UNIVERSIDAD NACIONAL DEL SANTA

FACULTAD DE INGENIERIA

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS E INFORMATICA

Modelo de seguridad informática basada en prospectiva para mejorar la protección de la red informática de la Sunat – Lima.

TESIS PARA OBTENER EL TITULO PROFESIONAL DE INGENIERO DE SISTEMAS E INFORMATICA

AUTORES:

Bach. Bermudez Silva Allan Eduardo
Bach. Lopez Mendoza Juan Eduardo

ASESOR:

Mg. Carlos Alfredo Gil Narvaez

Nuevo Chimbote – Perú
2022-08-22

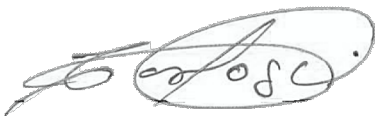
UNIVERSIDAD NACIONAL DEL SANTA
FACULTAD DE INGENIERIA

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS E INFORMÁTICA

“Modelo de seguridad informática basada en prospectiva para mejorar la protección de la red informática de la Sunat - Lima”.

TESIS PARA OBTENER EL TITULO PROFESIONAL DE INGENIERO DE SISTEMAS E INFORMATICA

Revisada y aprobada por:



Mg. Carlos Alfredo Gil Narvaez
DNI: 32970648
Cod ORCID: 0000-0003-0137-9545
Asesor

UNIVERSIDAD NACIONAL DEL SANTA
FACULTAD DE INGENIERIA

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS E INFORMÁTICA

“Modelo de seguridad informática basada en prospectiva para mejorar la protección de la red informática de la Sunat - Lima”.

TESIS PARA OBTENER EL TITULO PROFESIONAL DE INGENIERO DE SISTEMAS E INFORMATICA

Revisada y aprobada para sustentar ante el siguiente jurado:

Dr. Carlos Guerra Cordero
DNI: 32739372
Cod ORCID: 0000-0002-5958-4931
Presidente

Dr. Guillermo Edward Gil Albarran
DNI: 32960958
Cod ORCID: 0000-0003-3782-6765
Secretario

Mg. Carlos Alfredo Gil Narvaez
DNI: 32970648
Cod ORCID: 0000-0003-0137-9545
Integrante

FACULTAD DE INGENIERIA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

ACTA DE EVALUACIÓN PARA SUSTENTACIÓN DE TESIS

En el Campus Universitario de la Universidad Nacional del Santa, siendo las 6:00 pm. del día lunes 22 de agosto de 2022, en el Aula S1 del Pabellón nuevo de la EPISI, en atención a la Resolución Decanal N° 471-2022-UNS-FI de Declaración de Expedito de fecha 18.08.2022; se llevó a cabo la instalación del jurado Evaluador, designado mediante Resolución N° 241 – 2022 -UNS- CFI de fecha 17.06.2022, integrado por el **DR. CARLOS GUERRA CORDERO (Presidente), DR. GUILLERMO EDWARD GIL ALBARRÁN (Secretario), MS. CARLOS ALFREDO GIL NARVÁEZ (Integrante),** para dar inicio a la sustentación del Informe Final de Tesis, cuyo título es: **"MODELO DE SEGURIDAD INFORMÁTICA BASADA EN PROSPECTIVA PARA MEJORAR LA PROTECCIÓN DE LA RED INFORMÁTICA DE LA SUNAT - LIMA"** perteneciente al bachiller: **BERMUDEZ SILVA ALLAN EDUARDO** con código de matrícula **N° 0201214042,** tiene como **ASESOR** al **MS. Carlos Alfredo Gil Narváez,** según T/R.D. N° 467 -2021-UNS-FI de fecha 31.08.2021.

Terminada la sustentación, el tesista respondió a las preguntas formuladas por los miembros del Jurado Evaluador y el público presente.

El Jurado después de deliberar sobre aspectos relacionados con el trabajo, contenido y sustentación del mismo y con las sugerencias pertinentes y en concordancia con el artículo 73º y 103º del Reglamento General de Grados y Títulos, vigente de la Universidad Nacional del Santa; considera la siguiente nota final de Evaluación:

BACHILLER	CALIFICACIÓN	CONDICIÓN
ALLAN EDUARDO BERMUDEZ SILVA	17	muy buena

Siendo la 6: 30 pm. se dio por terminado el Acto de Sustentación y en señal de conformidad, firma el Jurado la presente Acta.

Nuevo Chimbote, 22 de agosto de 2022

DR. CARLOS GUERRA CORDERO
PRESIDENTE

DR. GUILLERMO EDWARD GIL ALBARRÁN
SECRETARIO

MS. CARLOS ALFREDO GIL NARVÁEZ
INTEGRANTE

UNS
UNIVERSIDAD NACIONAL DEL SANTA

FACULTAD DE INGENIERIA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

ACTA DE EVALUACIÓN PARA SUSTENTACIÓN DE TESIS

En el Campus Universitario de la Universidad Nacional del Santa, siendo las 6:00 pm. del día lunes 22 de agosto de 2022, en el Aula S1 del Pabellón nuevo de la EPISI, en atención a la Resolución Decanal N° 471-2022-UNS-FI de Declaración de Expedito de fecha 18.08.2022; se llevó a cabo la instalación del jurado Evaluador, designado mediante Resolución N° 241 – 2022 -UNS- CFI de fecha 17.06.2022, integrado por el **DR. CARLOS GUERRA CORDERO (Presidente), DR. GUILLERMO EDWARD GIL ALBARRÁN (Secretario), MS. CARLOS ALFREDO GIL NARVÁEZ (Integrante),** para dar inicio a la sustentación del Informe Final de Tesis, cuyo título es: **"MODELO DE SEGURIDAD INFORMÁTICA BASADA EN PROSPECTIVA PARA MEJORAR LA PROTECCIÓN DE LA RED INFORMÁTICA DE LA SUNAT - LIMA"** perteneciente al bachiller: **LOPEZ MENDOZA JUAN EDUARDO** con código de matrícula **N° 0201214053,** tiene como **ASESOR** al **MS. Carlos Alfredo Gil Narváez,** según T/R.D. N° 467 -2021-UNS-FI de fecha 31.08.2021.

Terminada la sustentación, el tesista respondió a las preguntas formuladas por los miembros del Jurado Evaluador y el público presente.

El Jurado después de deliberar sobre aspectos relacionados con el trabajo, contenido y sustentación del mismo y con las sugerencias pertinentes y en concordancia con el artículo 73º y 103º del Reglamento General de Grados y Títulos, vigente de la Universidad Nacional del Santa; considera la siguiente nota final de Evaluación:

BACHILLER	CALIFICACIÓN	CONDICIÓN
JUAN EDUARDO LOPEZ MENDOZA	16	bueno

Siendo la 6: 30 pm. se dio por terminado el Acto de Sustentación y en señal de conformidad, firma el Jurado la presente Acta.

Nuevo Chimbote, 22 de agosto de 2022

DR. CARLOS GUERRA CORDERO
PRESIDENTE

DR. GUILLERMO EDWARD GIL ALBARRÁN
SECRETARIO

MS. CARLOS ALFREDO GIL NARVÁEZ
INTEGRANTE

DEDICATORIA

A nuestros padres, quienes siempre nos brindaron su apoyo en el desarrollo académico en la universidad y en nuestros objetivos profesionales.

A los docentes que nos inculcaron los conocimientos necesarios para nuestro desenvolvimiento profesional.

AGRADECIMIENTO

A nuestros compañeros de trabajo y amigos que nos brindaron

información para el proyecto de tesis.

INDICE

INDICE DE FIGURAS

RESUMEN

La Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT) sede Lima, es la ubicación central de toda la organización a nivel nacional, a donde llega toda la información de los contribuyentes, existiendo siempre riesgos de seguridad tanto por amenazas internas como externas, pues cada usuario al ingresar a la red informática puede hacer uso indebido de los recursos.

La red informática es el principal medio a través de la cual se transporta los datos, y ayudan a lograr los objetivos estratégicos de la institución, y ante posibles escenarios, tanto optimistas, normales y pesimistas, donde se debe tener en cuenta planes de contingencias ante determinados problemas de seguridad, se propone realizar un Modelo de Seguridad Informática basada en prospectiva.

PALABRAS CLAVE:
Red informática, prospectiva, modelo de seguridad informática, gestión de seguridad informática.

ABSTRACT

The National Superintendence of Customs and Tax Administration (SUNAT) in Lima, is the central location of the entire organization at the national level, where all taxpayer information arrives, always existing security risks due to both internal and external threats, since each user when entering to the computer network may misuse resources.

The computer network is the main means through which the data is transported, and helps to achieve the strategic objectives of the institution, and in the face of possible scenarios, both optimistic, normal and pessimistic, where contingency plans must be taken into account before certain security problems, it is proposed to make an Information Security Model based on prospective.

KEYWORDS:
Computer network, foresight, computer security model, information security management.

PRESENTACIÓN

SEÑORES MIEMBROS DEL JURADO EVALUADOR

UNIVERSIDAD NACIONAL DEL SANTA

De nuestra mayor consideración:

Siguiendo con el Reglamento de Grados y Títulos y de conformidad a la Ley Universitaria Nº 30220, para optar el Título de INGENIERO DE SISTEMAS E INFORMATICA en la Escuela Profesional de Ingeniería de Sistemas e Informática, ponemos a disposición la presente tesis titulada "**MODELO DE SEGURIDAD INFORMATICA BASADA EN PROSPECTIVA PARA MEJORAR LA PROTECCION DE LA RED INFORMATICA DE LA SUNAT - LIMA**".

Esperando que la presente cubra las expectativas y características solicitadas por las leyes universitarias vigentes de la Universidad, ponemos a su disposición señores Miembros del Jurado este informe para su revisión y Evaluación.

Atentamente,

Los Autores

INTRODUCCIÓN

La Superintendencia Nacional de Aduanas y Administración Tributaria (SUNAT), es la encargada de gestionar la información tributaria de los contribuyentes a nivel nacional, información que viaja a través de la red informática de la institución, desde las diferentes sedes hacia la sede central en Lima, así como de los usuarios en forma directa a través de los servicios web y móviles; por lo cual se necesita tener un modelo de seguridad informática acorde a los objetivos estratégicos institucionales.

Un Modelo de Seguridad Informática basada en prospectiva permite gestionar los diferentes escenarios futuros de la institución de una manera segura, para mantener la integridad, autenticidad y disponibilidad de la información, que son los pilares de la seguridad informática.

El informe está dividido en capítulos estructurados de la siguiente manera:

CAPITULO I - LA INSTITUCION. - En este capítulo se realiza una descripción de la Superintendencia Nacional de Administración Tributaria.

CAPITULO II - PLAN DE INVESTIGACIÓN. – Aquí se determina el problema, los antecedentes del mismo, se enuncia hipótesis, el diseño de la investigación, los objetivos generales y específicos.

CAPITULO III - MARCO TEÓRICO. - En este capítulo se abarca los conceptos básicos involucrados en el desarrollo de la Tesis.

CAPITULO IV - MATERIALES Y METODOS. - En este capítulo se detallan los materiales y métodos utilizados en la tesis.

CAPITULO V - RESULTADOS. - En este capítulo se muestra los resultados de la tesis.

CAPITULO VI - DISCUSION. - Se realiza la contrastación de la Hipótesis.

CONCLUSIONES. - Se mencionan las conclusiones obtenidas del desarrollo del estudio.

RECOMENDACIONES. -En esta parte se dan las recomendaciones propuestas del estudio.

CAPÍTULO I

LA INSTITUCION

1.1 ANTECEDENTES DE LA INSTITUCION

Según (Zambrano Orosco, 2019): "La Superintendencia Nacional de Aduanas y de Administración Tributaria – SUNAT, de acuerdo a su Ley de creación N° 24829, Ley General aprobada por Decreto Legislativo Nº 501 y la Ley 29816 de Fortalecimiento de la SUNAT, es un organismo técnico especializado, adscrito al Ministerio de Economía y Finanzas, cuenta con personería jurídica de derecho público, con patrimonio propio y goza de autonomía funcional, técnica, económica, financiera, presupuestal y administrativa que, en virtud a lo dispuesto por el Decreto Supremo N° 061-2002-PCM, expedido al amparo de lo establecido en el numeral 13.1 del artículo 13° de la Ley N° 27658, ha absorbido a la Superintendencia Nacional de Aduanas, asumiendo las funciones, facultades y atribuciones que por ley, correspondían a esta entidad."

Tiene domicilio legal y sede principal en la ciudad de Lima, pudiendo establecer dependencias en cualquier lugar del territorio nacional.[1]

[1] https://www.sunat.gob.pe/institucional/quienessomos/index.html

Figura 1 – Ubicación Geográfica en Lima
Fuente: Google Map

1.2 FINALIDAD

Según (Sunat, 2022), "La SUNAT tiene como finalidad primordial administrar los tributos del gobierno nacional y los conceptos tributarios y no tributarios que se le encarguen por Ley o de acuerdo a los convenios interinstitucionales que se celebren, proporcionando los recursos requeridos para la solvencia fiscal y la estabilidad macroeconómica; asegurando la correcta aplicación de la normatividad que regula la materia y combatiendo los delitos tributarios y aduaneros conforme a sus atribuciones.

También tiene como finalidad la implementación, la inspección y el control del cumplimiento de la política aduanera en el territorio nacional y el tráfico internacional de mercancías, personas y medios de transporte, facilitando las actividades aduaneras de comercio exterior y asegurando la correcta aplicación de los tratados y convenios internacionales y demás normas que rigen la materia.

Asimismo, le corresponde participar en el combate contra la minería ilegal así como del narcotráfico, a través del control y fiscalización del ingreso, permanencia,

transporte o traslado y salida de los productos de la actividad minera, de insumos químicos y maquinarias que puedan ser utilizados en la minería ilegal, así como del control y fiscalización de los insumos químicos, productos y sus sub productos o derivados, maquinarias y equipos que puedan ser utilizados directa o indirectamente en la elaboración de drogas ilícitas; y otros fines que se establezcan mediante Ley.

Adicionalmente, debe proveer a los administrados los servicios que les faciliten el cumplimiento de sus obligaciones tributarias, aduaneras y otras vinculadas a las funciones que realiza la SUNAT, así como brindar servicios a la ciudadanía en general dentro del ámbito de su competencia."

(Establecido en el artículo 3° del Reglamento de Organización y Funciones de la SUNAT, aprobado por Resolución de Superintendencia N° 122-2014/SUNAT y modificatorias)

1.3 MISION

"Servir al país proporcionando los recursos necesarios para la sostenibilidad fiscal y la estabilidad macroeconómica, contribuyendo con el bien común, la competitividad y la protección de la sociedad, mediante la administración y el fomento de una tributación justa y un comercio exterior legítimo" (Sunat, 2022).

1.4 VISION

De acuerdo a Sunat (Superintendencia Nacional de Aduanas y de Administración Tributaria, 2022), establece como visión el "Convertirnos en la administración tributaria y aduanera más exitosa, moderna y respetada de la región.

- Exitosa, porque lograremos resultados similares a los de las administraciones de los países desarrollados.

- Moderna, porque incorporaremos en nuestros procesos las tecnologías más avanzadas y utilizaremos los enfoques modernos de gestión de riesgo y fomento del cumplimiento voluntario para enfrentar con éxito los desafíos.

Respetada por:

- El Estado: por mantener niveles bajos de evasión y de fraude en la tributación interna y el comercio exterior, y contribuir a financiar los programas sociales y el desarrollo del país.
- Los contribuyentes y usuarios de comercio exterior: porque aquellos que son cumplidores se sienten respetados; reciben todas las facilidades para el cumplimiento de sus obligaciones y tienen confianza en la capacidad de la institución de detectar y tratar los incumplimientos.
- Sus trabajadores: porque laboran en una institución con mística, modelo dentro del estado; orgullosos de pertenecer a la organización y comprometida con su misión.
- Sus trabajadores potenciales: porque es una institución atractiva para trabajar, que compite de igual a igual con las instituciones más atractivas del Estado y con las más respetadas empresas por los mejores egresados de las más prestigiosas instituciones educativas; y es capaz de atraer gente con experiencia que se destaque en el sector público o el privado.
- Otras administraciones: porque la consultan y la toman como referente."

1.5 PRINCIPIOS

De acuerdo a la página web de Sunat y sus documentos de gestión, (Sunat, 2022):

- "Autonomía

La SUNAT debe ejercer sus funciones aplicando sus propios criterios técnicos, preservando su independencia y estabilidad institucional.

- Honestidad

La actuación de la SUNAT y de sus miembros tiene que ser justa, recta, íntegra y de respeto a la verdad e implica la coherencia total entre el pensamiento, el discurso y la acción. Es la base en que se sustenta la SUNAT.

- Compromiso

Dado el carácter singular de la SUNAT como entidad que provee la mayor parte de los recursos al Estado y promueve la competitividad y la protección a la sociedad, la institución y sus miembros deben tener un fuerte compromiso con el bien común, basado en la justicia, respeto a los derechos humanos, y orientado a la búsqueda del progreso de nuestro país, el bienestar de todos los peruanos y a garantizar la igualdad de oportunidades.

Asimismo, el colaborador debe estar plenamente identificado con la institución, sus metas y tener predisposición para hacer más de lo esperado a efectos de lograr los objetivos. Debe desear pertenecer a la institución y estar orgulloso de ello.

- Profesionalismo

El capital humano de la SUNAT debe caracterizarse por su excelencia ética y técnica. Debe ser imparcial, objetivo y efectivo, en caso de conflicto de intereses debe preferir el interés público y abstenerse de participar en aquellas situaciones que pudieran poner en duda la transparencia de su proceder.

- Vocación de Servicio

La institución y sus miembros deben tener una permanente orientación a brindar un servicio de calidad que comprenda y satisfaga las necesidades de los contribuyentes, usuarios y operadores de comercio exterior, ciudadanos, así como

de los usuarios internos de la institución; utilizando eficientemente los recursos y optimizando la calidad de nuestros servicios.

- Trabajo en Equipo

  Debemos trabajar en un ambiente de colaboración en el que se comparte información y conocimiento, privilegiando los resultados colectivos por sobre los individuales.

- Flexibilidad

  Supone cuestionarse permanentemente cómo se pueden hacer mejor las cosas, tener disposición y capacidad para buscar nuevas alternativas; y, además, tener mente abierta y habilidad para adaptarse a lo nuevo".

1.6 FUNCIONES Y ATRIBUCIONES

Son funciones y atribuciones de la SUNAT, según su portal web (Sunat, 2022):

- "Administrar los tributos internos del Gobierno Nacional, así como los conceptos tributarios y no tributarios cuya administración o recaudación se le encargue por Ley o Convenio Interinstitucional.
- Proponer al Ministerio de Economía y Finanzas la reglamentación de las normas tributarias, aduaneras y otras de su competencia.
- Expedir, dentro del ámbito de su competencia, disposiciones en materia tributaria y aduanera, estableciendo obligaciones de los contribuyentes, responsables y/o usuarios del servicio aduanero, disponer medidas que conduzcan a la simplificación de los trámites correspondientes a los regímenes aduaneros, así como normar los procedimientos que se deriven de éstos.

- Dictar normas en materia de organización y gestión interna en el ámbito de su competencia.
- Sistematizar y ordenar la legislación e información estadística de comercio exterior, a fin de brindar información general sobre la materia conforme a Ley, así como la vinculada con los tributos internos y aduaneros que administra.
- Celebrar acuerdos y convenios de cooperación técnica y administrativa en materia de su competencia.
- Promover, coordinar y ejecutar actividades de cooperación técnica, de investigación, de capacitación y perfeccionamiento en materia tributaria y aduanera, en el país o en el extranjero.
- Otorgar el aplazamiento y/o fraccionamiento para el pago de la deuda tributaria o aduanera, de acuerdo con la Ley.
- Solicitar, y de ser el caso ejecutar, medidas destinadas a cautelar la percepción de los tributos que administra y disponer la suspensión de las mismas cuando corresponda, de acuerdo a Ley.
- Controlar y fiscalizar el tráfico de mercancías, cualquiera sea su origen y naturaleza a nivel nacional.
- Inspeccionar, fiscalizar y controlar las agencias de aduanas, despachadores oficiales, depósitos autorizados, almacenes fiscales, terminales de almacenamiento, consignatarios y medios de transporte utilizados en el tráfico internacional de personas, mercancías u otros.
- Prevenir, perseguir y denunciar al contrabando, la defraudación de rentas de aduanas, la defraudación tributaria y el tráfico ilícito de mercancías, así como aplicar medidas en resguardo del interés fiscal.

- Desarrollar y aplicar sistemas de verificación y control de calidad, cantidad, especie, clase y valor de las mercancías, excepto las que estén en tránsito y transbordo, a efectos de determinar su clasificación en la nomenclatura arancelaria y los derechos que le son aplicables.
- Desarrollar y administrar los sistemas de análisis y fiscalización de los valores declarados por los usuarios del servicio aduanero.
- Resolver asuntos contenciosos y no contenciosos y, en este sentido, resolver en vía administrativa los recursos interpuestos por los contribuyentes o responsables; elevar los recursos de apelación y dar cumplimiento a las Resoluciones del Tribunal Fiscal, y en su caso a las del Poder Judicial.
- Sancionar a quienes contravengan las disposiciones legales y administrativas de carácter tributario y aduanero, con arreglo a Ley.
- Ejercer los actos y medidas de coerción necesarios para el cobro de deudas por los conceptos que administra.
- Mantener en custodia las mercancías y bienes incautados, embargados o comisados, efectuando el remate de los mismos cuando ello proceda en el ejercicio de sus funciones.
- Adjudicar mercancías de acuerdo a Ley.
- Desarrollar programas de información, divulgación y capacitación en materia tributaria y aduanera.
- Editar, reproducir y publicar oficialmente el Arancel Nacional de Aduanas actualizado, los tratados y convenios de carácter aduanero, así como las normas y procedimientos aduaneros para su utilización general.

- Determinar la correcta aplicación y recaudación de los tributos que administra y de otros cuya recaudación se le encargue, así como de los derechos que cobren por los servicios que prestan, de acuerdo a Ley.
- Liderar las iniciativas y proyectos relacionados con la cadena logística del comercio exterior cuando tengan uno o más componentes propios de las actividades aduaneras, coordinando con las entidades del sector público y privado que corresponda, las cuales deberán implementar los procesos armonizados que se establezcan
- Controlar y fiscalizar el ingreso, permanencia, transporte o traslado y salida de los bienes controlados que puedan ser utilizados en la minería ilegal, así como en la elaboración de drogas ilícitas.
- Ejercer las demás funciones que le señale la Ley.
- Sólo por Ley se pueden establecer funciones adicionales a la SUNAT. "

(Establecido en el artículo 4° del Reglamento de Organización y Funciones de la SUNAT, aprobado por Resolución de Superintendencia N° 122-2014/SUNAT y modificatorias)

1.7 TRIBUTOS QUE ADMINISTRA

Con el fin de lograr un sistema tributario eficiente, permanente y simple se dictó la Ley Marco del Sistema Tributario Nacional (Decreto Legislativo N° 771), vigente a partir del 1 de enero de 1994.

La Ley define los impuestos aplicables y define quién es el acreedor fiscal: el gobierno central, el gobierno local y una serie de organizaciones con objetivos específicos.

En aplicación del Decreto Supremo 061-2002-PCM, publicado el 12 de julio del 2002, se dispone la fusión por absorción de la Superintendencia Nacional de Aduanas (SUNAD) por la Superintendencia Nacional de Tributos Internos (SUNAT), pasando la SUNAT a ser el ente administrador de tributos internos y derechos arancelarios del Gobierno Central. El 22 de diciembre de 2011 se publicó la Ley Nº 29816 de Fortalecimiento de la SUNAT, estableciéndose la sustitución de la denominación de la Superintendencia Nacional de Administración Tributaria-SUNAT por Superintendencia Nacional de Aduanas y de Administración Tributaria – SUNAT.

Los principales tributos que administra la SUNAT son los siguientes:

- Impuesto General a las Ventas: Este es un impuesto que se aplica a la venta e importación de bienes, así como a la prestación de diversos servicios comerciales, cuando se celebra un contrato de construcción o cuando se vende por primera vez un inmueble.
- Impuesto a la Renta: Es aquél que se aplica a las rentas que provienen del capital, del trabajo o de la aplicación conjunta de ambos.
- Régimen Especial del Impuesto a la Renta: Es un régimen tributario dirigido a personas naturales y jurídicas, sucesiones indivisas y sociedades conyugales domiciliadas en el país que obtengan rentas de tercera categoría provenientes de las actividades de comercio y/o industria; y actividades de servicios.
- Nuevo Régimen Único Simplificado: Es un régimen simple que establece un pago único por el Impuesto a la Renta y el Impuesto General a las Ventas (incluyendo al Impuesto de Promoción Municipal). A él pueden acogerse únicamente las personas naturales o sucesiones indivisas, siempre que desarrollen actividades generadoras de rentas de tercera categoría (bodegas,

ferreterías, bazares, puestos de mercado, etc.) y cumplan los requisitos y condiciones establecidas.

- Impuesto Selectivo al Consumo: Es el impuesto que se aplica sólo a la producción o importación de determinados productos como cigarrillos, licores, cervezas, gaseosas, combustibles, etc.
- Impuesto Extraordinario para la Promoción y Desarrollo Turístico Nacional: Impuesto destinado a financiar las actividades y proyectos destinados a la promoción y desarrollo del turismo nacional.
- Impuesto Temporal a los Activos Netos: Impuesto aplicable a los generadores de renta de tercera categoría sujetos al régimen general del Impuesto a la Renta, sobre los Activos Netos al 31 de diciembre del año anterior. La obligación surge al 1 de enero de cada ejercicio y se paga desde el mes de abril de cada año.
- Impuesto a las Transacciones Financieras: El Impuesto grava algunas de las operaciones que se realizan a través de las empresas del Sistema Financiero. Creado por el D. Legislativo N° 939 y modificado por la Ley N° 28194. Vigente desde el 1° de marzo del 2004.
- Impuesto Especial a la Minería: Creada mediante Ley Nº 29789 publicada el 28 de setiembre de 2011, es un impuesto que grava la utilidad operativa obtenida por los sujetos de la actividad minera proveniente de las ventas de los recursos minerales metálicos. Dicha ley establece que el impuesto será recaudado y administrado por la SUNAT.
- Casinos y Tragamonedas: Impuestos que gravan la explotación de casinos y máquinas tragamonedas.

- Derechos Arancelarios o Ad Valorem, son los derechos aplicados al valor de las mercancías que ingresan al país, contenidas en el arancel de aduanas.
- Derechos Específicos, son los derechos fijos aplicados a las mercancías de acuerdo a cantidades específicas dispuestas por el Gobierno.
- Aportaciones al ESSALUD y a la ONP: Mediante la Ley N° 27334 se encarga a la SUNAT la administración de las citadas aportaciones, manteniéndose como acreedor tributario de las mismas el Seguro Social de Salud (ESSALUD) y la Oficina de Normalización Previsional (ONP).
- Regalías Mineras: Se trata de un concepto no tributario que grava las ventas de minerales metálicos y no metálicos. El artículo 7° de la Ley 28258 - Ley de Regalías Mineras, autoriza a la SUNAT para que realice, todas las funciones asociadas al pago de la regalía minera. Se modificó mediante la Ley Nº 29788 publicada el 28 de setiembre de 2011.
- Gravamen Especial a la Minería: Creado mediante la Ley Nº 29790, publicada el 28 de setiembre de 2011, está conformado por los pagos provenientes de la explotación de recursos naturales no renovables y que aplica a los sujetos de la actividad minera que hayan suscrito convenios con el Estado. El gravamen resulta de aplicar sobre la utilidad operativa trimestral de los sujetos de la actividad minera, la tasa efectiva correspondiente según lo señalado en la norma. Dicha ley, faculta a la SUNAT a ejercer todas las funciones asociadas al pago del Gravamen.

1.8 SEDES DE LA SUNAT

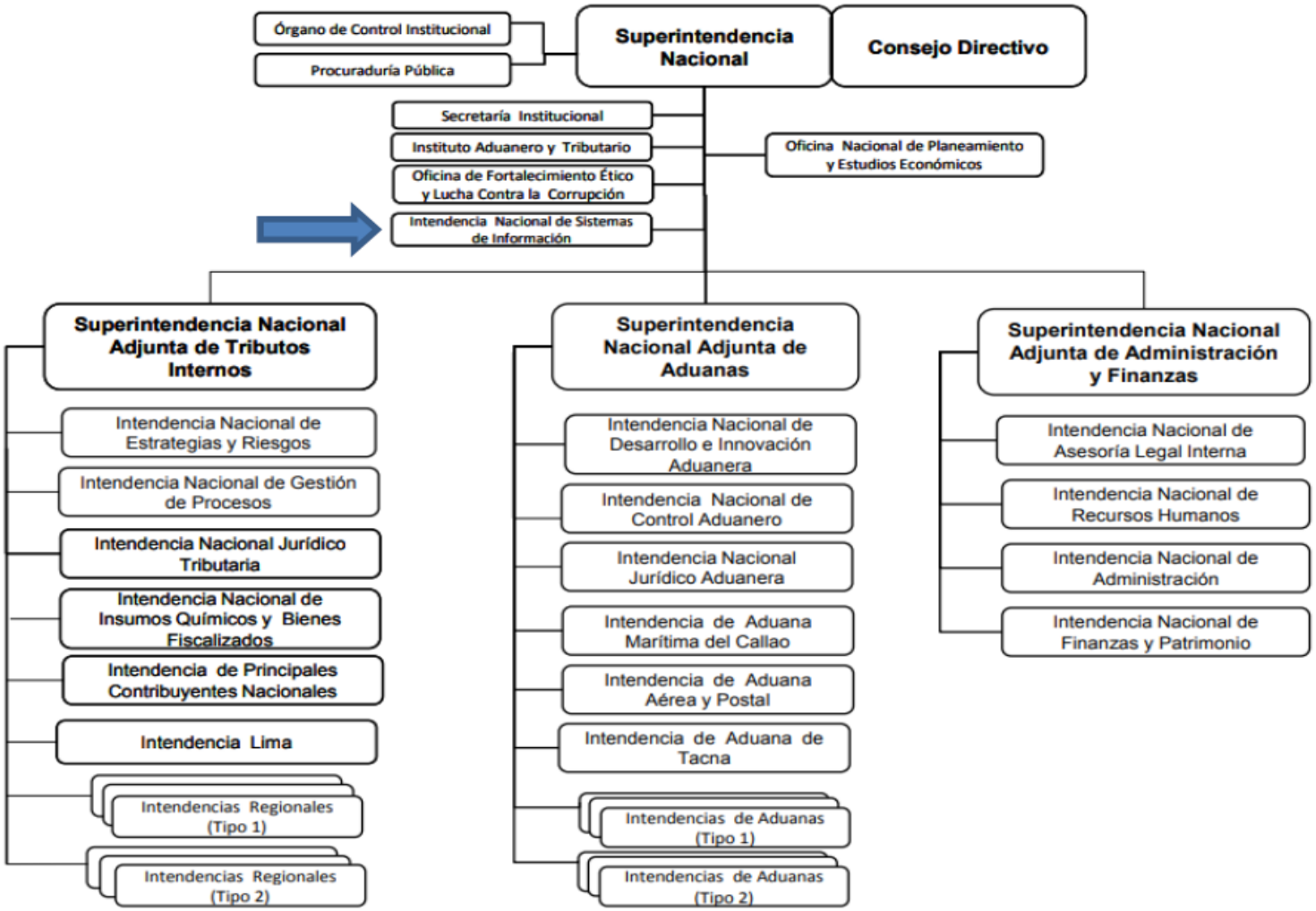
SUPERINTENDENCIA NACIONAL DE ADUANAS Y DE ADMINISTRACIÓN TRIBUTARIA	Lima	Av. Garcilaso de la Vega N° 1472 – Lima.

SUPERINTENDENCIA NACIONAL ADJUNTA DE ADUANAS
DEPENDENCIAS Y OFICINAS A NIVEL NACIONAL

DEPENDENCIA	PROVINCIA	DIRECCIÓN	CENTRAL TELEF - TELEFAX
SEDE CHUCUITO	Lima	Av. Gamarra Nº 680 – Chucuito - Callao	6343600
Intendencia Aduana de TUMBES	Tumbes	Complejo Fronterizo Zarumilla – Tumbes	072-523893
Intendencia Aduana de PAITA	Piura	Zona Industrial II, Mz. "X", Lote 2, Alt. Del Km. 2, Carretera Paita, Sullana	073-284730
Intendencia Aduana de CHICLAYO	Lambayeque	Av. José Leonardo Ortiz · 195 Chiclayo.	074-481000 Anexo 40802
Intendencia Aduana de SALAVERRY	La Libertad	Esquina Av. La Marina y Gamarra 200-210, Cercado de la Ciudad, Salaverry	044-481400
Intendencia Aduana de CHIMBOTE	Chimbote	Av. Francisco Bolognesi Cdra. 8 s/n. - Chimbote	043-483170 043-321961 telefax
Intendencia Aduana MARITIMA del Callao	Callao	Av. Guardia Chalaca 149, Callao – Costado de ENAPU	6343700
Intendencia Aduana Aérea y Postal	Callao	Sector D del Centro Aéreo Comercial sito en el cruce de las Av. Elmer Faucett y Tomás Valle	6121730
Agencia Postal de Lince	Callao	Teodoro Cardenas N° 265 Lince altura de la Cdra. 13 de la Av. Arequipa Lince (Dentro del local de Serpost)	6121730
Agencia Postal de Los Olivos	Callao	Av. Tomás Valle Cdra. 7 S/N - Jr. Antonio Cabos S/N espalda Cdra 7 Tomás Valle. (Dentro del local de Serpost)	6121730
Intendencia Aduana de PISCO	Ica	Av. Pérez Figueroa 112-118, Plaza de Armas de Pisco, Ica	056-581000
Intendencia Aduana de MOLLENDO	Mollendo	Av. Túpac Amaru N° 102 Urb. Miramar - Mollendo	054-381300
Sección de Técnica Aduanera	Arequipa	Av. Pizarro N° 160 A (Frente al Reservorio de Guardia Civil) - Paucarpata	054-381300
Intendencia Aduana de ILO	Ilo	Av. Venecia S/N Esquina Prolong. Calle Ilo - ILO	053-585030

Intendencia Aduana de TACNA	Tacna	Parque Industrial Mz. “A”, Lotes 05 y 06, Pocollay, Tacna	052-583850
Intendencia Aduana de IQUITOS	Iquitos	Av. 28 de Julio 810, Punchana - Maynas	065-251959 065-253435
Intendencia Aduana de PUCALLPA	Ucayali	Av. Salvador Allende 130, Pucallpa, Ucayali	061-571104 Telefax
Intendencia Aduana de CUSCO	Cusco	Calle Santa Teresa 366, Cusco	084-581120 084-581133 Telefax
Intendencia Aduana de PUERTO MALDONADO	Madre de Dios	Av. 26 de Diciembre 157, Puerto Maldonado – Madre de Dios	082-582290
Intendencia Aduana de PUNO	Puno	Av. Santa Rosa N° 475 esq. con Jr. Nazca N° 118 Barrio Santa Rosa	051 599400
Intendencia Aduana de TARAPOTO	San Martín	Jr. Ramírez Hurtado 301, Tarapoto, San Martín	042-523197
Agencia Aduanera LA TINA	Piura	Panamericana Norte s/n, Km. 1160, distrito de Suyo, Provincia de Ayabaca, Piura	073-837108 (Oficiales de Aduanas)

1.9 ESTRUCTURA ORGANICA DE LA SUNAT



CAPITULO II

PLAN DE INVESTIGACION

2.1 EL PROBLEMA

2.1.1 REALIDAD PROBLEMÁTICA

Las entidades públicas del estado cada día se encuentran transformando su infraestructura tecnologíca camino a la digitalización, lo que quiere decir que cada día dependen más de sus redes informáticas y de la seguridad en ellas implementadas.

Esto también sucede en la SUNAT, entidad donde todos los contribuyentes del estado registran su información comercial, ya sea sus ventas a través de boletas, facturas, recibos por honorarios o cualquier comprobante de pago; y esa información tiene que ser registrada en forma segura para no afectar la recaudación del país y a los mismos contribuyentes.

Las medidas de seguridad deben ser implementadas de la mejor manera teniendo en cuenta los diferentes riesgos que podrían darse en el presente y futuro.

Es por ello que el presente proyecto de investigación propone un "Modelo de Seguridad Informática basada en Prospectiva para mejorar la Protección de la Red Informática de la Sunat - Lima".

2.1.2 ANÁLISIS DEL PROBLEMA

La Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT) es la encargada de la recaudación tributaria en todo el país, teniendo sucursales en todas las principales ciudades de las regiones.

La economía nacional recibe los datos de recaudación a fin de planificar las políticas económicas necesarias, que se plasman anualmente a través del presupuesto de la república.

Por esto, los datos que circulan en su red informática, son reservados, los cuales no deben sufrir alteración ni destrucción, teniendo que proveerse mecanismos de seguridad adecuados, a fin de eliminar cualquier riesgo.

Es necesario que se proponga un sistema de seguridad en la red informática que puede tener en cuenta los riesgos que existieron en el pasado, que se dan en el presente y que posiblemente de puedan dar en el futuro.

En esta iniciativa se está utilizando la prospectiva, a fin de plantear escenarios adecuados para evaluar los riegos y tener la mejor propuesta de seguridad.

2.1.3 FORMULACIÓN DEL PROBLEMA

Después de Analizar la problemática que presenta la red informática de la Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT – Lima), hemos plasmado esta realidad en la siguiente pregunta.

¿De qué manera la Implementación de un Modelo de Seguridad Informática basada en Prospectiva mejorará la Protección de la Red Informática en la SUNAT - Lima?

2.1.4 ANTECEDENTES

Existen trabajos de investigación relacionados con el tema tales como:

a) TESIS DE PREGRADO: "SEGURIDAD EN INFORMATICA (AUDITORIA DE SISTEMAS)**"**[2]

Autor: LUIS DANIEL ALVAREZ BASALDUA

México, 2005

De acuerdo a Alvares Basaldúa (2005): "Los trascendentales cambios operados en el mundo moderno, caracterizado por su incesante desarrollo; la acelerada globalización de la economía, la acentuada dependencia que incorpora en alto volumen de información y los sistemas que la proveen; el aumento de la vulnerabilidad y el amplio espectro de amenazas, tales como las amenazas cibernéticas; la escala y los costos de las inversiones actuales y futuras en información y en sistemas de información; y el potencial que poseen las tecnologías para cambiar drásticamente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos, han impuesto nuevos retos a la práctica de la profesión de auditoría, en particular a la auditoria de sistemas."

b) TESIS DE PREGRADO: "METODOLOGIA DE GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION Y GESTION DE RIESGOS PARA LA PLATAFORMA SIEM DE UNA ENTIDAD FINANCIERA BASADA EN LA NORMA ISO/IEC 27035 E ISO/IEC 27005**"**

Autor: YESID ALBERTO TIBAQUIRA CORTES

Bogotá, Colombia, 2015

[2] http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf

Tibaquira Cortes (2015) establece que “El trabajo desarrollado se basa en la definición de un modelo de gestión de incidentes de seguridad de la información y de gestión de riesgos sobre estos incidentes, que son detectados o derivados de la implementación y operación de una herramienta SIEM (Correlacionador de Eventos de Seguridad). La definición de los modelos de gestión se realizó bajo las normas ISO 27035 para incidentes de seguridad y 27005 para la gestión de riesgos. Inicialmente fueron identificados los activos de información críticos que se encuentran configurados en el SIEM para definir el alcance del diseño en implementación de los modelos. Posterior, se definieron las políticas de seguridad de la información, en donde son descritos los lineamientos que se deben seguir para la gestión de incidentes y riesgos. Por último, fueron definidos los modelos, junto con la implementación y las herramientas que apoyarán su operación, basados en las recomendaciones que expresa cada una de las normas para cada modelo.”

c) TESIS PREGRADO: DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE INFORMACION PARA SERVICIOS POSTALES DEL PERU S.A.

Autor: David Arturo Aguirre Mollehuanca

Lima, Perú, 2014

“La exigencia de la implementación de la norma técnica peruana NTP-ISO/IEC 27001:2008 en las entidades públicas nace de la necesidad de gestionar adecuadamente la seguridad de la información en cada una de estas empresas. Sin embargo, el desconocimiento de estos temas por parte de la alta dirección, ha ocasionado que no se tomen las medidas

necesarias para asegurar el éxito de este proyecto en el tiempo estimado por la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), entidad responsable de apoyar a las entidades públicas durante el proceso de implementación de la norma. Debido a ello, para la realización de este proyecto de fin de carrera, se decidió trabajar con una entidad pública como caso de estudio, a fin de diseñar un Sistema de Gestión de Seguridad de Información o SGSI que se acople a la normativa a la cual está sujeta la organización y que pueda, en un futuro, servir como referencia para la implementación del mismo" (Aguirre Mollehuanca, 2014).

d) TESIS POSGRADO: "BUENAS PRACTICAS PARA LA IMPLEMENTACION DE LA SEGURIDAD EN UN CENTRO DE COMPUTO".[3]

Autor: Leticia Hernández Sánchez

México, 2014.

"Actualmente hay diferentes tipos de tecnologías las cuales van en aumento, dejando atrás la parte de seguridad en la información y en los distintos dispositivos con los que se cuenta. Por ejemplo, el caso de computadoras, celulares, tabletas, impresoras, etcétera.

En este tipo de dispositivos continúan surgiendo problemas de seguridad, debido a la falta de interés por parte de los usuarios, por no identificar la importancia de resguardar su información o datos personales, o simplemente al no elaborar una buena contraseña para sus correos electrónicos, cuentas bancarias, etcétera. En algunos casos

[3] http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/3735/Tesis.pdf?sequence=1

hay filtros de información confidencial y personal, como colocar datos personales en encuestas, en páginas de redes sociales, fotografías, ubicación, posesión de bienes materiales, entre otros datos" (Hernández Sánchez, 2014).

e) TESIS POSGRADO: "METODOLOGIA PARA LA SEGURIDAD DE TECNOLOGIAS DE INFORMACION Y COMUNICACIÓN EN LA CLINICA ORTEGA"[4].

Autor: Goyo Francisco Guzmán Pacheco

Huancayo, Perú, 2015

"Es un hecho que los sistemas de gestión y de información están muy arraigados en los procesos productivos, industriales, de servicios, gubernamentales y casi cualquier sector activo de la sociedad. Esta dependencia de los sistemas de información en general, requiere dotar de seguridad a los mismos para preservar la calidad de los servicios y velar por la eficacia y eficiencia de los procesos de negocio y el valor de sus activos. Ya no es suficiente con establecer controles en forma aislada ni ad hoc, tampoco es suficiente actuar de modo meramente reactivo y defensivo, se requiere de un sistema de gestión de seguridad de tecnologías de información y comunicaciones y un accionar proactivo. Si consideramos un grupo empresarial, donde dos o más empresas se integran verticalmente, el desafío de gestionar la seguridad de una manera conveniente es aún mayor" (Guzmán Pacheco, 2015).

2.1.5 JUSTIFICACIÓN DEL PROYECTO

[4] http://repositorio.uncp.edu.pe/bitstream/handle/UNCP/1478/Tesis-Goyo%20Francisco%20Guzman%20Pacheco.pdf?sequence=1&isAllowed=y

ECONÓMICA

- La Superintendencia Nacional de Aduanas y Administración Tributaria podrá reducir costos en la seguridad de la red informática, al tener el sistema implementado con anticipación.
- Se evitará perdidas de información, así como interferencias, lográndose brindar seguridad a los contribuyentes del país, de que su información está correctamente almacenada.
- La Sunat mantendrá su imagen de garantía de seguridad ante los contribuyentes y brindará información fiable para la confección del presupuesto del estado.

TÉCNICA

- La SUNAT hará uso de un modelo prospectivo actual en la red informática, a fin de garantizar la transferencia de datos entre los contribuyentes y el estado.
- Prevención, Detección y Corrección de Riesgos de seguridad en la red informática de la Sunat - Lima.

OPERATIVA

- El proyecto permitirá robustecer el sistema de seguridad en la red informática de la Sunat.
- La transferencia de datos a través de la red informática será segura, rápida y eficiente.
- El Modelo de Seguridad Informática basada en Prospectiva permitirá que se pueda proteger en forma fiable y transparente la información.

PERSONAL

Permitirá que los investigadores profundicen en los temas referentes a Seguridad de la Información, Redes Informáticas y Prospectiva; y asimismo les permitirá obtener su título profesional.

2.2 OBJETIVOS

2.2.1 OBJETIVO GENERAL

Implementar un Modelo de Seguridad Informática basada en Prospectiva para mejorar la Protección de la Red Informática de la Sunat - Lima.

2.2.2 OBJETIVOS ESPECÍFICOS

- Identificar las deficiencias de seguridad que existen en la red informática de la Sunat – Lima.
- Analizar los requerimientos de seguridad que debe tener el modelo de seguridad, para minimizar los riesgos.
- Diseñar la propuesta del Modelo de Seguridad Informática Prospectivo teniendo en cuenta el hardware y software.
- Evaluar el Modelo de Seguridad Informática Prospectivo en la Red Informática Sunat - Lima.

2.3 HIPOTESIS

"La implementación de un Modelo de Seguridad Informática basada en Prospectiva Mejora la Protección de la Red Informática de la Sunat - Lima".

2.4 VARIABLES

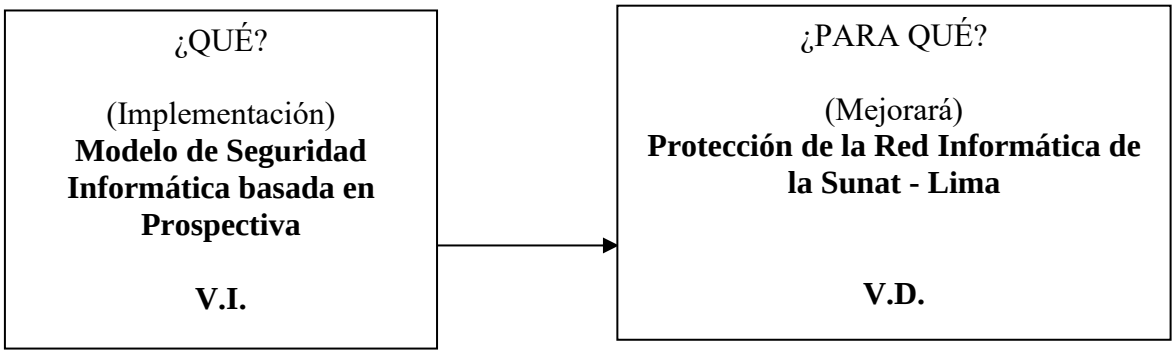
Para este proyecto de Investigación se han definido las siguientes variables:

2.4.1. Variable Independiente

Modelo de Seguridad Informática basada en Prospectiva.

2.4.2. Variable Dependiente

Protección de la Red Informática de la Sunat - Lima.



Indicadores

- VARIABLE INDEPENDIENTE: Modelo de Seguridad Informática basada en Prospectiva.
  - ✓ Facilidad de Implementación
  - ✓ Costos Reducidos
  - ✓ Nivel de Escenarios

- VARIABLE DEPENDIENTE: Protección de la Red Informática de la Sunat - Lima.
  - ✓ Tiempo de Respuesta
  - ✓ Fallas de Seguridad
  - ✓ Cantidad de Detecciones

CAPITULO III

MARCO TEÓRICO

3.1. SEGURIDAD INFORMATICA

La seguridad informática es una novedosa disciplina que se encuentra en crecimiento continuo, por el gran valor que dan a la información que fluye por las redes informáticas de las organizaciones. Mientras más se garantice la seguridad de los datos que circulan en forma de bits a través de los diferentes medios de comunicación, más valor tendrá la información y la organización que las genera y procesa.

"La seguridad informática es la disciplina que, con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riegos tanto físicos como lógicos, a los que está expuesta" **(Urbina Baca, 2016, pág. 12)**.

Como se aprecia, algunos autores ya reconocen a la seguridad informática como una disciplina, ya que su trabajo lo realizan en forma sistematizada, de acuerdo a un conjunto de procesos y herramientas.

"Por todo lo anterior se considera muy importante la seguridad informática, que se puede definir como un conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información en un sistema informático e intentar reducir las amenazas que pueden afectar al mismo" **(Garcia-Cervigon Hurtado & Alegre Ramos, 2011, pág. 2)**.

Un sistema informático está conformado por partes lógicas y partes físicas, por lo cual deben ser protegidos desde un punto de vista lógico (con el desarrollo de software) o

físico (vinculado al mantenimiento eléctrico, por ejemplo). Por otra parte, las amenazas pueden proceder desde programas dañinos que se instalan en la computadora del usuario (como un malware) o llegar por vía remota a través de las redes (los hackers que se conectan a Internet e ingresan al sistema aprovechando vulnerabilidades).

Uno de las principales prioridades de las organizaciones y sobre todo de la oficina de TICS es garantizar que la información fluya por la red en forma íntegra, así como de los sistemas informáticos que lo generan o usan, caso contrario se tendrían pérdidas económicas y de tiempo, y el riesgo de que accedan a nuestros sistemas por personal no autorizado.

En el caso de los virus hay que subrayar que en la actualidad es amplísima la lista de ellos que existen y que pueden vulnerar de manera palpable cualquier equipo o sistema informático. Así, por ejemplo, nos encontramos con los llamados virus residentes que son aquellos que se caracterizan por el hecho de que se hallan ocultos en lo que es la memoria RAM y eso les da la oportunidad de interceptar y de controlar las distintas operaciones que se realizan en el ordenador en cuestión llevando a cabo la infección de programas o carpetas que formen parte fundamental de aquellas.

De la misma forma también están los conocidos virus de acción directa que son aquellos que lo que hacen es ejecutarse rápidamente y extenderse por todo el equipo trayendo consigo el contagio de todo lo que encuentren a su paso.

Los virus cifrados, los de arranque, los del fichero o los de sobreescritura son igualmente otros de los peligros contagiosos más importantes que pueden afectar a nuestro ordenador.

Entre las herramientas más usuales de la seguridad informática, se encuentran los programas antivirus, los cortafuegos o firewalls, la encriptación de la información y el uso de contraseñas (passwords).

Herramientas todas ellas de gran utilidad como también lo son los conocidos sistemas de detección de intrusos, también conocidos como anti-spyware. Se trata de programas o aplicaciones gracias a los cuales se puede detectar de manera inmediata lo que son esos programas espías, que se encuentran en nuestro sistema informático y lo que realizan es una recopilación de información del mismo para luego ofrecérsela a un dispositivo externo sin contar con nuestra autorización en ningún momento.

Un sistema seguro debe ser íntegro (con información modificable sólo por las personas autorizadas), confidencial (los datos tienen que ser legibles únicamente para los usuarios autorizados), irrefutable (el usuario no debe poder negar las acciones que realizó) y tener buena disponibilidad (debe ser estable).

De todas formas, como en la mayoría de los ámbitos de la seguridad, lo esencial sigue siendo la capacitación de los usuarios. Una persona que conoce cómo protegerse de las amenazas sabrá utilizar sus recursos de la mejor manera posible para evitar ataques o accidentes.

En otras palabras, puede decirse que la seguridad informática busca garantizar que los recursos de un sistema de información sean utilizados tal como una organización o un usuario lo ha decidido, sin intromisiones.

Por tanto, la seguridad informática o seguridad de tecnologías de la información es una especialidad que se dirige en proteger todo lo referente a la infraestructura informática, tanto tangible como intangible, siempre su principal objetivo la información. Para todo esto existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. Los activos comprendidos son tanto el software, el hardware y todos los componentes relacionados a la organización que posibilite un riesgo a la confidencialidad de la información.

Por lo tanto, la seguridad de la información en una red informática empresarial es el conjunto de técnicas y métodos para identificar y eliminar vulnerabilidades. Se debe poner atención a la necesidad de salvaguardar la información y equipos físicos. Las amenazas están presentes siempre y para los diferentes tipos se deben tener planes de acción a fin de salvaguardar la seguridad y mantener en función la organización.

3.1.1. OBJETIVOS

La seguridad informática es una disciplina que debe determinar normas que reduzcan los riesgos a la información o infraestructura informática. Estas normas deben incluir horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo que respecta a un nivel de seguridad adecuado, teniendo presente a los recursos humanos y los sistemas de información.

La seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran los siguientes:

- La infraestructura informática: Es la parte hardware que existe en la organización, donde se realiza el procesamiento de los datos, así como se almacena los datos. Aquí se tiene que asegurar que los equipos funcionen adecuadamente y estar prevenidos ante posibles fallos y ataques.
- Los usuarios: Las personas que hacen uso de los sistemas de información de la organización, pudiendo ser los trabajadores de la organización, así como los clientes y proveedores. Se debe garantizar el uso adecuado de los sistemas.

- La información: es el principal activo. Son los datos que circulan por la organización, utilizando la infraestructura informática y usada por los usuarios.

3.1.2. AMENAZAS

Durante la transmisión de datos en la red informática se presentan fallas de seguridad o riesgos, lo cual vienen a ser las amenazas, lo que la seguridad informática tiene como función eliminar o reducir. Cada día se van generando nuevas amenazas, esto por el desarrollo de la tecnología, nuevas técnicas de hacking, nuevos protocolos, etc.

Hay amenazas que se dan en el nivel de la programación y en el nivel de funcionamiento de los dispositivos de almacenamiento.

Hay muchas actividades riesgosas que son imprevisibles o inevitables, de tal forma que se tienen que realizar protecciones basadas en redundancia, por ejemplo, teniendo doble línea de comunicación o doble servidor.

Las amenazas son originadas por:

- Usuarios: Los usuarios son el mayor recurso de una organización, de los que depende el éxito o fracaso, por lo cual su accionar es el que puede generar los riesgos informáticos en la organización. Hay que ver los atributos de acceso que tienen, a fin de que no tengan más de lo que necesitan.
- Programas maliciosos: Conocidos como Malwares, los que han sido codificados para producir daños en los sistemas informáticos, ya sea a la parte software o a la parte hardware. Muchas veces es instalado sin conocer su real alcance, ya que vienen enmascarados dentro de otro software. Existen malwares con diferentes funciones, los que son

llamados: virus informático, gusano informático, troyano, bomba lógica, programa spyware, etc.

- Errores de programación: Cuando se desarrolla programas, muchas veces se tienen errores, los que son llamados bugs, lo que son riesgos de programación. Estos bugs o fallas, son lo que aprovechan los hackers a través de exploits. Por eso se tiene que tener cuidado de este tipo de fallas y realizar las actualizaciones correspondientes.
- Intrusos: Son las personas que no pertenecen a la organización, pero acceden aprovechando fallas de seguridad.
- Un siniestro: Problemas en la parte física o lógica de un sistema informático que pueden producir perdidas a la organización.
- Personal técnico interno: el personal de la organización encargada de manejar el sistema informático, quienes se encargan de diferentes partes: la red informática, los servidores, el software, etc.
- Fallos electrónicos o lógicos de los sistemas informáticos en general.
- Catástrofes naturales: terremotos, inundaciones, maremotos, huracanes, etc.

3.2. MODELO DE SEGURIDAD "CIA"

El objetivo de la seguridad informática es buscar los riesgos que tienen que ver con la informática, como amenazas y vulnerabilidades del sistema de información que se quiere proteger, por lo que, todo sistema que quiera considerarse seguro debe cumplir con 3 aspectos fundamentales: confidencialidad (Confidentiality), integridad (Integrity) y disponibilidad (Availability), encontrando sus relaciones con la forma de un triángulo, por lo que es común referirse a este modelo como Triángulo CIA.

Estos aspectos se relacionan para mantener un sistema funcional y proteger la información.

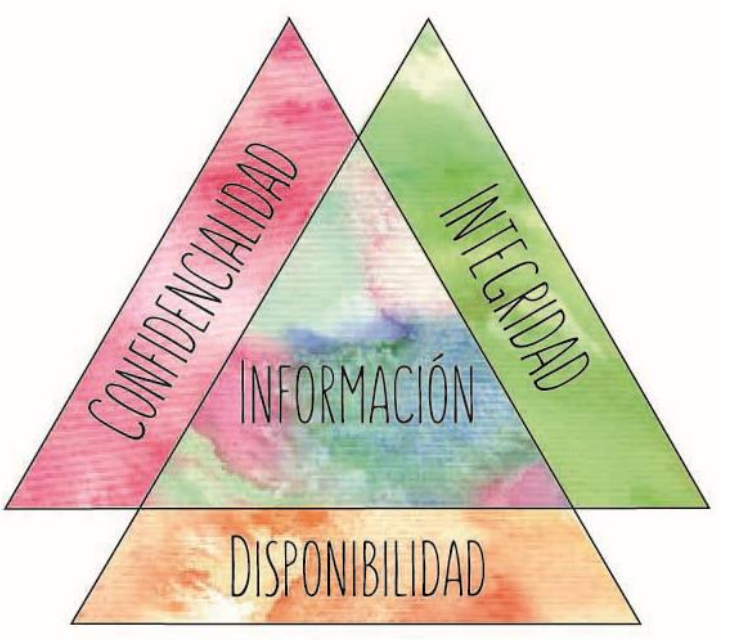


Figura 2 – Modelo de Seguridad CIA

Los vértices del triángulo son las dimensiones básicas de la seguridad, mientras que las aristas representan aspectos derivados o servicios básicos de la seguridad.

Confidencialidad

Consiste en la garantía de que la información que se proporciona al sistema, no pueda ser accedida por personas no autorizadas, ni será divulgada.

Integridad

Es el principio que se encarga de que la información en el sistema sea correcta y válida y que no pueda ser modificada por alguien no autorizado.

Disponibilidad

Consiste en que la información y los recursos relacionados estén disponibles para los usuarios autorizados cuando lo requieran, incluso en momentos de emergencia.

3.3. ISO 27001: 2013

Sistemas de Gestión la Seguridad de la Información

ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

El estándar ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

La aplicación de ISO-27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización.

La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002.

Estructura de la norma ISO 27001

1. **Objeto y campo de aplicación:** La norma comienza aportando unas orientaciones sobre el uso, finalidad y modo de aplicación de este estándar.
2. **Referencias Normativas:** Recomienda la consulta de ciertos documentos indispensables para la aplicación de ISO27001.
3. **Términos y Definiciones:** Describe la terminología aplicable a este estándar.
4. **Contexto de la Organización:** Este es el primer requisito de la norma, el cual recoge indicaciones sobre el conocimiento de la organización y su contexto, la comprensión de las necesidades y expectativas de las partes interesadas y la determinación del alcance del SGSI.
5. **Liderazgo:** Este apartado destaca la necesidad de que todos los empleados de la organización han de contribuir al establecimiento de la norma. Para ello la alta dirección ha de demostrar su liderazgo y compromiso, ha de elaborar una política de seguridad que conozca toda la organización y ha de asignar roles, responsabilidades y autoridades dentro de la misma.
6. **Planificación:** Esta es una sección que pone de manifiesto la importancia de la determinación de riesgos y oportunidades a la hora de planificar un Sistema de Gestión de Seguridad de la Información, así como de establecer objetivos de Seguridad de la Información y el modo de lograrlos.
7. **Soporte:** En esta cláusula la norma señala que para el buen funcionamiento del SGSI la organización debe contar con los recursos, competencias, conciencia, comunicación e información documentada pertinente en cada caso.
8. **Operación:** Para cumplir con los requisitos de Seguridad de la Información, esta parte de la norma indica que se debe planificar, implementar y controlar los procesos de la organización, hacer una valoración de los riesgos de la Seguridad de la Información y un tratamiento de ellos.

9. **Evaluación del Desempeño:** En este punto se establece la necesidad y forma de llevar a cabo el seguimiento, la medición, el análisis, la evaluación, la auditoría interna y la revisión por la dirección del Sistema de Gestión de Seguridad de la Información, para asegurar que funciona según lo planificado.
10. **Mejora:** Por último, en la sección décima vamos a encontrar las obligaciones que tendrá una organización cuando encuentre una no conformidad y la importancia de mejorar continuamente la conveniencia, adecuación y eficacia del SGSI.

Novedades de la ISO 27001:2013

Esta norma fue publicada recientemente, aportó una serie de cambios con respecto a su antecesora que los usuarios de los SGSI tienen que asimilar para continuar gestionando de forma eficaz la Seguridad de la Información. Las novedades que manifiesta son:

- No aparece la sección "Enfoque a procesos" con su respectiva metodología basada en el ciclo PHVA, ahora ofrece mayor flexibilidad.
- Se elimina la obligatoriedad de algunos documentos, conservando únicamente la declaración de aplicabilidad.
- Se han revisado los requisitos y controles.
- Se apuesta por un enfoque del análisis del riesgo en la fase de planificación y operación.

Controles de la norma ISO 27001

En el Anexo A de la Norma ISO 27001, hay un total de 114 controles de seguridad. La organización debe elegir cuáles se aplican mejor a sus necesidades, es importante

entender que no solo se limita al área de tecnología, sino que también involucra departamentos como el de recursos humanos, seguridad financiera, comunicaciones, entre otros.

En el 2013 se realizó este cambio, pues anteriormente en la norma del 2005 había un total de 133 controles y se eliminaron los estándares de acciones preventivas, y el requisito para documentar ciertos procedimientos.

Los 114 controles están divididos en 14 secciones:

1. Políticas de seguridad de la información.
2. Organización de la seguridad de la información.
3. Seguridad de los recursos humanos.
4. Gestión de activos.
5. Controles de acceso.
6. Criptografía – Cifrado y gestión de claves.
7. Seguridad física y ambiental.
8. Seguridad operacional.
9. Seguridad de las comunicaciones.
10. Adquisición, desarrollo y mantenimiento del sistema.
11. Relación de los proveedores
12. Gestión de incidentes de seguridad de la información.
13. Continuidad de negocios
14. Cumplimiento.

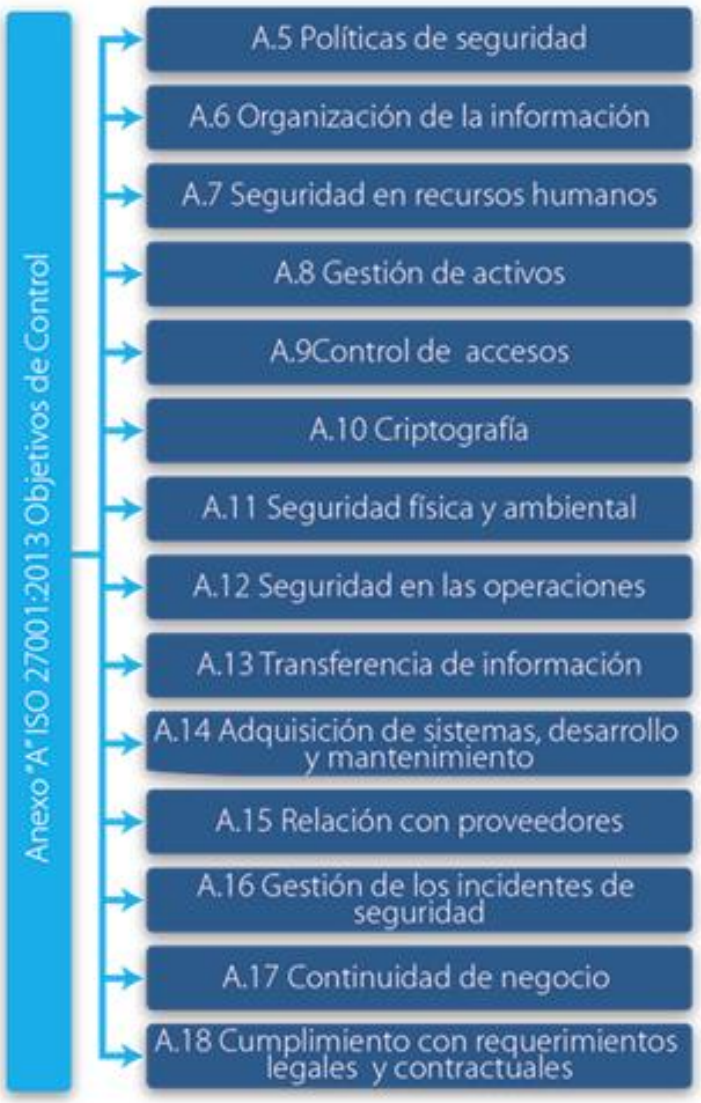


Figura 3 – Anexo A ISO 27001:2013

¿Qué debes tener en cuenta para implementar estos controles?

Los controles son obligatorios según la aplicabilidad en cada organización. Los encargados de la seguridad de la información son quienes deben definir cuáles son los que se van a poner en marcha para garantizar la protección de datos.

Es indispensable generar una capacitación sobre esta norma para establecer los controles adecuados en la gestión de la seguridad de la información.

Adicionalmente, la norma ISO 27001 requiere algo más sobre los controles de seguridad, por eso, es necesario llevar a cabo las siguientes acciones:

- Definir responsabilidades para administrar los controles.
- Medir y monitorear la efectividad de los controles.
- Implementar acciones correctivas cuando se detecten fallos en los controles, de tal forma que se asegure el logro de los objetivos propuestos.

3.4. ISO/IEC 27002:2005 e ISO/IEC 27002: 2013

ISO/IEC 27002 (anteriormente denominada ISO 17799) es un estándar para la seguridad de la información publicado por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC). La versión más reciente es la ISO/IEC 27002:2013.

El estándar ISO/IEC 17799 tiene su origen en el British Standard BS 7799-1 que fue publicado por primera vez en 1995. En el año 2000 la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional publicaron el estándar ISO/IEC 17799:2000, con el título de Information technology - Security techniques - Code of practice for information security management. Tras un periodo de revisión y actualización de los contenidos del estándar, se publicó en el año 2005 el documento modificado ISO/IEC 17799:2005.

Con la aprobación de la norma ISO/IEC 27001 en octubre de 2005 y la reserva de la numeración 27.000 para la Seguridad de la Información, el estándar ISO/IEC 17799:2005 pasó a ser renombrado como ISO/IEC 27002 en el año 2007.

Entonces nos encontramos con el estandar 27002:2005, que posteriorme fue actualizado al estandar 27002:2013.

La principal diferencia entre éstas sería la estructura de las mismas, puesta que la norma actual (27002:2013) posee 14 dominios de seguridad, 35 objetivos de control y 114 controles, mientras que la norma anterior (27002:2005) poseía 11 dominios de seguridad, 39 objetivos de control y 133 controles.

Figura 4 – Diferencia entre ISO 27002:2005 y ISO 27002:2013

ISO/IEC 27002[5] proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como *"la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)"*.

[5] https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27002:ed-2:v1:en

Este estándar tiene una versión de 2013, en la cual se están determinando 14 dominios:

1. **Políticas de Seguridad**: Aquí se detalla las directrices y las políticas en las que se basa la seguridad de la información. Y tiene como finalidad evaluar estas políticas y su aplicación a una realidad.
    1. Gestión directiva en seguridad
2. **Organización de la Seguridad de la Información**: La seguridad de la información tiene que organizarse, principalmente en forma interna: debiéndose asignar las responsabilidades relacionadas con la seguridad de la información. Para esto se cuenta con 2 actividades necesarias que se tienen que organizar para su implementación:
    1. Organización interna
    2. Dispositivos móviles y teletrabajo
3. **Seguridad de los Recursos Humanos**: Los recursos humanos son importantes en toda organización, y la seguridad debe alcanzar aspectos que se deben tener presente en forma previa, durante y también post. Cuando se vaya a contratar a un personal se tienen que hacer averiguaciones sobre sus antecedentes y establecer un contrato apropiado. En el trabajo que realizan durante el contrato, se deben determinar sus funciones, responsabilidades, un programa de capacitación. Asimismo, cuando se termina el contrato o se realiza un cambio de puesto de trabajo, se debe tener presente actividades de seguridad.
    1. Pre contratación
    2. Durante el contrato
    3. Finalización y cambio de contrato

4. **Gestión de los Activos**: Las instituciones tienen un conjunto de activos, que pueden ser tangibles o intangibles, por lo cual se debe determinar la responsabilidad sobre ellos (inventario, uso aceptable, propiedad y devolución de activos), se debe hacer una clasificación y la gestión de los dispositivos de almacenamiento (funcionamiento de dispositivos extraíbles y su eliminación).
    1. Responsabilidad por los activos
    2. Clasificación de la información
    3. Manejo de los medios de comunicación
5. **Control de Accesos**: Cada usuario de los sistemas en la institución deben tener definido los procedimientos para acceder, donde se encuentren sus responsabilidades.
    1. Requisitos de control de acceso
    2. Gestión de los accesos
    3. Responsabilidades
    4. Control de acceso en sistemas y aplicaciones
6. **Cifrado**: Todos los sistemas deben manejas protocolos de encriptamiento, principalmente para el manejo de claves.
    1. Controles en el cifrado
7. **Seguridad Física y Ambiental**: Se tiene que establecer áreas seguras (perímetro de seguridad física, controles físicos de entrada, seguridad de oficinas, despacho y recursos, protección contra amenazas externas y ambientales, trabajo en áreas seguras y áreas de acceso público) y la seguridad de los equipos (emplazamiento y protección de equipos, instalaciones de suministro, seguridad del cableado, mantenimiento de

equipos, salida de activos fuera de las instalaciones, seguridad de equipos y activos fuera de las instalaciones, reutilización o retiro de equipo de almacenamiento, equipo de usuario desatendido y política de puesto de trabajo y bloqueo de pantalla).

    1. Áreas seguras
    2. Equipamiento

8. **Seguridad de las Operaciones**: Todo tiene que ser protegido, por lo cual se deben determinar procedimientos y responsabilidades; lo cual va permitir estar resguardado contra malware y contra todo tipo de vulnerabilidad.

    1. Procedimientos y responsabilidades operativas
    2. Protección anti malware
    3. Copias de seguridad
    4. Registros y monitoreo
    5. Control del software operacional
    6. Gestión de vulnerabilidades técnicas
    7. Consideraciones en auditorias de sistemas

9. **Seguridad de las Comunicaciones**: Las transferencias de datos a través de las redes siempre está supeditada a ataques y fallos, por lo cual se debe gestionar el envío a través de canales apropiados y con los protocolos seguros.

    1. Gestión de la seguridad en red
    2. Transferencia de información

10. **Adquisición de sistemas, desarrollo y mantenimiento**: Cuando se adquieren sistemas para la organización, o se está desarrollando y dando

mantenimiento, se deben determinar los procesos apropiados a fin de evitar fallas que puedan permitir problemas en la seguridad de la información.

    1. Requisitos de seguridad en sistemas de la información
    2. Seguridad en el desarrollo y proceso de soporte
    3. Pruebas

11. **Relaciones con los Proveedores**: Los proveedores son socios estratégicos de la organización, por lo cual las relaciones que mantenemos deben estar bien definidas, esto tanto en las relaciones como en la entrega de servicios.
    1. Seguridad de la información en las relaciones con proveedores
    2. Gestión de la entrega con proveedores
12. **Gestión de Incidencias que afectan a la Seguridad de la Información**: Todas las fallas que se generen deben ser gestionadas, a través de una bitácora y lecciones aprendidas.
    1. Gestión de incidentes y mejoras
13. **Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio**: Ya con el funcionamiento de la organización y ante fallas, se debe tener los planes de contingencia apropiados para que el negocio siga funcionando apropiadamente.
    1. Continuidad en la seguridad de la información
    2. Redundancias
14. **Conformidad**: Todas las actividades que realiza la organización en su trabajo de gestión de la seguridad, deben encontrarse dentro de la ley y cumplir los requisitos contractuales.
    1. Conformidad con la ley y los requisitos de contratos

2. Revisiones en la seguridad de la información

En cada una de las 14 secciones, se establecen los objetivos de los controles. Para cada uno de los controles se indica asimismo una guía para su implantación. Se ha establecido un total de 114 controles, aunque su aplicación dependerá de cada organización según sus necesidades.

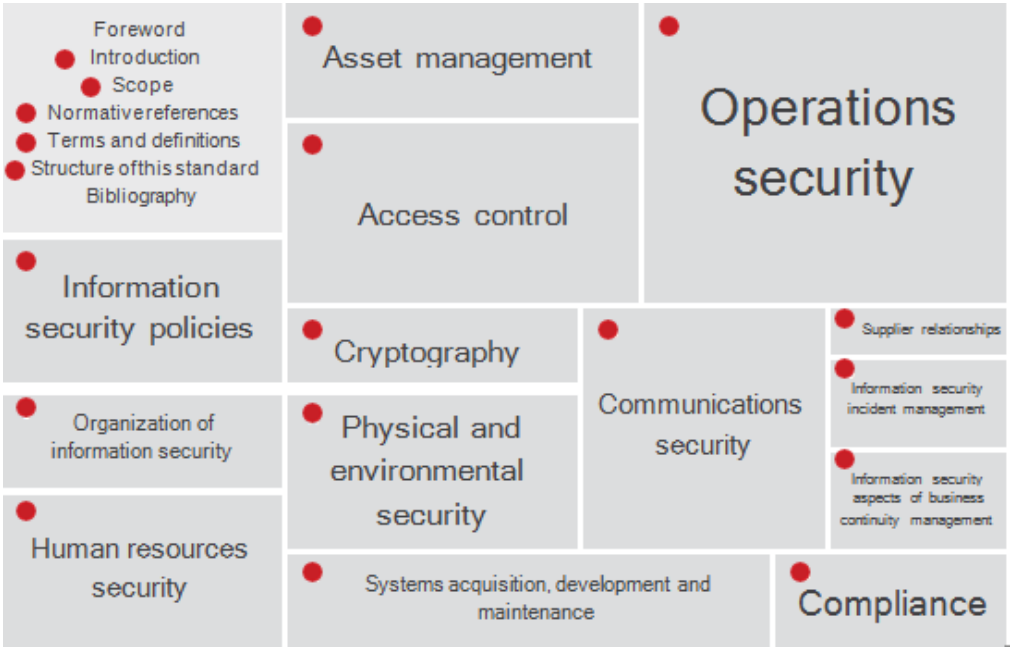


Figura 5 – Objetivos de la ISO 27002:2013

También se tiene a la ISO 27001, que es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

El estándar ISO 27001:2013 para los Sistemas de Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

La aplicación de ISO 27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización.

La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002.

La aplicación de la norma ISO 27001 se da en los diferentes niveles de una organización: Operacional, Táctico y Estratégico.

Figura 6 – Dominios de la Norma ISO 27001

3.5. METODOLOGIA DE SEGURIDAD INFORMATICA

Existen diversas metodologías propuestas para el desarrollo de la seguridad informática en las organizaciones, todas las cuales tienen en cuenta el modelo CIA y la norma ISO 27001. En este caso se tendrá en cuenta un estudio que dará una propuesta de metodología para la gestión de la automatización de la seguridad y

control. La seguridad informática se basa en 3 etapas. Esta metodología, resultante de un artículo científico, servirá como punto de partida para proponer un modelo de seguridad informática prometedora.

Determinación de Fases y actividades de la metodología de seguridad informática

Fase 1: Planificación

En esta primera fase se va determinar los principales objetivos del control a partir del análisis de los riesgos a los que pueden estar expuestos los diferentes recursos de TI. Se van a realizar cuatro actividades que originarán la información útil que nos ayudará a pasar a la siguiente fase. Ellas son:

- **Realizar caracterización del sistema de información**: Esta actividad cubre parte de la misión definida en ISO/IEC 27001, que se centra en describir el sistema de información desde el punto de vista de la organización de gestión que representa, una descripción realista del entorno, el tiempo que ocupa, la retención y características de los empleados que utilizan la tecnología de la información. Además, como parte de esta actividad, se debe establecer un grupo de trabajo para llevar a cabo las tareas relacionadas con la implementación del SGSI, designando así a las personas que desempeñarán los roles especificados en la jurisprudencia. El siguiente paso importante es identificar las leyes, reglamentos, estatutos y otros documentos que rigen la seguridad informática de su organización en un nivel superior.
- **Identificar activos informáticos**: Esta acción es el resultado de ISO/IEC 27001 y es responsable de los activos en el sistema de TI, manteniendo el inventario de los mismos. Además, calcular el valor de la propiedad para la organización mediante el método de análisis cuantitativo, en el que cada

atributo o medición de información (seguridad, integridad, usabilidad, autenticidad e identidad, etc.) se le asigna un valor (de 0 a 10), que refleja la importancia de un atributo específico para este recurso.

- **Realizar análisis de riesgos**: El análisis de riesgos es la actividad de determinar el nivel de riesgo asociado con un activo en función de la probabilidad de que ocurra un evento malicioso, el uso de una vulnerabilidad o amenaza en un sistema de TI y el impacto del evento malicioso en un sistema específico.
- **Definir controles automatizables**: Respondiendo a las tareas 4.2.1.f, 4.2.1.g, 4.2.1.h, 4.2.1.i y 4.2.1.j, definidas en el estándar ISO/IEC 27001, se procederá con el tratamiento de los riesgos identificados, lo cual implica cuatro acciones posibles: reducirlos, aceptarlos, evitarlos o transferirlos. La redacción de las políticas de seguridad es el comienzo de esta actividad, que se dictan con el objetivo de darle tratamiento a los riesgos, y exponen explícitamente las acciones a tomar sobre los mismos; deben estar alineadas con los objetivos de la organización y disposiciones legales o regulaciones regionales dictadas por organismos superiores.

Si se decide trabajar en la reducción de los riesgos, es necesario comenzar a definir los objetivos de control y seleccionar los controles apropiados que puedan calificarse como automatizables (Tabla 1). Además, se deben identificar los controles que puedan ya estar implementados dentro de la organización.

Tabla 1. Dominios de amenazas por macro-control

No.	Macro-control	Dominios
1	Inventario de activos	hardware, software, comunicaciones y recursos físicos
2	Gestión de usuarios	recursos humanos
3	Gestión de trazas	información, datos y servicios
4	Monitoreo de los sistemas	software
5	Protección contra programas malignos	software
6	Detección de vulnerabilidades y gestión de parches	software
7	Configuraciones de seguridad y cumplimiento de políticas	información, datos, servicios, software, hardware, comunicaciones, recursos administrativos, recursos físicos y recursos humanos
8	Respaldo de información	información, datos
9	Seguridad física	recursos físicos
10	Gestión de incidentes	información, datos, servicios, software, hardware, comunicaciones, recursos administrativos, recursos físicos y recursos humanos

Fase 2: Implementación y Operación

El objetivo de esta fase será presentar un informe sobre la realización de las pruebas de seguridad informática automatizadas y describir los procedimientos utilizados en la implementación y operación de las herramientas. La implementación de controles automatizados implica la instalación y configuración de aplicaciones que automatizan parcial o totalmente algunos controles de seguridad informática y los complementan con cambios menores si es necesario. Esta fase propone la realización de tres actividades descritas a continuación:

- **Seleccionar herramientas de gestión**: Esta actividad responde a las tareas recogidas en el acápite 4.2.2 del estándar ISO/IEC 27001. Los objetivos a alcanzar son identificar, seleccionar e instalar las herramientas necesarias para la implantación de los controles definidos en la primera fase de esta metodología.
- **Realizar ajustes y configuraciones**: Después de seleccionar e instalar el sistema, sigue el proceso de instalación y configuración. Si es necesario, se

realizarán pequeñas inversiones y se gravarán con este fin. Durante esta actividad, debe preparar un manual de procedimientos que explique claramente los pasos de todo el proceso de instalación, configuración y desarrollo de cada herramienta de seguridad informática que utilice.

- **Operar los controles de seguridad informática**: Mientras mantiene la seguridad de TI, debe definir y aplicar métricas que le permitan obtener información sobre las métricas basadas en los datos existentes en el sistema. La información sobre estos indicadores debe comunicarse a la gerencia de la organización y a los especialistas en gestión del SGSI de manera oportuna.

Fase 3: Medición

Los controles implantados actúan disminuyendo la probabilidad o frecuencia de incidentes asociados a una amenaza y/o sobre el impacto que tiene la misma sobre un activo, reduciendo el daño o la degradación que sufre el mismo (CORTI, 2006).

El paso final del enfoque propuesto es probar la efectividad de los controles automatizados, medir qué tan bien se identifican los recursos de TI en la organización y volver a calcular su impacto y riesgos después de aplicar las medidas de control. El objetivo principal es realizar el plan de acciones correctivas en caso de ser necesario, en correspondencia con las tareas recogidas en la sección 4.2.4 referente a la mantención y el mejoramiento del SGSI del estándar ISO/IEC 27001.

Las actividades definidas para esta fase consisten en:

- **Revaloración de impacto:** Teniendo en cuenta ciertos controles implementados y la madurez de los procesos de gestión, el sistema se mantiene en una situación de posibilidad de impacto, denominada residual. Se dice que se ha modificado el impacto desde un valor potencial a un valor residual (MINHAP, 2012).

- **Revaloración de riesgo**: El riesgo residual es la cantidad de riesgo que queda en el SGSI después de implementar los controles y depende del impacto residual y la probabilidad de peligros después de implementar los controles automatizados.
- **Elaborar plan de acciones correctivas**: El análisis de riesgo e impacto residual lo ayuda a comprender dónde se encuentra su organización después de implementar ciertos controles. Con base en sus valores, puede identificar las acciones apropiadas a tomar y dónde llevarlas a cabo para reducirlas aún más.

3.6. PROSPECTIVA

Según (Beinstein, 2016), el siglo XXI presencia una verdadera explosión de estudios prospectivos. Gobiernos nacionales, organismos internacionales, empresas, organizaciones sociales utilizan dicho instrumento. Inicialmente, el tema se limitó a Europa occidental y algunas grandes empresas e instituciones oficiales, pero se extendió rápidamente y, a fines del siglo XX, se habían realizado cientos de investigaciones de vanguardia, principalmente débiles en países altamente desarrollados. Actualmente asistimos a un lado del proceso de triplicación de la investigación de punta tanto en los países centrales como periféricos, especialmente la investigación para el desarrollo a través de actividades específicas, instituciones, agencias, programas permanentes y centros especializados.

Por otro lado, los ejercicios futuros incluyen el alcance creciente de los campos temáticos: industria, tecnología, territorio, sociedad, política, religión, agricultura, etc. Problemas, gran desarrollo de tecnología internacional, campos de fabricación a nivel global o regional, etc.), pero también se aplica a áreas de tamaño mediano (grupos de empresas medianas y pequeñas, comunitarias, etc.), y recientemente a micro niveles

(pequeñas y medianas empresas por separado), en micro ejercicios, no hay relación a nivel macro.

Desde un principio, los ejercicios futuristas intentaron basarse en una visión sistemática de la realidad, pero en sus inicios podríamos catalogarlo como la perspectiva "clásica" (o del "primer siglo"), como señalan autores como Gono y Antoine. Es un análisis de sistemas con una fuerte actitud cartesiana, simplificador, no matizado, categorizador demasiado rígido, con visión de tiempo, fuertemente saturado de visión de previsión, con un conjunto de técnicas muy limitado.

Esas limitaciones fueron gradualmente superadas y actualmente emerge una práctica mucho más flexible, menos esquemática.

3.6.1. Metodologías Prospectivas

A. METODO DELPHI. - Una herramienta potencialmente cualitativa que solicita la opinión de un panel de expertos para evaluar situaciones de las que no conocemos con exactitud. Implica movilizar paneles de expertos y analizar las respuestas a una encuesta, juzgados por el mayor número posible de expertos de la industria.

B. HOJA DE RUTA. - Es una herramienta de planificación para establecer metas, establecer compromisos para el futuro y establecer claramente la dirección que desea tomar. Gracias a la participación de expertos se lleva a cabo el análisis de la situación actual, las barreras para alcanzar el futuro deseado y las acciones a realizar para llegar a él. Movilizar expertos a través de paneles.

C. ESCENARIOS DE FUTURO. - Una metodología para determinar estrategias de futuro en un entorno complejo y cambiante con un alto grado de incertidumbre. Se basa en la movilización de equipos de expertos para analizar tendencias cambiantes y analizar contratos de futuros alternativos y sus posibles consecuencias.

D. TECNOLOGIAS CRITICAS. - Identificar tendencias tecnológicas que satisfagan las necesidades de un contexto dado a partir de oportunidades existentes, ayudando a identificar oportunidades de crecimiento. A partir del proceso de dos grupos de expertos y un cuestionario, identificar variables que se centren en los objetivos perseguidos.

3.6.2. Método de Escenarios

Según J. Mchale (1969), El futuro es un símbolo importante a través del cual las personas pueden transformar el presente en presente y dar sentido al pasado. Hay muchos futuros, hay varios futuros posibles y el camino hacia ambos no es necesariamente único. El escenario es una descripción del futuro y la trayectoria asociada.

Existen los siguientes tipos de escenarios:

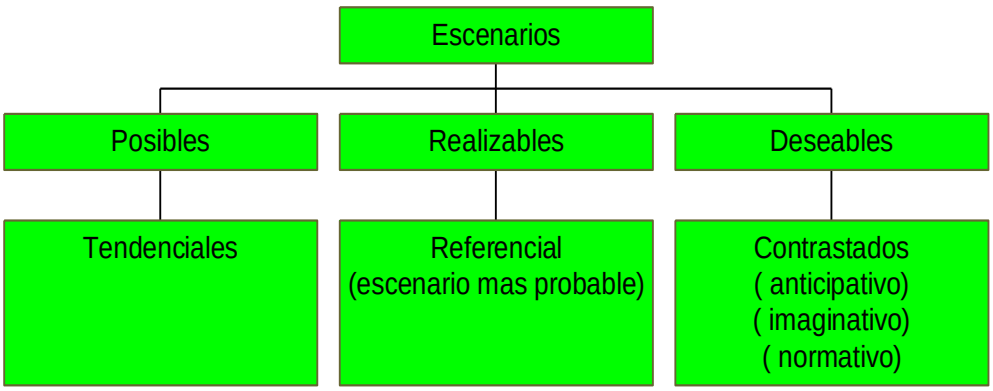


Figura 7 – Tipos de Escenarios

Objetivos del Método de Escenarios

1. Encontrar los sitios de investigación preferidos (variables importantes) combinando, a través del análisis explicativo global más completo, las variables específicas del sistema en estudio.
2. Identificar, principalmente en términos de variables clave, los actores clave que utilizan sus estrategias y recursos para llevar a cabo sus proyectos.
3. Una descripción de escenarios de la evolución del sistema analizado, teniendo en cuenta la evolución más probable de las principales variables y sobre la base de un conjunto de hipótesis sobre el comportamiento de las

variables.

Fases del Método de Escenarios

1. **Construcción de la base analítica e histórica**.

    - Detallada y en profundidad en el plano cuantitativo y cualitativo.
    - Global (económica, política, sociológica, ecológica...)
    - Determinación de las variables esenciales.
    - Retrospectiva y estrategia de los actores.

2. **Elaboración de escenarios**.

    - Dimensiones clave de los escenarios.
    - Elección de imágenes finales.
    - Evolución y trayectorias.
    - Desglose del periodo de estudio.
    - Estudio diacrónico de un periodo.
    - Estudio sincrónico de una imagen intermedia

3. **Cuantificación de los escenarios y modelos de previsión**.

    - Aportes de la prospectiva a los modelos de previsión.
    - La necesidad de explicación: la determinación de las variables principales conocidas u otras ocultas mejoras la selección de los indicadores.
    - La necesidad de hipótesis: la construcción de los escenarios, es decir, de juegos de hipótesis coherentes y probables sobre

variables explicativas garantiza la validez del modelo de previsión.

- La necesidad de Cuantificación: la previsión por escenarios permite evaluar los resultados y las consecuencias de la prospectiva. Todo y teniendo en cuenta lo no cuantificable.

4. Definición y elección de las opciones estratégicas.

Conjunto de acciones

Sus consecuencias a corto, mediano y largo plazo no contradicen las metas establecidas, sino que por el contrario contribuyen a su consecución. Haz que sean consistentes entre sí. El conjunto de acciones realizadas o continuadas es siempre acorde con la evolución del entorno.

Las acciones deben apuntar a:

Siempre que sea posible, trabaje para implementar con éxito los mejores escenarios para los objetivos de su organización.

Limitar las terribles consecuencias de la evolución a una perspectiva pesimista.

Facilitar la inserción de futuras actividades por parte de la organización.

Multiplicidad de acciones:

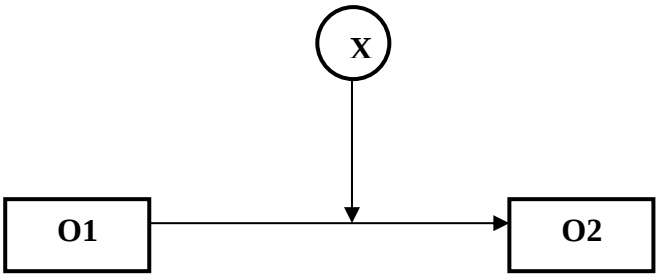
Evaluar las consecuencias de cada posible acción en los diferentes contextos descritos en las situaciones.
Evaluar cada actividad frente a los criterios que la organización debe considerar (financieros, técnicos, estratégicos, comerciales, etc.).

Dar un grupo de acciones a tomar en orden de prioridad, teniendo en cuenta las probabilidades de diferentes situaciones.

CAPITULO IV

MATERIALES Y METODOS

4.1. DISEÑO DE INVESTIGACIÓN



- **Observación N°01:** Situación Actual
- **Observación N°02:** Situación Final
- **X:** Implementación del Modelo de Seguridad Informática basada en Prospectiva**.**

4.2. METODOLOGIA A SEGUIR

En el presente proyecto, se va a utilizar el método experimental que consistirá en 7 fases, con el fin de realizar una investigación más completa y precisa, permitiendo realizar correcciones en la etapa que la necesite.

1ra Fase: Estudio bibliográfico sobre Seguridad Informática y la Superintendencia Nacional de Aduanas y Administración Tributaria.

2da Fase: Recopilación y análisis de la información obtenida en la Red Informática de la Sunat - Lima.

3ra Fase: Evaluación de la Seguridad en la Red Informática de la Sunat - Lima.

4ta Fase: Análisis y Diseño del Modelo de Seguridad Informática basada en Prospectiva.

5ta Fase: Evaluación del Modelo de Seguridad Informática basada en Prospectiva.

6ta Fase: Realización de la contrastación de la Hipótesis.

7ma Fase: Desarrollo del Informe de Resultados Finales.

4.3. COBERTURA DEL ESTUDIO

4.3.1. POBLACIÓN:

La Red Informática de la Sunat – Lima, conformado por 200 Hosts.

4.3.2. MUESTRA:

La Muestra será toda la población, constituida por la Red Informática de la Sunat - Lima.

4.4. FUENTES TÉCNICAS E INSTRUMENTOS DE RECOLECCION DE DATOS

TÉCNICAS	INSTRUMENTOS
Prácticas de laboratorio	Fichas de laboratorio.
Observación	Ficha de observación
Revisión Bibliográfica.	Fichas bibliográficas.
Entrevista	Formato de Entrevista
Encuesta	Cuestionario

CAPITULO V

RESULTADOS

5.1. RED INFORMATICA DE LA SUNAT – LIMA

La red informática de la SUNAT se encuentra centralizada en Lima, con un Data Center donde se encuentran los servidores, a la cual se enlazan todas las sedes a nivel nacional a través de conexiones VPN.

Asimismo, la red informática está conectada a Internet, a fin de que los usuarios tengan acceso a los diferentes servicios de los contribuyentes.

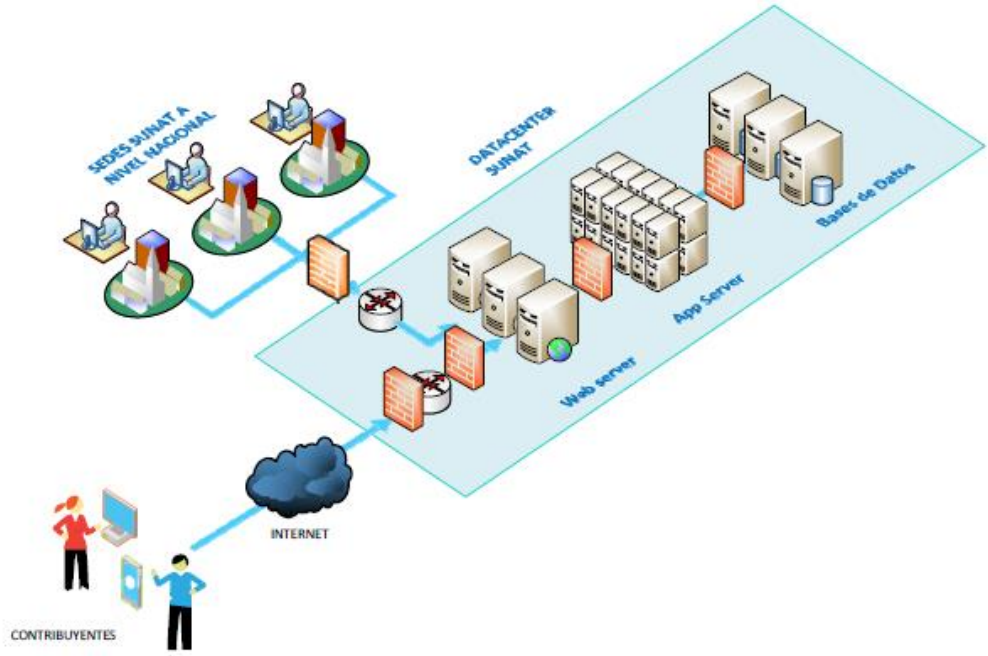


Figura 8. Diagrama de Arquitectura de Alto Nivel de los Sistemas de SUNAT

Fuente: Propuesta de un Marco de Seguridad de la Información en la Nube Publica para la SUNAT: Caso Sistema de Cuenta Única de Contribuyente[6]

[6] https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/625625/SullcaR_N.pdf?sequence=13

Se puede apreciar en la figura anterior, que todos los componentes físicos involucrados con el funcionamiento de los Sistemas le pertenecen a SUNAT y están bajo su control.

Tenemos a los siguientes componentes:

- Infraestructura de Red
- Infraestructura de Servidores de Aplicaciones
- Infraestructura de Servidores de Base de Datos
- Infraestructura de Servidores de Web

El personal que se encarga de la Administración, configuración, monitorización son personal que se encuentran bajo el control de la SUNAT y se rigen por sus políticas internas.

Se tiene que tener en cuenta que la gestión de la red informática de la SUNAT – LIMA y a nivel nacional está a cargo de la Intendencia Nacional de Sistemas de Información – INSI, de la cual se puede decir lo siguiente:

5.1.1. Misión de la INSI:

Impulsar la transformación institucional con el uso intensivo de Tecnologías de la Información y las Comunicaciones (TIC), promoviendo la continua innovación y virtualización de los servicios de la Superintendencia Nacional de Aduanas y de Administración Tributaria y el desarrollo del talento en beneficio de los ciudadanos.

5.1.2. Visión de la INSI:

Convertirnos en un área estratégica que lidere la generación de soluciones tecnológicas innovadoras, logrando ser un modelo en el uso de tecnologías

de información y comunicaciones en las administraciones tributarias y aduaneras de la región.

5.1.3. Localización y Dependencia Estructural y Funcional:

Mediante Resolución de Superintendencia 122-2014/SUNAT y normas modificatorias se aprueba el nuevo Reglamento de Organización y Funciones de la Superintendencia Nacional de Aduanas y de Administración Tributaria con vigencia a partir de 12 de mayo del 2014. De acuerdo con él, la Intendencia Nacional de Sistemas de Información es un órgano dependiente de la Superintendencia Nacional, encargada de dirigir la provisión de los procedimientos, servicios, sistemas de información e infraestructura tecnológica requeridos para la implementación de las estrategias de cambio y soportar a los procesos de la Superintendencia Nacional de Aduanas y de Administración Tributaria.

Su estructura interna es la siguiente:

Áreas de línea:

1. Gerencia de Gestión de Procesos y Proyectos de Sistemas
    - 1.1 División de Gestión de Proyectos de Sistemas
    - 1.2 División de Gestión de Procesos de Sistemas
2. Gerencia de Desarrollo de Sistemas
    - 2.1 División de Desarrollo de Sistemas Tributarios
    - 2.2 División de Desarrollo de Sistemas Aduaneros
    - 2.3 División de Desarrollo de Sistemas Administrativos
    - 2.4 División de Desarrollo de Sistemas Analíticos
3. Gerencia de Calidad de Sistemas
    - 3.1 División de Control de Calidad

3.2 División de Aseguramiento de Calidad

4. Gerencia de Arquitectura

4.1 División de Arquitectura de Información y de Aplicaciones

4.2 División de Arquitectura Tecnológica

5. Gerencia de Operaciones y Soporte a Usuarios

5.1 División de Soporte y Operación de la Infraestructura Tecnológica

5.2 División de Gestión de Infraestructura Tecnológica

5.3 División de Atención a Usuarios

Área de apoyo:

6. Oficina de Seguridad Informática.

5.1.4. Recursos Humanos

El personal de la Intendencia Nacional de Sistemas de Información – INSI se encuentra organizado en Gerencias y Divisiones, de acuerdo a la siguiente tabla.

Nº	Cargos	Cantidad
	Intendencia Nacional de Sistemas de Información	
1	Intendente	1
3	Secretaria	1
4	Apoyo Administrativo	4
	Gerencia de Gestión de Procesos y Proyectos de Sistemas	
1	Gerente	1
2	Secretaria	1
3	Apoyo Administrativo	2
	División de Gestión de Proyectos de Sistemas	
1	Jefe de División	1
2	Personal de División	31
	División de Gestión de Procesos de Sistemas	
1	Jefe de División	1
2	Personal de División	28
	Gerencia de Desarrollo de Sistemas	
1	Gerente	1
2	Secretaria	1
3	Profesional	2
	División de Desarrollo de Sistemas Tributarios	
1	Jefe de División	1
2	Personal de División	100
	División de Desarrollo de Sistemas Aduaneros	
1	Jefe de División	1
2	Personal de División	60
	División de Desarrollo de Sistemas Administrativos	
1	Jefe de División	1
2	Personal de División	49
	División de Desarrollo de Sistemas Analíticos	
1	Jefe de División	1
2	Personal de División	31
	Gerencia de Calidad de Sistemas	
1	Gerente	1
2	Secretaria	1
	División de Control de Calidad	
1	Jefe de División	1
2	Personal de División	81
	División de Aseguramiento de la Calidad	
1	Jefe de División	1
2	Personal de División	25
	Gerencia de Arquitectura	
1	Gerente	1
2	Secretaria	1
3	Profesional	1

División de Arquitectura de Información y de Aplicaciones		
1	Jefe de División	1
2	Personal de División	12
División de Arquitectura Tecnológica		
1	Jefe de División	1
2	Personal de División	18
Gerencia de Operaciones y Soporte a Usuarios		
1	Gerente	1
2	Secretaria	2
3	Apoyo Administrativo	1
División de Soporte y Operación de la Infraestructura Tecnológica		
1	Jefe de División	1
2	Personal de División	51
División de Gestión de Infraestructura Tecnológica		
1	Jefe de División	1
2	Personal de División	79
División de Atención a Usuarios		
1	Jefe de División	1
2	Personal de División	56
Oficina de Seguridad Informática		
1	Jefe de Oficina	1
2	Personal de Oficina	18

5.1.5. Recursos Tecnológicos e Informáticos existentes

La SUNAT tiene diferentes recursos tecnológicos en su red informática, pudiéndose especificar los siguientes:

HARDWARE

Nº	HARDWARE	CANTIDAD
Servidores		
1	DELL	18
2	CISCO	19
3	HP	25
4	AVAYA	4
5	HITACHI	24
6	IBM	184
7	LENOVO	1
8	IBM, Sol PURE 02, (17 Nodos Blades) 641 Servidores Virtuales	28
9	HITACHI, Sol NUBE 02 (16 Nodo Blades) 859 Servidores Virtuales	16
10	IBM Servidores Power02 (795, 740, 770) 128 Lpars Creadas	11
11	Servidores Hitachi	2
12	Servidores IBM (DCs y Correo en virtuales)	21
13	Servidores IBM Web y Windows en Si y Mir	34

Computadoras personales		
14	De escritorio	4731
15	Portátiles	95
Impresoras		
16	Laser	13
17	Matriciales	3
Scanner		
18	Scanner	6
Otros		
19	Proyector multimedia	15

SOFTWARE

Nº	Software	Cantidad
Sistemas Operativos		
1	Red Hat Enterprise Linux	1331
2	Windows 2000 Server	8
3	Windows 2003 Server	21
4	Windows 2008 Server	156
5	Windows 2012 Server	143
6	Windows NT Server	3
Motores de Bases de Datos		
7	IBM Informix	157
8	Microsoft SQL Server	10
9	Oracle Database	3
Herramientas de Desarrollo		
10	Active TLC (Corporativo)	1
11	CVA (Corporativo)	1
12	Data Stage	1
13	Eclipse (Corporativo)	1
14	Informix 4GL (Corporativo)	1
15	Java Development Kit (Corporativo)	1
16	Power Builder	15
17	Power Builder Enterprise	55
18	Tortoise CVS (Corporativo)	1

19	Visual Basic	6
20	Visual Fox Pro	37
21	Win CVS (Corporativo)	1
De Oficina		
22	7-zip	568
23	Adobe Acrobat Reader	568
24	Internet Explorer	568
25	Microsoft Office	568
26	Outlook	568
Diseño de Web		
27	Apache (corporativo)	2
28	Bea Weblogic	690
29	IPlanet (corporativo)	55
30	JBoss (corporativo)	2
31	Lomboz (corporativo)	2
32	NitroX (corporativo)	2
33	OHS	36
34	Kubernetes	95
35	Nginx	94
36	Jetty	7
Antivirus		
37	Software Antivirus (7840)	568
Otros		
38	NVU (corporativo)	1
39	Power Designer	35
40	Sas base	1
41	TOAD	40

EQUIPOS DE COMUNICACIONES

Nº	Conectividad	Cantidad
Switches		
1	Switch para Red	730
Otros		
2	Enlaces RF con equipos Cambium Network 650	32
3	Enlaces RF con equipos Cambium Network 800	10

4	Enlaces RF con equipos REDLINE RD- 3000	12
5	Access Point	586
6	Centrales de Telefonía IP	35
7	Teléfonos IP	6500
8	Equipamiento videoconferencia	91
9	Firewall	125
10	Multiplexores ópticos	4
11	Balanceadores	8
12	Consolas de gestión	3
13	Repositorios de Logs y Reportes	6
14	Servidor de acceso Remoto Seguro	4
15	Servidor de Autenticación	1

5.1.6. Análisis FODA

Aquí se muestran un listado de las diferentes características encontradas en el análisis FODA de la Intendencia Nacional de Sistemas de Información – INSI.

DEBILIDADES

N°	Listado de Debilidades
D1	Limitada capacidad de procesar, poner a disposición de los usuarios y de analizar grandes volúmenes de datos.
D2	Arquitectura de sistemas antigua y compleja, dificultando su operación y monitoreo.
D3	Planeamiento, control estratégico y gobierno de tecnologías de información (TI) no formalizado.
D4	Perfil de puestos y brecha de capacitación en TI no definidos.
D5	Insatisfacción de los usuarios de los servicios de TI respecto del manejo y priorización de la cartera de requerimientos informáticos.
D6	Nivel de calidad de las aplicaciones desarrolladas in–house no uniforme, debido al apremio en las nuevas implementaciones.
D7	Débil gestión de problemas e incidentes: limitada priorización de la atención a sistemas heredados con problemas recurrentes.

FORTALEZAS

N°	Listado de Fortalezas
F1	Personal con competencias, con experiencia y "know-how" del negocio.
F2	Personal de TI con habilidades y experiencia para gestionar TIC de gran complejidad así como de altos volúmenes de información.
F3	Personal con valores éticos.
F4	La Superintendencia Nacional de Aduanas y de Administración Tributaria reconoce a la tecnología como recurso estratégico.

AMENAZAS

N°	Listado de Amenazas
A1	Amenazas a la seguridad de la información.
A2	Desastres naturales y climatológicos.
A3	Normatividad relacionada que limita las contrataciones y la evolución de soluciones tecnológicas.
A4	Oportunidades laborales más favorables en el mercado generan alta rotación de los profesionales de la INSI.

OPORTUNIDADES

N°	Listado de Oportunidades
O1	Tecnología innovadora, disponible en el mercado.
O2	Contribuyentes habituados a consumir servicios virtuales. Las nuevas generaciones de jóvenes, que pronto serán ciudadanos, son nativos digitales.
O3	Oferta de servicios TI especializados en el mercado.
O4	La Superintendencia Nacional de Aduanas y de Administración Tributaria resulta atractiva laboralmente para captar personal en TI.
O5	Coordinación con la Secretaría de Gobierno Digital (SeGDi), mediante sus mesas de trabajo y participación en la Plataforma de Interoperabilidad del Estado (PIDE).

5.1.7. OBJETIVOS ESTRATEGICOS

La Intendencia Nacional de Sistemas de Información – INSI tiene los siguientes objetivos alineados a los objetivos estratégicos de la SUNAT.

N°	Listado de Objetivos
1	**R1 – Construir la SUNAT del futuro.** Contar con servicios que aprovechen al máximo las TI vigentes para alcanzar los objetivos estratégicos institucionales con calidad, eficiencia y oportunidad. Ello con una transformación del negocio para lograr una mayor recaudación, una disminución del tiempo de despacho aduanero y un incremento en la satisfacción del usuario final.
2	**R2 – Crear capacidad analítica.** Lograr la toma de decisiones efectivas y basadas en hechos, al proveerse herramientas y tecnologías para utilizar rápida e intuitivamente la gran cantidad de datos disponibles, transformados para tal fin y ponerlos a disposición de nuestros usuarios. Ello, con el objetivo de conseguir resultados medibles, con impacto en la recaudación y en la mejor percepción de los contribuyentes.
3	**C1 – Operar con Excelencia.** La adecuada definición y gestión de las tecnologías de la información en la SUNAT debe llevarnos a brindar servicios seguros, correctos, confiables y eficientes, que apunten a lograr cero pérdidas de recaudación y de tiempo, tanto de los contribuyentes como de los usuarios internos.

OETI	Entregables/Proyectos informáticos	Contribución al logro del objetivo
R1 – Construir la SUNAT del futuro.	- Comprobantes electrónicos. - Cuenta Única. - Notificación Electrónica y Expediente Virtual. - Procesos de Ingreso (FAST). - Procesos de Salida (FAST). - Gestión de Operadores (FAST). - Gestión de Riesgo Aduanero y Seguridad de la Carga (FAST). - Implementación del Registro de Bienes Fiscalizados. - Optimización del IGV. - Sistema Integrado de Gestión y Administración.	Los proyectos informáticos implican una participación más activa de la INSI, contribuyendo así con su rol de socio estratégico del negocio mediante el apoyo directo al logro de los objetivos.
R2 – Crear capacidad analítica.	- Gestión Integral del Riesgo.	El análisis oportuno de los riesgos mejora la capacidad de la Superintendencia Nacional de Aduanas y de Administración Tributaria para detectar y corregir el incumplimiento tributario, incrementando el control en las operaciones y/o contribuyentes de alto riesgo y facilitando aquellos de bajo riesgo.

5.1.8. Estrategias para el logro del Plan Operativo Informático

Aquí están las estrategias de la INSI para alcanzar las metas del Plan Operativo Informático.

N°	Listado de Estrategias
1	Alta participación en la formulación de proyectos y soluciones con componente tecnológico entregando valor al negocio, buscando simplificar y facilitar el acceso a la información, garantizando la confidencialidad, integridad y disponibilidad de la información.
2	Para alcanzar el objetivo de operar con excelencia se ha establecido un indicador general de disponibilidad de servicios críticos externos y un indicador de los servicios críticos internos, de esta manera se busca brindar una infraestructura tecnológica con alto grado de disponibilidad y un tiempo de respuesta adecuado para los servicios definidos como críticos por la institución.
3	Uno de los objetivos de TI es generar simplificación y productividad para satisfacer los requerimientos del negocio, por lo que es necesario contar con una eficaz gestión de los requerimientos y de los proyectos. De ahí que se hayan establecido indicadores que tienen como meta el 100% de cumplimiento para los entregables con componente informático de programas de cambio y proyectos.

5.2. EVALUACION DE LA SEGURIDAD EN LA RED INFORMATICA DE LA SUNAT – LIMA

En el Aspecto Documental, se puede apreciar que la SUNAT cuenta con los siguientes documentos que regulan la seguridad de la Información:

a. Políticas de Seguridad Informática:

Se refiere a las políticas de seguridad informática. Su objetivo es definir los lineamientos que determinan las actividades que están permitidas al personal de la SUNAT con el propósito de proteger los activos críticos que soportan los procesos informáticos.

Cubre los siguientes aspectos:

- Acceso Físico
- Cuentas de Acceso
- Fiscalización del uso de los Sistemas Informáticos
- Los Sistemas Informáticos
- Sistema y servicios de red
- Uso de licencias
- Uso responsable de los recursos informáticos
- Manejo de la Información

b. Normas y Pautas para la Solicitud y Atención de Cuentas de Acceso:

Contiene las Políticas y Normas para la solicitud, creación, entrega y utilización de las cuentas y claves de acceso a los sistemas de información en ambientes de producción.

c. Políticas y Normas para la utilización del software en la SUNAT:

Regula la utilización del software autorizado en la SUNAT. Todo el personal de la SUNAT al cual se le asigne temporal o definitivamente cualquier equipo informático tiene que responder a esta política.

d. Normas y Pautas para la Atención de Solicitudes Sobre Servicios Informáticos

Establece lo que es necesario para la atención de solicitudes de incidentes y peticiones que brinda la Intendencia Nacional de Sistemas de Información (INSI) y las Unidades Orgánicas (UUOO) que cumplan con las funciones de soporte informático.

e. Normas y Pautas para el acceso y uso del Sandbox SUNAT:

Trata las normas para acceso a un ambiente de trabajo de análisis de información denominado "SandBox" de SUNAT. Cualquier órgano de la SUNAT puede solicitar acceso al mismo. También se norma como solicitar información, disponible en el "Data Warehouse" Empresarial de SUNAT, que será accesible desde el "SandBox" para su análisis respectivo por parte de los colaboradores que tenga el acceso debido.

f. Normas y Pautas para el registro y atención de incidentes y vulnerabilidades de seguridad:

Tiene como objetivo establecer los lineamientos generales para la gestión de incidentes y las vulnerabilidades de seguridad de la información/informática, de la Superintendencia Nacional de Aduanas y Administración Tributaria (SUNAT) y se tomen las acciones correctivas necesarias para prevenir su ocurrencia.

g. Proceso de Seguridad para la generación y custodia de los respaldos informáticos Institucionales:

Trata del proceso de seguridad para la generación y custodia de los respaldos informáticos Institucionales. En ese documento se tienen las directrices de implementación de los lineamientos, políticas, normas y procedimientos que aseguren la adecuada asignación, ejecución, verificación, custodia y control de los respaldos informáticos en medios magnéticos u ópticos.

Y con respecto a la implementación de la norma NTP-ISO 27001 u otras regulaciones, no se puede confirmar completamente; pero si se puede corroborar que la SUNAT ha implementado diversas políticas de Seguridad tanto a nivel de Hardware, Software y Procesos, destinados a proteger los activos críticos que soportan sus procesos informáticos.

La SUNAT busca cubrir los siguientes aspectos:

- Acceso Físico
- Cuentas de Acceso
- Fiscalización del uso de los Sistemas Informáticos
- Los sistemas Informáticos
- Sistema y servicios de red
- Uso de licencias
- Uso responsable de los recursos informáticos
- Manejo de la Información
- Solicitudes de Accesos a Datos de Producción
- Registro de Incidentes de Seguridad
- Respaldos de Información

Las Capacidades Esenciales que deberá tener el equipo de seguridad son las siguientes:

- Es una tarea extremadamente complicada si solo se ven algunas brechas.
- Tener determinados los activos que se deben proteger
- Ubicar los activos que son vulnerables a los ataques
- De qué forma están siendo atacados mis activos
- Como sé si ha tenido lugar una brecha de seguridad
- Que acciones tendrán un impacto mayor sobre la actitud del equipo de seguridad

Y con respecto a la seguridad informática, siempre se están evaluando la adquisición de herramientas, como una herramienta de test de vulnerabilidades, que permita a los profesionales de seguridad informática ejecutar acciones para identificar y corregir vulnerabilidades que puedan ser empleadas para una intrusión no autorizada a la plataforma informática de la Institución. Estas acciones de aseguramiento o corrección de vulnerabilidades buscan incrementar los niveles de seguridad de los servicios informáticos y transacciones electrónicas que presta la Institución a los Contribuyentes y Operadores de Comercio Exterior a través de la plataforma informática y el portal web (www.sunat.gob.pe).

En seguida se muestra una evaluación que realizó la oficina de seguridad informática con respecto a 2 herramientas: Qualys Guard y McAfee Vulnerability Manager.

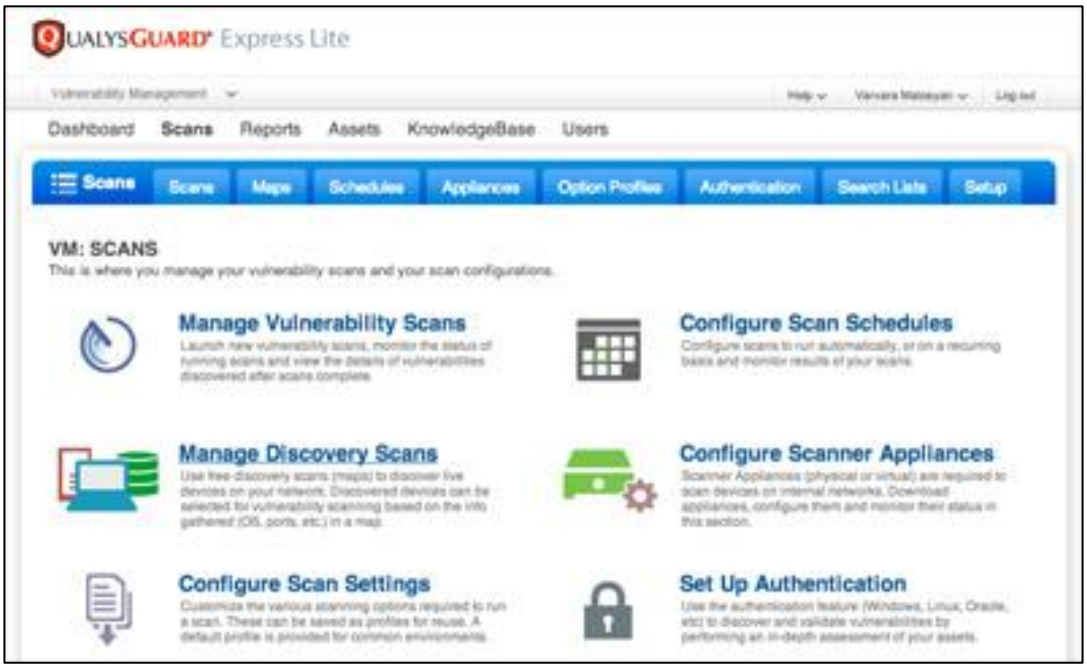


Figura 9 – Interface de Qualys Guard

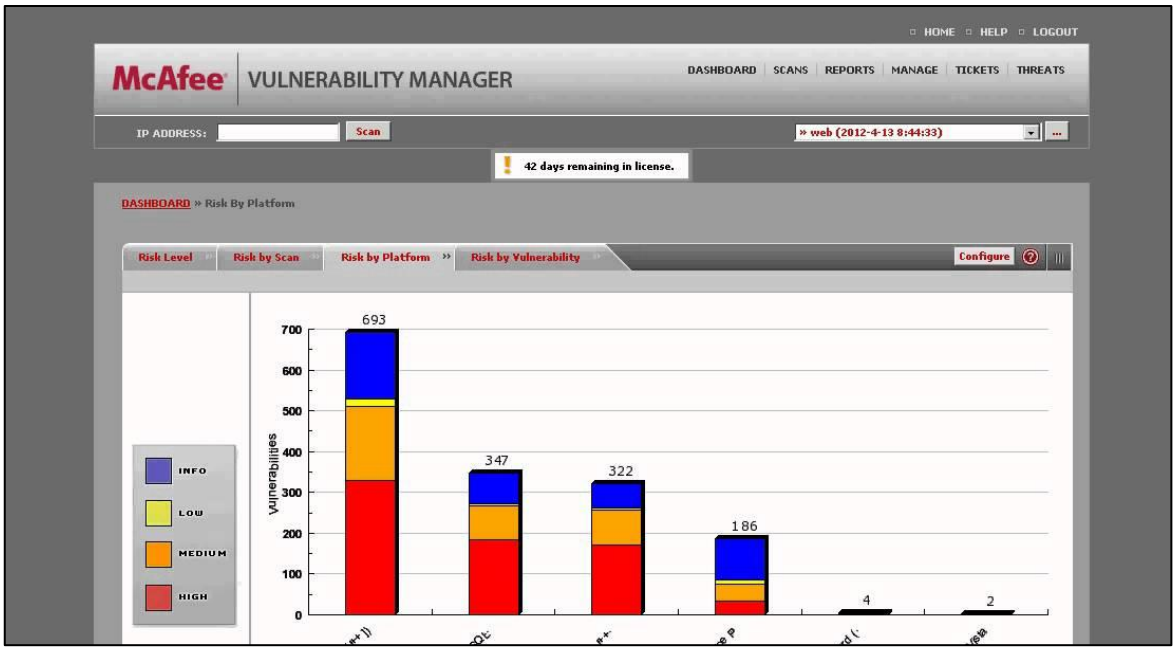


Figura 10 – McAfee Vulnerability Manager

Evaluación de las 2 Herramientas para la Red Informática de la SUNAT

	Puntaje Max. 100 pts.	Qualys Guard	McAfee Vulnerability Manager
ATRIBUTOS INTERNOS	**35**	**35**	**35**
Funcionalidad: ***Adecuación.*** Incluir el software necesario para las funciones de escaneo de las vulnerabilidades de las redes pública, privadas y DMZ's, la cual no debe de estar publica en internet.	5	5	5
Funcionalidad: ***Interoperatividad*** El software debe ser compatible con el hardware ofertado y debe permitir realizar un test de vulnerabilidad sobre un rango cómo mínimo de 250 dispositivos o direcciones de red IP físicas.	5	5	5
Funcionalidad: ***Interoperatividad*** Programar escaneos de vulnerabilidad de los dispositivos tanto de manera local como remota en toda la red corporativa.	5	5	5
Funcionalidad: ***Adecuación*** Incluir funciones de actualización constante de vulnerabilidades de manera automática y a demanda en cada uno de los componentes de la herramienta.	5	5	5
Funcionalidad: ***Exactitud*** Asignación de valores para identificación de la criticidad de las vulnerabilidades.	5	5	5
Funcionalidad: ***Exactitud*** Identificar los dispositivos conectados a la red y que usan una dirección IP.	5	5	5
Funcionalidad: ***Exactitud*** Identificación de servicios corriendo en puertos que no son estándar, por ejemplo HTTP corriendo en un puerto diferente al 80.	5	5	5

ATRIBUTOS EXTERNOS	**35**	**35**	**35**
Eficiencia: ***Utilización de recursos*** Debe contar con sistemas de notificación para el administrador.	7	7	7
Funcionalidad: ***Interoperatividad*** La solución debe contar con plantillas de escaneo intrusivos y no intrusivos.	7	7	7
Usabilidad: ***Operabilidad*** Permitir hacer filtros y búsquedas en la información de los activos por parámetros.	7	7	7
Usabilidad: ***Operabilidad*** Los escaneos podrán ser programados para ejecutarse recurrentemente o bajo demanda. Sin intervención de ningún usuario.	7	7	7
Capacidad de Mantenimiento: ***Conformidad de la facilidad de mantenimiento.*** Soporte directo del fabricante.	7	7	7
ATRIBUTOS DE USO	**30**	**30**	**30**
Seguridad Administración de la solución desde una interfase web segura.	10	10	10
Productividad El sistema deberá generar y asignar tickets de incidentes, que permitan dar seguimiento a los procesos de remediación.	10	10	10
Eficacia Asignación y monitoreo de las tareas de remediación.	10	10	10
PUNTAJE TOTAL	100	100	100

HERRAMIENTA TEST DE VULNERABILIDAD	**QUALYS GUARD**	**MCAFEE VULNERABILITY MANAGER**
Provisión, instalación, configuración, puesta en producción, capacitación. Incluye Hardware.	108,717.00	182,213.00
Garantía de buen funcionamiento, mantenimiento y soporte de la herramienta 3 años.	46,593.00	98,395.00
TOTAL Nuevos Soles S/. inc. IGV	155,310.00	280,608.00

5.3. ANALISIS Y DISEÑO DEL MODELO DE SEGURIDAD INFORMATICA BASADA EN PROSPECTIVA

5.3.1. ANALISIS DEL MODELO DE SEGURIDAD INFORMATICA BASADA EN PROSPECTIVA

Al ser la SUNAT una institución pública encargada de recaudar los tributos necesarios para el presupuesto del país, por lo que está de acuerdo al plan estratégico del Perú y las políticas tributarias, lo que quiere decir que va de acuerdo a los cambios que se dan en el mundo y le afectan la situación económica, social, cultural, política, etc.

El Modelo de Seguridad Informática a proponer debe reunir las siguientes características:

1. Establecer Escenarios para lograr que los objetivos y metas planteadas por la institución en el aspecto de tecnologías de información y comunicación se logren a largo plazo. Para esta propuesta se va a considerar 3 escenarios:
    A. Escenario Deseado (Riesgo Bajo)
    B. Escenario Probable (Riesgo Medio)
    C. Escenario Pesimista (Riesgo Alto)

2. Debe tener en cuenta el Modelo de Seguridad Informática “CIA”:
    A. Confidencialidad (Confidentiality)
    B. Integridad (Integrity)
    C. Disponibilidad (Availability)

3. Se debe tener en cuenta la norma ISO 27001:2013 con sus 14 secciones de acuerdo a su Anexo A:

- A.5: Políticas de Seguridad de la Información: hace referencia a los controles sobre cómo escribir y revisar políticas de seguridad.
- A.6: Organización de la Seguridad de la información: los controles se encargan de establecer responsables. Al mismo tiempo también se centra en dispositivos móviles y situaciones como la de teletrabajo.
- A.7: Seguridad de los Recursos Humanos: controles para las situaciones previas y posteriores referentes a la contratación y finalización de contrato de personal.
- A.8: Gestión de Recursos: establecidos para realizar inventario, clasificación de información y manejo de los medios de almacenamiento.
- A.9: Control de Acceso: control del acceso tanto a la información como a aplicaciones u otro medio que contenga información.
- A.10: Criptografía: controles para gestionar encriptación de información.
- A.11: Seguridad física y ambiental: controles para garantizar factores externos, seguridad de equipo y medios que puedan comprometer la seguridad.
- A.12: Seguridad Operacional: controles relacionados con gestión de la protección de malware o vulnerabilidades.
- A.13: Seguridad de las comunicaciones: Control sobre la seguridad de las redes, transmisión de información, mensajería…
- A.14: Adquisición, desarrollo y mantenimiento de Sistemas: controles que establecen los requisitos de seguridad en desarrollo y soporte.

- A.15: Relaciones con los proveedores: incluye lo necesario a la hora de realizar contratos y seguimiento a proveedores.
- A.16: Gestión de Incidentes en Seguridad de la Información: sirven para reportar eventos las debilidades, así como procedimientos de respuesta.
- A.17: Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio: referidos a la planificación de continuidad de negocio.
- A.18: Cumplimiento: control relacionado a la hora de identificar regulaciones relacionadas con seguridad de la información y hacer que se cumplan.

4. Se debe dividir el modelo en fases, así será más fácil su seguimiento y control por parte de la institución. Tener presente las 3 fases que desarrolla la propuesta de metodología para la implementación de la gestión automatizada de controles de seguridad:
    A. Planificación
    B. Implementación y Operación
    C. Medición

5. Asimismo, considerar el ciclo PHVA, una herramienta de gestión plenamente vigente, presentada en los años 50 por el estadístico estadounidense Edward Deming. Tras varias décadas de uso, este sistema o método de gestión de calidad se encuentra plenamente vigente (ha sido adoptado recientemente por la familia de normas ISO) por su comprobada eficacia para: reducir costos, optimizar la

productividad, ganar cuota de mercado e incrementar la rentabilidad de las organizaciones. Logrando, además, el mantenimiento de todos estos beneficios de una manera continua, progresiva y constante.

Las fases del ciclo PHVA (acrónimo compuesto por las iniciales de las palabras Planificar, Hacer Verificar y Actuar):

- Planificar: En la etapa de planificación se establecen objetivos y se identifican los procesos necesarios para lograr unos determinados resultados de acuerdo a las políticas de la organización. En esta etapa se determinan también los parámetros de medición que se van a utilizar para controlar y seguir el proceso.
- Hacer: Consiste en la implementación de los cambios o acciones necesarias para lograr las mejoras planteadas. Con el objeto de ganar en eficacia y poder corregir fácilmente posibles errores en la ejecución, normalmente se desarrolla un plan piloto a modo de prueba o testeo.
- Verificar: Una vez se ha puesto en marcha el plan de mejoras, se establece un periodo de prueba para medir y valorar la efectividad de los cambios. Se trata de una fase de regulación y ajuste.
- Actuar: Realizadas las mediciones, en el caso de que los resultados no se ajusten a las expectativas y objetivos predefinidos, se realizan las correcciones y modificaciones necesarias. Por otro lado, se toman las decisiones y acciones pertinentes para mejorar continuamente el desarrollo de los procesos.

5.3.2. DISEÑO DEL MODELO DE SEGURIDAD INFORMATICA BASADA EN PROSPECTIVA

Teniendo en cuenta los requerimientos establecidos en el punto 5.3.1., a continuación, se muestra el modelo de seguridad informática basada en prospectiva, la que está conformada en las siguientes fases:

FASE 1: DEFINICION DE ESCENARIOS

Se define los 3 escenarios que servirán de alcance para la evaluación de la seguridad informática en la institución, estos teniendo en cuenta un panorama de 3 años mínimo.

1.1. Escenario Deseado: Es a lo que realmente quiere llegar la institución, cumpliéndose todas las medidas necesarias y los controles.

1.2. Escenario Probable: Algunos problemas e inconvenientes que se podrían realizar a través del tiempo.

1.3. Escenario Pesimista: Es la situación en la cual se producen muchos problemas a pesar de los controles, siendo necesario aplicar planes de contingencia.

FASE 2: ESTABLECER LOS PUNTOS CRITICOS "CIA"

2.1. Confidencialidad: Se realiza una evaluación de los niveles de confidenciales que existe en la institución, sobre todo en los sistemas de información. El manejo de cuentas de usuarios, las claves, los registros de bitácora, enlace con otro dispositivo, etc.

2.2. Integridad: La información que viaja a través de la red informática por los distintos sistemas de información, debe mantenerse inalterables,

debiendo verificarse la seguridad de la línea y de los sistemas de información en el envío de datos.

2.3. Disponibilidad: Verificar los sistemas redundantes en la institución, ya sea equipos proveedores de electricidad, de internet o los equipos servidores donde se procesa los datos.

FASE 3: IMPLEMENTAR CICLO DE CALIDAD PHVA

1.1. Planificar

Realizar un plan de seguridad informática a través de un cronograma, donde se especifique los recursos y tiempos en que se realizara cada actividad.

1.2. Hacer

Se realiza las actividades programadas que estén dentro de las normas de seguridad informática.

1.3. Verificar

Se realizar el control del cumplimiento de las normas y los estándares, así como si algún riesgo planteado ha sucedido.

1.4. Actuar

Ante la ocurrencia de algún riesgo, se debe realizar las acciones programadas por las personas responsables. Esto permite controlarlo y retornar a un estado estable de los sistemas informáticos en la entidad.

FASE 4: CUMPLIMIENTO DE LA NORMA ISO 27001:2013

La institución debe cumplir con las 14 secciones de la norma ISO 27001:2013:

4.1. Políticas de Seguridad de la Información: hace referencia a los controles sobre cómo escribir y revisar políticas de seguridad.

4.2. Organización de la Seguridad de la información: los controles se encargan de establecer responsables. Al mismo tiempo también se centra en dispositivos móviles y situaciones como la de teletrabajo.

4.3. Seguridad de los Recursos Humanos: controles para las situaciones previas y posteriores referentes a la contratación y finalización de contrato de personal.

4.4. Gestión de Recursos: establecidos para realizar inventario, clasificación de información y manejo de los medios de almacenamiento.

4.5. Control de Acceso: control del acceso tanto a la información como a aplicaciones u otro medio que contenga información.

4.6. Criptografía: controles para gestionar encriptación de información.

4.7. Seguridad física y ambiental: controles para garantizar factores externos, seguridad de equipo y medios que puedan comprometer la seguridad.

4.8. Seguridad Operacional: controles relacionados con gestión de la protección de malware o vulnerabilidades.

4.9. Seguridad de las comunicaciones: Control sobre la seguridad de las redes, transmisión de información, mensajería.

4.10. Adquisición, desarrollo y mantenimiento de Sistemas: controles que establecen los requisitos de seguridad en desarrollo y soporte.

4.11. Relaciones con los proveedores: incluye lo necesario a la hora de realizar contratos y seguimiento a proveedores.

4.12. Gestión de Incidentes en Seguridad de la Información: sirven para reportar eventos las debilidades, así como procedimientos de respuesta.

4.13. Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio: referidos a la planificación de continuidad de negocio.

4.14. Cumplimiento: control relacionado a la hora de identificar regulaciones relacionadas con seguridad de la información y hacer que se cumplan.

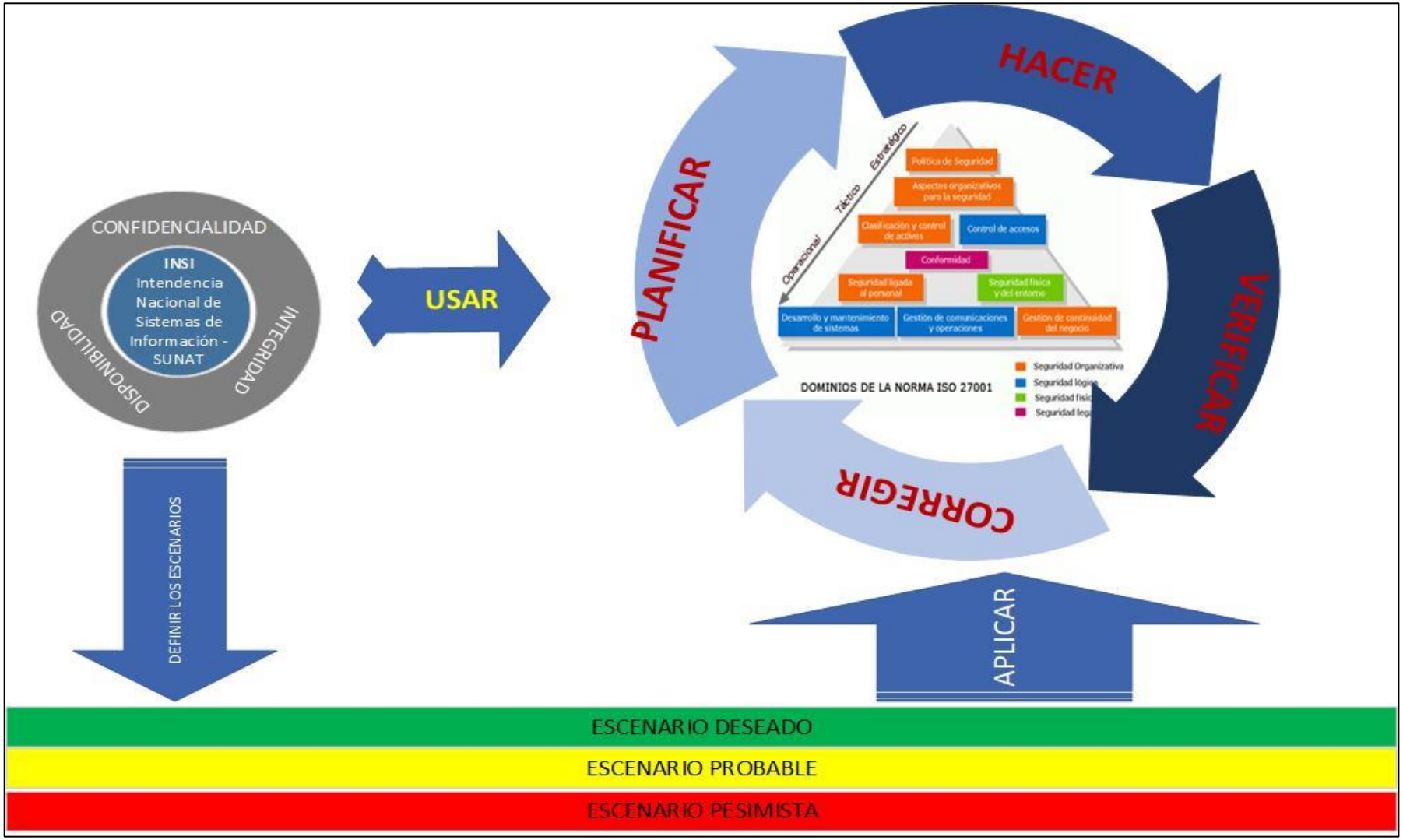


Figura 11 – Modelo de Seguridad Informática basada en Prospectiva

5.4. EVALUACION DEL MODELO DE SEGURIDAD INFORMATICA BASADA EN PROSPECTIVA

Para el caso de la red informática de la SUNAT – Lima se aplica el modelo de seguridad informática basada en prospectiva, teniendo en cuenta las 4 fases propuestas, de acuerdo a los siguientes detalles:

FASE 1: DEFINICION DE ESCENARIOS

Los escenarios que se definen para la red informática de la SUNAT – Lima son los siguientes:

1.1. **Escenario Deseado:** La red informática de la SUNAT debe contar con todas las medidas de seguridad necesarias, donde no exista ningún riesgo de accesos no autorizados, ni perdidas de información. Los equipos de seguridad instalados, son controlados en forma centralizada y restringen el ingreso de virus, DDoS, spams, etc. En resumen, la seguridad está plenamente controlada, y manteniendo un servicio permanente a los usuarios.

1.2. **Escenario Probable:** La seguridad se controlará en forma centralizada, pero se producirán accesos no autorizados ya sea por usuarios externos a la institución, como personal de la institución, generando caídas del sistema o perdida de información, que será rápidamente solucionada, ayudado por las copias de seguridad o software de recuperación. Hay brechas de tiempo donde las nuevas variantes de virus pueden ocasionar problemas, por lo que el acceso a la red interna debe ser restringido con sistema de seguridad adicionales.

1.3. **Escenario Pesimista:** En este escenario, la Sunat sufre un fallo de seguridad, que permite que las bases de datos se encuentren disponibles a usuarios externos, lo que pone en riesgo la información confidencial de millones de

contribuyentes. Los sistemas de seguridad fallan, como los antivirus, firewall, etc.; permitiendo que accedan a la red, y difundiendo software malicioso a los equipos de la red. Se hace necesario activar planes de contingencia para recuperar los servidores, la red informática, los sistemas de información, etc.

FASE 2: ESTABLECER LOS PUNTOS CRITICOS "CIA"

2.1. **Confidencialidad:** Se hace necesario contar con la información referente a la política sobre las cuentas de usuarios:

- Como se asignan los nombres de las cuentas de usuarios, se usan nombres y apellidos, se usan las iniciales, se usa algún número, o se deja libre a los usuarios establezcan el nombre de la cuenta. Esto es importante para evaluar la seguridad en el acceso. La asignación de la cuenta de usuario es con el nombre y apellido del usuario.
- En cuanto a las claves o passwords, se ha habilitado un mínimo en el tamaño de la clave, se establece que tienen que tener diferentes tipos de caracteres para evitar que sean adivinados, el tiempo de cambio tiene que ser máximo de 1 mes, se ha habilitado la autenticación en 2 pasos para un nivel mayor de seguridad. Actualmente las claves tienen que ser mínimo de 10 caracteres y utilizando diferentes tipos de caracteres.
- El acceso de los equipos a la red informática está basado en su MAC ADDRESS si son inalámbricos, adicional a la clave; y en el caso de equipos conectados a la red, el control se hace por su nombre.
- Todos los accesos a sistemas de información, bases de datos, etc., son con sus cuentas de usuarios y claves, no utilizando las cuentas por defectos que vienen en el producto que han sido deshabilitadas.

2.2. **Integridad:** La evaluación de la integridad es transmitiendo datos entre diferentes puntos de la red, a fin de comprobar que está llegando en forma oportuna y confiable, sin ningún tipo de alteración. Asimismo, el envío tiene que ser desde fuera de la red, por los usuarios de la Sunat, para comprobar la transmisión, ya sea a los sistemas de información como a las consultas que se realizan al portal web de la institución.

De las consultas y envíos realizados se puede apreciar que los datos llegan en forma correcta, actualizándose inmediatamente, por lo que la integridad está manteniéndose. Esta comprobación debe realizarse en forma continua a través de sistema de control.

También se debe verificar que los equipos informáticos se encuentren actualizados con los sistemas operativos y softwares, que le permitan trabajar más eficientemente y de forma segura.

2.3. **Disponibilidad:** Se tiene que comprobar la existencia de sistemas redundantes en la institución, como:

- Los servidores que tiene la institución, deben tener equipos redundantes en línea y con el sistema RAID, para que, en caso de alguna caída o falla, se puedan recuperar inmediatamente. Esto significa una inversión para la Sunat, pero favorece la alta disponibilidad, permitiendo que se logre el objetivo de 24x365, ósea disponibilidad las 24 horas, durante los 365 días del año.
- Se tiene que contar con línea de internet alternativas, ya sea por medio inalámbricos o fibra óptica, a fin de mantener la conexión de caso de alguna caída.

- En cuanto a la energía eléctrica, se debe contar con UPS para los equipos servidores, y un grupo electrógeno automático, que debe iniciarse apenas exista un corte de energía, a fin de que se mantenga estable el flujo de energía eléctrica, y los equipos no sufran daños.
- Asimismo, se deben contar con backup incrementales de toda la información que se almacene en las diferentes bases de datos de la institución, para la recuperación ante caídas.
- Se debe contar con máquinas virtuales de los servidores, lo que es más fácil y rápido de ponerse en funcionamiento.

FASE 3: IMPLEMENTAR CICLO DE CALIDAD PHVA

3.1. Planificar

Teniendo en cuenta 4 actividades principales, las que se desarrollaran en forma sucesiva a través del tiempo, las que engloban las diferentes normas de seguridad informática. Esto se realiza al iniciar el modelo, y es lo propuesto para la Red Informática de la Sunat.

Modo de	Nombre de tarea	Duración	Comienzo	Fin	Pred
	Determinacion de SituacionActual de la Red Informatica	30 días	vie 1/01/21	jue 11/02/21	
	Evaluar la seguridad logica implementada	30 días	vie 12/02/21	jue 25/03/21	1
	Evaluar la seguridad fisica implementada	30 días	vie 26/03/21	mié 5/05/21	2
	Realizar Pruebas de Caja Blanca, Gris y Negra	45 días	jue 6/05/21	mié 7/07/21	3
	Elaborar Planes de Contingencia	50 días	jue 8/07/21	mié 15/09/21	4
	Realizar las correciones a los sistemas de seguridad	30 días	jue 16/09/21	mié 27/10/21	5

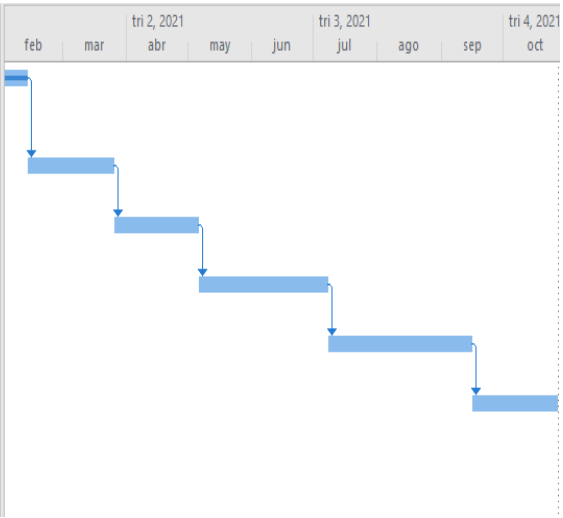


Figura 12 – Planificación de Actividades

3.2. Hacer

Se ejecutaron las actividades en la red informática de la Sunat según lo planificado, teniendo en cuenta la norma 27001:2013, esto con el fin de ir comprobando la factibilidad de su realización en forma progresiva. Su inicio fue en enero del 2021, y concluyó en octubre del 2021, teniendo en cuenta las restricciones por la pandemia y el trabajo remoto.

3.3. Verificar

Durante la etapa de HACER, se va verificando que se vaya cumpliendo los estándares y la existencia de riesgos, Se realiza el control del cumplimiento de las normas y los estándares, así como si algún riesgo planteado ha sucedido. Al finalizar la verificación se debe contar con una lista de riesgos detectados, ya sea a nivel físico como lógico, lo que servirá para estableces planes de contingencia o propuestas de solución permanentes.

3.4. Actuar

Ante la ocurrencia de riesgos, se hace la propuesta de planes de contingencia y propuestas de solución permanente, a fin de mitigar estos errores. Todo este trabajo que se va ejecutando tiene que tomar en cuenta los 3 escenarios planteados, sobre todo el escenario pesimista, donde se puede determinar un mayor número de riesgos.

FASE 4: CUMPLIMIENTO DE LA NORMA ISO 27001:2013

La norma ISO 27001:2013, establece 14 secciones o líneas de acción, que se debe tener en cuenta durante todo el desarrollo del modelo de seguridad informática, con el fin de tener un alcance sistémico de toda la red informática y sus componentes.

4.1. **Políticas de Seguridad de la Información:** La Sunat si cuenta con políticas de seguridad, pero que necesitan ser actualizadas permanentemente a fin de

controlar los nuevos riesgos informáticos que se van generando a lo largo del tiempo.

4.2. **Organización de la Seguridad de la información:** El responsable de determinar los controles necesarios a realizar en la red informática de Sunat, será la Oficina de Seguridad Informática, la cual determinará los responsables de las diferentes gerencias y oficinas, tanto en la seguridad física y lógica. Asimismo, se debe establecer los controles que se deben realizar a los usuarios que se conectan a la red informática a través de dispositivos móviles y teletrabajo (VPN).

4.3. **Seguridad de los Recursos Humanos:** Se establecen manuales de controles sobre el ingreso o contratación del personal, la forma de accesos a la red, la creación de sus cuentas, su horario; y así también se establece las reglas y acciones a la finalización del contrato de un trabajador que tenga acceso a la red, a fin de prevenir daños que pudiera causar.

4.4. **Gestión de Recursos:** Se realiza el inventario de todos los equipos informáticos con que cuenta la institución, asimismo se clasifica la información que se transfiere a través de las redes y se encuentran almacenadas en los servidores, habiendo información pública, sensible y privada. Los servidores de almacenamiento con información privada deben tener máxima protección.

4.5. **Control de Acceso:** Se implementa una bitácora para registrar el acceso de los usuarios a los diferentes recursos de la red informática en la institución, a fin de conocer el trabajo y cualquier falla o acceso no autorizado que se realice. Esto controla y protege la información, así como las aplicaciones.

4.6. **Criptografía:** Se utiliza un sistema de criptografía WPA3 en las comunicaciones WiFi dentro de la empresa, SSL para la transmisión en la

intranet, y protocolos avanzados como AES para enviar datos a través de la red informática.

4.7. **Seguridad física y ambiental:** Se implementan Firewall y Proxis para controlar el acceso externo no autorizado, esto a través de servidores dedicados que muestren en forma inmediata los ataques y riesgos que estén sucediendo en el borde la red institucional. Asimismo, se tiene que disponer de controles de seguridad biométricos para acceder físicamente a los equipos y que se encuentren los centros de datos en lugares alejados de los usuarios.

4.8. **Seguridad Operacional:** Se instala un servidor Antivirus a fin de controlar los malwares en la red informática institucional, y llegando a un mayor nivel se implementará un COS (Centro de Operaciones de Seguridad) donde se gestionan todas las vulnerabilidades en los recursos de la red.

4.9. **Seguridad de las comunicaciones:** Todos los equipos de comunicaciones tienen que tener claves o password, bajo la responsabilidad del encargado de la red informática, quien determinaba las reglas para su cambio y configuración. Los paquetes deben viajar en forma segura utilizando Ipsec, para evitar escuchas en la red.

4.10. **Adquisición, desarrollo y mantenimiento de Sistemas:** Los sistemas que tiene la institución son desarrolladas in house, los cuales pasan por procesos de auditoría para verificar el código, así no generen riesgos en su uso a través de la red informática. Se implementan reglas de auditoría para el desarrollo y su mantenimiento.

4.11. **Relaciones con los proveedores:** Se implementa las directivas de como relacionarse con los proveedores, para tener en cuenta las cláusulas necesarias de los contratos en cuanto a garantía, responsabilidad, fecha de entrega, etc. Así mismo se tiene que ir evaluando los proveedores y las nuevas ofertas.

4.12. **Gestión de Incidentes en Seguridad de la Información:** Se tendrá un registro de todos los riesgos presentes en los recursos de la red informática, así como los eventos posibles de acuerdo a los escenarios, estableciendo los responsables y las acciones de respuesta ante ese evento.

4.13. **Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio:** Durante los procedimientos que se realizan ante fallos o ataques en la red informática, se debe mantener el servicio mientras se recupera la red, utilizando equipos de resguardo.

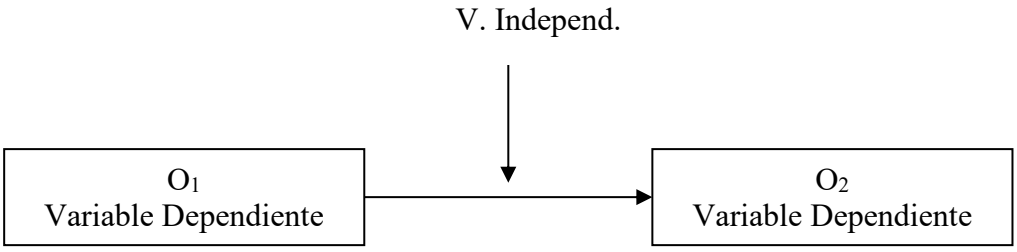
4.14. **Cumplimiento:** Todos los controles y acciones a realizar como parte del proceso de seguridad informática tienen que ser documentados, identificando a los responsables y las normas apropiadas. Esto permitirá programar su cumplimiento.

CAPITULO VI

DISCUSIÓN

6.1 CONTRASTACION

Para efectos de la Contrastación de la hipótesis propuesta en la presente investigación se utilizó el modelo de sucesión en línea.



La implementación de un Modelo de Seguridad Informática basada en Prospectiva Mejora la Protección de la Red Informática de la Sunat - Lima.

Dónde:

I = Modelo de Seguridad Informática basada en Prospectiva.

D = Protección de la Red Informática de la Sunat - Lima.

Estímulo = Facilidad de Implementación, Costos Reducidos y Nivel de Escenarios.

A través de esto se evaluó la variable dependiente, en este caso la Protección de la Red Informática de la Sunat – Lima, en base a los efectos de la aplicación de la variable independiente, que está representada por el Modelo de Seguridad Informática basada en Prospectiva.

6.2. EVALUACIÓN DE INDICADORES

Para la evaluación de los efectos, en la variable dependiente con respecto a la variable independiente, usamos tres indicadores, como son:

- **Facilidad de Implementación**
- **Costos Reducidos**
- **Nivel de Escenarios**

A continuación, se muestran los resultados de la evaluación de los indicadores.

FACILIDAD DE IMPLEMENTACION: RANGO [10 mejor – 5 regular – 0 peor]

Indicadores	**Facilidad de Implementación**	
	Sin la Solución	**Con la Solución**
Fases detalladas claramente	4	8
Alcance a todo la Red	4	8
Riesgos plenamente identificados	5	9
Personal responsable identificado	4	9
Activos Protegidos totalmente	3	8
Promedio Final	**20**	**42**

Fuente: Datos de Pruebas realizadas en campo.

Interpretación

El resultado obtenido luego de las pruebas realizadas, nos permite apreciar que con el Modelo de Seguridad Informática basada en Prospectiva a través de su

implementación se mejora la protección de la red informática de la Sunat – Lima, esto teniendo en cuenta los 3 escenarios y la norma de seguridad, en respuesta a las fases detalladas, alcance a la red, riesgos identificados, personal responsable y activos protegidos.

COSTOS REDUCIDOS: RANGO [10 mejor – 0 peor]

Indicadores	**Costos Reducidos**	
	Sin Solución	**Con Solución**
Costos Reducidos de Recuperación de Servidores	4	9
Costos Reducidos de Recuperación de Equipos de Comunicación	5	9
Costos Reducidos de Capacitación del Personal	5	9
Costos Reducidos de Implementación de Plan de Contingencias	4	8
Costos Reducidos de Perdidas de Datos	5	8
Promedio Final	**23**	**43**

Fuente: Datos de Pruebas realizadas en campo.

Interpretación

El resultado obtenido luego de las pruebas realizadas, nos permite apreciar que con el Modelo de Seguridad Informática basada en Prospectiva a través de su implementación se reducen los costos, incrementando el nivel de la protección de la red informática de la Sunat – Lima. Al tener un modelo de seguridad donde se establece las actividades a realizar, se logra evitar riesgos inesperados, con lo cual los costos que ocurrían antes ya no se darán o serán en menor nivel.

NIVEL DE ESCENARIOS: RANGO [10 mejor – 0 peor]

Indicadores	**Nivel de Escenarios**	
	Sin Solución	**Con Solución**
Numero de Escenarios	4	8
Escenario Pesimista	0	9
Escenario Normal	5	7
Escenario Optimista	3	9
Alcance de los escenarios	4	8
Promedio Final	**16**	**41**

Fuente: Datos de Pruebas realizadas en campo.

Interpretación

El resultado obtenido luego de las pruebas realizadas, nos permite apreciar que con el Modelo de Seguridad Informática basada en Prospectiva se logra tener presente 3 escenarios, donde se considera diferentes niveles de riesgo, lo que hace que el nivel de la protección de la red informática de la Sunat – Lima sea superior. No sucede lo mismo cuando no se considera el modelo, ya que la

presencia de mayor número de riesgo es más probable y consiguientemente menor protección.

6.3. CONCLUSIÓN:

Por los resultados de los tres indicadores de evaluación: Facilidad de Implementación, Costos Reducidos y Nivel de Escenarios, se puede inducir y determinar que el modelo de Seguridad Informática basada en prospectiva mejora la protección de la Red Informática de la Sunat – Lima, al tener presente acciones y riesgos, antes de que puedan suceder y dentro de la norma ISO.

CONCLUSIONES

1. Se implementó el Modelo de Seguridad Informática basada en Prospectiva para mejorar la Protección de la Red Informática de la Sunat - Lima, basado en 3 escenarios, el modelo de calidad PHVA, los puntos críticos “CIA” y la Norma ISO 27001:2013, permitiendo estar preparados ante riesgos y lograr la protección de la red informática de la Sunat - Lima.
2. Se identificaron las deficiencias de seguridad que existen en la red informática de la Sunat – Lima, a fin de tenerlos en cuenta en el modelo de seguridad informática basada en prospectiva.
3. Se analizó los requerimientos de seguridad que deben ser considerados en el modelo que se estaba implementando, logrando minimizar los riesgos.
4. El Diseño del Modelo de Seguridad Informática basada en prospectiva tuvo en cuenta los recursos con los que cuenta Sunat – Lima, como son el hardware, software y recursos humanos.
5. Se realizó una evaluación de cumplimiento de las fases y actividades propuestas en el Modelo de Seguridad Informática, de acuerdo a la red informática de Sunat - Lima.

RECOMENDACIONES

1. Realizar capacitación al personal especialista de informática de la SUNAT – LIMA, para la implementación del modelo de seguridad informática basada en prospectiva.
2. Se debe definir los responsables de las diferentes actividades plasmadas en el modelo de seguridad informática que se va a implementar en la SUNAT – LIMA, a fin de hacer un mejor seguimiento sobre el desarrollo.
3. Se debe anualmente evaluar el modelo a fin de encontrar las deficiencias o errores a corregir, para ir optimizando el modelo.

BIBLIOGRAFIA

a) BIBLIOGRAFÍA BÁSICA

1. Hernandez R., Fernandez C. y Baptista P. (1991), Metodología de la Investigación, México, McGraw - Hill Interamericana de México.
2. Bernal Torres, Cesar Augusto. (2000) Metodología de la Investigación para Administración y Economía. Santa fe de Bogotá, Colombia. Pearson Educación de Colombia Ltda.
3. Rivas Galarreta, Enrique. (1995). Metodología de la Investigación Bibliográfica. Perú: Ed. Trujillo. 2da Edición.

b) BIBLIOGRAFÍA ESPECIALIZADA

4. VON BERTALANFFY LUDWIG. Teoría General de los Sistemas, 1989, Editorial Fondo Cultura Económica, 7ma Edición, México.
5. JIMENO G., MARIA TERESA. “Hacker“, Ed. Anaya, España, 2009.
6. TANENBAUM A. & WETHERALL D. "Redes de Computadoras", Pearson Educación, 5ta Edición, México, 2012.
7. RAMIO AGUIRRE, JORGE “Seguridad Informática y Criptografía v 4.1”, Dpto. de Publicaciones E.U.I., 2006.
8. BEINSTEIN JORGE. Manual de Prospectiva: Guía para el Diseño e Implementación de Estudios Prospectivos, 2016, Buenos Aires: Ministerio de Ciencia, Tecnología e Innovación Productiva

ANEXOS

ANEXO 01

ENCUESTA PARA EVALUAR EL MODELO DE SEGURIDAD INFORMATICA BASADA EN PROSPECTIVA PARA MEJORAR LA PROTECCION DE LA RED INFORMATICA DE LA SUNAT - LIMA

COLOCAR UN VALOR DENTRO DEL RANGO: [10 mejor – 5 regular - 0 peor]

FACILIDAD DE IMPLEMENTACION

1) **Las fases se detallan claramente: …….**
2) **Se logra determinar el alcance a toda la red: …….**
3) **Los riesgos se identifican plenamente: ……..…**
4) **El Personal responsable está identificado: …….**
5) **Los activos a proteger se encuentran identificados: ….……..**

COSTOS REDUCIDOS

6) **Recuperación de Servidores: …….**
7) **Recuperación de Equipos de Comunicación: ……**
8) **Capacitación del Personal: …….**
9) **Implementación de Plan de Contingencias: …….**
10) **Perdidas de Datos: ……..**

NIVEL DE ESCENARIOS

11) **Numero de Escenarios Identificados: …….**
12) **Identificación de Escenario Pesimista: …….**
13) **Identificación de Escenario Normal: …….**
14) **Identificación de Escenario Optimista: …….**
15) **Alcance de los Escenarios: ……**

Tesis Completa

INFORME DE ORIGINALIDAD

29%	29%	0%	19%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	scielo.sld.cu Fuente de Internet	3%
2	1library.co Fuente de Internet	3%
3	share.pdfonline.com Fuente de Internet	3%
4	Submitted to Universidad Catolica Los Angeles de Chimbote Trabajo del estudiante	2%
5	es.wikipedia.org Fuente de Internet	2%
6	www.sunat.gob.pe Fuente de Internet	2%
7	www.pmg-ssi.com Fuente de Internet	2%
8	www.slideshare.net Fuente de Internet	2%

9	seguridadinformatica-luisdavidaguilar.blogspot.com Fuente de Internet	1 %
10	coggle.it Fuente de Internet	1 %
11	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	1 %
12	sunatkarla.blogspot.com Fuente de Internet	1 %
13	www.coursehero.com Fuente de Internet	1 %
14	docplayer.es Fuente de Internet	1 %
15	www.powershow.com Fuente de Internet	1 %
16	Submitted to Universidad Católica de Santa María Trabajo del estudiante	1 %
17	dspace.unitru.edu.pe Fuente de Internet	1 %
18	repositorio.unprg.edu.pe Fuente de Internet	1 %
19	www.euroinnova.edu.es Fuente de Internet	1 %