que nos ayuden reducir y mitigar estos riesgos.

“Actualmente sólo existen buenas prácticas y lineamientos con respecto a la seguridad de la información, no existe una metodología que brinde herramientas para todo el ciclo de la gestión de un sistema de seguridad

de la información. El tener de apoyo una metodología clara y sencilla que sea entendible y no genere mayores confusiones a los encargados de implementar el sistema de gestión de seguridad de la información, les ayudará a poder implementarlo con mayor confianza sin dudas y dificultades que se tienen acerca de la seguridad de la información debido al poco entendimiento que aún se tiene de la misma; permitiéndoles medir y, por tanto, gestionar el nivel de seguridad de la información de la institución de acuerdo a la estrategia del negocio y a las regulaciones vigentes**”** (Aquije Quijandria & Jave Bodadilla, 2012).

Mediante el análisis de seguridad de la informática y seguridad de la información La Dirección de Salud Virgen de Cocharcas al igual que muchas organizaciones cuenta con información muy valiosa para la institución, por lo que podrá conocer y aplicar controles de seguridad en la información que se maneja en la entidad para que se garantice la confidencialidad, integridad y disponibilidad de la misma que esté siendo utilizada adecuadamente y solo tenga acceso las personas autorizadas, para ello existe la Organización Internacional de Normalización la que crea una norma específica para la Seguridad de la Información, la cual es denominada como un Sistema de Gestión de Seguridad de la Información (SGSI), la que está establecida a través de la ISO 27001.

La tesis contendrá un Diseño de un Sistema de Gestión de Seguridad de la Información bajo el enfoque de la NTP ISO/IEC 27001:2014 para la Dirección de Salud Virgen de Cocharcas, que permitirá conocer las vulnerabilidades existentes en el manejo de la información física y digital, así como la que está contenida en los sistemas de procesamiento de información, de tal forma que se puede tomar acciones preventivas y correctivas dentro de la entidad para evitar que se lleguen a comprometer datos confidenciales.

1.4. Objetivos

1.4.1. Objetivo General

Implementar un Diseño de un Sistema de Gestión de Seguridad de la Información bajo el enfoque de la NTP - ISO/IEC 27001:2014 para la Dirección de Salud Virgen de Cocharcas - Chincheros.

1.4.2. Objetivos Específicos

- Concretar el alcance del diseño de Sistema de Gestión de Seguridad de la Información para la Dirección de Salud Virgen de Cocharcas - Chincheros.
- Mitigar los riesgos de los recursos activos y la información con el método octave en la Dirección de Salud Virgen de Cocharcas - Chincheros.
- Determinar el modelado de los procesos correspondientes al alcance del sistema de gestión de seguridad de la información según la norma ISO/IEC 27001:2014 para la Dirección de Salud Virgen de Cocharcas - Chincheros.

CAPITULO II

2. ANTECEDENTES

2.1. Antecedentes

Durante muchos años las empresas se han preocupado por perfeccionar todos los sistemas informáticos, dejando en una prioridad casi nula la seguridad de la información. La evolución de los sistemas computacionales, del internet y de las comunicaciones en general han abierto una puerta para que las personas empiecen a descubrir el valor de la información y la facilidad de acceder a los datos.

En un mundo actual de constantes cambios tecnológicos, el manejo de seguridad de la información a todo nivel se convierte en un problema crítico cuando no se les brinda el control y tratamiento apropiado a los activos de información. Una efectiva administración sobre este tema es un aspecto de negocio y regulación, no sólo de tecnología.

Desafortunadamente ese fácil acceso a la información la expone a que también sea utilizada por personas no autorizadas. Existen miles de personas que se dedican a realizar ataques informáticos con la finalidad de obtener información para cometer actos ilícitos, de tal manera que pueda llegar a perjudicar una empresa.

“Actualmente es necesario garantizar que en los perfeccionamientos realizados en los sistemas informáticos y en la manipulación física se incluyan criterios de seguridad de la información, pues esta debe resguardarse y limitarse para lidiar con estos aspectos de una manera proactiva y oportuna, para así poder ser considerada como efectiva, estando siempre alienada a los objetivos y estrategias evitando exponerla a personas ajenas a la utilización de la misma**”** (Bermudez M & Bailon S, 2015, pág. 9).

(Ccesa Quincho, 2017), tesis para optar el título profesional de Ingeniero Informático de la Universidad Nacional San Cristóbal de Huamanga - Ayacucho Mercedes Ccesa Quincho intitulado "DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BAJO LA NTP ISO/IEC 27001:2014 PARA LA MUNICIPALIDAD PROVINCIAL DE HUAMANGA, 2016", en la tesis establece que la empresa a ser evaluada debe garantizar la confidencialidad, integridad y disponibilidad de sus activos y la de sus clientes; acorde a la normativa vigente de la misma que está alineada a estándares de seguridad como la ISO 27001, al ser una institución nueva, requiere establecer lineamientos internos para cumplir ese objetivo junto a un plan estratégico del área de seguridad y alineado a los objetivos institucionales.

Por lo que respecta a esta tesis, tomé como guía para la implementación de fases para el diseño del Sistema de Gestión de Seguridad de la Información.

(Rosales Bravo & Suarez Leon, 2015), tesis para optar el título de ingeniero de sistemas Informáticos y de computación de la escuela politécnica nacional de Quito de Rosales Bravo Paul Fernando intitulado “PLAN DE GESTION DE SEGURIDAD DE LA INFORMACION, BAJO LA NORMA ISO/IEC 27001:2013, EN UNA INSTITUCION FINANCIERA ECUATORIANA”, en la tesis establece que el alcance del sistema que desea implementar, esto se realiza en términos de la naturaleza del negocio, locación, activos de información, aspectos legales y tecnológica de la institución evaluada.

Determinado el alcance, seleccionaremos el tipo de controles requeridos y se establecerá la política de seguridad que servirá de marco referencial para el cumplimiento de los objetivos institucionales y regulatorios, basados en una estrategia de evaluación, control y mitigación del riesgo.

Respecto a esta tesis me ayudó en el análisis, evaluación y tratamiento de riesgos.

(Carrera Villamarin, 2012), tesis parta optar el título de master en ciencias de la computación y comercio electrónico de la escuela politécnica nacional de Quito de Walter G. Carrera Villamarin intitulado “DISEÑO DE UN MODELO DE GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACION BASADO EN EL ACOPLAMIENTO DE LA NORMA ISO/IEC 27005:2008 Y EL METODO OCTAVE”, en la tesis establece que va orientado a presentar una propuesta de un modelo de gestión de riesgos de la seguridad de la información que pretende establecer los procesos y actividades que le permitirían a una organización gestionar sus riesgos de seguridad de la información.

La tesis se compone de cinco capítulos organizados de tal manera que permitan generar una guía clara y practica de cómo generar y validar la aplicabilidad de un modelo de gestión de riesgos de seguridad de la información basado en el acoplamiento de la norma ISO/IEC27005:2008 y el método octave.

Por otra parte, se tomó como guía esta tesis para aplicar el método octave durante el desarrollo del Sistema de Gestión de Seguridad de la Información.

Bajo las consideraciones mencionadas es importante realizar un análisis de seguridad en los procesos ejecutados en una empresa, de esta manera se podría detectar posibles vulnerabilidades y amenazas que puedan afectar la continuidad de la Dirección de Salud Virgen de Cocharcas.

CAPITULO III

3. MARCO TEORICO

3.1. Octave

“El método OCTAVE permite la comprensión del manejo de los recursos, identificación y evaluación de riesgos que afectan la seguridad dentro de una organización, centrándose en:

- Identificar los elementos críticos y las amenazas a esos activos.
- La identificación de las vulnerabilidades, tanto organizativas y tecnológicas, que exponen a las amenazas, creando un riesgo a la organización.
- El desarrollo de una estrategia basada en la protección de prácticas y planes de mitigación de riesgos para apoyar la misión de la organización y las prioridades**”** (Anonimo, 2014).

3.1.1 Beneficios del método OCTAVE:

- **“**Identifica los riesgos de la seguridad que pueden impedir el logro del objetivo de la organización.
- Enseña a evaluar los riesgos de la seguridad de la información.
- Crea una estrategia de protección con el objetivo de reducir los riesgos de seguridad de la información prioritaria.
- Ayuda a la organización a cumplir regulaciones de la seguridad de la información**”** (Ccesa Quincho, 2017, pág. 36).

3.2. Riesgo

De manera general, puede definirse el termino de riesgo como: **“**cualquier tipo de evento o circunstancia que de ocurrir amenazarían los objetivos de una organización, estos riesgos tienen una posibilidad de ocurrencia por lo que se miden como la multiplicación de impacto por probabilidad.

El riesgo indica lo que le podría pesar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en

cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema**”** (INDECOPI, 2007).

3.2.1. Criterio para el tratamiento del riesgo

Para (Guanoluisa Huertas & Maldonado Soliz, 2015), el tratamiento de riesgos es tomar decisiones frente a los diferentes riesgos existentes de acuerdo a la estrategia de la organización. Las posibles acciones de tratamiento de riesgo son:

a) Reducir

Consiste en elegir controles de corrección, eliminación, prevención, mitigación del impacto, detección, recuperación, monitoreo y concienciación con el fin de reducir el nivel de riesgo.

b) Aceptar

No es necesario implementar controles adicionales, estos riesgos podrán ser aceptados teniendo en cuenta que se pueda asumir los daños provocados por la materialización del riesgo.

c) Evitar

O eliminar el riesgo, que no suele ser la mejor opción ya que resulta difícil o demasiado costoso, pues muchas de las veces se basan en eliminación de procesos o incluso del activo involucrado.

d) Transferir

A un tercero de forma que se asegure el activo, o subcontratando el servicio.

3.2.2. Análisis de riesgos

“El objetivo del análisis de riesgos es identificar los activos que aportan a la institución, las amenazas que podrían afectar el funcionamiento normal de las actividades de la organización, además del impacto que podrían causar estas de llegar a darse, y las medidas que se deben llevar a cabo para minimizar o eliminar el impacto de los riesgos existentes**”** (Guanoluisa Huertas & Maldonado Soliz, 2015).

3.2.3. Análisis y Evaluación de Riesgos

(López, 2011). Por su parte, indica que el análisis de riesgos es “un proceso sistemático para evaluar la dimensión de los riesgos a que está expuesta una Organización”. Sabiendo lo que podría pasar, hay que tomar decisiones para tratar estos riesgos.

El análisis y gestión de riesgos de los sistemas de información es el núcleo de las actuaciones relacionadas con el análisis, la evaluación y la gestión del riesgo. Es así que siguiendo una metodología de gestión de riesgos se puede analizar los riesgos, identificar las amenazas y su impacto.

3.3. ISO 27001

(Lloyd's Register (LR), 2018), la ISO 27001 es una norma de carácter internacional que tiene como objetivo garantizar que los controles que existen para salvaguardar la información de las partes interesadas sean adecuados para proteger la confidencialidad, integridad y disponibilidad de la información. Estos controles deben tener en cuenta la información de clientes, empleados, socios, y las necesidades de la sociedad en general.

La ISO 27001, es la única norma reconocida y certificable que especifica los requisitos para establecer, implementar, operar, realizar seguimiento, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos globales del negocio de la organización.

3.3.1. Beneficio de la Norma ISO/IEC 27001

Para (Bermudez M & Bailon S, 2015), definen que los beneficios de la norma permiten disminuir posibles riesgos de vulnerabilidades en los sistemas informáticos y en la información en general manejada por personal de la empresa, además mejora en los procesos y servicios prestados, teniendo una mejor organización de los procesos, aumentando la competitividad de la empresa debido a que se demuestra el interés por salvaguardarla integridad, confiabilidad y disponibilidad de la información de los clientes.

3.3.2. NTP - ISO/IEC 27001:2014

(INDECOPI, 2014), la norma NTP - ISO/IEC 27001:2014 es una adaptación de la ISO/IEC 27001. La Presidencia del Consejo de Ministros a través de la Oficina Nacional de Gobierno Electrónico, dispone el uso obligatorio de la Norma Técnica Peruana "NTP - ISO/IEC 27001:2014", Tecnología de la Información, técnicas de seguridad, Sistemas de Gestión de Seguridad de la Información.

Esta Norma Técnica Peruana ha sido preparada para proporcionar los requisitos, para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. La implementación de un sistema de gestión de seguridad de la información de la organización está influenciada por las necesidades y objetivos de la organización, por los requisitos de seguridad, por el tamaño y estructura de la organización.

- **Estructura de la NTP - ISO/IEC 27001:2014**

  (ISOTools Excellence, 2015), la norma ISO 27001:2013 (en el Perú NTP - ISO/IEC 27001:2014) no sólo establece cambios en el contenido (respecto a la ISO 27001:2005) sino también en la estructura, lo que verá reflejado en otros documentos que forman parte de la familia ISO 2700. La norma ISO 27001, en la que se proporciona un formato y un conjunto de alineamiento que siguen el desarrollo documental de un sistema de gestión sin que le importe el enfoque empresarial, se alinean bajo la misma estructura todos los documentos que se relacionan con el sistema de gestión de seguridad de la información y así se evitan problemas de integración con otros marcos de referencia.

  La estructura de la norma queda así:

  0. Introducción

1. Objeto y campo de aplicación
2. Referencias Normativas
3. Términos y definiciones
4. Contexto de la organización
5. Liderazgo
6. Planificación
7. Soporte
8. Operación
9. Evaluación del desempeño
10. Mejora
11. Anexo A - Lista de controles.

(Gómez & Fernández, 2015), señalan que cuando una organización quiere cumplir los requisitos de la NTP - ISO/IEC 27001, debe demostrar la efectiva implantación de los apartados 4 al 10, que son los que conforman el cuerpo principal de la norma.

3.4. Ciclo de mejora continua

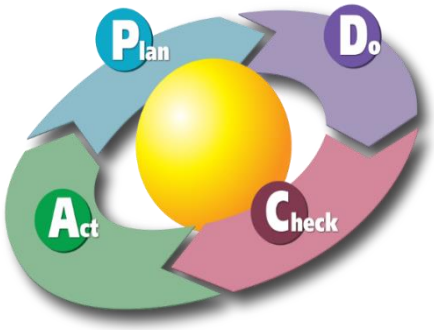
“La ISO/IEC 27001 se basa en el conocido "Ciclo de Deming" *Plan-Do-Check-Act,* que significa "Planificar-Hacer-Verificar-Actuar" siendo este un enfoque de mejora continua:

El modelo PDCA consta de un conjunto de fases, que permiten establecer un modelo comparable a lo largo del tiempo, de manera que se pueda medir el grado de mejora alcanzado:

- **Plan (Planificar):** En esta fase se planifica la implantación de SGSI. Se determina el contexto de la organización, se definen los objetivos y las políticas que permitirán alcanzarlos.
- **Do (Hacer)**: Se implementa y pone en funcionamiento el SGSI. Se ponen en práctica las políticas y los controles que, de acuerdo al análisis de riesgos, se han seleccionado para cumplirlas.

- **Check (Verificar):** En esta fase se realiza la monitorización y revisión del SGSI. Se controla que los procesos se ejecutan de la manera prevista y que además permiten alcanzar los objetivos de la manera más eficiente.
- **Act (Actuar):** En esta fase se mantiene y mejora el SGSI, definiendo y ejecutando las acciones correctivas necesarias para rectificar los fallos detectados en la anterior fase**”** (Gómez & Fernández, 2015).

FIGURA 1: CICLO PDCA EN ISO/IEC 27001:2013



Fuente: *https://bit.ly/2WrJK0T*

3.5. Seguridad de la Información

De manera general, puede definirse el termino de seguridad de la información como: **“**La protección de la confidencialidad, integridad y disponibilidad de la información; es decir, es asegurarse que esta sea accesible solo a las personas autorizadas, sea exacta sin modificaciones no deseadas y que sea accesible a los usuarios cuando lo requieran. Así también puede involucrar otras propiedades como la autenticidad, no repudio y confiabilidad. La seguridad de la información protege a la información (implantando un conjunto adecuado de controles - que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones de software y hardware, monitoreándolos, revisándolos y mejorándolos donde sea necesario) de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización

y maximizar el retorno de las inversiones y las oportunidades de negocio**”** (INDECOPI, 2007).

3.6. Sistema de Gestión de Seguridad de la Información (SGSI)

(Gómez & Fernández, 2015), definen al sistema de gestión de seguridad de la información como 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. Así mismo mencionan que la implementación de un SGSI supone el establecimiento de procesos formales y una clara definición de responsabilidades en base a una serie de políticas, planes y procedimientos que deberán constar como información documentada.

Fundamentalmente se distinguen dos tipos de procesos:

1) **Procesos de gestión:** Controlan el funcionamiento del propio sistema de gestión y su mejora continua.
2) **Procesos de seguridad:** Se centran en los aspectos relativos a la propia seguridad de la información.

(INDECOPI, 2014), define que es importante que el sistema de gestión de la seguridad de la información sea parte de y esté integrado con los procesos de la organización y la estructura de gestión general y que la seguridad de la información se considere en el diseño de procesos, sistemas y controles de la información.

3.7. Oficial de Seguridad de la Información

(Aguirre Mollehuanca D. , 2014), el oficial de seguridad de la información es la persona encargada de planificar, presupuestar y verificar el rendimiento de los componentes de la seguridad de la información. Así como de realizar una correcta gestión de riesgo para la toma de decisiones.

Por otra parte, (Peltier T. R., Peltier, & Blackley, 2005), definen las responsabilidades de cada oficial de seguridad de la información varían dependiendo de la organización en la que se encuentren, debido a que la protección de la información está limitada por la cultura organizacional.

El oficial de seguridad de la información debe entender que el programa básico de protección de la información se implementará en todas las empresas. Sin embargo, cada unidad de negocios debe tener la libertad de hacer modificaciones para satisfacer sus necesidades específicas,

3.8. Política de Seguridad

"La política de seguridad es la información documentada en la que se reflejan en términos generales los objetivos de la organización y las principales líneas de acción que permiten proteger la información frente a pérdidas de confidencialidad, integridad y disponibilidad. La definición de esta política debe tener en cuenta los requisitos del negocio, contractuales, legales y sistemáticos, este documento debe ser comunicado a todas las partes interesadas del SGSI**"** (Gómez & Fernández, 2015).

Por otra parte, (Peltier T. R., Peltier, & Blackley, 2005), consideran a la política de seguridad de la información como la piedra angular de una efectiva arquitectura de seguridad de la información, ya que de ella nacen otros documentos importantes tales como directivas, estándares, procedimientos y guías y nos mencionan que estas cumplen con 2 roles importantes, un rol interno y otro externo.

TABLA 1: ROLES DE POLÍTICA DE SEGURIDAD

ROL	DESCRIPCION
Rol Interno	Ya que se menciona a cada uno de los miembros de la organización, qué se espera que realicen y cómo se evaluará el trabajo realizado.
Rol Externo	Ya que sirve para mostrarle al mundo como es que se trabaja dentro de la organización, que somos conscientes de la necesidad de proteger nuestra información y la de los clientes y que estamos trabajando para realizarlo.

Fuente: *Elaboración propia*

3.9. Metodología de Investigación

3.9.1. Hipótesis de la investigación

Para (Carrasco Diaz, 2006), la investigación aplicada se distingue por tener propósitos prácticos inmediatos, bien definidos, es decir se investiga para actuar, transformar, modificar o producir cambios en un determinado sector de la realidad.

3.9.2. Nivel de la investigación

Para (Bernal, 2010), las investigaciones descriptivas muestran, narran e identifican hechos, situaciones, características de un objeto de estudio o se diseñan productos, modelos, prototipos, guías, etc. Pero no se dan explicaciones o razones del porqué de las situaciones, los hechos, los fenómenos, etc.

3.9.3. Diseño de la investigación

(Hernandez Sampieri & Fernandez Collado, 2014), la investigación no experimental se clasifica en transeccionales y longitudinales. La investigación transeccional (que a su vez se divide en exploratorios, descriptivo y correlaciónales - causales) tiene como propósito describir variables y analizar su incidencia e interrelación en un momento dado, mientras que la investigación longitudinal, recolecta datos en diferentes momentos o periodos para hacer inferencias respecto al cambio, sus determinantes y consecuencias.

3.10. Definición operacional de la variable

(Carrasco Diaz, 2006), la operacionalización de las variables es un proceso metodológico que consiste en descomponer o desagregar deductivamente las variables que componen el problema de investigación, partiendo desde lo general a lo específico; es decir, las variables se dividen (si son complejas) en dimensiones, áreas, aspectos, indicadores, índices, subíndices e ítems; pero si son concretas solamente en indicadores, índices e ítems.

CAPITULO IV

4. METODOLOGÍA DE LA INVESTIGACIÓN

La metodología adoptada en esta investigación tiene en cuenta el marco de referencia la NTP - ISO/IEC 27001:2014 que especifica, entre otros aspectos, los requerimientos y actividades que se deben desarrollar para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información.

4.1. Hipótesis de la investigación

La presente tesis es descriptiva, porque tiene como propósito diseñar un SGSI para de la Dirección de Salud Virgen de Cocharcas, tomando como base los riesgos de seguridad a los que se enfrenta, contribuyendo con una solución a la mejora de la seguridad de la información dentro de la institución.

4.2. Nivel de la investigación

El nivel de investigación de la presente tesis es descriptivo, porque busca identificar y describir las características fundamentales del diseño de un SGSI (teniendo como guía la NTP ISO/IEC 27001:2014 para la DISA V.C.

4.3. Diseño de la investigación

el diseño de investigación de la presente tesis es no experimental - transeccional descriptivo.

Hipótesis General

- Se implementará el diseño de SGSI bajo el enfoque de la NTP ISO/IEC 27001:2014 para la DISA V.C. - Chincheros.

Hipótesis Especificas

- Se concretará el alcance del diseño de SGSI para la Dirección de Salud Virgen de Cocharcas - Chincheros.
- Con la implementación del diseño del SGSI se reducirá los riesgos de los recursos activos y la información en la DISA V.C. - Chincheros.

- Se determinará el modelado de los procesos correspondientes al alcance del SGSI según la NTP ISO/IEC27001:2014 para DISA V.C. - Chincheros.

4.4. Variables e indicadores

4.4.1. Definición conceptual de la variable

- **X. Diseño de un SGSI**

  Es un conjunto de procesos que permiten establecer la seguridad de la información, tomando como base para ello los riesgos a los que se enfrenta la organización.

Indicadores

- **"X1 - Alcance:** Es el ámbito de la organización que queda sometido al SGSI**"** (ISO 27000, 2005)
- **"X2 - Análisis de riesgo:** Es el proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo**"** (ISO 27000, 2005)
- **"X3 - Controles de seguridad:** Son las políticas, los procedimientos, las prácticas y las estructuras organizativas creadas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. El control es también sinónimo de salvaguarda. En una definición más simple, es una medida que modifica el riesgo**"** (ISO 27000, 2005)

4.4.2. Definición operacional de la variable

En la presente tesis se utiliza, para la definición operacional de la variable de investigación, el criterio de descomposición atendiendo a sus componentes o elementos, debido a que la variable diseño de un sistema de gestión de seguridad de la información va a ser estudiada en atención a los elementos que la conforman **(Ver Tabla 2)**.

TABLA 2: OPERACIONALIZACIÓN DE LA VARIABLE DE UN SGSI

VARIABLE	INDICADORES	INDICES	ITEMS
X. DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION	**1.** Alcance	**1.1.** Aspectos externos e internos relevantes para el SGSI. **1.2.** Requisitos de las partes interesadas relevantes al SGSI.	**1.** ¿Por qué implementas un diseño de SGSI? **2.** ¿A quiénes le interesa que se implemente el SGSI? **3.** ¿Qué área o proceso debe ser cubierta por el SGSI?
	2. Análisis de Riesgo	**2.1.** inventario de activos **2.2.** identificar los riesgos **2.3.** probabilidad e impacto del riesgo **2.4.** propiedades del riesgo	**1.** ¿Qué activos de tipo dato/información son fundamentales para que la dependencia consiga sus objetivos y estos estén alineados con los objetivos de la organización? **2.** ¿Qué activos de tipo servicio, software y hardware son fundamentales para que la dependencia consiga sus objetivos y estos estén alineados con los objetivos de la organización? **3.** ¿Qué dispositivos físicos utiliza la dependencia para almacenar información de forma permanente o por largos periodo de tiempo? **4.** ¿Qué activos sirven de soporte a los sistemas de información? **5.** ¿A qué amenazas están expuestos y cuan perjudicado resultarían los activos? **6.** ¿Cuál es la probabilidad de que se materialice la amenaza? **7.** ¿Qué daño causaría sobre el activo la materialización de la amenaza? **8.** ¿Cuál es nivel de riesgos al que se encuentra expuesto el activo?
	3. Controles de seguridad	**3.1.** Criterios de aceptación de riesgos **3.2.** Políticas de seguridad **3.3.** Roles y responsabilidades	**1.** ¿Qué nivel de riesgo acepta la DISA V.C.? **2.** ¿Qué opciones de tratamiento de riesgos se va a seleccionar? **3.** ¿Qué medidas de seguridad se van a implantar?

Fuente: *Elaboración propia*

4.6. Técnicas e instrumentos

Las técnicas e instrumentos utilizados en esta investigación se muestran en la **(Ver tabla 3)**.

TABLA 3: TÉCNICAS E INSTRUMENTOS PARA LA RECOLECCIÓN DE INFORMACIÓN

TECNICA	INSTRUMENTO	INTRUMENTO DE REGISTRO	DETALLE
Análisis documental	Fichas bibliográficas − Referencia	Formato de citas y referencia bibliográfica de esta investigación.	Se utilizó esta técnica para analizar material impreso y digital sobre el tema de investigación. Se usó diferentes fuentes de información, tales como: **-** Libros, normas de seguridad, tesis, etc.
Entrevista	Guía de entrevista (Cuestionarios)	Formato: Anexo A	Se realizaron entrevistas a los trabajadores de la DISA V.C. para conocer su opinión sobre el SGSI a diseñar.
Encuesta	Cuestionario autoadministrado y autoadministrado grupal	Formato: Anexo **B, F, G**. (Tabla 12, Tabla 14, Tabla 19)	Se utilizó esta técnica para recabar información sobre el estado de seguridad de la información y la posibilidad de aceptación del SGSI, para identificar y valorar los activos de información y degradación de los activos de información
Internet	Tecnologías de información y comunicaciones	Referencia bibliográfica de esta investigación	El internet es uno de los medios principales, utilizados hoy en día para recabar información. Se utilizó está técnica para búsqueda de libros, revistas, etc.

Fuente: *Elaboración propia*

4.7. Herramientas para el tratamiento de datos

Las herramientas que se emplearon para el análisis y tratamiento de los datos, son las siguientes:

TABLA 4: HERRAMIENTAS PARA EL TRATAMIENTO DE DATOS

HERRAMIENTA	DESCRIPCION
Microsoft Excel	Herramienta que organiza los datos, numéricos o de texto, en hojas o libros de cálculo. Permite realizar análisis sobre los datos y tomar decisiones.
Análisis PEST	PEST (iniciales de factores Políticos - legales, Económicos, Socio-culturales y Tecnológicos). Se utiliza esta herramienta para analizar los factores que pueden afectar a la DISA V.C. en la implementación del SGSI.
Matriz DAFO	La matriz DAFO muestra el conjunto de factores DAFO: Debilidades, Amenazas, Fortalezas y Oportunidades.

Fuente: *Elaboración propia*

4.7.1. Matriz DAFO

TABLA 5: MATRIZ DAFO

DEBILIDADES	AMENAZAS
➢ Inexistencia de personal dedicado exclusivamente a la seguridad de la información. ➢ Uso de licencias de software para S.O y programas (no son originales). ➢ Se cuenta con un solo proveedor de internet para la salida de todos los sistemas de información. ➢ No existe un plan de capacitación para el personal en temas de seguridad de la información. ➢ Falta de políticas de S.I.	➢ Alto costo de consultores. ➢ Aparición de nuevas tecnologías. ➢ Falta de recursos económicos. ➢ Inestabilidad de fluido eléctrico, sobre todo en época de lluvia. ➢ Actualización de software de los navegadores. ➢ Falta de compromiso en la implementación del SGSI.
FORTALEZAS	**OPORTUNIDADES**
➢ Disposición del personal de la DISA V.C. para la implementación del SGSI. ➢ Optimización de la seguridad/entorno informático ➢ Reducción de riesgos, perdidas. ➢ Reducción de riesgos que afecten la seguridad, disponibilidad y confidencialidad de la información.	➢ Aparición de nuevas tecnologías. ➢ Aumentar la confianza de la organización. ➢ Definición de políticas de seguridad de la información, estableciendo controles y normas para el manejo de seguridad. ➢ Definir procedimientos y políticas para el ciclo de vida de la información.

Fuente: *Elaboración propia*

4.8. Fases para el diseño de SGSI

Con el fin de alcanzar los objetivos propuestos en la presente tesis, se establecieron las siguientes fases:

1. Fase I. Diagnóstico del SGSI:

a) Evaluación del estado inicial de la Dirección de Salud Virgen de Cocharcas con respecto a los requisitos de la NTP - ISO/IEC 27001.

b) Estudio de la posibilidad de aceptación del SGSI y el diagnóstico del estado inicial de la seguridad de la información.

2. Fase II. Preparación del SGSI:

a) Análisis del contexto de la Dirección de Salud Virgen de Cocharcas e identificación de las partes interesadas afectadas por el SGSI.

b) Definición del alcance del SGSI.

c) Elaboración de la política y objetivos de seguridad.

d) Identificación de los requisitos legales.

e) Comité de seguridad.

3. Fase III. Planificación del SGSI:

a) Evaluación de riesgos. Para efectos de esta investigación se adoptó OCTAVE como metodología de análisis y gestión de riesgos. Las tareas realizadas fueron las siguientes:

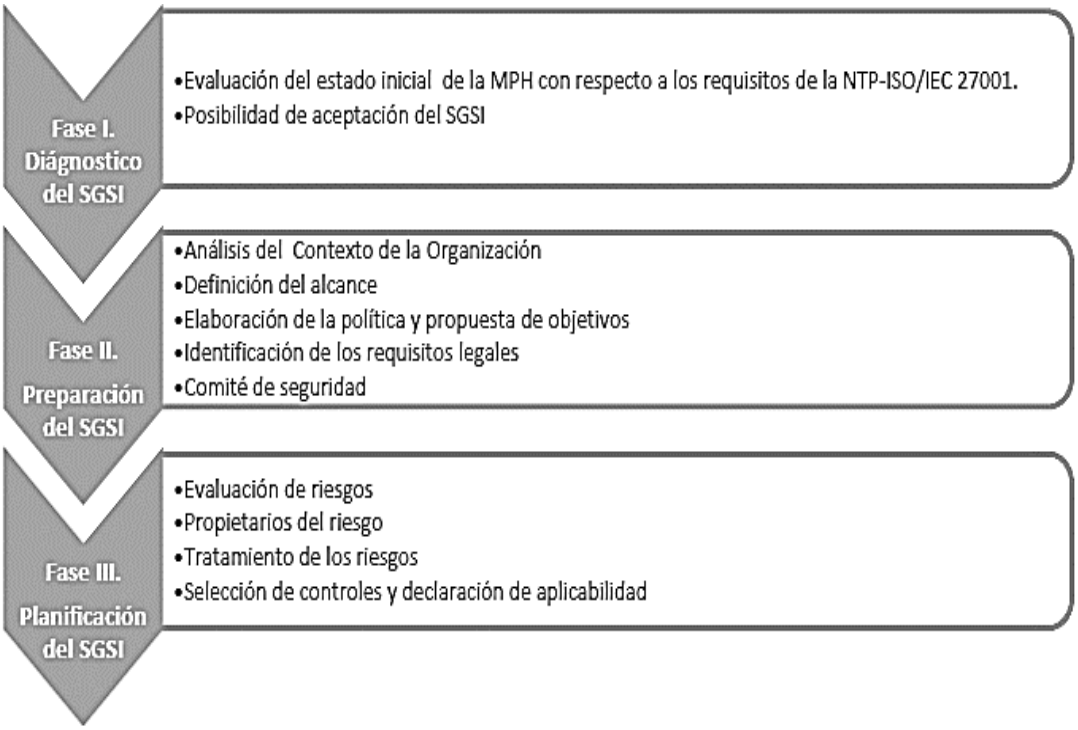
- Se identificaron los activos que dan soporte a los procesos del negocio delimitados en el alcance, de este modo se elaboró un inventario de activos.
- Se cuantificó el valor de los activos en términos de confidencialidad, integridad y disponibilidad.
- Se identificaron y valoraron las amenazas
- Se calculó el impacto de materialización de las amenazas identificadas.
- Se calculó el riesgo para cada activo.

b) Identificación de los propietarios del riesgo

c) Tratamiento de los riesgos

d) Selección de controles y declaración de aplicabilidad.

FIGURA 2: FASES PARA EL DISEÑO DEL SGSI



Fuente: *Adaptado de "Cómo implementar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad", Gómez. 2015, p.48.*

CAPITULO V

5. RESULTADOS

5.1. FASE I: Diagnóstico del SGSI

En esta fase se presentan las actividades que se realizaron para conocer la situación de la DISA V.C. frente a la seguridad de la información y el diseño del SGSI.

5.1.1 Evaluación del estado inicial de la DISA V.C. con respecto a los requisitos de la NTP - ISO/IEC 27001

Para evaluar el estado inicial de la DISA V.C. con respecto a los requisitos de la ISO/IEC 27001, se ha definido dos maneras de presentar los resultados: una descriptiva y otra cuantificable **(Ver Tabla 6)**. Esta técnica se basa en calificar el estado de los requerimientos en función a una escala de Likert aplicando cinco opciones que van de menor a mayor.

TABLA 6: CRITERIO PARA EVALUAR EL ESTADO INICIAL DE LA DISA V.C.

CRITERIO DE CALIFICACION	VALORACION
No diseñado: Las actividades/métodos demuestran que no se tiene el requisito y/o no se ha bosquejado su implementación.	0%
Parcialmente diseñado: Las actividades/métodos demuestran que se tiene el requisito definido, pero este no es del todo conforme con el requisito de la NTP ISO/IEC 27001.	25%
Diseñado: Los métodos son conformes con el requisito de la NTP ISO/IEC 27001, pero sin evidencias de aplicación**.**	50%
Parcialmente implementado: Las actividades/métodos son conformes con el requisito de la NTP ISO/IEC 27001, pero con pocas evidencias de aplicación.	75%
Completamente implementado: Las actividades/métodos son conformes con el requisito de la NTP ISO/IEC 27001, y se cuenta con evidencias de aplicación permanentes.	100%

Fuente: *Elaboración propia*

El resultado que se obtuvo de la evaluación del estado inicial de la DISA V.C. respecto a los requisitos de la NTP - ISO/IEC 27001 se muestra en forma de tabla. Un extracto de esta evaluación se muestra a continuación **(la tabla completa se encuentra en el ANEXO E de este documento).**

TABLA 7: ESTADO INICIAL DE LA DISA V.C. RESPECTO A LA NTP - ISO/IEC 27001

SECCION	REQUISITOS DE LA NTP - ISO/IEC 27001	ESTADO	EVIDENCIA/SUGERENCIA (¿COMO LO CUMPLE? / ¿Qué SE TENDRIA QUE HACER?)	VALORACION
4	**CONTEXTO DE LA ORGANIZACIÓN**	No diseñado	Se sugiere realizar el análisis del contexto de la DISA V.C. para comprender tanto los aspectos externos como internos, las partes interesadas y relevantes al SGSI.	0%
4.1	**Comprender la Organización y contexto**. La organización debe determinar los aspectos externos e internos que son relevantes para este propósito y que afectan su capacidad de lograr el(los) resultado(s) deseados de este SGSI	Parcialmente diseñado	La DISA V.C. posee documentos visibles de su Misión, Visión, FODA, Manual de Organización y Funciones (MOF), Reglamento de Organización y Funciones (ROF). Pero no contempla de manera clara los ítems de seguridad de la información. **Sugerencia:** Establecer objetivos de seguridad de la Información que estén alineados con los objetivos estratégicos.	25%
4.2	**Comprender las necesidades y expectativas de las partes interesadas.** La organización **debe** determinar las partes interesadas y los requisitos de las mismas.	No Diseñado	**Sugerencia:** Determinar las partes interesadas y comprender las necesidades y expectativas de éstas, referentes a la seguridad de la información.	0%
4.3	Determinar el alcance del SGSI.	No Diseñado	**Sugerencia.** Determinar el alcance del SGSI teniendo en consideración los aspectos referidos, documentarlo y ponerlo a disposición de las partes interesadas.	0%
...	**…**	…	…	…
PUNTAJE TOTAL DE LA EVALUACION DE REQUISITOS DE LA NTP ISO/IEC 27001				**10%**

Fuente: *Elaboración propia*

5.1.2. Resultado de la evaluación del estado inicial de la DISA V.C. con respecto a los requisitos de la NTP - ISO/IEC 27001

Según la evaluación realizada, de un total de 100% de los requisitos de la NTP ISO/IEC 27001 que se deben cumplir, la DISA V.C. obtuvo un puntaje total de 10%, por lo que se puede determinar que la DISA V.C. se encuentra en una etapa básica de cumplimiento de la norma (no diseñado).

El resultado anterior muestra también que la Seguridad de la Información dentro de la organización no es gestionada, que el diseño e implementación del SGSI implicará un mayor esfuerzo, dependerá del compromiso y disponibilidad del personal de la DISA V.C.

5.1.3. Posibilidad de aceptación del SGSI y diagnóstico inicial de la SI

La recolección de datos se realizó mediante la encuesta mostrada en el **Anexo B** de esta investigación. La encuesta consistió en dieciocho (18) preguntas claves para medir actitudes, opiniones y el estado básico de SI dentro de la DISA V.C. Esto con el fin de corroborar el estado de la seguridad de la información y la posibilidad de aceptación del diseño del SGSI.

5.2. FASE II. Preparación del SGSI:

Los objetivos de esta fase fueron: definir el alcance del SGSI, elaborar la política y los objetivos de seguridad, identificar los requisitos legales (aplicables al SGSI) y proponer del comité de seguridad de la DISA V.C. Estos objetivos se consiguieron tras analizar los contextos externos e internos de la DISA V.C. y comprender las necesidades y expectativas de las partes interesadas en el SGSI.

5.2.1. Contexto de la organización

La NTP - ISO/IEC 27001 menciona en el capítulo 4: Contexto de la organización, la importancia de comprender la organización y su contexto, esto es, comprender los aspectos internos y externos que

son relevantes para el establecimiento del SGSI, asimismo comprender también las necesidades y expectativas de las partes interesadas y determinar el alcance del SGSI.

5.2.1.1. Contexto Externo

En este ítem se analizó los factores externos (relevantes) que afectan a la DISA V.C. en la implementación del SGSI. Para ello se utilizó la herramienta de análisis PEST (iniciales de factores Políticos - Legales, Económicos, Socio-culturales y Tecnológicos).

El resultado del análisis se muestra en la siguiente figura:

TABLA 8: ANÁLISIS PEST

Político – Legal	✓ Interés del estado por la seguridad de la información en todas las entidades. ✓ Marco regulatorio sobre seguridad de la información ✓ Estandarización de procesos y sistemas de gestión
Económico	✓ Alto costo de consultores para establecer un SGSI
Socio - Cultural	✓ Sociedad peruana cada vez más tecnológica ✓ Sociedad preocupada por la seguridad de su información
Tecnológico	✓ Aparición de nuevas tecnologías de información. ✓ Nuevas necesidades de implementación tecnológica ✓ Vulnerabilidad en la seguridad de la información

Fuente: *Elaboración propia*

5.2.1.2. Contexto Interno

El SGSI debe alinearse con la cultura, los procesos, la estructura y la estrategia de la organización.

a) Misión

"Somos una Dirección de Salud que tiene como finalidad velar por la salud de las personas en el ámbito de la provincia de Chincheros; a través de una gestión eficiente brindamos una atención integral que comprende; la recuperación de la salud, promoción de la salud y prevención de las enfermedades, con calidad, universalidad e interculturalidad."

b) Visión

"Ser una organización sólida regida por la filosofía del mejoramiento continuo, que promueve el desarrollo del potencial humano, de esta manera ser un referente en la región en el cumplimiento de indicadores de gestión que reflejen una mejor calidad de vida de las personas, familias y comunidades en cuanto a su salud plena; física y mental."

c) Líneas Estratégicas

- **Recursos y tecnología:** comprende la situación de personal, bienes institucionales, patrimonio, presupuesto, implementación de sistemas computarizados, tecnología de información y comunicaciones, etc.
- **Gestión institucional:** incluye el estilo de gestión, la capacidad de liderazgo, la toma de decisiones, el estado de los documentos de gestión, entre otros aspectos.

d) Objetivos Estratégicos

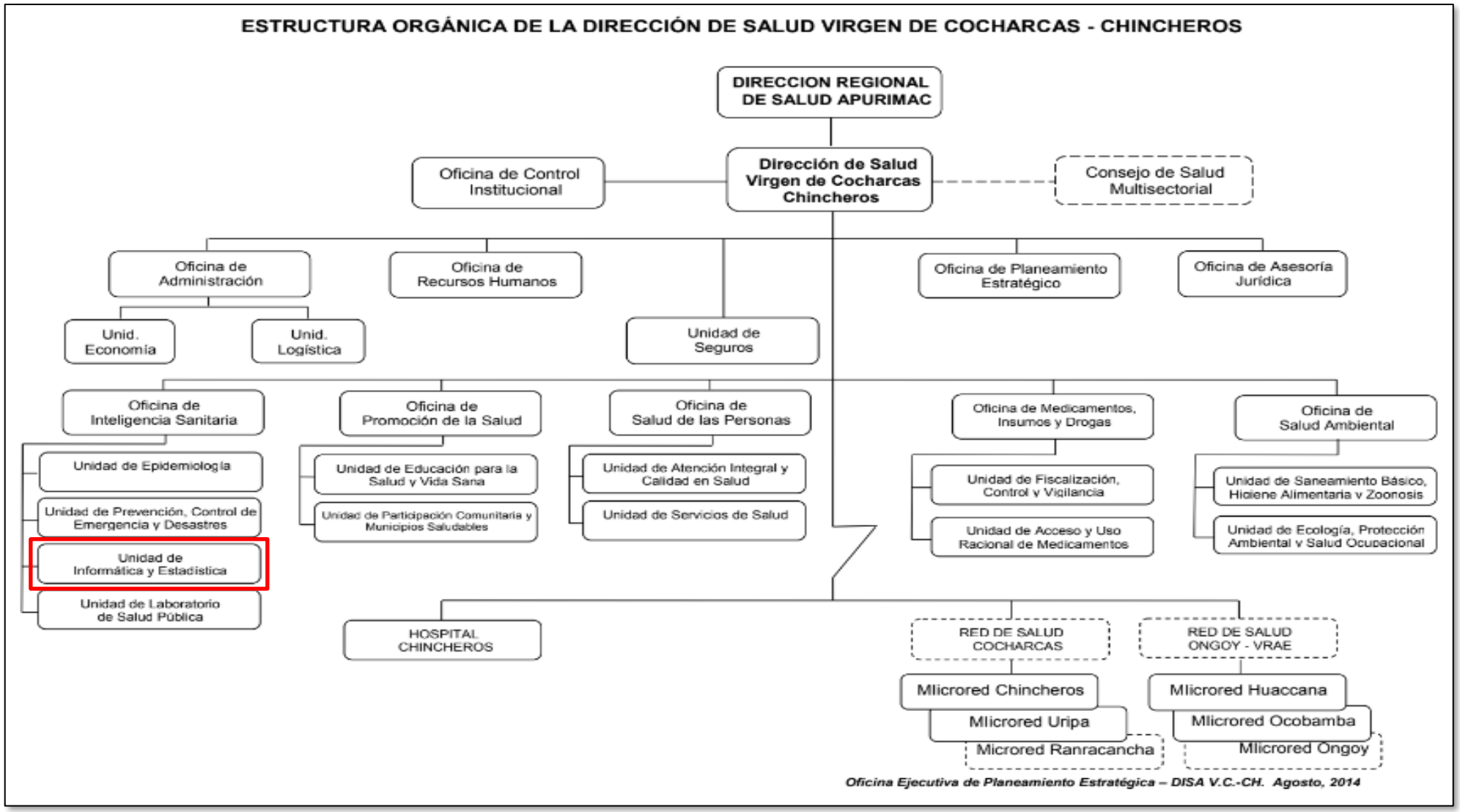
La DISA V.C. directamente y a través de las entidades competentes deberá cumplir las siguientes funciones en su respectiva jurisdicción:

1. Formular, proponer, ejecutar, dirigir, controlar, evaluar y administrar las políticas de salud del ámbito de la DISA V.C. en concordancia con las políticas regionales y planes sectoriales.
2. Promover, coordinar y ejecutar en forma prioritaria las actividades de promoción de la salud y prevención de riesgos y daños, sin descuidar las acciones de recuperación y rehabilitación en materia de salud, en coordinación con los gobiernos locales.
3. Organizar los establecimientos de salud que brindan servicios de salud en la provincia de Chincheros.
4. Ejecutar, en coordinación con los gobiernos locales de la provincia de Chincheros, acciones efectivas que contribuyan a elevar los niveles nutricionales de la población.

e) Estructura Orgánica

En la **Figura 3** se muestra la estructura orgánica de la DISA V.C. en este organigrama se ha designado a la Unidad de Informática y Estadística como responsable de la seguridad de la información dentro de la entidad.

FIGURA 3: ORGANIGRAMA DE LA DIRECCIÓN DE SALUD VIRGEN DE COCHARCAS



Fuente: *Dirección de Salud Virgen de Cocharcas*

f) Aspectos técnicos

La DISA V.C. dispone, en la sede central de una red de área local (LAN), formada por un total de 36 estaciones de trabajo, 01 servidor, 01 página Web (*https://disachincheros.webnode.es*) y correo corporativo Gmail para sus usuarios, cuenta con un área de informática.

En el servidor y las PCs se centralizan toda la información necesaria para el funcionamiento de los sistemas, además de los accesos a la red de la entidad, también se realizan copias de seguridad y se almacenan en el mismo servidor y PCs.

Para la salida de los sistemas de información se cuenta con línea de Fibra Óptica.

Cabe mencionar que en la DISA V.C. el cableado de red está expuesto, enmarañado, y tendido por el suelo en algunas áreas, y todos los activos expuestos a amenazas que afecten sus dimensiones de integridad, disponibilidad y confidencialidad. En el **Anexo C** se pueden ver algunas imágenes del Servidor.

g) Partes interesadas

Conforme al requisito 4.2 (Comprender las necesidades y expectativas de las partes interesas) de la NTP ISO/IEC 27001:2014. En este apartado se identificaron las partes interesadas afectadas por el diseño y posterior a la implementación del SGSI.

- **Alta dirección**

  Debe demostrar liderazgo y compromiso respecto al SGSI, asegurando que los objetivos que se establecen

sean compatibles con la planeación estratégica de la organización y estableciendo una política de seguridad de la información.

- **Responsable de Informática**

  Es el responsable de la seguridad de la información y continuidad tecnológica de la entidad.

- **Responsable de Recursos Humanos**

  Responsable de la SI antes, durante y después de la vinculación de los funcionarios y trabajadores.

- **Trabajadores de la DISA V.C**.

  Responsables de velar por la seguridad de los activos de información de la DISA V.C, cumplir a cabalidad con las normas y políticas de seguridad establecidas en la entidad. Además, tienen la responsabilidad del tratamiento de los datos personales de los titulares vinculados de alguna forma con la entidad.

En la **Tabla 9** se muestran los requisitos de las partes interesadas del SGSI.

TABLA 9: REQUISITOS DE LAS PARTES INTERESADAS

PARTES INTERESADAS	REQUISITOS
Alta Dirección	➢ Supervisar las actividades y proyectos del responsable de informática en temas de seguridad de la información. ➢ Debe demostrar liderazgo y compromiso con la seguridad de la información.
Responsable de Informática	➢ Levantamiento de no conformidades (respecto a la seguridad de la información) de la auditoría presupuestal y financiera practicada a la DISA V.C. ➢ Capacitar a los trabajadores en temas de seguridad de la información
Responsable de RR. HH	➢ Verificar la seguridad de la información antes, durante y después de la vinculación de los funcionarios y trabajadores.
Trabajadores de la DISA V.C.	➢ Conocer las normas y políticas en temas de seguridad de la información ➢ Velar por los activos de información de la DISA V.C. ➢ Protección de su información personal. ➢ Capacitación en temas de seguridad de la información

Fuente: *Elaboración propia*

5.2.2. Política de seguridad de la información

En este apartado, se definió la política de seguridad de la información de la DISA V.C. (acorde al requisito 5.2 de la NTP ISO/IEC 27001:2014). La política de seguridad será aprobada por la alta Dirección y revisada anualmente.

Una vez aprobada la política de seguridad, la Dirección de Salud Virgen de Cocharcas comunicará esta política a todos los trabajadores de la organización.

FIGURA 4: POLÍTICA DE SEGURIDAD

La Dirección de Salud Virgen de Cocharcas - Chincheros, en cumplimiento de nuestra misión, visión y objetivo estratégico, y para satisfacer las necesidades de la comunidad, proveedores, y demás partes interesadas, establece la función de seguridad de la información dentro la entidad con el objetivo de:

- Proteger los activos de información de la Dirección de Salud Virgen de Cocharcas.
- Es política de la Dirección de Salud asegurar que:
  - ✓ La información esté protegida contra pérdidas de disponibilidad, confidencialidad e integridad.
  - ✓ Se cumplan los requisitos legales y normas aplicables a la entidad respecto a la seguridad de la Información.
  - ✓ Se gestionen los riesgos de seguridad de la información a través de la aplicación de una metodología, estándares y controles orientados a preservar los activos de información de la entidad.
  - ✓ Se fortalezca la cultura de seguridad de la información en los trabajadores de la entidad.
  - ✓ Cada trabajador es responsable de cumplir esta política y sus procedimientos según aplique a su puesto de trabajo (*).
  - ✓ Es política de la Dirección de Salud Virgen de Cocharcas implementar, mantener y realizar un seguimiento del SGSI.

(*) La entidad se reserva el derecho de tomar medidas disciplinarias con el personal que incumpla con lo dispuesto en la presente política, conforme a las disposiciones señaladas en los documentos normativos de la institución, sin perjuicio de las acciones civiles o penales que pudieran corresponder.

Fuente: *Elaboración propia*

5.2.3. Alcance del SGSI

El alcance del Sistema de Gestión de Seguridad de la Información (SGSI) de la DISA V.C. está incluido dentro del documento que se referencia en el **Anexo D**. A continuación, se muestra un extracto del mismo.

FIGURA 5: ALCANCE DEL SGSI

El alcance del sistema de gestión de seguridad de la información aplica sólo para el proceso de GESTIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA, sub proceso de gestión de seguridad de la información, dentro de los sistemas de información que sustentan los procesos de negocio.

Se tienen en cuenta los activos de información considerados como relevantes dentro del alcance.

El sistema de gestión de seguridad de la información aplica para la Dirección de Salud Virgen de Cocharcas - Chincheros.

Fuente: *Elaboración propia*

5.2.4. Objetivos de seguridad de la información

Los objetivos del SGSI se muestran en la siguiente figura:

FIGURA 6: OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

- Asegurar la confidencialidad de la información almacenados en los sistemas de información, del personal de la Dirección de Salud Virgen de Cocharcas - Chincheros.
- Asegurar la confidencialidad, integridad y disponibilidad de la información sensible de la Dirección de Salud Virgen de Cocharcas - Chincheros.
- Garantizar que nuestras operaciones, procesos actuales y futuros cumplan con la legislación y normatividad vigente en materia de seguridad de la información.
- Reducir los riesgos de seguridad de la información a un nivel aceptable para la DISA V.C.
- Difundir la política de seguridad a través de cada uno de los responsables de área.
- Evaluar la efectividad del SGSI y llevar a cabo la mejora continua.

Fuente: *Elaboración propia*

5.2.5. Comité de seguridad de la información

De acuerdo al requisito 5.3 Roles, responsabilidades y autoridades organizacionales de la NTP ISO/IEC 27001:2014 la alta dirección debe

asegurar que las responsabilidades y la autoridad para los roles relevantes a la seguridad de la información estén asignadas y comunicadas.

Asimismo, la RM N.º 004 - 2016 - PCM en su artículo 5, establece la creación del comité de gestión de seguridad de la información para dar cumplimiento al requisito 5.3 de la NTP ISO/IEC 27001:2014. Este comité de gestión de seguridad de la Información, estará conformado por:

1. El director
2. El administrador
3. El responsable de informática
4. El responsable de asesoría jurídica
5. El oficial de seguridad de la información.

A continuación, se describen los roles y responsabilidades propuestos.

5.2.5.1. El director

- Aprobar la política de seguridad de la información y comunicarla a todos los trabajadores de la entidad.
- Definir y establecer los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo.
- Promover una cultura de seguridad de la información en la entidad.

5.2.5.2. El administrador

- Proponer al director la política de seguridad de la información para la entidad.
- Hacer cumplir la política de seguridad de la información dentro de la entidad.

- Revisar la política de seguridad de la información en intervalos planificados o cuando se produzcan cambios significativos en la normatividad de seguridad.
- Controlar el avance de seguridad de la información dentro de la DISA V.C.

5.2.5.3. El responsable de informática

- Garantizar la disponibilidad y operatividad de los SI, de equipos informáticos de la entidad.
- Establecer los mecanismos adecuados para la gestión y administración de riesgos, seguridad de la información, velar por la capacitación del personal de la entidad en lo referente a estos temas.
- Informar al Administrador y director sobre los aspectos relacionados con el SGSI.
- Asegurar la existencia de metodologías para el tratamiento de riesgos y oportunidades, políticas de SI, así como la existencia de los documentos exigidos por la NTP ISO/IEC 27001:2014.
- Asegurar el cumplimiento de las políticas y requerimientos de seguridad establecidos para la adquisición, diseño, desarrollo, operación, administración y mantenimiento de infraestructura tecnológica de la entidad.
- Asignar las funciones, roles y responsabilidades de seguridad, a los trabajadores a su cargo para la operación y administración de la infraestructura tecnológica de la entidad.

5.2.5.4. El responsable de asesoría jurídica

- Conocer e interpretar las leyes y normatividad vigente relacionada con la seguridad de la información bajo el contexto de la entidad.

- Evaluar el cumplimiento de las leyes y normatividad vigente en temas de seguridad de la información dentro de la entidad.
- Mantener actualizado un archivo de normas legales relacionadas con la seguridad de la información.

5.2.5.5. El oficial de seguridad de la información

- Diseñar y coordinar la implementación de las políticas, normas y procedimientos de SI, con la participación activa de las dependencias de la entidad.
- Identificar los riesgos a los que se encuentran expuestos los activos de información de la DISA V.C.
- Definir los controles asociados al SGSI y evaluarlos.
- Desarrollar charlas de capacitación y concientización en temas de seguridad de información para el personal de la entidad.
- Atender auditorías internas y externas de aspectos asociados a la seguridad de la información.
- Reportar al responsable de informática los incidentes de SI, los resultados de las auditorias, la revisión y supervisión del SGSI.

5.3. FASE III. Planificación del SGSI:

En este apartado se llevó a cabo las actividades para tratar los riesgos y asegurar que el diseño del SGSI alcance los objetivos de: evaluar los riesgos de seguridad de la información de la DISA V.C. y elaborar la lista de controles de seguridad para mitigar los riesgos identificados.

5.3.1. Evaluación de riesgos

5.3.1.1. Evaluación de riesgos

De acuerdo a la metodología de análisis y gestión adoptada, se definió la siguiente clasificación de activos:

TABLA 10: CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

TIPO DE ACTIVO	DESCRIPCION
Dato / Información	Los datos son el corazón que permite a una organización prestar sus servicios. La información es un activo abstracto que será almacenado en equipos o soportes de información (BD)
Servicios	Los servicios satisfacen la necesidad de los usuarios, contempla servicios prestados por el sistema.
Software / Aplicaciones Informáticas	Se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios
Equipos Informáticos	Son los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos.
Redes de Comunicaciones	Siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.
Soporte de Información	Dispositivos físicos que permiten almacenar información de forma permanente o al menos durante largos periodos de tiempo.
Instalaciones	En este punto entran los lugares donde se hospedan los sistemas de información y comunicaciones.
Personal	Personas relacionadas con los sistemas de información.

Fuente: *elaboración propia.*

Para identificar los activos de información de la DISA V.C. se utilizó el formato del **Anexo F**: Cuestionario para identificar activos.

Un extracto de la relación de activos identificados en el proceso gestión de la infraestructura tecnológica se muestra en **(Ver tabla 11)**. El inventario completo se encuentra en el **Anexo G** de esta tesis.

TABLA 11: INVENTARIO DE ACTIVOS DE INFORMACIÓN

Nombre del activo	Descripción del activo	Tipo de activo	Ubicación
Datos vitales	Datos que almacenan los diferentes SI esenciales para el funcionamiento de la DISA V.C.	Dato/Información	Servidor
Archivos personales	Documentos personales de los trabajadores de la DISA V.C.	Dato/Información	Computadoras personales / Archivo físico (estantería)
Copias de seguridad	Copias de respaldo de los datos/información que manejan los distintos sistemas de la DISA V.C.	Dato/Información	Servidor / computadoras personales
Datos de configuración de los sistemas de información	Corresponde a los documentos, manuales y procedimientos relacionados con la administración de los diferentes sistemas de información	Dato/Información	Archivo físico (estantería) / virtual
Datos de gestión interna	Corresponde a los documentos de la DISA V.C.	Dato/Información	Archivo físico (estantería)/ virtual
Correo electrónico	Correo electrónico institucional	Servicio	Servicio de correo Gmail
SIAF- SIGA	Sistema que manejan la oficina de Contabilidad, Planeamiento y Presupuesto, Tesorería, Estadística.	Software / Aplicaciones informática	Servidor, Computadoras Personales
Aplicaciones comerciales	Office, sistemas operativos, antivirus, entre otros.	Software/ Aplicaciones informática	Servidor, Computadoras Personales
Computador del funcionario	Computadoras que utilizan los funcionarios de la entidad	Equipos informáticos	S.G. de Sistemas y Tecnología
Internet	Red de comunicaciones contratado a terceros	Redes de comunicaciones	Red inalámbrica
Disco duro externo	Disco duro externo	Soporte de información	Servidor/oficina de Estadística
Soportes no electrónicos	Dispositivos físicos de almacenamiento no electrónico como material impreso	Soporte de información	Archivo físico o estantería

Fuente: *Elaboración propia*

5.3.1.2. Valoración de activos

Para valorar los activos de información se consideró tres aspectos: el económico, el legal y la imagen, que pueden

afectar a los activos en sus dimensiones de confidencialidad, integridad y disponibilidad.

El criterio que se siguió para valorar los activos de información se muestra en la **Tabla 12**.

TABLA 12: CRITERIO PARA LA VALORACIÓN DE ACTIVOS

ASPECTOS	CRITERIO DE CALIFICACION	VALORACION
Económico (E) Pérdidas económicas para la Dirección de Salud	Pérdidas económicas excepcionalmente elevadas	5
	Causa de pérdidas económicas elevadas	4
	Causa de graves pérdidas económicas	3
	Causa pérdidas financieras o pérdida de ingresos	2
	Supondría pérdidas económicas mínimas.	1
Legal (L) Incumplimiento de leyes y normas	Probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación	5
	Probablemente cause un incumplimiento grave de una ley o regulación	4
	Probablemente sea causa de incumplimiento de una ley o regulación	3
	Probablemente sea causa de incumplimiento leve o técnico de una ley o regulación	2
	Pudiera causar el incumplimiento leve o técnico de una ley o regulación	1
Imagen (IMG) Afecta a la imagen de la Dirección de Salud	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones con otras organizaciones	5
	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones	4
	Probablemente por publicidad negativa y afecte las relaciones con otras organizaciones	3
	Probablemente afecte negativamente a las relaciones internas de la organización	2
	Pudiera causar una pérdida menor de la confianza dentro de la Organización	1

Fuente: *Elaboración propia.*

Asimismo, se estableció preguntas para determinar la criticidad del activo de información. Estas preguntas se muestran en la siguiente tabla.

TABLA 13: PREGUNTAS PARA DETERMINAR LA CRITICIDAD DEL ACTIVO DE INFORMACIÓN

PARAMETRO	ASPECTO	PREGUNTA
Confidencialidad (C)	Económico	¿Su divulgación no autorizada puede relevar información sensible de la entidad requerida para la toma de decisiones estratégicas y financieras causando pérdida económica?
	Legal	¿Su divulgación no autorizada puede afectar el cumplimiento de leyes o normas impartidas por entes de control?
	Imagen	¿Su divulgación no autorizada puede afectar la imagen de la entidad?
Integridad (I)	Económico	¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede generar pérdidas económicas para la entidad?
	Legal	¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede generar sanciones de entes de control?
	Imagen	¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede afectar la imagen de la entidad?
Disponibilidad (D)	Económico	¿Si el activo o la información que se gestiona a través de él no están disponibles puede generar pérdidas económicas para la entidad?
	Legal	¿Si el activo o la información que se gestiona a través de él no están disponibles puede generar sanciones legales de entes de control?
	Imagen	¿Si el activo o la información que se gestiona a través de él no están disponibles puede afectar la imagen de la entidad?

Fuente: *Elaboración propia.*

Por último, para determinar el nivel de criticidad del activo valorado, se usó el criterio establecido en la **Tabla 14**. De esta manera se determinó la importancia de los activos de información dentro del proceso: gestión de la infraestructura tecnológica.

TABLA 14: NIVEL DE CRITICIDAD DE LOS ACTIVOS DE INFORMACIÓN

CRITERIO DE EVALUACION	VALOR	NIVEL
El activo de información compromete en un nivel alto la integridad y/o confidencialidad y/o disponibilidad de la información.	3 < VF <= 5	Alto
El activo de información compromete en un nivel medio la integridad y/o confidencialidad y/o disponibilidad de la información.	VF = 3	Medio
El activo de información compromete en un nivel bajo la integridad y/o confidencialidad y/o disponibilidad de la información.	0 < VF < 3	Bajo

Fuente: *Elaboración propia.*

En la **Tabla 15**, se muestra un extracto del resultado de la valoración de activos su nivel de criticidad

TABLA 15: VALORACIÓN DE ACTIVOS DE INFORMACIÓN Y NIVEL DE CRITICIDAD

Nº	NOMRE DEL ACTIVO	CONFIDENCIALIDAD			INTEGRIDAD			DISPONIBILIDAD			VFC	VFI	VFD	VF	NIVEL DE CRITICIDAD
		E	L	IMG	E	L	IMG	E	L	IMG					
1	Copias de respaldo	3	4	2	4	4	3	5	4	5	4	4	5	5	ALTO
2	Datos de configuración de los S.I.	2	1	1	2	2	3	3	3	1	2	3	3	3	MEDIO
3	Datos de gestión interna	4	4	3	3	3	3	4	3	3	4	3	4	4	ALTO
4	Credenciales (contraseñas)	4	4	5	5	4	3	4	4	4	5	5	4	5	ALTO
5	Datos de control de acceso	5	5	5	5	4	5	5	5	5	5	5	5	5	ALTO
6	Registro de los S.I.	3	3	3	3	3	3	3	3	3	3	3	3	3	MEDIO
7	Correo electrónico	2	3	3	2	2	3	2	3	3	3	3	3	3	MEDIO
8	Gestión de privilegios	2	2	1	2	2	3	2	3	3	2	3	3	3	MEDIO
9	Base de datos	2	4	2	4	4	4	3	3	4	4	4	4	4	ALTO
10	Página Web	3	4	1	1	2	2	1	3	4	4	2	4	4	ALTO
11	SIAF	3	4	1	5	4	3	4	4	4	4	5	4	5	ALTO
12	SIGA	3	4	1	5	4	3	4	4	4	4	5	5	4	ALTO
13	Servidor	5	4	4	5	4	4	5	5	5	5	5	5	5	ALTO
14	Computadores del personal	3	4	3	3	3	3	4	4	5	4	4	5	5	ALTO
15	Impresoras	1	1	1	2	2	2	3	3	3	1	2	3	3	MEDIO
16	Soporte de la red	2	2	2	2	2	2	3	3	3	2	2	3	3	MEDIO
17	Red local	2	2	3	2	3	2	4	2	2	3	3	4	4	ALTO
18	Internet	2	2	2	3	3	3	4	3	3	2	3	4	4	ALTO

Fuente: *Elaboración propia*

Nota: E=Económico, L=Legal, IMG=Imagen,

- VFC = Valor Final de Confiabilidad,
- VFI = Valor Final de Integridad,
- VFD = Valor Final de Disponibilidad,
- VF = Valor Final del Activo de Información.

De la Tabla 15:

- El valor de la columna VFC (valor final de confiabilidad), corresponde al máximo valor de los aspectos: económico, legal e imagen, que afectan a la seguridad del activo en su dimensión de confiabilidad. Este mismo criterio se siguió para obtener los valores de VFI (valor final de integridad) y VFD (valor final de disponibilidad) cada uno dentro de la dimensión que le corresponde.

- El valor de VF (valor final del activo de información), es el máximo valor de VFC, VFI y VFD.

- El nivel de criticidad del activo se obtiene de acuerdo a **(Ver tabla 14)**.

Terminada la valoración de los activos de información, se seleccionó aquellos activos con nivel de criticidad alto y medio, para luego agruparlos en los activos que lo contienen. El resultado de esta actividad se muestra en la **Tabla 16**.

TABLA 16: ACTIVOS POR CONTENEDOR

ACTIVO DE INFORMACION	NIVEL DE CRITICIDAD	CONTENEDOR
Copias de respaldo	**Alto**	Servidor/disco duro externo/PCs
Datos de configuración de los SI	**Medio**	Estantería
Datos de gestión interna	**Alto**	Estantería
Datos de control de acceso	**Alto**	Servidor de BD / usuario interno
Registro de los SI	**Medio**	Registro de Eventos servidores
Base de datos	**Alto**	Servidor de Base de datos
Página Web	**Alto**	VPS servidor proveedor
SIAF	**Alto**	Servidor
SIGA	**Alto**	Servidor
Credenciales (contraseñas)	**Alto**	PC informática
Servidor de base de datos	**Alto**	Servidor de Base de datos
Computador del funcionario	**Alto**	Local de la Institución
Computadores de escritorio	**Alto**	Local de la Institución
Impresoras	**Alto**	Local de la Institución
Soporte de la red	**Medio**	Local de la Institución - Proveedor
Red local	**Medio**	Red LAN
Internet	**Alto**	Servidor, Local DISA V.C.

Fuente: *Elaboración propia*

5.3.1.3. Identificación y valoración de amenazas

Es esta etapa, para identificar las amenazas que afectan a los activos de información, se elaboró una lista de amenazas, (**ver Anexo A**).

Luego, junto con el personal de informática de la Disa V.C. se procedió a identificar aquellas amenazas que afectan a los activos valorados en el ítem anterior y se determinó la probabilidad de ocurrencia de estas amenazas.

Para determinar la probabilidad de que éstas amenazas se materialicen se estableció el criterio mostrado en la **Tabla 17**.

TABLA 17: PROBABILIDAD DE MATERIALIZACIÓN DE AMENAZAS

PROBABILIDAD DE QUE SE MATERIALICE LA AMENAZA		
CRITERIO	**VALOR**	**PUNTUACION**
Más de 02 años	Imposible	1
Anual	Poco probable	2
Mensual	Posible	3
Semanal	Probable	4
Diario	Muy probable	5

Fuente: *Elaboración propia*

A continuación, se muestra en la **Tabla 18,** la relación de amenazas identificadas, la dimensión de seguridad en que se ve afectado el activo y la probabilidad de materialización de las amenazas. El **Anexo H** de este documento, contiene la tabla general de identificación de amenazas, riesgos y consecuencias.

- ✓ Las amenazas pueden afectar a los activos de información en uno, dos, o sus tres dimensiones de seguridad. Para efectos de esta tesis, se muestra la(s) dimensión(es) de seguridad afectada en orden de relevancia, donde: 1 es muy relevante, 2 medianamente relevante y 3 poco relevante.

TABLA 18: IDENTIFICACIÓN DE AMENAZAS

N°	AMENAZAS	DIMENSIONES AFECTADAS			PROBABILIDAD DE OCURRENCIA
		C	I	D	
01	Fuego			2	2
02	Tormenta eléctrica, rayo			3	2
03	Error de usuario	2	1	3	4
04	Errores del administrador	3	2	1	3
05	Alteración accidental de la información		1	1	2
06	Destrucción de información			1	2
07	Fugas de información	1		1	2
08	Vulnerabilidades de los programas (software)	3	1	2	3
09	Errores de mantenimiento /actualización de programas software		1	2	3
10	Errores de mantenimiento / actualización de equipos (hardware)			1	3
11	Indisponibilidad del personal			1	3
12	Suplantación de la identidad del usuario	1	3	2	2
13	Abuso de privilegios de acceso	1	2	3	4
14	Difusión de software dañino	3	2	1	3
15	Acceso no autorizado	1	2	1	2
16	Modificación deliberada de información			1	1
17	Inestabilidad de la línea de internet			1	4
18	Manipulación de programas	1	2	3	2
19	Manipulación de equipos	1	2	3	4
20	Robo de equipos	2		1	2
21	Corte del suministro eléctrico			1	3
22	Condiciones inadecuadas de temperatura o humedad			1	3
23	Degradación de los soportes de almacenamiento de la información	1	2	1	2
24	Instalación de software no autorizado	1	2	2	4

Fuente: *Elaboración propia*

Nota: C=Confidencialidad, I=integridad, D=disponibilidad.

Como no todas las amenazas afectan a todos los activos, sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir, se clasificó las amenazas por activo de información.

Finalmente, se valoró la degradación de cada activo de acuerdo al criterio de la tabla 19. El resultado final de esta valoración se muestra la **Tabla 20**.

TABLA 19: CRITERIO PARA VALORAR LA DEGRADACIÓN DEL ACTIVO

CRITERIO	VALOR
Sin degradación (SD)	1
Degradación baja (B)	2
Degradación media (M)	3
Degradación alta (A)	4

Fuente: *Elaboración propia*

TABLA 20: DEGRADACIÓN DE LOS ACTIVOS: SERVIDOR, PC´S

AMENAZAS	PROBABILIDAD	DEGRADACION CONFIDENCIALIDAD	DEGRADACION INTEGRIDAD	DEGRADACION DISPONIBILIDAD
SERVIDOR - SIGA - SIAF				
Fuego	2	3	2	4
Tormenta eléctrica, rayos	2	3	2	4
Errores del administrador	2	2	2	3
Suplantación de la identidad del usuario	2	3	2	3
Error de mantenimiento /actualización de programas (software)	2	2	1	2
Abuso de privilegios de acceso	3	3	3	4
Acceso no autorizado	3	4	2	3
Robo de equipos	2	2	1	4
Corte del suministro eléctrico	3	2	3	4
Condiciones inadecuadas de temperatura o humedad	2	2	2	4
PC´s				
Fuego	2	3	2	4
Tormenta eléctrica, rayos	2	3	2	4
Error de usuario	4	3	3	3
Error de configuración	2	2	2	2
Suplantación de la identidad del usuario	2	3	2	3
Error de mantenimiento /actualización de programas (software)	2	2	1	2
Abuso de privilegios de acceso	3	2	2	3
Acceso no autorizado	2	3	3	4
Robo de equipos	2	2	1	4
Corte del suministro eléctrico	3	2	3	4
Condiciones inadecuadas de temperatura o humedad	2	2	2	4

Fuente: *Elaboración propia*

5.3.1.4. Cálculo del impacto

En este ítem, se calculó el impacto, que viene dado en función el valor del activo y la degradación que producirá la amenaza en caso de materializarse. Para ello se estableció el siguiente criterio:

TABLA 21: CRITERIO PARA CALCULAR EL IMPACTO

DEGRADACION DE LA AMENAZA	VALOR DEL ACTIVO				
	1	2	3	4	5
1 (Sin degradación)	1	1	1	1	1
2 (Degradación baja)	1	2	2	3	4
3 (Degradación media)	1	2	3	4	4
4 (Degradación alta)	1	3	4	4	5

Fuente: *Elaboración propia*

TABLA 22: VALOR DEL IMPACTO

VALOR	DESCRIPCION
1	Insignificante
2	Menor
3	Medio
4	Crítico
5	Catastrófico

Fuente: *Elaboración propia*

Conviene aclarar, que esta valoración se calculó sin considerar las posibles medidas de seguridad que actualmente se estén aplicando. De esta manera se trata de calcular el máximo riesgo para cada uno de los activos.

En la **Tabla 25** se muestra el resultado del impacto para los activos Servidor - SIGA - SIAF, PCs.

5.3.1.5. Cálculo de riesgos

El cálculo del riesgo está en función del impacto que se producirá sobre el activo en caso de materializarse y de la probabilidad de materialización.

El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo. Para la presente investigación se elaboró la siguiente matriz de evaluación de riesgos:

TABLA 23: MATRIZ DE EVALUACIÓN DE RIESGOS

IMPACTO		MATRIZ DE EVALUACION DE RIESGOS				
Catastrófico	5	15	19	22	24	25
Critico	4	10	14	18	21	23
Medio	3	6	9	13	17	20
Menor	2	3	5	8	12	16
Insignificante	1	1	2	4	7	11
		1	2	3	4	5
		Prácticamente imposible	Poco posible	Posible	Probable	Muy probable
		PROBABILIDAD (DE LA AMENAZA) = FUTURO				

Fuente: *Elaboración propia*

En la matriz se puede distinguir niveles de riesgo: alto, medio y bajo.

Estos niveles fueron asignados de acuerdo al siguiente criterio:

TABLA 24: NIVELES DE RIESGO

NIVELES DE RIESGO	
CRITERIO	NIVEL
0< nivel de riesgo <= 8	Bajo
9 < nivel de riesgo <= 17	Medio
18 < nivel de riesgo <= 25	Alto

Fuente: *Elaboración propia*

En la **Tabla 25** se muestra el resultado de la valoración de riesgo para los activos Servidor, SIGA y SIAF.

TABLA 25: IMPACTO Y RIESGO PARA EL SERVIDOR - SIGA - SIAF, PC´S

AMENAZAS	PROBABILIDAD	DEGRADACION			IMPACTO			ESTIMACION DEL RIESGO		
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
SERVIDOR - SIGA - SIAF										
Fuego	2	3	2	4	Medio	Menor	Critico	Medio	Bajo	Medio
Tormenta eléctrica, rayos	2	3	2	4	Medio	Menor	Critico	Medio	Bajo	Alto
Errores del administrador	2	2	2	3	Menor	Menor	Medio	Bajo	Bajo	Medio
Suplantación de la identidad del usuario	2	3	2	3	Medio	Menor	Medio	Medio	Bajo	Medio
Error de mantenimiento /actualización de programas (software)	2	2	1	2	Menor	Insignificante	Medio	Bajo	Bajo	Bajo
Abuso de privilegios de acceso	3	3	3	4	Medio	Medio	Medio	Medio	Medio	Alto
Acceso no autorizado	3	4	2	3	Critico	Medio	Medio	Alto	Bajo	Medio
Robo de equipos	2	2	1	4	Menor	Insignificante	Critico	Bajo	Bajo	Medio
Corte del suministro eléctrico	3	2	3	4	Menor	Medio	Critico	Bajo	Medio	Alto
Condiciones inadecuadas de temperatura o humedad	2	2	2	4	Menor	Menor	Critico	Bajo	Bajo	Medio
PCs										
Fuego	2	3	2	4	Medio	Menor	Critico	Medio	Bajo	Medio
Tormenta eléctrica, rayos	2	3	2	4	Medio	Menor	Critico	Medio	Bajo	Alto
Error de usuario	4	3	3	3	Medio	Medio	Medio	Medio	Medio	Medio
Error de configuración	2	2	2	2	Menor	Menor	Menor	Bajo	Bajo	Bajo
Suplantación de la identidad del usuario	2	3	2	3	Medio	Menor	Medio	Medio	Bajo	Medio
Error de mantenimiento /actualización de programas (software)	2	2	1	2	Medio	Insignificante	Medio	Bajo	Bajo	Bajo
Abuso de privilegios de acceso	3	2	2	3	Menor	Menor	Medio	Bajo	Bajo	Medio
Acceso no autorizado	2	3	3	4	Medio	Medio	Critico	Medio	Medio	Medio
Robo de equipos	2	2	1	4	Menor	Insignificante	Critico	Bajo	Bajo	Medio
Corte del suministro eléctrico	3	2	3	4	Menor	Medio	Critico	Bajo	Medio	Alto
Condiciones inadecuadas de temperatura o humedad	2	2	2	4	Menor	Menor	Critico	Bajo	Bajo	Medio

Fuente: *Elaboración propia*

5.3.2. Propietarios del riesgo

En esta etapa, se identificó al propietario del riesgo, éste es el responsable de aprobar los riesgos excedentes y los planes de tratamiento de riesgos (para reducir los riesgos a un nivel aceptable). Para la presente tesis, se determinó que el único propietario del riesgo es la oficina de informática de la DISA V.C.

5.3.3. Tratamiento de los riesgos

De acuerdo a la naturaleza del riesgo, las opciones para tratarlos pueden ser: eliminar, transferir, mitigar o asumir el riesgo.

TABLA 26: JERARQUÍA DE CONTROLES

TRATAMIENTO	DESCRIPCION
Eliminar	Una de las alternativas más difíciles de implementar y más costosas ya que puede implicar la eliminación de un activo, proceso o del área del negocio que es fuente de riesgo.
Transferir	El riesgo fuera del apetito del riesgo se comparte con una o varias partes, pueden ser agentes externos.
Mitigar	Reducir el riesgo cuando se encuentra fuera del apetito del riesgo, se puede cambiar la probabilidad de ocurrencia o cambiar las consecuencias.
Asumir	En este escenario se decide aceptar el riesgo cuando no es posible mitigarlo y se debe continuar la actividad que lo originó.

Fuente: Adaptado de: "*Diseño de un sistema de gestión de seguridad de información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013"* (tesis), Justino Salinas. 2015, p.50.

En la presente tesis dados los valores y niveles de riesgos obtenidos, se estableció como máximo riesgo asumible los riesgos de nivel bajo; para todos los riesgos que tienen niveles medio y alto se aplicaron controles que ayudaron a reducir los riesgos producidos por las amenazas a un nivel aceptable en las dimensiones afectadas.

Se priorizó el tratamiento de los riesgos de nivel medio y alto, a ellos se aplicó todas las medidas de seguridad. Asimismo, cabe mencionar que los riesgos de nivel bajo fueron monitoreados para evitar que su impacto y probabilidad crezcan con el tiempo.

5.3.4. Determinar los controles y declaración de aplicabilidad

En este apartado, se determinó en función de las amenazas identificadas los controles que ayudaron a reducir los riesgos a un nivel aceptable. En la **Tabla 27** se muestran los controles para reducir los riesgos de los activos de la DISA V.C.

TABLA 27: CONTROLES PARA EL TRATAMIENTO DE RIESGOS DE LA DISA V.C.

ACTIVO Y VALORACION	AMENAZAS Y VULNERABILIDAD		ANÁLISIS Y EVALUACIÓN DEL RIESGO			TRATAMIENTO DEL RIESGO			
NOMBRE DEL ACTIVO	AMENAZA	VULNERABILIDAD	ESTIMACIÓN DEL RIESGO			JERARQUÍA DE CONTROL	CONTROL ALINEADO A LA NTP ISO/IEC 27001:2014	CONTROL ESPECIFICO	RESPONSABLE
			C	I	D				
Servidor - PCs	Errores del administrador	No existe un plan/manual de las BDs que se manejan y sus requerimientos técnicos, ausencia de procedimientos de control de cambios	Bajo	Bajo	Medio	Mitigar	**A.8.2** Clasificación de la información **A.12.4.3** Registros del administrador y del operador	Manual de sistemas y requerimientos técnicos. Elaboración de un procedimiento formal de control de cambios, de un procedimiento formal de manejo de servidores. Capacitación en temas de seguridad.	Oficial de seguridad/ Administrador de Servidor de BD
	Alteración y destrucción accidental de la información	Inexistencia de normas de seguridad, mala configuración de roles y permisos.	Bajo	Medio	Alto	Mitigar	**A.8.2** Clasificación de la información **A.12.4.3** Registros del administrador y del operador. **A.12.4.1** Registro de eventos.	Control de versiones del software. Procedimiento formal de control de cambios. Verificación de roles y permisos.	Oficial de seguridad/ Administrador de Servidor de BD
	Fugas de información	Inadecuada administración de seguridad, contraseñas no seguras.	Alto	Bajo	Bajo	Mitigar	**A.12.4.3** Registros del administrador y del operador **A.7.2.3** Proceso disciplinario.	Respaldar data (backup). Gestión de Permisos.	Oficial de seguridad/ Administrador de Servidor de BD
	Vulnerabilidades de los programas (software)	Falta de licencia, inexistencia de monitorización de software/versiones.	Bajo	Alto	Bajo	Mitigar	**A.14.2.4** Restricción sobre cambios a los paquetes software. **A.12.6.1** Gestión de vulnerabilidades técnicas.	Adquisición de licencia de programas y/o evaluación del uso de software libre. Gestión de vulnerabilidades	Oficial de seguridad/ Administrador de Servidor de BD
	Errores de mantenimiento /actualización de programas software	Falta de licencia, inexistencia de plan de mantenimiento y vigilancia tecnológica.	Bajo	Alto	Bajo	Mitigar	**A.12.6.1** Gestión de vulnerabilidades técnicas	Elaboración de un plan de mantenimiento y actualización de software. Elaboración de un plan de contingencia.	Oficial de seguridad/ Administrador de Servidor de BD
	Errores de mantenimiento / actualización de equipos (hardware)	Inexistencia de plan de mantenimiento y vigilancia tecnológica, falta de equipos de contingencia.	Bajo	Alto	Bajo	Mitigar	**A.11.2.4** Mantenimiento de equipos	Elaboración de un Plan de contingencia – Equipos de contingencia. Plan de mantenimiento de hardware	Oficial de seguridad/ Administrador de Servidor de BD
	Caída del sistema por agotamiento de recursos	No existe un monitoreo de consumo de recursos hardware de los sistemas, falta de mantenimiento de equipos.	Bajo	Bajo	Alto	Mitigar	**A.11.2.3** Seguridad del cableado. **A.13.1.3** Segregación en redes.	Plataforma de seguridad perimetral. Elaboración de un Plan de contingencia – monitoreo preventivo de consumo de recursos Hardware de los sistemas.	Oficial de seguridad/ Administrador de Servidor de BD

Servidor - PCs	Errores de configuración	Inexistencia de plan de configuración y manejo de almacenamiento de información (log)	Medio	Bajo	Alto	Mitigar	**A.12.4.3** Registros del administrador y del operador. **A.12.4.1** Registro de eventos.	Elaboración del manual de configuración de servidores. Actualización de log de eventos.	Oficial de seguridad/ Administrador de Servidor de BD
	Abuso de privilegios de acceso	Falta de políticas de acceso y auditorías internas. (cuentas de usuario sin auditar)	Medio	Alto	Medio	Mitigar	**A.7.2.3** Proceso disciplinario **A.9.4.1** Restricción de acceso a la información.	Elaboración de políticas de acceso. Diseñar esquemas de seguridad basado en roles y permisos. Diseñar un esquema de privilegios sobre el servicio de almacenamiento online de ficheros (fileserver).	Oficial de seguridad/ Administrador de Servidor de BD/ jefe de RR. HH.
	Acceso no autorizado	Falta de monitoreo de la institución y reglas del firewall, antivirus, configuración incorrecta de las cuentas de usuario.	Alto	Bajo	Medio	Mitigar	**A.14.2.8** Pruebas de seguridad del seguridad	Diseñar esquemas de seguridad basado en roles y permisos Diseñar un esquema de privilegios sobre el fileserver. Plataforma de seguridad perimetral.	Oficial de seguridad/ Administrador de Servidor de BD
	Modificación deliberada de información	Administradores de plataformas descontentos, falta de seguridad en los soportes de red.	Bajo	Bajo	Medio	Mitigar	**A.7.2.3** Proceso disciplinario	Establecimiento de métodos de cifrado y backup. Procedimientos disciplinarios establecidos en los contratos.	Oficial de seguridad/ Administrador de Servidor de BD/ Jefe de RR.HH
	Corte del suministro eléctrico	probabilidad a las variaciones de tensión.	Bajo	Bajo	Alto	Mitigar	**A.11.2.2** Servicios de suministro	Contar con sistema de alimentación ininterrumpida. Mantenimiento de sistema de alimentación ininterrumpida.	Oficial de seguridad/ Administrador de Servidor de BD
	Condiciones inadecuadas de temperatura o humedad	Probabilidad a la humedad, recalentamiento, polvo y suciedad	bajo	bajo	Alto	Mitigar	**A.11.2.1** Emplazamiento y protección de los equipos. **A.11.2.4** Mantenimiento de equipos	Ubicación adecuada de equipos según estándares internacionales. Plan de mantenimiento de equipos.	Oficial de seguridad/ Administrador de Servidor de BD
	Degradación de los soportes de almacenamiento de la información	Equipos/dispositivos probables a cambios de temperatura y humedad, falta de esquemas de reemplazo.	Bajo	Bajo	Alto	Mitigar	**A.11.2.4** Mantenimiento de equipos	Plan de mantenimiento de soportes de información. Inventario de activos y monitoreo del funcionamiento y tiempo de vida.	Oficial de seguridad/ Administrador de Servidor de BD
	Inestabilidad de la línea de internet	Un solo proveedor de servicios de comunicaciones, gestión inadecuada de la red.	Bajo	Bajo	Alto	Mitigar	**A.13.1.2** Seguridad de servicios de red.	Plan de contingencia- Uso de varias líneas dedicadas y redundancia de servicios con diversos proveedores del servicio. – balanceo de carga. Acuerdos de nivel de servicio con el(los) proveedor(es) de comunicaciones	Oficial de seguridad/ Administrador de Servidor de BD

Fuente: *Elaboración propia*

Finalmente se elaboró la declaración de aplicabilidad según lo contemplado en el requisito 6.1.3 ítem d) de la NTP - ISO/IEC 27001:2014, esta declaración de aplicabilidad incluye todos los controles necesarios identificados, así como la justificación de la inclusión o exclusión de los controles del **Anexo E**.

Este documento puede ser revisado en el **Anexo I** de la presente tesis.
La declaración de aplicabilidad contempla la siguiente información:

- ✓ **Sección:** Contiene el identificador de sección de los controles propuestos en el Anexo A de la NTP ISO/IEC 27001:2014.
- ✓ **Objetivo:** Es el objetivo de control.
- ✓ **Control:** Es el nombre del control propuesto por la norma para lograr el objetivo de control y este hace referencia a un tema específico al que un riesgo puede estar relacionado.
- ✓ **Estado:** Menciona el estado del control dentro de la DISA V.C. es decir si está aplicado, se va a aplicar o no.
- ✓ **Justificación:** La justificación de la aplicabilidad o no aplicabilidad del control en mención.

CAPITULO VI

6. DISCUSION

En primer lugar, se realizó el análisis de la evaluación del estado inicial de la Dirección de Salud Virgen de Cocharcas con respecto a la NTP - ISO/IEC 27001, se obtuvo un puntaje total de 10%, por lo que se puede determinar que la DISA V.C. se encuentra en una etapa básica de cumplimiento de la norma (no diseñado), luego se procedió con el estudio de la posibilidad de aceptación del Sistema de Gestión de Seguridad de la Información.

En segundo lugar, se procedió con la preparación del Sistema de Gestión de Seguridad de la Información, haciendo el análisis del contexto interno y externo de la DISA V.C. se definió el alcance del SGSI, a su vez se elaboró las políticas y objetivos de seguridad y el comité de seguridad.

En tercer lugar, en la planificación del SGSI, se hizo la evaluación de riesgos y para efectos de esta tesis se adoptó OCTAVE como metodología de análisis y gestión de riesgos. Logrando identificar los activos y elaborando un inventario de ellos. En referente a las amenazas se lograron identificarlos y valorarlos, de las amenazas identificadas se calculó el impacto de materialización. Además, se calculó el riesgo para cada activo, del mismo modo se logró la identificación de los propietarios del riesgo. Por último, se hizo el tratamiento de los riesgos.

Por último, se logró implementar los controles y la declaración de aplicabilidad según lo contemplado en el requisito 6.1.3 ítem d) de la NTP - ISO/IEC 27001:2014, esta declaración de aplicabilidad incluye todos los controles necesarios identificados del SGSI para la Dirección de Salud Virgen de Cocharcas.

CONCLUSIONES

- Con el apoyo de la alta dirección y el compromiso de los trabajadores de la entidad, se logró implementar el diseño de un SGSI bajo el enfoque de la NTP - ISO/IEC 27001 para la Dirección de Salud Virgen de Cocharcas - Chincheros.

- Se logró determinar el alcance del SGSI para el proceso de gestión de la infraestructura tecnológica para la Dirección de Salud Virgen de Cocharcas - Chincheros.

- Teniendo en consideración la aceptación de OCTAVE como metodología de análisis y gestión de riesgos, se elaboró los controles de seguridad para minimizar los riesgos de los recursos activos y la información a los que se encuentra expuesta la Dirección de Salud Virgen de Cocharcas - Chincheros.

- los controles de seguridad de la NTP - ISO/IEC 27001, nos permiten establecer métricas que ayudan a medir la eficacia y eficiencia del SGSI, una vez implementados se logró determinar los procesos correspondientes al alcance del SGSI según la NTP - ISO/IEC 27001:2014 en la Dirección de Salud Virgen de Cocharcas - Chincheros.

RECOMENDACIONES

- Los procedimientos utilizados en esta investigación pueden ser usados para diseñar los Sistemas de Gestión de Seguridad de la Información de otras Direcciones de Salud.

- Se recomienda, a los responsables del área de TI de las entidades públicas, adoptar los lineamientos propuestos por la NTP - ISO/IEC 27001:2014, por tener carácter de obligatoriedad.

- Durante el desarrollo de esta tesis, se observó la necesidad que tiene la DISA V.C. de implementar un SGSI y contar con los documentos de gestión referentes a la seguridad de la información. Se recomienda contratar los servicios de una consultora que le guíe en la implementación exitosa de la norma y se asigne presupuesto para la implantación del SGSI (establecimiento de controles, capacitaciones, mantenimiento, mejora continua).

- Dentro de la entidad existe un personal que hace las veces de oficial de seguridad de la información, pero a su vez está encargado de otras funciones y tareas, se recomienda a la entidad segregar y definir claramente las funciones y responsabilidades del oficial de seguridad de la información.

- Como gran parte de la seguridad depende de las personas, se recomienda generar conciencia de seguridad de la información en los funcionarios y trabajadores de la entidad, mediante capacitaciones y charlas informativas.

REFERENCIAS BIBLIOGRAFICAS

Aguirre Mollehuanca, D. A. (2014). Diseño de un sistema de gestión de seguridad de información para Servicios Postales del PERÚ S.A (Tesis de grado). Pontificia Universidad Católica del Perú. Lima, Perú.

Anonimo. (2014). Blogdiario.com. Obtenido de http://riesgoscontrolinformatico.blogspot.es/tags/metodo-elegido-octave/

Aquije Quijandria, J. G., & Jave Bodadilla, L. L. (2012). Metodologia de Gestion de Seguridad de la Informacion para el Sector Financiero Peruano. Lima-Peru.

Barrantes Porras, C. E. (2012). "Diseño e Implementacion de una sistema de Gestion de Seguridad de Informacion en procesos tecnologicos". (tesis de pregrado). Lima.

Bermudez M, K. G., & Bailon S, E. R. (2015). Analisis en Seguridad Informatica y Seguridad de la Informacion basado en la Norma ISO/IEC27001- Sistemas de la Gestion de Seguridad de la Informacion dirigido a una empresa de servicios financieros (tesis de pregrado). Universidad Politecnica Salesiana. Guayaquil.

Bernal, T. (2010). "Metodologia de la Investigacion" (Tercera Ed.). Colombia: Pearson Educacion.

Blogdiario.com. Obtenido de http://riesgoscontrolinformatico.blogspot.es/tags/metodo-elegido-octave/

Carrasco Diaz, S. (2006). metodología de la Investigación Científica. Lima, Perú: Editorial San Marcos.

Carrera Villamarin, W. G. (2012). "Diseño de un modelo de gestion de Riesgos de Seguridad de la Informacion Basado en el Acoplamiento de la Norma ISO/IEC 27005:2008 y el Metodo Octave" (Tesis de Master (Msc)), Escuela Politecnica Naciaonal. Quito.

Ccesa Quincho, M. (2017). Diseño de un Sistema de Gestion de Seguridad de la Informacion bajo el enfoque de la NTP ISO/IEC 27001:2014 para la Municipalidad Provincial de Huamanga, 2016. (tesis de maestría). Universidad Nacional San Cristobal de Huamanga. Ayacucho.

Chiavenato, I. (2006). Introduccion a la Teoría General de la Administración. México: McGraw-Hill Interamericana.

disachincheros.webnode.es. (2014).

Gómez, L., & Fernández, P. (2015). Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad. Primera edición. Madrid: España, AENOR.

Guanoluisa Huertas, J. E., & Maldonado Soliz, I. F. (2015). Analisis de Riesgos y Diseño de un Plan de Seguridad de la Informacion para el Consejo Nacional de Igualdad de Discapacidades "CONADIS" (Proyecto previo a la obtencion del título de Ingeniero en Sistemas Informáticos y de Computación). Quito.

Hernandez Sampieri, R., & Fernandez Collado, C. (2014). Metodologia de la Investigacion (Sexta Ed.). Mexico: McGRAW-HILL Interamericana Editores.

INDECOPI. (2007). Norma Técnica Peruana “NTP-ISO/ IEC 17799:2007 EDI (ISO 27002:2005). Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. . Lima, Perú: Segunda edicion.

INDECOPI. (2014). Norma Tecnica Peruana ntp-ISO-IEC-27001. Obtenido de https://canvas.utp.edu.pe/courses/8870/files/42244

ISO 27000. (2005). ISO.27000.es. Obtenido de http://www.iso27000.es/glosario.html#section10p

ISO 27000. (2012). www.iso27000.es. El Portal de ISO 27001 en Español. Obtenido de http://www.iso27000.es/iso27000.html

ISOTools Excellence. (18 de Agosto de 2015). La norma ISO 27001:2013 2013 ¿Cuál es su estructura? [Entrada en Blog]. Obtenido de http://www.pmg-ssi.com/2015/08/norma-iso-27001-2013-estructura/

Justino Salinas, Z. I. (2015). Diseño de un sistema de gestión de seguridad de información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013 (Tesis de grado). Pontificia Universidad Católica del Perú, Lima, Perú.

Lloyd's Register (LR). (15 de Octubre de 2018). http://www.lrqa.es. Obtenido de http://www.lrqa.es/certificaciones/iso-iec27001/

López. (2011). "Diseño de un plan de gestion de seguridad de la informacion. Caso: direccion de informática de la alcaldía del municipio jimenez del estado lara" (trabajo de maestría). Universidad Centroccidental Lisandro Alvarado Barquisimetro. Venezuela.

Mcmillan, J. Y., & Schumacher, S. (2005). Investigación Educativa. Madrid, España: Pearson Educación.

Peltier T. R., Peltier, J., & Blackley, J. (2005). Information Secutirty Fundamentals. Obtenido de https://binhthanhdang.files.wordpress.com/2010/08/information-security-fundamentals-ebook-een.pdf

Rosales Bravo, & Suarez Leon. (2015). Plan de Gestion de Seguridad de la Informacion, Bajo la Norma ISO/IEC 27001:2013, en una Institucion Financiera Ecuatoriana. (tesis de pregrado). Escuela Politecnica Nacional. Quito.

GLOSARIO DE TERMINOS

- **Información:** Es cualquier forma de registro electrónico, óptico, magnético o en otros medios, previamente procesado a partir de datos, que puede ser almacenado, distribuido y sirve para análisis, estudios, toma de decisiones.
- **Tecnología de Información (TI):** Es el conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, servicios asociados, entre otros.
- **Integridad (I):** Es la garantía de mantener totalidad y exactitud de la información y de los métodos de procesamiento.
- **Disponibilidad (D);** Es la garantía de que los usuarios autorizados tienen acceso a la información cada vez que o requieren a través de los medios adecuados que satisfagan sus necesidades.
- **Confidencialidad (C):** Es la garantía de que solo el personal autorizado accede a la información preestablecida.
- **Seguridad de la Información (SI):** Son los mecanismos implantados que garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella.
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, infraestructura, personas) que tenga valor para la organización.
- **Alcance:** Ámbito de la organización que queda sometido al SGSI.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

- **Control:** Herramienta de la gestión del riesgo, incluido políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal. El control es también usado como sinónimo de salvaguardia.

- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el SGSI de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

- **Degradar:** Reducir o desgastar las cualidades inherentes a algo.

- **Impacto:** El costo para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros. Ejem., pérdida de reputación, implicaciones legales, etc.

- **Probabilidad:** Frecuencia con que ocurre una amenaza.

- **Vulnerabilidad:** Se denomina vulnerabilidad a toda debilidad que puede ser aprovechada por una amenaza, o más detalladamente a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial.

ANEXOS

ANEXO A

CUESTIONARIO PARA IDENTIFICAR AMENAZAS Y ESTABLECER PROBABILIDAD DE OCURENCIA - MARCA CON UN ASPA (X)

AMENAZAS	PROBABILIDAD DE OCURRENCIA				
	1	2	3	4	5
Fuego					
Tormenta eléctrica, rayo					
Error de usuario					
Errores del administrador					
Alteración accidental de la información					
Destrucción de la información					
Fugas de la información					
Vulnerabilidades de los programas (software)					
Errores de mantenimiento /actualización de programas software					
Errores de mantenimiento / actualización de equipos (hardware)					
Indisponibilidad del personal por salud					
Manipulación de los registros de actividad					
Suplantación de la identidad del usuario					
Abuso de privilegios de acceso					
Difusión de software dañino					
Acceso no autorizado					
Modificación deliberada de información					
Inestabilidad de la línea de internet					
Manipulación de programas					
Manipulación de equipos					
Robo de equipos					
Corte del suministro eléctrico					
Condiciones inadecuadas de temperatura o humedad					
Degradación de los soportes de almacenamiento de la información					
Instalación de software no autorizado					

VALOR	PUNTUACION
Prácticamente imposible	1
Poco probable	2
Posible	3
Probable	4
Muy probable	5

ANEXO B

CUESTIONARIO SOBRE LA POSIBILIDAD ACEPTACIÓN DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION (SGSI) Y DIAGNOSTICO INICIAL DE SEGURIDAD DE LA INFORMACIÓN - MARCA CON UN ASPA (X)

NOMBRE: …….. CARGO: ……

Nº	PREGUNTA	SI	NO
1	¿Sabe Ud. ¿Si dentro de la Dirección de Salud Virgen de Cocharcas existe un sistema de gestión de seguridad de la información?		
2	¿Cree usted que el diseño de un sistema de gestión de seguridad de la información permitirá mejorar la seguridad de la información de su área de trabajo?		
3	¿Cree usted que en su área de trabajo se logrará un cambio positivo con la aplicación de este sistema de gestión de seguridad de la información?		
4	¿Aprobaría usted la implementación del sistema de gestión de seguridad de la información en su área de trabajo?		
5	En su área de trabajo, ¿Aprobaría usted programas dirigidos a todos los empleados para sensibilizar sobre la seguridad de la información?		
6	¿Estaría Ud. dispuesto a colaborar para que el diseño e implementación del sistema de gestión de seguridad de la información se lleve a cabo en su área de trabajo?		
7	¿Considera Ud. que en su área de trabajo existe información que debe ser protegida?		
8	¿Ha recibido Ud. capacitación sobre la seguridad de la información de acuerdo a su función laboral?		
9	¿Su contrato contempla ítems que estipulen responsabilidades con respecto a la seguridad de la información?		
10	Dentro de su área de trabajo ¿se considera la seguridad de información cuando se gestiona un proyecto?		
11	¿Cuenta Ud. con un computador/laptop para realizar sus funciones? (Si la respuesta es **No** pasar a la **pregunta 14**)		
12	¿Cuenta Ud. con una clave de acceso para ingresar a su computador y/o laptop?		
13	Cuando su computador está indefenso ¿Se activa el bloqueo de pantalla con contraseña para proteger la información?		
14	¿En lo que va del año ha sufrido modificación y/o pérdida de información ya sea por virus, acceso de personas no autorizadas, deterioro, tras papeleo, etc.?		
15	¿En su área de trabajo se han realizado evaluación de riesgos relacionados con la información?		
16	¿En su área de trabajo se han realizado una evaluación de vulnerabilidades de la red?		
17	¿Su área de trabajo cuenta con software antivirus actualizado?		
18	¿Considera que su oficina está protegida contra amenazas externas y/o ambientales que ocasionen pérdidas de información?		

ANEXO C

IMÁGENES DEL SERVIDOR DE LA DISA V.C

Figura 1: Servidor de la DISA V.C.

Fuente: *Elaboración propia*

Figura 2: UPS del Servidor de la DISA V.C.

Fuente: *Elaboración propia*

Figura 3: Firewall de la DISA V.C.

Fuente: *Elaboración propia*

ANEXO D

ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

1. Propósito, alcance y usuarios

El propósito de este documento es definir claramente cuáles son los límites del Sistema de Gestión de Seguridad de la Información (SGSI) de la Dirección de Salud Virgen de Cocharcas - Chincheros y es aplicable a toda la documentación perteneciente al SGSI.

Los únicos usuarios autorizados a este documento son los miembros del comité de seguridad de la información y el personal autorizado de la dirección y el área de informática de la Dirección de Salud Virgen de Cocharcas - Chincheros.

2. Alcance del SGSI

El alcance del Sistema de Gestión de Seguridad de la Información aplica sólo para el proceso de GESTIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA, sub proceso de gestión de seguridad de la información, dentro de los sistemas de información que sustentan los procesos de negocio.

Se consideran los activos de información considerados como relevantes dentro del alcance.

El Sistema de Gestión de Seguridad de la Información aplica para la Dirección de Salud Virgen de Cocharcas - Chincheros.

ANEXO E

EVALUACION COMPLETA DEL ESTADO INICIAL DE LA DIRECCION DE SALUD VIRGEN DE COCHARCAS RESPECTO A LA NTP ISO/IEC 27001:2014

SECCION	REQUISITOS DE LA NTP ISO/IEC 27001: 2014	ESTADO	EVIDENCIA/SUGERENCIA (¿COMO LO CUMPLE? / ¿QUÉ SE TENDRIA QUE HACER?)	VALORACION
4	**CONTEXTO DE LA ORGANIZACIÓN**	No diseñado	Se sugiere realizar el análisis del contexto de la DISA V.C. para comprender tanto los aspectos externos como internos, las partes interesadas y relevantes al SGSI.	0%
4.1	**Comprender la Organización y contexto**. La organización **debe** determinar los aspectos externos e internos que son relevantes para este propósito y que afectan su capacidad de lograr el(los) resultado(s) deseados de este SGSI	Parcialmente diseñado	La DISA V.C. posee documentos visibles de su Misión, Visión, FODA, Manual de Organización y Funciones (MOF), Reglamento de Organización y Funciones (ROF). Pero no contempla de manera clara los ítems de seguridad de la información. **Sugerencia:** Establecer objetivos de seguridad de la Información que estén alineados con los objetivos estratégicos.	25%
4.2	**Comprender las necesidades y expectativas de las partes interesadas.** La organización **debe** determinar las partes interesadas y los requisitos de las mismas.	No Diseñado	**Sugerencia:** Determinar las partes interesadas y comprender las necesidades y expectativas de éstas, referentes a la seguridad de la información.	0%
4.3	Determinar el alcance del SGSI.	No Diseñado	**Sugerencia.** Determinar el alcance del SGSI teniendo en consideración los aspectos referidos, documentarlo y ponerlo a disposición de las partes interesadas.	0%
4.4	**Sistema de Gestión de Seguridad de la información.** La organización **debe** establecer, implementar, mantener y mejorar continuamente un SGSI, en conformidad con los requisitos de esta NTP.	No Diseñado	**Sugerencia.** Establecer un plan para la mejora continua del SGSI conforme a la NTP Vigente.	10%
5	**LIDERAZGO**	No diseñado	El Titular de la Entidad, debe mostrar liderazgo y compromiso respecto al SGSI. Entonces, debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la Seguridad de la Información estén asignadas y comunicadas. Por lo tanto, es necesario establecer: Políticas de Seguridad de la Información, y los Objetivos de Seguridad de la Información acorde al propósito de la organización.	15%
5.1	**Liderazgo y compromiso.** La alta dirección **debe** demostrar liderazgo y compromiso respecto al SGSI.	No diseñado	El titular de la entidad debe mostrar liderazgo y compromiso	20%
5.2	Política	No diseñado	Establecer la Política de Seguridad de la Información acorde al propósito de la organización, incluir los objetivos de seguridad de la Información, mantenerla disponible y comunicada a toda la organización.	10%
5.3	Roles, responsabilidades y autoridades organizacionales.	No diseñado	La alta dirección debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la Seguridad de la Información estén asignadas y comunicadas.	10%
6	**PLANIFICACION**	No diseñado	Adoptar, planificar y documentar el procedimiento de valoración y tratamiento de riesgos de la seguridad de la información. Establecer y documentar los objetivos de seguridad de la información conforme a los propósitos de la organización y elaborar un plan para lograr estos objetivos de seguridad de la información.	5%
6.1	Acciones para tratar los riesgos y oportunidades	No diseñado	Adoptar, planificar y documentar el procedimiento la valoración y tratamiento de riesgos de la seguridad de la información.	5%
6.2	Objetivos de seguridad de la información y planificación para conseguirlos	No diseñado	Establecer los objetivos de seguridad de la información alineados a los objetivos estratégicos de la organización y elaborar un plan para lograr estos objetivos de seguridad.	0%
7	**SOPORTE**	No diseñado		10%
7.1	**Recursos** La organización **debe** determinar y proporcionar los	No diseñado	Asignar presupuesto para la implementación, mantenimiento y mejora continua del SGSI.	0%

	recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI.			
7.2	Competencia	No diseñado	Determinar las competencias del personal a su cargo para un correcto desempeño del SGSI, cuando sea necesario tomar acciones para adquirir las competencias necesarias sobre la seguridad de la información.	0%
7.3	**Concientización** Las personas que trabajan bajo el control de la organización **deben** ser conscientes de la política de seguridad, su contribución a la efectividad del SGSI y las implicancias de no tener la conformidad de los requisitos del SGSI.	No diseñado	Concientizar al personal que trabaja en la organización sobre la importancia de la seguridad de la información, la política de seguridad y el papel crucial que cumple cada uno de ellos en el correcto desempeño de SGSI, asimismo concientizarlos sobre las consecuencias de no cumplir con los requisitos del SGSI.	5%
7.4	**Comunicación** La organización **debe** determinar la necesidad de comunicaciones internas y externas relevantes al sistema de gestión de seguridad de la información	Parcialmente diseñado	Existe un ítem de seguridad de la información y el medio por donde se responde es a través de la web. **Se recomienda** documentar los procedimientos de comunicación para tenerlos como evidencia e incluir en el mismo la comunicación interna.	25%
7.5	Información documentada	No diseñado	Existe documentación de origen externo (Resoluciones, etc.) identificados pero que aún se han analizado completamente para empezar la planificación y posterior implementación del SGSI en la DISA V.C. Se sugiere empezar a elaborar la documentación necesaria exigida por la NTP vigente para lograr la efectividad del SGSI asimismo determinar los procedimientos de creación, actualización y control de la documentación.	5%
8	**OPERACIÓN**	No diseñado		0%
8.1	Planificación y control operacional	No diseñado	Planificar, controlar y documentar los procesos necesarios para cumplir con los requisitos de seguridad de la información y estar seguros de que los procesos se llevan a cabo acorde a lo planeado.	0%
8.2	Evaluación de riesgos de seguridad de la información	No diseñado	Planificar los intervalos de tiempo en los que se llevarán a cabo las evaluaciones de riesgos de seguridad de la información, documentar los resultados de estas evaluaciones.	0%
9	**EVALUACION DEL DESEMPEÑO**	No diseñado	Implementar el SGSI y elaborar un plan para evaluar periódicamente su funcionamiento y garantizar que el sistema se mantiene eficaz a lo largo del tiempo. Asimismo, documentar dichas evaluaciones.	0%
9.1	Monitoreo, medición, análisis y evaluación	No diseñado	Establecer procedimientos para realizar el monitoreo, medición, análisis y evaluar el desempeño de seguridad de la información y la efectividad del SGSI. Documentar los resultados del monitoreo, medición, análisis y evaluación del SGSI.	0%
9.2	Auditoría interna	No diseñado	No existen documentos del resultado de la auditoría realizado por el órgano de control interno en el que se contempla la no conformidad de seguridad de la información. **Se recomienda** planificar auditorías internas y levantar la no conformidad de la auditoría interna para el cumplimento legal.	0%
9.3	Revisión por la gerencia	No diseñado	No existe documentación (resultado de auditoría y memorandos a la subgerencia de Sistemas y Tecnología) que dan a conocer el estado actual de la organización respecto al SGSI (no implementado) y la orden de implementación de las funciones de seguridad.	0%
10	**MEJORAS**	No diseñado	Implantar el SGSI y elaborar un plan de mejora continua para actualizar el SGSI de acuerdo a los cambios y novedades de la organización, las tecnologías, las amenazas, etc., tratando de mantener los riesgos controlados en todo momento.	0%
10.1	No conformidades y acción correctiva	No diseñado		0%
10.2	Mejora Continua La organización debe mejorar continuamente la conveniencia, adecuación y efectividad del sistema de gestión de seguridad de la información.	No diseñado		0%
PUNTAJE TOTAL DE LA EVALUACION DE REQUISITOS DE LA NTP ISO/IEC 27001:2014				10%

ANEXO F

RELACION DE ACTIVOS - EN CADA TABLA MARQUE (X) LOS ACTIVOS CON LOS QUE CUENTA LA DIRECCION DE SALUD VIRGEN DE COCHARCAS

TABLA DE RELACION DE ACTIVOS DE TIPO DATO/INFORMACION
( ) Ficheros o bases de datos
( ) Copias de respaldo
( ) Datos de configuración de los sistemas de información
( ) Datos de gestión interna
( ) Credenciales (Ejem. contraseñas)
( ) Datos de validación de credenciales
( ) Datos de control de acceso
( ) Registro de actividad o de los sistemas de información
( ) Código fuente de los sistemas de información
( ) Código ejecutable de los sistemas de información
( ) Datos de prueba para la implementación de los sistemas de información

TABLA DE RELACION DE ACTIVOS DE TIPO SERVICIO
( ) Anónimo (sin requerir identificación del usuario)
( ) Al público en general (sin relación contractual)
( ) A usuarios externos (bajo una relación contractual)
( ) Interno (a usuarios de la propia organización)
( ) Internet
( ) Acceso remoto a cuenta local
( ) Correo Electrónico
( ) Almacenamiento de ficheros (File Server)
( ) Transferencia de ficheros (FTP)
( ) Intercambio electrónico de datos (EDI)
( ) Servicios de directorio
( ) Gestión de identidades (Servicios que permiten altas y bajas de usuarios de los sistemas)

TABLA DE RELACION DE ACTIVOS DE TIPO SOFTWARE/APLICACIONES INFORMATICAS
( ) Software de desarrollo propio
( ) Software a medida (subcontratado)
( ) Página Web
( ) Intranet
( ) Servidor de aplicaciones
( ) ERP (Enterprise Resource Planning – Planificación de Recursos Empresariales)
( ) Correo electrónico
( ) Sistema de gestión de bases de datos
( ) Ofimática
( ) Antivirus
( ) Sistema operativo
( ) Gestor de máquinas virtuales
( ) Servidor de Terminales
( ) Sistema de backup

TABLA DE RELACION DE ACTIVOS DE TIPO EQUIPOS INFORMATICOS
( ) PCs ( ) Servidor ( ) Equipamiento de respaldo ( ) Medios de impresión (impresoras y servidores de impresión) ( ) Escáneres ( ) Módems ( ) Conmutadores (Swicth) ( ) Encaminadores (Router) ( ) Cortafuegos (Firewall) ( ) Punto de acceso inalámbrico ( ) Teléfono IP ( ) Otros. ……..

TABLA DE RELACIÓN DE ACTIVOS DE TIPO REDES DE COMUNICACIONES
( ) Red telefónica ( ) Comunicaciones radio ( ) Red inalámbrica ( ) Telefonía móvil ( ) Red local ( ) Internet

TABLA DE RELACIÓN DE ACTIVOS DE TIPO SOPORTE DE INFORMACIÓN
( ) Discos Duros ( ) Discos virtuales ( ) Almacenamiento en red ( ) Disquetes ( ) Cederrón (CD-ROM) ( ) Memorias USB ( ) DVD ( ) Cinta magnética ( ) Tarjetas de memoria ( ) Tarjetas inteligentes ( ) Material impreso ( ) Cinta de papel ( ) Otros. ……

TABLA DE RELACIÓN DE ACTIVOS DE EQUIPAMIENTO AUXILIAR
( ) Fuentes de alimentación ( ) Generadores eléctricos ( ) Cable eléctrico ( ) Fibra óptica ( ) Equipos de destrucción de soportes de información ( ) Suministros esenciales ( ) Mobiliario, armarios, etc. ( ) Otros: ……

ANEXO G

INVENTARIO DE ACTIVOS DEL PROCESO GESTIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA

Nº	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	TIPO DE ACTIVO	UBICACIÓN
1	Datos vitales	Datos que almacenan los diferentes sistemas de información esenciales para el funcionamiento de la DISA V.C.	Dato/Información	Servidor
2	Archivos personales	Documentos personales de los trabajadores de la DISA V.C.	Dato/Información	Computadoras personales, estantería
3	Copias de respaldo	Copias de respaldo de Datos/Información que manejan los distintos sistemas de la DISA V.C.	Dato/Información	Servidor y PCs personales
4	Datos de configuración de los SI	Corresponde a los documentos, manuales y procedimientos relacionados con la administración de los diferentes SI	Dato/Información	Archivo físico (estantería)
5	Datos de gestión interna	Corresponde a los documentos de la DISA V.C.	Dato/Información	Archivo físico (estantería)/VPS
6	Credenciales (contraseñas)	Usuario y contraseña que utilizan los usuarios para ingresar a los recursos tecnológicos	Dato/Información	C/trabajador guarda de sus contraseñas
7	Datos de control de acceso	Corresponde a los datos de los usuarios internos que utilizan los sistemas de información y/o aplicaciones	Dato/Información	BD/Usuario interno
8	Log de los sistemas de información	Log que contiene los registros de los eventos de seguridad y de los eventos de administración sobre aplicaciones	Dato/Información	Servidor
9	Correo electrónico	Correo electrónico institucional	Servicio	correo electrónico GMAIL
10	Gestión de privilegios	Corresponde al mecanismo para la administración y asignación de privilegios de acceso a los recursos tecnológicos y aplicaciones	Servicio	Sistemas de información
11	Base de Datos	BD de los diferentes sistemas que almacenan la información de la entidad	Servicio	Servidor
12	Página Web	Página Web de la entidad	Software	VPS
13	SIAF	Sistema que maneja las dependencias de las oficinas de logística, planeamiento y presupuesto, tesorería, contabilidad	Software/Aplicaciones informática	Servidor
14	SIGA	Sistema que maneja las dependencias de las oficinas de logística, coordinaciones, patrimonio, almacenes	Software/Aplicaciones informática	Servidor
15	Computador de los trabajadores	Computadores que utilizan los trabajadores de la entidad	Equipos informáticos	Oficinas
16	Impresoras	Impresoras de la entidad	Equipos informáticos	Oficinas
17	Soporte de la red	Equipamiento necesario para transmitir datos: routers, switch	Equipos informáticos	Servidor
18	Red local	Red de comunicaciones cableada	Redes de comunicación	Red local
19	Internet	Red de redes	Redes de comunicación	Red local
20	Disco Duro externo	Disco Duro externo	Soporte de información	Oficina de informática
21	Dispositivos de almacenamiento externo	CDs, DVDs, etc	Soportes de información	Archivo físico o estante
22	Soportes no electrónicos	Dispositivos físicos de almacenamiento no electrónico como material impreso	Soportes de información	Archivo físico o estante
23	Sistema de alimentación ininterrumpida	UPS	Equipamiento auxiliar	Oficinas de la DISA V.C.
24	Gabinetes/estantes	Armarios de soporte a los sistemas de información	Equipamiento auxiliar	Oficinas de la DISA V.C.
25	Servidor	Centro principal de procesamiento donde reside la infraestructura para soportar la operación del negocio	Instalación	Oficina de la DISA V.C.
26	Usuarios externos	Usuarios externos a la DISA V.C. y que usan los servicios a través de la página Web, redes sociales	Personal	Usuarios externos
27	Usuarios internos	personal propio de la DISA V.C.	Personal	Oficinas de la DISA V.C.
28	Personal de soporte técnico	Personal encargado del soporte técnico de la DISA V.C.	Personal	Oficina de Unidad de Seguros

ANEXO H

TABLA DE DESCRIPCIÓN DE AMENAZAS, RIESGOS Y CONSECUENCIAS.

AMENAZAS							RIESGOS	
Nº	AMENAZA	DESCRIPCION	TIPOS DE ACTIVOS AFECTADOS	DIMENSIONES			RIESGO	CONCURRENCIA
				C	I	D		
1	Fuego	Incendios: posibilidad de que el fuego acabe con recursos del sistema.	Equipos informáticos, soportes de información, equipamiento auxiliar.			2	Incendio	pérdida de los activos de información
2	Tormenta eléctrica, rayo	Incidentes que se producen sin intervención humana	Equipos informáticos, soportes de información, equipamiento auxiliar.			2	Apagón	No disponibilidad de la infraestructura tecnológica
3	Error de usuario	Equivocaciones de las personas cuando usan los servicios, datos, etc.	Datos/información, servicios, aplicaciones (software), soportes de información	2	1	3	Equivocaciones de los usuarios	No disponibilidad, de los datos/información, soportes de información, etc.
4	Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación de los sistemas de información	Datos/información, servicios, aplicaciones (SW), equipos informáticos, redes de comunicaciones, soportes de información	3	2	1	Equivocaciones de los administradores	Mal funcionamiento de los servicios/SI
5	Alteración accidental de la información	Alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	Datos/información, servicios, aplicaciones (SW) comunicaciones (tránsito), soportes de información.		1		Alteración de los datos	Pérdida de la disponibilidad
6	Destrucción de información	Pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	Datos/información, servicios, aplicaciones (SW), comunicaciones (tránsito), soportes de información.			1	Eliminación de la Información	Pérdida total de información.
7	Fugas de información	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc.	Datos/información, servicios, aplicaciones (SW), comunicaciones (tránsito), soportes de información.	1			Mal uso de la información	Pérdida de la confidencialidad
8	Vulnerabilidades de los programas (software)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario, pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.	Aplicaciones (software)	3	1	2	Defectos en el código	Pérdida de la integridad de los datos o la capacidad de operar de los sistemas y/o aplicaciones.
9	Errores de mantenimiento /actualización de programas software	Defectos en los procedimientos o controles de actualización del código que permiten que sigan 10utilizándose programas con defectos conocidos y reparados por el fabricante.	Aplicaciones (software)		1	2	Defectos en los procedimientos o controles de actualización del código.	Pérdida de la disponibilidad de los sistemas y/o aplicaciones.
10	Errores de mantenimiento / actualización de equipos (hardware)	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.	Equipos informáticos, soportes electrónicos, equipamiento auxiliar.			1	Defectos en los procedimientos o controles de actualización de los equipos.	Mal funcionamiento de los equipos
11	Indisponibilidad del personal	Ausencia accidental del puesto de trabajo: por salud, alteraciones del orden público.	Personal interno			1	Insatisfacción de los usuarios	No se atiendan los servicios adecuadamente
12	Suplantación de la identidad del usuario	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.	Datos/información, servicios, aplicaciones (software), redes de comunicaciones	1	3	2	Mal uso intencionado de la infraestructura tecnológica	Modificación de la información

13	Abuso de privilegios de acceso	Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.	Datos/información, servicios, aplicaciones (SW), equipos informáticos, redes de comunicaciones	1	2	3	Abuso de privilegios para realizar tareas que no son de su competencia.	Modificación a los accesos o información
14	Difusión de software dañino	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, etc.	Aplicaciones (software)	3	2	1	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, etc.	Pérdida de dato/información
15	Acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.	Datos/información, servicios, aplicaciones (SW), equipos informáticos, redes de comunicaciones, soportes de información, equipamiento auxiliar.	1	2		Ataque a los recursos del sistema	Hackeo
16	Modificación deliberada de información	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.	Datos/información, servicios (acceso), aplicaciones (SW), soportes de información.			1	Eliminación intencional de información	Información no disponible
17	Inestabilidad de la línea de internet	Fallo en el servicio prestado por un tercero	Servicios			1	No disponibilidad de los servicios	Insatisfacción de los trabajadores
18	Manipulación de programas	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	Aplicaciones (software)	1	2	3	Alteración intencionada del funcionamiento de los programas.	Mal funcionamiento de los programas
19	Manipulación de equipos	Alteración intencionada del funcionamiento de los equipos, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	Aplicaciones (hardware)	1	2	3	Alteración intencionada del funcionamiento de los equipos	Mal funcionamiento de los equipos
20	Robo de equipos	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.	Equipos informáticos, soportes de información, equipamiento auxiliar.	2		1	Carencia de un medio para prestar los servicios, es decir una indisponibilidad.	pérdida económica, Insatisfacción de los clientes, llamadas de atención, sanciones graves
21	Corte del suministro eléctrico	Interrupción de la alimentación de potencia	Equipos informáticos, soportes de información, equipamiento auxiliar.			1	Malogren los equipos, pérdida de la información	Dejen de funcionar los servicios, insatisfacción del cliente
22	Condiciones inadecuadas de temperatura o humedad	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, etc.	Equipos informáticos, soportes de información, equipamiento auxiliar.			1	Malogren los equipos	No disponibilidad de los equipo y servicios prestados a través de ellos
23	Degradación de los soportes de almacenamiento de la información	Degradación como consecuencia del paso del tiempo	Soportes de información			1	Pérdida de información	No disponibilidad de la información
24	Instalación de software no autorizado	Instalación de software no autorizado por parte del personal interno.	Aplicaciones (software)	1	2		Infectar/malograr el sistema	sanciones por uso de software no autorizado y sin licencia, funcionamiento incorrecto

ANEXO I

Declaración de aplicabilidad

SECCIÓN	OBJETIVO	CONTROL	ESTADO	JUSTIFICACION
A.5	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**			
A.5.1	Proporcionar directrices de gestión de seguridad de la información en concordancia con los requerimientos del negocio, las leyes y las regulaciones	**5.1.1** Políticas para la seguridad de la Información	Aplicar	Exigido por la NTP ISO/IEC 27001:2014
		5.1.2 Revisión de las políticas para la seguridad de la información	Aplicar	Exigido por la NTP ISO/IEC 27001:2014
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**			
A.6.1	Organización interna	**6.1.1** Roles y responsabilidades en seguridad de la información	Aplicar	Exigido por la NTP ISO/IEC 27001:2014
		6.1.2 Segregación de funciones	Aplicar	Se deben segregar las funciones para la realización de actividades, para evitar usos indebidos y el impacto de los incidentes de seguridad.
		6.1.3 Contacto con autoridades	Aplicar	Será necesario mantener comunicación con la ONGEI que es la entidad encargada de verificar el estado de seguridad de la información en las entidades del estado, con PeCERT. Es necesario mantener contacto con foros especializados, revistas de interés, etc.
		6.1.4 Contacto con grupos especiales de interés	Aplicar	Será necesario mantener contacto con foros especializados, revistas, etc. en temas de seguridad para estar alertas a la aparición de nuevas amenazas
		6.1.5 Seguridad de información en la gestión de proyectos	Aplicar	Será necesario identificar riesgos derivados de los proyectos
A.6.2	**Dispositivos móviles y teletrabajo:** Asegurar la seguridad del teletrabajo y el uso de dispositivos móviles	**6.2.1** Política de dispositivos móviles	No aplicar	No se usan dispositivos móviles para el tratamiento y almacenamiento de información.
		6.2.2 Teletrabajo	No aplicar	No se realiza teletrabajo en la entidad.
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**			
A.7.1	**Antes del empleo:** Asegurar que los empleados y contratistas entienden sus responsabilidades y son convenientes para los roles para los que se les considera	**7.1.1** Investigación de antecedentes	Aplicado	Se controla la selección del personal y se solicitan referencias.
		7.1.2 Términos y condiciones del empleo	Aplicado	Están establecidos en el contrato. Aunque se recomienda revisar para asegurar que no se excluyen responsabilidades de seguridad de la información relevantes.
A.7.2	**Durante el empleo:** Asegurar que los empleados y contratistas sean conscientes y cumplan con sus responsabilidades de seguridad de la información.	**7.2.1** Responsabilidades de la gerencia	Aplicar	Es necesario documentar y comunicar las responsabilidades antes de capacitar al personal para que cumpla con las políticas de seguridad.
		7.2.2 Conciencia, educación y capacitación sobre la seguridad de la información	Aplicar	Según el análisis de riesgos, una amenaza habitual es la falta de formación en materia de seguridad.
		7.2.3 Proceso disciplinario	Aplicar	En la comunicación de responsabilidades y políticas se informará de las consecuencias de su incumplimiento.
A.7.3	**Terminación y cambio de empleo:** Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.	**7.3.1** Responsabilidades ante la finalización o cambio de empleo	Aplicar	Es necesario definir y contemplar en los contratos las responsabilidades ante la finalización del empleo, especialmente en relación a la confidencialidad de la información.
A.8	**GESTIÓN DE ARCHIVOS**			
A.8.1	**Responsabilidad sobre los activos:** Identificar los activos de la organización y definir responsabilidades de protección apropiadas.	**8.1.1** Inventario de activos	Aplicar	Necesario para llevar a cabo el proceso de evaluación de riesgos según la metodología adoptada.
		8.1.2 Propiedad de los activos	Aplicar	Es necesario identificar a los responsables de la seguridad de los activos.
		8.1.3 Uso aceptable de los activos	Aplicar	Se marcarán pautas de utilización de los activos.
		8.1.1 Retorno de activos	Aplicar	Cuando el contrato del empleado termina, éste devuelve todos los activos que poseía.
A.8.2	**Clasificación de la información:** Asegurar que la información recibe un nivel apropiado de protección	**8.2.1** Clasificación de la información	Aplicar	Es necesario identificar la información acorde a los requisitos legales, valor, criticidad dentro de la Subgerencia para aplicar medidas adecuadas.

	en concordancia con su importancia para la organización.	**8.2.2** Etiquetado de la información	Aplicar	Necesario para que los usuarios de la información identifiquen las protecciones a aplicar.
		8.2.3 Manejo de activos	Aplicar	Para adoptar medidas de seguridad en función a la clasificación establecida.
A.8.3	**Manejo de los medios:** Prevenir la divulgación, modificación, remoción o destrucción no autorizada de información almacenada en medios.	**8.3.1** Gestión de medios removibles	Aplicar	Necesario dado el incremento de soportes USB.
		8.3.2 Disposición de medios	Aplicar	Es necesario poner a disposición los medios de manera segura cuando ya no se requieran, sobre todo en los Backups, formalizar el procedimiento.
		8.3.3 Transferencia de medios físicos	No Aplicar	No se extraerían soportes con información relevante fuera de la oficina.
A.9	**CONTROL DE ACCESO**			
A.9.1	**Requisitos de la empresa para el control de acceso:** Limitar el acceso a la información y a las instalaciones de procesamiento de la información.	**9.1.1** Política de control de acceso	Aplicado	Los usuarios cuentan con la información pertinente respecto a los permisos de acceso que poseen.
		9.1.2 Acceso a redes y servicios de red	Aplicado	Se controla el acceso a los servicios de red en función de la necesidad de uso.
A.9.2	**Gestión de acceso de usuario:** Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios.	**9.2.1** Registro y baja de usuarios	Aplicar	El movimiento de alta y baja de usuarios en los sistemas haría indispensable este control. Contar con documentos formales autorizado por el jefe del proceso sobre la creación o baja de usuario.
		9.2.2 Aprovisionamiento de acceso a usuario	Aplicado	Se conceden o retiran los permisos, en función de las necesidades de acceso de los usuarios.
		9.2.3 Gestión de derechos de acceso privilegiados	Aplicar	Es necesario restringir y controlar la asignación y uso de acceso privilegiado.
		9.2.4 Gestión de información de autentificación secreta de usuarios	Aplicar	Dado el resultado del análisis de riesgo, se cree conveniente aplicar este tipo de control. Es decir, establecer un proceso de gestión controlado para la asignación de información confidencial de autenticación.
		9.2.5 Revisión de los derechos de acceso de usuarios.	Aplicar	Realizar revisiones de privilegios de acceso a los diferentes sistemas de información por parte de los usuarios manteniendo los registros de las revisiones y hallazgos.
		9.2.6 Remoción o ajuste de derechos de acceso	Aplicado	Se hace bajo petición del responsable directo del usuario.
A.9.3	**Responsabilidades de los usuarios:** Hacer que los usuarios respondan por la salvaguarda de su información de autentificación	**9.3.1** Uso de información de autentificación secreta	Aplicar	Buenas prácticas de seguridad serían necesario para proteger el acceso a la información.
A.9.4	**Control de acceso a sistemas y aplicaciones:** Prevenir el acceso no autorizado a los sistemas y aplicaciones	**9.4.1** Restricción de acceso a la información	Aplicado	Los usuarios acceden únicamente a la información que requieren para desarrollar su trabajo.
		9.4.2 Procedimientos de ingreso seguro	Aplicado	Se requiere usuario y contraseña para el acceso a sistemas y aplicaciones.
		9.4.3 Sistema de gestión de contraseñas	Aplicar	Se reforzará la gestión de contraseñas implantada actualmente al identificarse riesgos en este sentido.
		9.4.4 Uso de programas utilitarios privilegiados	Aplicar	Controlar el uso de utilidades software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas para evitar incidentes de seguridad.
		9.4.5 Control de acceso de código fuente de los programas	Aplicar	Se reforzará el control de acceso al código fuente dado los riesgos identificados.
A.10	**CRIPTOGRAFÍA**			
A.10.1	**Controles criptográficos:** Asegurar el uso apropiado y efectivo de la criptografía para proteger la información	**10.1.1** Política sobre el uso de controles criptográficos	Aplicar	Establecer políticas para determinar el uso de técnicas criptográficas que ayuden a proteger la información de la organización.
		10.1.2 Gestión de claves	No Aplicar	No se gestionan claves secretas en la entidad.
A.11	**SEGURIDAD FÍSICA Y AMBIENTAL**			
A.11.1	**Áreas seguras:** impedir acceso físico no autorizado, daño e interferencia a la información y a las instalaciones de procesamiento de la información de la organización	**11.1.1** Perímetro de seguridad física	Aplicar	Exigido por la NTP ISO/IEC 27001:2014
		11.1.2 Controles de ingreso físico	Aplicar	Establecer controles para indicar las áreas accesibles por los visitantes, implementar control de acceso restringido y controlar el acceso.
		11.1.3 Asegurar oficinas, áreas e instalaciones	Aplicar	Exigido por la NTP ISO/IEC 27001:2014
		11.1.4 Protección contra amenazas externas y ambientales	Aplicar	No se cuenta con lo básico para hacer frente a amenazas ambientales externas y ambientales (equipo contra incendios, otros)
		11.1.5 Trabajo en áreas seguras	Aplicado	El servidor se encuentra en una oficina dentro de la misma entidad, pero se debe mejorar este control supervisando lo que se realiza en el servidor.
		11.1.6 Áreas de despacho y carga	Aplicado	Se establece una zona en recepción para carga y descarga.

A.11.2	**Equipos:** Prevenir la pérdida, daño, robo o compromiso de activos o interrupción de las operaciones de la organización	**11.2.1** Emplazamiento y protección de los equipos	Aplicado	Los equipos están en áreas controladas por personal autorizado.
		11.2.2 Servicios de suministro	Aplicado	Se dispone de un sistema de alimentación ininterrumpida.
		11.2.3 Seguridad del cableado	Aplicado	La instalación del cableado es segura.
		11.2.4 Mantenimiento de equipos	Aplicado	Existe personal de soporte técnico que da mantenimiento a los equipos. Mejorar el control manteniendo registros de todas las fallas sospechadas y reales, y todo mantenimiento preventivo y correctivo
		11.2.5 Remoción de activos	No aplicar	No salen equipos con información sensible de la entidad.
		11.2.6 Seguridad de equipos y activos fuera de las instalaciones	Aplicar	Controlar el uso de los equipos que se prestan y supervisar el estado de salida y retorno.
		11.2.7 Disposición y reutilización segura de equipos	Aplicado	Los equipos descartados se formatean e instalan de nuevo cuando se ponen de nuevo en servicio. Mejorar el control analizando la información confidencial que maneja el equipo y decidir si es necesario aplicar otra técnica que haga imposible recuperar esa información.
		11.2.8 Equipos de usuarios desatendidos	Aplicado	Los equipos cuentan con una clave de protección en caso estén desatendidos. Mejorar el control para el equipo de secretaría.
		11.2.9 Política de escritorio limpio y pantalla limpia	Aplicar	Se evitará así filtraciones de información indeseadas.
A.12	**SEGURIDAD DE LAS OPERACIONES**			
A.12.1	**Procedimientos y responsabilidades operativas:** asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras.	**12.1.1** Procedimientos operativos documentados	Aplicar	Será necesario documentar algunos de los procedimientos de seguridad, especialmente los de requisito más técnico (copias de seguridad, mantenimiento del equipo, manejo de medios, manejo del correo y seguridad, recuperación del sistema)
		12.1.2 Gestión del cambio	Aplicar	Los cambios se realizarán de manera controlada.
		12.1.3 Gestión de la capacidad	Aplicar	Se implementará, por ejemplo, una línea dedicada para los sistemas más críticos.
		12.1.4 Separación de los entornos de desarrollo, pruebas y operaciones	Aplicar	Los entornos de desarrollo, prueba y operación serán separados para reducir los riesgos de acceso no-autorizado o cambios en los sistemas operacionales.
A.12.2	Protección contra códigos maliciosos	**12.2.1** Controles contra códigos maliciosos	Aplicado	Se dispone de antivirus, aunque es necesario complementar este control con capacitación y concienciación de los usuarios.
A.12.3	**Respaldo:** Proteger contra la pérdida de datos	**12.3.1** Respaldo de la información	Aplicado	Se realizan copias de seguridad. Mejorar este control estableciendo periodos de prueba de recuperación de Backup, almacenamiento fuera de daños y desastres del local principal.
A.12.4	**Registros y monitoreos:** Registrar eventos y generar evidencias	**12.4.1** Registro de eventos	Aplicar	El registro de los operadores y el registro de fallas deberían ser usados para garantizar la identificación de los problemas del sistema de información.
		12.4.2 Protección de información de registros	Aplicar	Es necesario proteger contra posibles alteraciones y accesos no autorizados la información de los registros.
		12.4.3 Registro del administrador y del operador	Aplicar	Necesario para revisar y proteger los registros asociados a las actividades del administrador y del operador del sistema.
		12.4.4 Sincronización del reloj	Aplicar	Para evitar fallas en las comunicaciones y asegurar la integridad de registro de eventos.
A.12.5	**Control de software operacional:** Asegurar la integridad de los sistemas operacionales	**12.5.1** Instalación de software en sistemas operacionales	Aplicado	Se realizan instalaciones con el conocimiento de la oficina de Estadística de la DIRESA y con personal autorizado.
A.12.6	**Gestión de vulnerabilidad técnica:** Prevenir la explotación de vulnerabilidades técnicas	**16.6.1** Gestión de vulnerabilidades técnicas	Aplicado	Se instalan las actualizaciones de seguridad en los puestos de los usuarios y el servidor.
		16.6.2 Restricción sobre la instalación de software	Aplicar	Restringir los permisos de instalación a los usuarios.
A.12.7	**Consideraciones para la auditoría de sistemas de información:** Minimizar el impacto de las actividades de auditoría en sistemas operacionales	**12.7.1** Controles de auditoría de sistemas de información	Aplicar	Planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio.
A.13	**SEGURIDAD DE LAS COMUNICACIONES**			
A.13.1	Gestión de seguridad de la red	**13.1.1** Controles en la red	Aplicado	Se dispone de un firewall.
		13.1.2 Seguridad de servicios de red	Aplicar	Verificar los acuerdos de nivel de servicio con el proveedor y que estén estipulados en el contrato
		13.1.3 Segregación en redes	Aplicar	Las redes se encontrarán separadas para prevenir accesos no autorizados.

A.13.2	**Transferencia de información:** Mantener la seguridad de la información transferida dentro de una organización y cualquier entidad externa	**13.2.1** Políticas y procedimientos de transferencia de la información	Aplicar	Se realizará configuraciones para proteger la transferencia de información por las redes.
		13.2.2 Acuerdo sobre transferencia de información	Aplicado	Se firman acuerdos de intercambio con los proveedores.
		13.2.3 Mensajes electrónicos	Aplicado	Los sistemas antivirus, el firewall disponen de medidas de protección.
		13.2.4 Acuerdos de confidencialidad o no divulgación	Aplicado	Los contratos con proveedores y personal incluyen acuerdos de confidencialidad.
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**			
A.14.1	**Requisitos de seguridad de los SI**: Garantizar que la seguridad de información es una parte integral de los SI a través del ciclo de vida completo.	**14.1.1** Análisis y especificación de requisitos de seguridad de la información	Aplicar	Se exigirá a los analistas programadores y documentar el establecimiento de medidas de seguridad en el desarrollo de software.
		14.1.2 Aseguramiento de servicios de aplicaciones sobre redes públicas	Aplicar	Utilizar sistema de cifrado para la información, exigir al proveedor donde se aloja la PW acuerdos de seguridad. Nivel de confianza de la dirección.
		14.1.3 Protección de transacciones en servicios de aplicación	Aplicar	Realizar informe sobre el nivel global de confianza de la dirección, basado en el análisis de los últimos test de penetración, incidentes actuales o recientes, vulnerabilidades actuales conocidas para prevenir ataques web.
A.14.2	**Seguridad en los procesos de desarrollo y soporte:** Garantizar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información	**14.2.1** Política de desarrollo seguro	Aplicar	Se establecerá una política para contemplar los requisitos de seguridad al desarrollar SI.
		14.2.2 Procedimiento de control de cambio del sistema	Aplicado	Cada cambio debe ser controlado y documentado.
		14.2.3 Revisión técnica de aplicaciones después de cambios a la plataforma operativa	Aplicado	Se realizan pruebas al realizar cambios en los SI para comprobar que funcionen correctamente.
		14.2.4 Restricciones sobre cambios a los paquetes de software	No Aplicar	No se realizan cambios en los paquetes de software de terceros.
		14.2.5 Principios de ingeniería de sistemas seguros	Aplicar	Se deberá establecer, documentar, mantener y aplicar los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información.
		14.2.6 Ambiente de desarrollo seguro	Aplicar	Proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema.
		14.2.7 Desarrollo contratado externamente	No Aplicar	No se contrata desarrollo externo
		14.2.8 Pruebas de seguridad del sistema	Aplicar	Realizar pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo.
		14.2.9 Pruebas de aceptación del sistema	Aplicado	Realizar pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo.
	Datos de prueba: Asegurar la protección de datos utilizados para las pruebas	**14.3.1** Protección de datos de prueba	Aplicar	Seleccionar cuidadosamente, proteger y controlar los datos de prueba. Tener autorización de uso de datos reales.
A.15	**RELACIONES CON PROVEEDORES**			
A.15.1	**Seguridad de la información en las relaciones con los proveedores:** Asegurar protección a los activos de la organización que son accesibles por los proveedores.	**15.1.1** Política de seguridad de la información para las relaciones con los proveedores	No Aplicar	Se considera que el coste de implementación de este control superaría el beneficio que se obtendría.
		15.1.2 Abordar la seguridad dentro de los acuerdos con los proveedores	Aplicado	En los contratos con los proveedores se incluyen acuerdos de confidencialidad. Verificar otros temas relacionados a la seguridad.
		15.1.3 Cadena de suministro de tecnología de información y comunicaciones	Aplicar	Los acuerdos con los proveedores deberían incluir los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones.
A.15.2	Gestión de entrega de servicios del proveedor	**15.2.1** Monitoreo y revisión de servicios de los proveedores	Aplicado	Monitorea y revisa la prestación de servicios de tercero para saber si ¿Lo que se recibe vale lo que se paga por ello?
		15.2.2 Gestión de cambios a los servicios de proveedores	Aplicado	Se firman nuevos contratos con los proveedores ante un cambio en las condiciones, revisar implicaciones en temas de seguridad.
A.16	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**			
A.16.1	**Gestión de incidentes de seguridad de la información y mejoras:** Asegurar un enfoque	**16.1.1** Responsabilidades y procedimientos	Aplicar	Necesario para implicar al personal en la gestión de incidencias.

	consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y debilidades	**16.1.2** Reporte de eventos de seguridad de la información	Aplicado	La entidad genera un procedimiento para gestionar adecuadamente cada uno de los eventos de SI reportados por el personal o detectados por cada uno.
		16.1.3 Reporte de debilidades de seguridad de la información	Aplicar	La entidad deberá capacitar adecuadamente a todo el personal para que sea capaz de detectar debilidades en el SGSI y puedan reportarlas adecuadamente,
		16.1.4 Evaluación y decisión sobre eventos de seguridad de la información.	Aplicar	Es necesario identificar a una persona responsable de evaluar las incidencias y determine las acciones que se deben tomar.
		16.1.5 Respuestas a incidentes de seguridad de la información	Aplicar	Para solucionar las incidencias y documentarlos.
		16.1.6 Aprendizaje de los incidentes de seguridad de la información	Aplicar	Tener para esto un registro de incidencias y revisarlas periódicamente para prevenir incidencias.
		16.1.7 Recolección de evidencias	Aplicar	Mantener un registro de incidencias y de las operaciones realizadas.
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO**			
A.17.1	**Continuidad de seguridad de la información:** la seguridad de la información debe estar embebida en los sistemas de gestión de continuidad del negocio.	**17.1.1** planificación de continuidad de seguridad de la información	Aplicar	Necesario para identificar puntos débiles en cuanto a la continuidad de las operaciones.
		17.1.2 implementación de continuidad de seguridad de la información	Aplicar	Necesario para garantizar la continuidad de los servicios.
		17.1.3 verificación, revisión y evaluación de continuidad de seguridad de la información	Aplicar	Necesario para verificar la adecuación a los planes y de mejora continua.
	Redundancias: Asegurar la disponibilidad de las instalaciones y procesamiento de la información	**17.2.1** Instalaciones de procesamiento de la información	No Aplicar	Por el momento se considera que no es necesario debido a que el coste supera los beneficios obtenidos.
A.18	**CUMPLIMIENTO**			
A.18.1	**Cumplimiento con requisitos legales y contractuales:** Evitar infracciones de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad.	**18.1.1** Identificación de requisitos contractuales y de legislación aplicables	Aplicar	Se debe identificar las leyes aplicables a la organización
		18.1.2 Derechos de propiedad intelectual	Aplicado	Se contempla como propiedad de la DISA V.C. los desarrollos realizados en la entidad. Disponer de los derechos de propiedad de software originales.
A.18.2	**Revisiones de seguridad de la información:** Asegurar que la seguridad de la información está implementada y es operada de acuerdo con las políticas y procedimientos organizativos.	**18.1.3** Protección de registros	Aplicar	Se deben proteger los registros mediante medidas de seguridad física y lógica. Se debe establecer guías y procedimiento que especifiquen por cuanto tiempo la organización está dispuesta a almacenar la información.
		18.1.4 Privacidad y protección de datos personales	Aplicar	Se debe establecer un procedimiento para el adecuado manejo de la información, personal almacenada dentro de la organización, en conformidad con la ley de protección de datos personales.
		18.1.5 Regulación de controles criptográficos	Aplicar	A nivel nacional existe una directiva que indica que la información sensible debe ser encriptado para asegurar su integridad y confidencialidad, esta directiva es la 007-95-INEI-SJI. (Recomendaciones Técnicas para la Seguridad e Integridad de la Información que se procesa en la Administración Pública).
		18.2.1 Revisión independiente de la seguridad de la información	Aplicar	Se debe revisar el enfoque de la organización para la implementación (los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información) y gestión de la seguridad de la información, planificar las revisiones.
		18.2.2 Cumplimiento de políticas y normas de seguridad	Aplicar	En las auditorias se verificará el cumplimiento de políticas, procedimientos y normas.
		18.2.3 Revisión del cumplimiento técnico	Aplicar	Establecer un plan de revisión de los SI y verificar si cumplen con las políticas y normas de seguridad dispuesta por la organización.