

Resolución Directoral

Lima, 05 de octubre del 2018

002-2018-VIVIENDA/OGEI

VISTOS:

El informe N° 026-2018-VIVIENDA/OGEI-GFN del Oficial de Seguridad de la Información y el informe N° 069-2018-VIVIENDA/OGEI del Director de la Oficina de Tecnología de la Información;

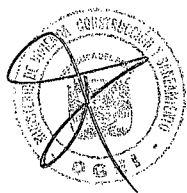
CONSIDERANDO:

Que, las Normas de Control Interno aprobadas mediante Resolución de Contraloría N° 320-2006-CG, en el numeral 1.3 Administración Estratégica del rubro Normas Básicas para el Ambiente de Control, señala que las entidades del Estado requieren la formulación sistemática y positivamente correlacionada con los planes estratégicos y objetivos para su administración y control efectivo, de los cuales se derivan la programación de operaciones y sus metas asociadas, así como su expresión en unidades monetarias del presupuesto anual; agregando en su Comentario 03 que los productos de las actividades de formulación, cumplimiento, seguimiento y evaluación deben estar formalizadas en documentos debidamente aprobados y autorizados, con arreglo a la normativa vigente respectiva;

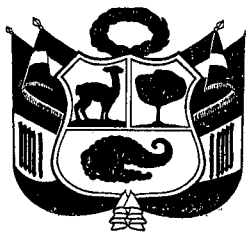
Que, mediante Decreto Supremo N° 004-2013-PCM, se aprueba la Política Nacional de Modernización de la Gestión Pública, siendo el principal instrumento orientador de la modernización de la gestión pública en el Perú, que establecerá la visión, los principios y lineamientos para una actuación coherente y eficaz del sector público, al servicio de los ciudadanos y el desarrollo del país; agregando en el numeral 3.2 los ejes transversales de la Política de Modernización en el Gobierno Electrónico;

Que, de acuerdo al reglamento de Organización y Funciones del Ministerio de Vivienda, Construcción y Saneamiento MVCS, aprobado mediante Decreto Supremo N° 010-2014-VIVIENDA, se establece en el artículo N° 55 que la Oficina General de Estadística e Informática – OGEI, es el órgano encargado responsable de la gestión de la infraestructura de tecnologías de la información y comunicaciones, así como planificar, desarrollar, implantar y gestionar proyectos de desarrollo de soluciones basadas en tecnologías de la información y comunicación para la administración y gestión de la informática estadística sectorial;

Que, mediante Resolución Ministerial N° 004-2016-PCM, se aprueba la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición" en todas las



REPUBLICA DEL PERÚ



Resolución Directoral

entidades integrantes del Sistema Nacional de Informática, con la finalidad de coadyuvar con la infraestructura del Gobierno Electrónico, por considerar a la seguridad de la información, como un componente crucial para dicho objetivo;

Que, mediante Resolución Ministerial RM-348-2017-VIVIENDA se aprobó el Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETIC) 2017-2021 del Ministerio de Vivienda, Construcción y Saneamiento, que entre sus objetivos estratégicos ha establecido: "garantizar la seguridad y privacidad de la información del sector", entre otros;

Que, con Resolución Ministerial N° 374-2017-VIVIENDA, del 2 de octubre del 2017, se aprobó el documento de gestión interno denominado "Política de Seguridad de la Información del Ministerio del Ministerio de Vivienda, Construcción y Saneamiento", que tiene como objetivo establecer el marco general de gestión para proteger la información del Ministerio, defendiendo directrices generales de actuación que aseguren el tratamiento adecuado de los riesgos y que conduzcan al fortalecimiento de una cultura institucional en seguridad de la información;

Que, estando a lo expuesto y conforme a la propuesta remitida por el Oficial de Seguridad de la Información, contando con la opinión favorable de la Oficina de Tecnologías de la Información, corresponde expedir la presente Resolución aprobando el Plan de Seguridad de Información del MVCS, según lo expresado en los documentos de vistos;

SE RESUELVE:

Artículo 1.- Aprobar el "Plan de Seguridad de la Información del MVCS", el mismo que forma parte integrante de la presente resolución.

Artículo 2.- Disponer la publicación de la presente Resolución en el Portal Institucional del Ministerio de Vivienda, Construcción y Saneamiento (www.gob.pe/vivienda).

Regístrese y comuníquese

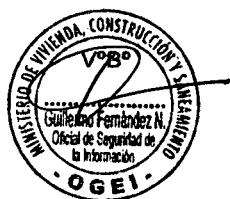
Ing. Daniel Alfonso Camacho Zárate
Director General
Oficina General de Estadística e Informática
Ministerio de Vivienda, Construcción
y Saneamiento

Plan de Seguridad de la Información

OFICINA GENERAL DE ESTADÍSTICA E INFORMÁTICA

Ing. Guillermo Fernández Namuche

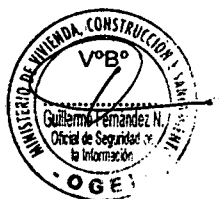
Oficial de Seguridad de la Información



RESUMEN

El presente plan tiene como objetivo desarrollar la Seguridad de la Información para el Ministerio de Vivienda, Construcción y Saneamiento – MVCS, orientado a reducir los riesgos a los que está expuesta la información hasta unos niveles aceptables a partir del análisis del inventario de activos, aplicando la metodología de Análisis y Gestión de Riesgos MAGERIT, la norma ISO/IEC 27001 y 27002 como base para la implementación del Sistema de Gestión de Seguridad de la Información, basado en el concepto de mejora continua.

Dicho Plan de Seguridad tomará como insumos el análisis diferencial en materia de seguridad de la información del MVCS y los resultados del análisis de riesgos para plantear un conjunto de proyectos, que permitan generar la base del Sistema de Gestión de Seguridad de la Información. Adicionalmente se entrega el modelo de madurez en materia de seguridad de la información del MVCS, usando los controles NTP-ISO/IEC 27002:2017.



Contenido

RESUMEN

1. INTRODUCCIÓN

- 1.1 Planteamiento del problema
- 1.2 Alcance del Plan de Seguridad de la Información
- 1.3 Alcance del SGSI
- 1.4 Objetivos del Plan de Seguridad
- 1.5 Metodología utilizada para el desarrollo del plan
- 1.6 Socialización
- 1.7 Concientización
- 1.8 Oficialización

2. MARCO NORMATIVO: ISO 27000

- 2.1 Norma NTP-ISO/IEC 27001:2014
- 2.2 Norma NTP-ISO/IEC 27002:2017

3. ENTIDAD OBJETO DE ESTUDIO: Ministerio de Vivienda, Construcción y Saneamiento

- 3.1 Infraestructura del MVCS
- 3.2 Composición organizativa (Oficina General de Estadística e Informática)
- 3.3 Sistemas de Información del MVCS
- 3.4 Infraestructura Tecnológica del MVCS
- 3.5 Análisis diferencial del MVCS con respecto a NTP-ISO/IEC 27001:2014 + NTP-ISO/IEC 27002:2017

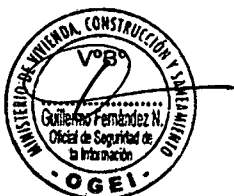
4. SISTEMA DE GESTIÓN DOCUMENTAL

- 4.1 Esquema documental del SGSI
 - 4.1.1 Política de Seguridad de la Información
 - 4.1.2 Procedimiento de auditorías internas
 - 4.1.3 Gestión de indicadores
 - 4.1.4 Gestión de roles y responsabilidades
 - 4.1.5 Metodología de análisis de riesgos
 - 4.1.6 Declaración de aplicabilidad

5. ANÁLISIS DEL RIESGO

- 5.1 Caracterización de los activos
 - 5.1.1 Identificación de los activos
 - 5.1.2 Valoración de los activos
- 5.2 Caracterización de las amenazas

6. PROPUESTA DEL PLAN



6.1 Proyectos propuestos

- 6.1.1 Plan de capacitación sobre seguridad de la información y SGSI a todos los responsables que tratan la información
- 6.1.2 Revisión de nuevos roles y funciones de seguridad en la Oficina de Tecnologías de la Información.
- 6.1.3 Cifrado de discos duros de dispositivos móviles (portátiles, tabletas y móviles) de personal que maneje información sensible.
- 6.1.4 Actualización del Plan de Contingencia de OGEI.
- 6.1.5 Selección, adquisición e implementación de un sistema gestor de eventos y seguridad de la información (SIEM).
- 6.1.6 Selección, adquisición e implementación de un sistema de prevención y detección de intrusos para la red de datos del MVCS (IDS e IPS).
- 6.1.7 Selección e implementación de un servicio de Ethical Hacking para la detección de vulnerabilidades en el Centro de Datos y la red de datos del MVCS.
- 6.1.8 Parametrización del sistema de Mesa de Ayuda para que incluya la gestión de incidentes.
- 6.1.9 Selección, adquisición e implementación de un DLP (Data Loss Prevention).
- 6.1.10 Compra de memorias USB cifradas para uso en el Centro de Datos y dependencias que manejan información sensible.
- 6.1.11 Hardening (fortalecimiento) de servidores del MVCS.
- 6.1.12 Proceso de archivado, backup y recuperación en la nube.

7. AUDITORÍA DE CUMPLIMIENTO

- 7.1 Metodología
- 7.2 Nivel de madurez del SGSI del MVCS.

8. CONCLUSIONES

BIBLIOGRAFÍA

- Norma Técnica Peruana NTP-ISO/IEC 27001:2014. Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias – INDECOPI
- Norma Técnica Peruana NTP-ISO/IEC 27002:2017. Dirección de Normalización INACAL
- Consejo Superior de Administración Electrónica de España. (2012). MAGERIT - versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid: Ministerio de hacienda y Administraciones Públicas.
- Wikipedia. (s.f.). Obtenido de https://es.wikipedia.org/wiki/ISO/IEC_27000-series

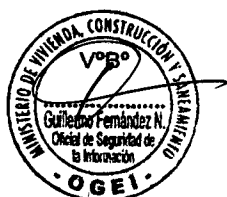


LISTA DE IMAGENES

- Figura 1. Metodología usada para el Plan de Seguridad de la Información en el MVCS.
- Figura 2. Contenido de NTP-ISO/IEC 27001:2014 de acuerdo al ciclo de Deming. Construcción propia.
- Figura 3. Organigrama funcional de la Oficina de Tecnología de la Información de OGEI. Elaboración propia.
- Figura 4. Mapa de enlaces de red del MVCS.
- Figura 5. Gráfico de radial. Cumplimiento de la norma SGSI anterior al Plan de Seguridad de la Información.
- Figura 6. Gráfico de radial de estado de los controles del Anexo 1 de NTP-ISO/IEC 27001:2014.
- Figura 7. Método de análisis del riesgo. Tomado de MAGERIT
- Figura 8. Nivel de madurez de los controles NTP-ISO/IEC 27001:2014

LISTA DE TABLAS

- Tabla 1. Familia ISO/IEC 27000.
- Tabla 2. Norma NTP-ISO/IEC 27001:2014 en el MVCS.
- Tabla 3. Evaluación de los controles NTP-ISO/IEC 27001:2014.
- Tabla 4. Valoración de los activos
- Tabla 5. Clasificación de amenazas
- Tabla 6. Valoración del impacto
- Tabla 7. Valoración del riesgo
- Tabla 8. Cartera de Proyectos Estratégicos del PETIC del MVCS 2017-2021
- Tabla 9. Proyectos propuestos y su impacto en NTP-ISO/IEC 27001:2014 y Matriz de riesgos a mitigar
- Tabla 10. Procedimientos nuevos a elaborar para soportar el SGSI del MVCS
- Tabla 11. Criterios de evaluación del modelo de madurez del SGSI
- Tabla 12. Modelo de madurez SGSI de acuerdo con los controles NTP-ISO/IEC 27002:2017
- Tabla 13. Controles de seguridad NTP-ISO/IEC 27001:2014
- Tabla 14. Síntesis de cumplimiento de Dominios, Objetivos de control y controles NTP-ISO/IEC 27002:2017



1. INTRODUCCIÓN

Las tecnologías de la información y las comunicaciones vienen dando un gran soporte a los procesos organizativos de las entidades, tanto en el apoyo al funcionamiento como para la toma de decisiones estratégicas que propendan el cumplimiento de sus metas. La mayoría de los procesos son soportados, gestionados y automatizados por sistemas informáticos. En una entidad del estado, dichos sistemas de información cuentan con interfaces que permiten a los ciudadanos, realizar consultas y modificación de información en cualquier lugar donde se encuentren.

En dicho escenario de alta conectividad, que la mayoría de los procesos organizativos en las entidades del estado se soportan en su infraestructura tecnológica, se cuenta con innumerables ventajas, pero a la vez, conlleva un conjunto de riesgos en el manejo de datos confidenciales y en la disponibilidad de los servicios que presta el ministerio y hace que la seguridad de la información sea uno de los puntos fundamentales a tener en cuenta para la continuidad de los procesos relacionados con su misión crítica y la operatividad en los niveles acordados a pesar de dichos riesgos.

Organizaciones del tamaño de un ministerio deben manejar el tema de la seguridad de la información de forma metodológica, planificada, con enfoque de continuidad del negocio y de mejora continua. Además es fundamental tener en cuenta su participación en el entorno en la que se deben obedecer regulaciones, garantizar la protección de los datos de carácter personal de los colaboradores, ciudadanos y de empresas proveedoras con las que se tiene relación de carácter contractual.

El desafío del MVCS en seguridad de la información es por tanto, encontrar e implementar una metodología que conduzca al desarrollo de su Sistema de Gestión de Seguridad de la Información, que provea los niveles de seguridad requeridos, y que sustenten la confianza necesaria a la misma institución, a sus proveedores y a sus trabajadores (colaboradores civiles y directivos), teniendo en cuenta:

- Las necesidades de los procesos del negocio con respecto a la información, aplicaciones y servicios telemáticos.
- El uso eficaz y eficiente de los recursos tecnológicos como soporte a dichos procesos de negocio.
- El desarrollo de un enfoque estratégico, racional económicamente y proactivo para la evaluación y tratamiento de riesgos, con criterios amplios y basados en costo-beneficio.

1.1 Planteamiento del problema

Debido al tamaño del ministerio, a la cantidad de procesos soportados por la tecnologías de información, a la legislación actual peruana, la cual obliga al MVCS a velar por la protección de los datos personales de los servidores civiles y ciudadanía, además de los nuevos problemas que está enfrentando el ministerio en materia de Tecnologías de la Información y Comunicaciones - TIC, se hace fundamental el planteamiento de una estrategia en materia de la seguridad de la información.



La Norma Técnica Peruana ISO/IEC 27001 en su versión 2014 se adecúa de forma coherente al sistema de calidad del MVCS, debido a los cambios que se realizaron respecto a la versión anterior y además es certificable, por lo que la alta dirección se encuentra interesada en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).

Pero dicha implementación debe ser realizada en el marco de un diagnóstico del estado actual en el que se encuentra el ministerio y de la mano de una metodología adecuada para realizar dicha implementación, la cual será implantada a través de un conjunto de proyectos de seguridad de la información.

El objetivo de dichos proyectos será encaminado a reducir los riesgos a los que se expone la institución a unos niveles aceptables.

1.2 Alcance del Plan de Seguridad de la Información

El alcance que tiene el Plan de Seguridad viene determinado en la importancia que el Ministerio plantea para la implementación del Sistema de Gestión de Seguridad de la Información. Con la implementación del Plan de Seguridad se persigue la identificación de riesgos que corren los activos de la organización, los cuales deben ser identificados, cuantificado su impacto y con la propuesta de un plan de acción para hacer frente, evaluando el impacto residual que la implantación de dicho plan lleva consigo.

1.2.1 Interesados

El Despacho Ministerial en su calidad de órgano máximo del MVCS, según el manual de operaciones vigente, debería ser el principal interesado del proyecto durante sus etapas de planeamiento, gestión, mejora continua y auditorías del SGSI, puesto que es un sistema de gestión transversal a todo el MVCS. El establecimiento de la máxima autoridad orgánica posible como interesado del proyecto, está establecido en los estándares internacionales ISO relacionados a la seguridad de la información sobre todo en las ISO's 27001 y 27002.

El Ministerio no tiene un SGSI implantado y no se han realizado estudios previos en el área de seguridad para tomar de base, por tanto el análisis respecto a los activos, sus amenazas y los planes de acción se desarrollarán en el presente plan.

1.3 Alcance del SGSI

La propuesta de alcance para el SGSI para el desarrollo del Plan de Seguridad de la Información es la siguiente:

“Los sistemas de información que sustentan los procesos críticos del negocio para la provisión del Centro de Datos Principal”

1.4 Objetivos del Plan de Seguridad

Objetivos General

Plantear el Plan de Seguridad para el MVCS orientado a reducir los riesgos a los que está expuesta la información hasta unos niveles aceptables a partir del



análisis del inventario de activos, aplicando la metodología de Análisis y Gestión de Riesgos MAGERIT, la NTP-ISO/IEC 27001 y 27002, como base para la implementación del Sistema de Gestión de Seguridad de la Información, basado en el concepto de mejora continua.

Objetivos Específicos

- Revisar el estado actual del MVCS respecto a la seguridad de la información, con base a la NTP-ISO/IEC 27001 y NTP-ISO/IEC 27002.
- Revisar la correcta implementación de las herramientas de seguridad de la información implementadas actualmente.
- Revisar el cumplimiento de la regulación y la normatividad en materia de seguridad de la información por parte del Ministerio.
- Realizar el inventario de activos del Ministerio en materia de seguridad de la información.
- Proponer mejoras al sistema de gestión de incidentes.
- Definir roles y responsabilidades de propietarios de activos.
- Analizar las amenazas a los que están dispuestos dichos activos.
- Definir el impacto potencial de dichas amenazas en los activos.
- Proponer un plan de acción para luchar contra dicha amenazas.
- Desarrollar la auditoría de cumplimiento de acuerdo al modelo de madurez resultado de la revisión de los controles de la NTP-ISO/IEC 27001:2014

1.5 Metodología utilizada para el desarrollo del plan

El Plan de Seguridad resultado del presente plan, pretende ser una hoja de ruta para que el Ministerio inicie su proceso de implementación del Sistema de Gestión de la Seguridad de la Información, objetivo que la misma se ha fijado como parte de los planes de acreditación para garantizar la calidad de sus procesos, basándose en los estándares de Alta Calidad propuestos por el estado. El Ministerio se encuentra realizando esfuerzos en materia de seguridad de la información y es por ello que el Plan de Seguridad servirá como modelo para la gestión adecuada en el marco regulatorio y legal peruano en materia de seguridad de la información.

El desarrollo del plan se abordó por medio de un esquema metodológico de implementación por fases, y cada una de las cuales busca abordar un objetivo específico, las cuales se sintetizan en el siguiente diagrama:



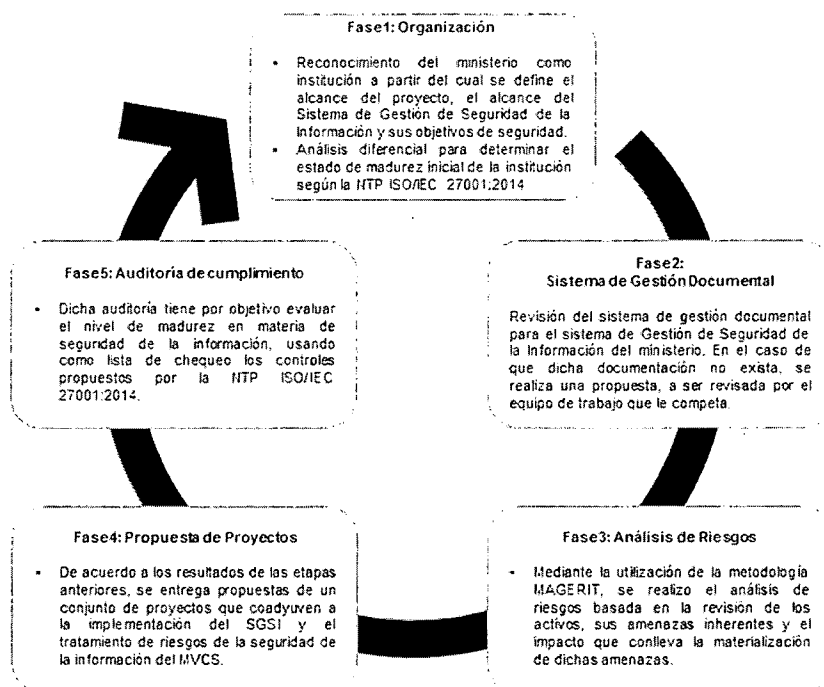


Figura 1. Metodología usada para el Plan de Seguridad de la Información en el MVCS

1.6 Socialización

La socialización del SGSI permitirá que las partes interesadas del SGSI sean informadas de su existencia mediante un procedimiento que deberá ser establecido por el Comité de Gestión de Seguridad de la Información. Asimismo, se hará entrega de políticas, procedimientos, acuerdos y otros documentos relacionados a sus actividades y necesarios para salvaguardar la privacidad y seguridad de la información.

Dentro del MVCS se deberán realizar las siguientes actividades de manera oficial y permanente:

- 1.6.1 Entrega de un kit de documentos a todo el personal contratado nuevo, donde se incluya:
 - a. Política de seguridad de la información del MVCS.
 - b. Acuerdo de confidencialidad.
 - c. Otras políticas de seguridad de la información existentes en el momento de la incorporación del nuevo personal.
- 1.6.2 Sesiones de inducción mensuales a todo el personal nuevo incorporado al MVCS.
- 1.6.3 Publicaciones de todas las políticas y procedimientos de seguridad de la información en la intranet del MVCS.

1.7 Concientización

La concientización de las partes interesadas del SGSI, sobre todo del personal vinculado a tiempo completo o parcial al MVCS, es un proceso de mejora continua que debe realizarse mediante campañas de difusión masiva y aulas virtuales. Este proceso contribuirá con la cultura organizacional y los objetivos estratégicos del MVCS.

1.8 Oficialización

Todas las políticas, procedimientos, planes, manuales, acuerdos y reglamentos asociados a la seguridad de la información, deberán oficializarse mediante Resolución Directoral como mínimo, y serán equivalentes a las siguientes categorías documentarias:

	Documento	Categoría documentaria
1	Política	Política
2	Plan	Plan
3	Procedimiento	Directiva
4	Acuerdo	Acta
5	Manual	Instructivo interno
6	Reglamento	Instructivo interno

2. MARCO NORMATIVO: ISO 27000

Las normas ISO/IEC 27000 es un conjunto de estándares que han sido publicados por la Organización Internacional de Estandarización - ISO y la Comisión Internacional Electrotécnica – IEC que contiene las mejores prácticas para la seguridad de la información recomendadas para desarrollar, implementar y mantener Sistemas de Gestión de la Seguridad de la Información (Wikipedia, s.f.).

Las normas de la familia ISO/IEC 27000 incluyen:

ISO/IEC 27000	Definiciones y vocabulario
ISO/IEC 27001	Requerimiento para un SGSI
ISO/IEC 27002	Técnicas de seguridad. Código de práctica para controles de la seguridad de la información.
ISO/IEC 27003	Guía de implementación de un SGSI
ISO/IEC 27004	Métricas para la gestión de seguridad de la información
ISO/IEC 27005	Gestión de riesgos en seguridad de la información
ISO/IEC 27006	Requisitos para la acreditación de las organizaciones que certifican las empresas con sistemas de gestión de seguridad de la información
ISO/IEC 27007	Guía para realizar la auditoría del SGSI
ISO/IEC 27016	Norma para el análisis financiero y económico de equipos y procedimientos de seguridad de la información
ISO/IEC 27017	Guía de seguridad para Cloud Computing
ISO/IEC 27035	Gestión de incidentes de seguridad de la información

Tabla 1: Familia ISO/IEC 27000

2.1 NTP ISO/IEC 27001:2014

La presente Norma Técnica Peruana ha sido elaborada por el Comité Técnico de Normalización de Codificación electrónico de datos, utilizando como antecedentes a la norma ISO/IEC 27001:2013 Information Technology – Security techniques – Information security management systems requirements y la ISO/IEC 27001:2013/COR 1 2013 Information Technology – Security techniques – Information security management sistema – Requirements, para suministrar requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información”. El



desarrollo de un SGSI en una organización será producto de las necesidades y objetivos de la misma, de los requerimientos de seguridad de sus activos, de los procesos organizacionales implantados y del tamaño y estructura de dicha organización. La seguridad de la información basada en esta norma se definirá en base de preservar la confidencialidad, integridad y disponibilidad de la información para sus usuarios.

La NTP ISO/IEC 27001:2014 promueve la adopción de un enfoque basado en procesos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el SGSI de una organización. Para que dicho sistema funcione de forma eficaz, la organización debe gestionar actividades que usan recursos o procesos.

La NTP ISO/IEC 27001:2014 cuenta con 10 capítulos, en los cuales se aplica el método PDCA, también conocido como ciclo de Deming de mejora continua, estrategia de calidad en la cual se basan los sistemas de gestión desarrollados bajo las normas ISO.

La adopción del modelo PDCA, refleja los principios establecidos en las Directrices que controlan la seguridad de sistemas y redes de información. Esta norma brinda un modelo robusto para implementar los principios en aquellas directrices que controlan la evaluación de riesgos, diseño e implementación de la seguridad, gestión y reevaluación de la seguridad.

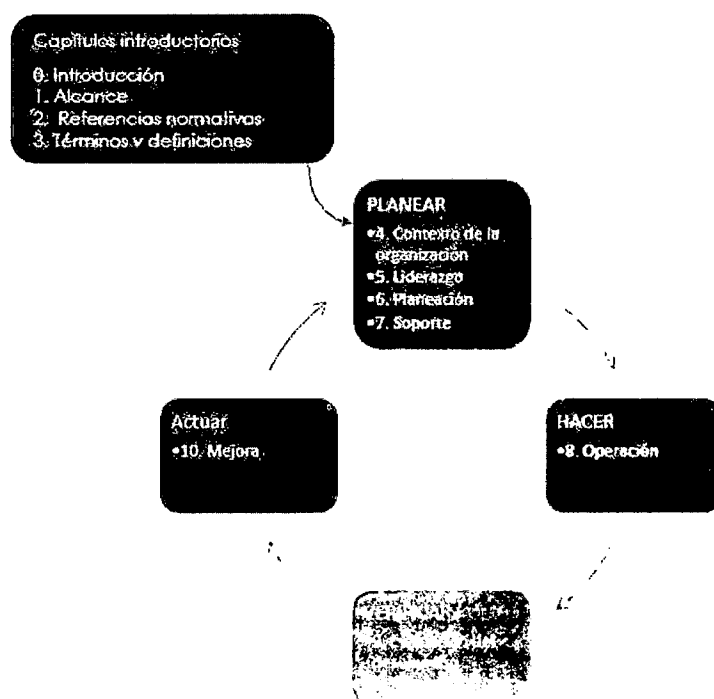


Figura 2: Contenido de NTP ISO/IEC 27001:2014 de acuerdo al ciclo de Deming

2.2 Norma NTP-ISO/IEC 27002:2017

La presente Norma Técnica Peruana ha sido elaborada por el Comité Técnico de Normalización de Codificación electrónico de datos, mediante el Sistema 1 o de Adopción, durante los meses de agosto de 2015 a octubre de 2017, utilizando como antecedentes a la NTP-ISO/IEC 27002:2017 Information technology – Security techniques – Code of practice for information security controls, ISO/IEC 27002:2013/Cor.1:2014 and ISO/IEC 27002:2013/Cor.2:2015 y fue diseñada para usarse como referencia para la selección de controles al momento de implementar el Sistemas de Gestión de Seguridad de la Información, con base a la norma técnica ISO 27001.

Esta Norma Técnica Peruana proporciona lineamientos para la seguridad de la información en las organizaciones y prácticas de gestión para la seguridad de la información, incluyendo la selección, la implementación y la gestión de controles tomando en consideración los riesgos del entorno para la seguridad de la información de la organización.

Esta Norma Técnica Peruana está diseñada para ser utilizada por las organizaciones que pretendan:

- a) seleccionar los controles dentro del proceso de implementación del Sistema de Gestión de Seguridad de la Información basado en la Norma ISO/IEC 27001;
- b) Implementar los controles de seguridad de la información comúnmente aceptados;
- c) Desarrollar sus propios lineamientos de gestión de seguridad de la información.

3. ENTIDAD OBJETO DE ESTUDIO: Ministerio de Vivienda, Construcción y Saneamiento

El Ministerio de Vivienda, Construcción y Saneamiento (MVCS), fundado el 11 de Julio del 2002, es un organismo del Poder Ejecutivo que tiene personería jurídica de derecho público y constituye un pliego presupuestal, con autonomía técnica administrativa, económica y financiera de acuerdo a Ley. El MVCS tiene competencia en las siguientes materias:

- ✓ Vivienda
- ✓ Construcción
- ✓ Saneamiento
- ✓ Urbanismo y Desarrollo Urbano
- ✓ Bienes Estatales
- ✓ Propiedad Urbana

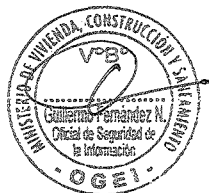
Es el ente rector de las competencias antes descritas y como tal, es responsable del diseño, ejecución, supervisión y evaluación de las políticas nacionales y sectoriales, que son de obligatorio cumplimiento por los tres niveles de gobierno. Durante los años 2016 y 2017 el MVCS se ha desconcentrado en todas las regiones del Perú dando prioridad a cerrar brechas en materia de agua y saneamiento urbano y rural.

a. Misión

Somos el Ente Rector en materia de Urbanismo, Vivienda, Construcción y Saneamiento, responsable de diseñar, normar, promover, supervisar, evaluar y

11

Plan de Seguridad de la Información



ejecutar la política sectorial, contribuyendo a la competitividad y al desarrollo territorial sostenible del país, en beneficio preferentemente de la población de menores recursos.

b. Visión

Los peruanos viven en un territorio ordenado, en centros poblados urbanos y rurales sostenibles, en viviendas seguras, con servicios de agua y saneamiento de calidad.

c. Objetivos Estratégicos

En general, los objetivos estratégicos del sector están orientados a la reducción de las principales brechas de servicios de competencia del sector, tales como el déficit de vivienda, agua, saneamiento, formalización de la propiedad predial y equipamiento urbano en los centros poblados del país.

Sobre la base de los macro problemas identificados, se han determinado los objetivos estratégicos que orientarán el desempeño del sector para el período 2016-2021. Los objetivos estratégicos, por definición son objetivos de mediano y largo plazo y están orientados al logro de la visión sectorial.

Bajo esta perspectiva, se han determinado siete objetivos estratégicos para el período 2016-2021, los cuales se detallan a continuación.

- OE1. Mejorar el ordenamiento de los centros poblados urbanos y rurales.
- OE2. Incrementar el acceso de la población a una vivienda segura.
- OE3. Disminuir la informalidad de la propiedad predial urbana.
- OE4. Incrementar la oferta del sector inmobiliario y de la industria de la construcción.
- OE5. Incrementar el acceso de la población rural a servicios de agua y saneamiento sostenibles y de calidad.
- OE6. Incrementar el acceso de la población urbana a servicios de agua y saneamiento sostenibles y de calidad.
- OE7. Mejorar la capacitación de gestión de las entidades del sector.

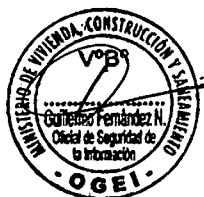
3.1 Infraestructura del MVCS

El local principal del Ministerio de Vivienda, Construcción y Saneamiento está ubicado en la Av. Paseo de la Republica 3361 – Edificio de Petroperú – San Isidro, en sus instalaciones se cuenta con el personal de seguridad física apropiado desde la puerta de ingreso principal, así como en cada uno de los pisos, los cuales se encargan de controlar el acceso del personal interno y externo, además de verificar la entrada y salida de los equipos informáticos.

Adicionalmente, el MVCS cuenta con otras 7 sedes que están ubicadas en: Miraflores, Olavechea, Callao, Blondet, Vitrina Inmobiliaria, Cisnes y Baltazar. Además de 24 Centro de Atención al Ciudadano (CAC's) a nivel nacional: Amazonas, Ancash, Apurímac, Arequipa, Ayacucho, Cajamarca, Cusco, Huancavelica, Huánuco, Ica, Junín, La Libertad, Lambayeque, Huacho, Loreto, Madre de Dios, Moquegua, Pasco, Piura, Puno, San Martín, Tacna, Tumbes, Ucayali. Se tiene un estimado de 2,900 usuarios distribuidos en todas sus sedes, según información obtenida de la herramienta de gestión de Microsoft "Directorio Activo" al mes de diciembre del 2017.

3.2 Composición organizativa (Oficina General de Estadística e Informática)

a. Definición



La Oficina General de Estadística e Informática es el órgano responsable de la gestión de la infraestructura de tecnologías de la información y comunicaciones, así como de planificar, desarrollar, implantar y gestionar los proyectos de desarrollo de soluciones basadas en tecnologías de la información y comunicación para la administración y gestión de la información estadística sectorial. Depende jerárquicamente de la Secretaría General.

b. Estructura del equipo

Para el logro de los objetivos estratégicos de la Dirección General de Estadística e Informática, en el corto plazo se necesita implementar la siguiente estructura orgánica:

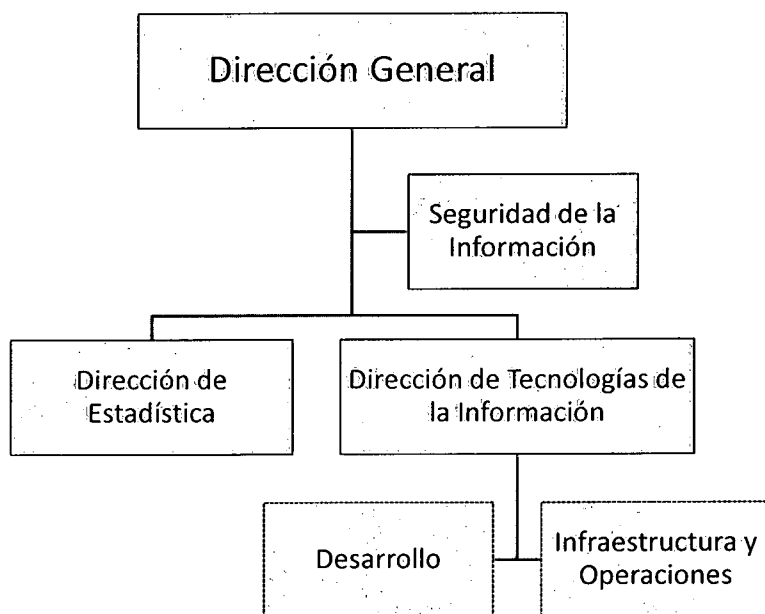


Figura 3: Organigrama funcional de la Oficina de Tecnología de la Información de OGEI

Asimismo, se deben establecer las funciones de los roles mencionados en dicha estructura orgánica.

3.3 Sistemas de Información del MVCS

El MVCS cuenta con muchos sistemas de información que sirven de soporte a los distintos procesos tanto misionales como de apoyo.

ITEM	SISTEMA	FUNCIÓN
1	Sistema de Seguimiento de Proyectos	Seguimiento de proyectos en las modalidades de transferencia financiera, ejecución directa y núcleos ejecutores.
2	Sistema de Trámite Documentario	Gestión de expedientes ingresados por mesa de partes y documentos generados por los órganos y unidades orgánicas del Ministerio.
3	Sistema de Información Sectorial	Indicadores, mapas y reportes sectoriales.
4	Plataforma de Registro, Evaluación y Seguimiento de Expedientes Técnicos (PRESET)	Sistema creado para el acceso de autoridades locales, regionales y de las EPS para tramitar evaluaciones de expedientes técnicos de obras de saneamiento en el marco de la RM-155-2017-VIVIENDA.



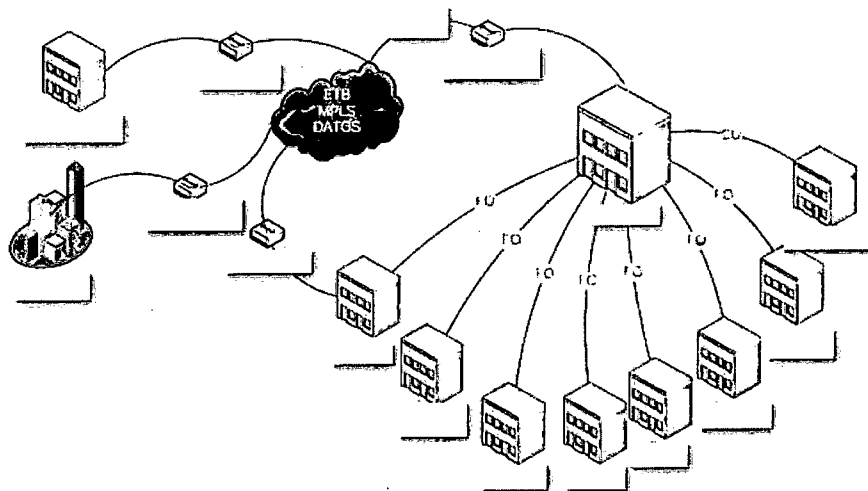


Figura 4: Mapa de enlaces de red del MVCS

3.5 Análisis diferencial del MVCS con respecto a NTP-ISO/IEC 27001:2014 + NTP-ISO/IEC 27002:2017

La norma ISO/IEC 27001 es un estándar para la implementación de un Sistema de Gestión de Seguridad de la Información, la cual especifica los requisitos para establecer, implementar, mantener y mejorar de forma continua dicho sistema dentro del contexto de la organización. La versión que se usa en el presente plan es la 2014, debido al cambio de enfoque realizado por la ISO para que en el caso de organizaciones que cuentan con sistemas de gestión, puedan integrar los requisitos y se pueda cumplir con todos los que sean implementados en base a los estándares de dicha organización.

La NTP-ISO/IEC 27002:2017 fue desarrollada como elemento de referencia para la selección de controles dentro del proceso de implementación de un Sistema de Gestión de Seguridad de Información (SGSI) con base en la NTP-ISO/IEC 27001 o bien como un manual de buenas prácticas que sirva de guía para organizaciones que implementan controles de seguridad comúnmente aceptados.

De forma preliminar, se necesita conocer de manera global el estado actual del Ministerio de Vivienda, Construcción y Saneamiento en relación de la Seguridad de la Información, por lo que es necesario realizar el análisis diferencial del ministerio basados en la NTP-ISO/IEC 27001:2014.

Para ello se han realizado un conjunto de entrevistas al Director de Tecnologías de Información y los ingenieros de infraestructura, la cual nos dio los resultados del estado preliminar de la Seguridad de Información de acuerdo a las normas anteriormente citadas y el estado de madurez del sistema al momento de iniciar el Plan de Seguridad de la Información.

Numeral	Dominio	Cumplimiento
4	Contexto de la organización	20%
5	Liderazgo	15%
6	Planificación	5%
7	Soporte	12%



8	Operación	5%
9	Evaluación del desempeño	5%
10	Mejoras	22%

Tabla 2: Norma NTP-ISO/IEC 27001:2014 en el MVCS

Por el hecho de no contar con un Sistema de Gestión de Seguridad de la Información, el porcentaje de cumplimiento es mínimo, como en el numeral de liderazgo, soporte y mejoras.



Figura 5: Gráfico de Radial. Cumplimiento de la norma SGSI anterior al Plan de Seguridad de la Información

Con el gráfico de radial, se puede inferir que algunos dominios tienen controles implementados en gran porcentaje, como en el caso de seguridad en las telecomunicaciones y gestión de incidentes. Por esta razón hay que enfocar las propuestas producto del presente plan en la implementación de controles en los dominios que no cuentan con ninguno y que hagan parte del alcance del SGSI planteado por la entidad.



Figura 6: Gráfico de radial de estado de los controles del Anexo 1 de NTP-ISO/IEC 27001:2014

Respecto a los objetivos de control y controles que se presentan como anexo en la NTP-ISO/IEC 27001:2014, se obtuvieron los resultados expuestos en el Anexo 1 en la sección de controles, los cuales podemos resumir, asociando una valoración cuantitativa, según el nivel de implementación, en la siguiente tabla:

Dominio (Anexo A)	Controles	Sin Implementar	Parcialmente Implementado	Implementado	Porcentaje de Implementación
A.5 Políticas de Seguridad de la Información	2	-	1	1	75%
A.6 Organización de la Seguridad de la Información	7	4	1	2	36%
A.7 Seguridad de los Recursos Humanos	6	4	2	-	17%
A.8 Gestión de Activos	10	10	-	-	0%
A.9 Control de Acceso	14	5	8	1	36%
A.10 Criptografía	2	2	-	-	0%
A.11 Seguridad Física y Ambiental	15	-	12	3	60%
A.12 Seguridad de las Operaciones	14	8	6	-	21%
A.13 Seguridad de las Comunicaciones	7	2	5	-	36%
A.14 Adquisición, Desarrollo y Mantenimiento de Sistemas	13	10	3	-	12%
A.15 Relaciones con los Proveedores	5	5	-	-	0%
A.16 Gestión de Incidentes de Seguridad de la Información	7	4	3	-	21%
A.17 Aspectos de Seguridad de la Información en la Gestión de Continuidad del Negocio	4	-	4	-	50%
A.18 Cumplimiento	8	1	7	-	44%

Tabla 3: Evaluación de los controles NTP-ISO/IEC 27001:2014

4. SISTEMA DE GESTIÓN DOCUMENTAL

4.1 Esquema documental del SGSI

Toda organización que piense en certificarse en NTP-ISO/IEC 27001:2014 debe contar con un esquema documental que soporte el Sistema de Gestión de la Seguridad de la Información. Los documentos que soportan dicho sistema son:

- ✓ Definición del Alcance del Sistema de Gestión de la Seguridad de la Información (definida en el capítulo anterior).
- ✓ Política General de Seguridad de la Información.
- ✓ Procedimientos para:
 - Control de documentación o auditorías internas
 - Medidas preventivas y correctivas
- ✓ Metodologías de evaluación de riesgos.
- ✓ Declaración de Aplicabilidad.
- ✓ Plan de tratamiento de riesgos.
- ✓ Registros.

En este capítulo revisaremos el estado de dicha documentación para el MVCS.



4.1.1 Política de Seguridad de la Información

El MVCS cuenta con una Política de Seguridad de la Información actualizada en el año 2017.

4.1.2 Procedimiento de auditorías internas

De acuerdo con la definición de auditoría de la norma ISO 19011: "La auditoría es un proceso sistemático, independiente y documentado para obtener evidencias de la auditoría y evaluarlas de manera objetiva con el fin de determinar la extensión en que se cumplen los criterios de auditoría".

Para el caso de los Sistemas de Gestión de Seguridad de la Información, el MVCS debe llevar a cabo auditorías internas de forma programada y planificada para verificar si el plan del SGSI cumple con los requisitos de la institución respecto al sistema y a los requisitos de la NTP-ISO/IEC 27001:2014 y para verificar si el sistema está implementado y es mantenido de forma eficaz.

Al momento de realizar el plan, este procedimiento no se encuentra definido en el SGSI en el Ministerio, por lo que se realiza una propuesta de procedimiento acorde a las necesidades del ministerio para los procesos involucrados.

4.1.3 Gestión de indicadores

La creación de indicadores de gestión está orientada principalmente en la medición de efectividad, eficiencia y eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, indicadores que servirán como insumo para el componente de mejora continua permitiendo adoptar decisiones de mejora.

Los objetivos de estos procesos de medición en seguridad de la información son:

- ✓ Evaluar la efectividad de la implementación de los controles de seguridad.
- ✓ Evaluar la eficiencia de la Información al interior de la institución.
- ✓ Proveer estados de seguridad que sirvan de guía en las revisiones de la información, facilitando mejoras en seguridad de la información y nuevas entradas a auditar.
- ✓ Comunicar valores de seguridad al interior de la institución.
- ✓ Servir como insumos al plan de análisis y tratamiento de riesgos.

Se ha tomado de base el Modelo de Seguridad y Privacidad de la Información por parte del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.



A continuación se definen una serie de indicadores para medir la gestión y el cumplimiento en el avance del SGSI y la seguridad de la información alineados al “Plan Estratégico de Tecnologías de la Información y Comunicaciones del MVCS 2017-2021”, los cuales son:

INDICADOR 01 – TRATAMIENTOS DE EVENTOS RELACIONADOS EN EL MARCO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		
IDENTIFICADOR	ID-01	
DEFINICIÓN		
El indicador permite determinar la eficiencia en el tratamiento de eventos relacionados a la seguridad de la información. Los eventos serán reportados por los usuarios o determinadas en las auditorías planeadas para el SGSI.		
OBJETIVO		
El objetivo del indicador es reflejar la gestión y evolución del modelo de seguridad y privacidad de la información al interior de una entidad.		
TIPO DE INDICADOR		
Indicador de Gestión		
DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
V01: Número de incidencias de seguridad solucionados.	(V01 / V02) x 100	Auditorías internas, herramientas de monitoreo, registro de incidentes.
V02: Número de incidentes de seguridad reportados.		Auditorías internas, herramientas de monitoreo, registro de incidentes.
RESPONSABLE Y FRECUENCIA		
RESPONSABLE: Oficial de Seguridad de la Información		
FRECUENCIA: Anual		
METAS		
MINIMA: 75-80%		
SATISFACTORIA: 81-90%		
CUMPLIMIENTO: 91-100%		
OBSERVACIONES		

INDICADOR 02 –PROGRAMA DE MANTENIMIENTO PREVENTIVO DE LA PLATAFORMA DE SERVIDORES DEL MVCS		
IDENTIFICADOR	ID-02	
DEFINICIÓN		
El indicador permite determinar el cumplimiento de los programas de mantenimiento preventivo de la plataforma de servidores del MVCS, previniendo algún tipo de indisponibilidad de los servicios o fallas en los servidores.		
OBJETIVO		
El objetivo del indicador es mostrar la ejecución de los mantenimientos preventivos de la plataforma de servidores del MVCS.		
TIPO DE INDICADOR		
Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
V03: ¿La entidad ha cumplido con el programa de mantenimiento preventivo de la plataforma de servidores del MVCS?	V03 = 1 (SI se evidencia) V03 = 0 (NO se evidencia)	Informe de mantenimiento preventivo de la plataforma de servidores del MVCS.
RESPONSABLE Y FRECUENCIA		
RESPONSABLE: Oficina de Tecnología de la Información		
FRECUENCIA: Anual		
METAS		
CUMPLE: 1		
NO CUMPLE: 0		
OBSERVACIONES		



INDICADOR 03 – DISPONIBILIDAD DEL CENTRO DE DATOS		
IDENTIFICADOR	ID-03	
DEFINICIÓN		
El indicador permite determinar el porcentaje de disponibilidad del Centro de Datos en un año.		
OBJETIVO		
El objetivo del indicador es garantizar la disponibilidad del Centro de Datos del MVCS, logrando con ello la disponibilidad de los servicios tecnológicos brindados por el MVCS a las partes interesadas del SGSI.		
TIPO DE INDICADOR		
Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
V04: Número de horas sin disponibilidad del Centro de Datos.	$(V04 / V05) \times 100$	Sistema de Gestión de eventos de seguridad de la información.
V05: Número de horas de disponibilidad necesaria.		
RESPONSABLE Y FRECUENCIA		
RESPONSABLE: Oficina de Tecnología de la Información		
FRECUENCIA: Anual		
METAS		
MINIMA: 75-80%		
SATISFACTORIA: 81-90%		
CUMPLIMIENTO: 91-100%		
OBSERVACIONES		

INDICADOR 04 – SENSIBILIDAD EN SEGURIDAD DE LA INFORMACIÓN		
IDENTIFICADOR	ID-04	
DEFINICIÓN		
El indicador permite medir la aplicación de los temas sensibilizados en seguridad de la información por parte de los usuarios finales.		
OBJETIVO		
El objetivo del indicador es establecer la efectividad de un plan de capacitación y sensibilización previamente definido como medio para el control de incidentes de seguridad.		
TIPO DE INDICADOR		
Indicador de Gestión		
DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
V06: Número de campaña de sensibilización realizadas (capacitaciones, mailing, e-learning)	$(V06 \times 100) / 12$	Plan de comunicación interna
RESPONSABLE Y FRECUENCIA		
RESPONSABLE: Oficial de Seguridad de la Información / OGGRH		
FRECUENCIA: Anual		
METAS		
MINIMA: 25-49%		
SATISFACTORIA: 50-74%		
CUMPLIMIENTO: 75-100%		
OBSERVACIONES		

INDICADOR 05 – IMPLEMENTACIÓN DE CONTROLES		
IDENTIFICADOR	ID-05	
DEFINICIÓN		
El indicador permite determinar el grado de avance en la implementación de controles de seguridad.		
OBJETIVO		
Busca identificar el grado de avance en la implementación de controles de seguridad.		
TIPO DE INDICADOR		
Indicador de Gestión		
DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
V07: Número de controles implementados durante el año.		Plan de tratamiento de riesgos



V08: Número de controles que se planificaron implementar.	$(V07 / V08) \times 100$	
RESPONSABLE Y FRECUENCIA		
RESPONSABLE: Oficial de Seguridad de la Información		
FRECUENCIA: Anual		
METAS		
MINIMA: 75-80%		
SATISFACTORIA: 81-90%		
CUMPLIMIENTO: 91-100%		
OBSERVACIONES		

INDICADOR 06 – ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN		
IDENTIFICADOR	ID-06	
DEFINICIÓN		
El indicador permite determinar y hacer seguimiento al compromiso de la dirección, en cuanto a seguridad de la información, en lo relacionado con la asignación de personas y responsabilidades relacionadas a la seguridad de la información al interior de la institución.		
OBJETIVO		
Hacer un seguimiento a la asignación de recursos y responsabilidades en gestión de seguridad de la información, por parte de la alta dirección.		
TIPO DE INDICADOR		
Indicador de Gestión		
DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
V09: Número de personas con su respectivo rol.	$(V09 / V10) \times 100$	Anexo A.6.1.1 del de la NTP-ISO/IEC 27001
V10: Número de personas con su respectivo rol definido después de un año		Actas de asignación de personal.
RESPONSABLE Y FRECUENCIA		
RESPONSABLE: Oficial de Seguridad de la Información		
FRECUENCIA: Anual		
METAS		
MINIMA: 75-80%		
SATISFACTORIA: 81-90%		
CUMPLIMIENTO: 91-100%		
OBSERVACIONES		
De acuerdo a lo establecido en el Anexo A de la NTP-ISO/IEC 27001: Todas las responsabilidades de seguridad de la información deben ser definidas y asignadas, por lo tanto, el indicador está enfocado, no solo a la contratación de nuevas personas, si no a la asignación de responsabilidades.		

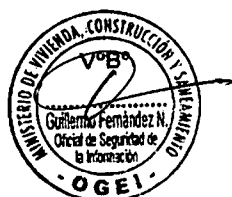
INDICADOR 07 – CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN EL MVCS		
IDENTIFICADOR	ID-07	
DEFINICIÓN		
Cumplimiento de políticas de seguridad de la información en la entidad.		
OBJETIVO		
Busca identificar el nivel de estructuración de los procesos de la entidad orientados a la seguridad de la información.		
TIPO DE INDICADOR		
Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
V11: ¿La entidad ha definido una política general de seguridad de la información?	VX = 1 (Sí se evidencia) VX = 0 (NO se evidencia)	Guía del Modelo de Operación / Usuarios Internos.
V12: ¿La entidad ha definido una organización interna en términos de personas y responsabilidades con el fin de cumplir las políticas de seguridad de la información y documenta estas actividades?		Guía del Modelo de Operación / Usuarios Internos.
V13: ¿La entidad cumple con los requisitos legales, reglamentarios y contractuales con respecto al manejo de la información?		Guía del Modelo de Operación / Usuarios Internos.



RESPONSABLE Y FRECUENCIA	
RESPONSABLE: Oficial de Seguridad de la Información	
FRECUENCIA: Anual	
METAS	
CUMPLE: 1 NO CUMPLE: 0	
OBSERVACIONES	

INDICADOR 08 – VERIFICACIÓN DEL CONTROL DE ACCESO		
IDENTIFICADOR	ID-08	
DEFINICIÓN		
Grado de control de acceso en la entidad.		
OBJETIVO		
Busca identificar la existencia de lineamientos, normas o estándares en cuanto al control de acceso en la entidad.		
TIPO DE INDICADOR		
Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
V14: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar el acceso de los usuarios a sus servicios de Gobierno en Línea y a sus redes de comunicaciones?	VX = 1 (Sí se evidencia) VX = 0 (NO se evidencia)	Usuarios Internos.
V15: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar el uso y el acceso a los sistemas de información, las aplicaciones y los depósitos de información con las que cuenta la entidad?		Usuarios Internos.
V16: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar las terminales móviles y accesos remotos a los recursos de la entidad?		Usuarios Internos.
RESPONSABLE Y FRECUENCIA		
RESPONSABLE: Oficial de Seguridad de la Información		
FRECUENCIA: Anual		
METAS		
CUMPLE: 1 NO CUMPLE: 0		
OBSERVACIONES		

INDICADOR 09 – POLÍTICAS DE PRIVACIDAD Y CONFIDENCIALIDAD		
IDENTIFICADOR	ID-09	
DEFINICIÓN		
Grado de implementación de políticas privacidad y confidencialidad de la entidad.		
OBJETIVO		
Busca identificar el nivel de implementación de políticas privacidad y confidencialidad de la entidad.		
TIPO DE INDICADOR		
Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
V17: ¿La entidad ha implementado lineamientos, normas y/o estándares para proteger la información personal y privada de los ciudadanos que utilicen sus servicios?	VX = 1 (Sí se evidencia) VX = 0 (NO se evidencia)	Usuarios Internos.
V18: ¿La entidad ha implementado lineamientos, normas y/o estándares para proteger la información privada de las entidades que utilicen sus servicios?		Usuarios Internos.
RESPONSABLE Y FRECUENCIA		
RESPONSABLE: Oficial de Seguridad de la Información		



FRECUENCIA: Anual
METAS
CUMPLE: 1 NO CUMPLE: 0
OBSERVACIONES

INDICADOR 10 – VERIFICACIÓN DE LAS POLÍTICAS DE INTEGRIDAD DE LA INFORMACIÓN		
IDENTIFICADOR	ID-10	
DEFINICIÓN		
Grado de implementación de mecanismos para la integridad de la información de la entidad.		
OBJETIVO		
Busca identificar el nivel de implementación de políticas privacidad y confidencialidad de la entidad.		
TIPO DE INDICADOR		
Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
V19: ¿La entidad ha implementado lineamientos contra modificación o pérdida accidental de información?	VX = 1 (Sí se evidencia)	Usuarios Internos.
V20: ¿La entidad ha implementado lineamientos, normas y/o estándares para recuperar información en caso de modificación o pérdida intencional o accidental?	VX = 0 (NO se evidencia)	Usuarios Internos.
RESPONSABLE: Oficial de Seguridad de la Información y la Oficina de Tecnologías de la Información		
FRECUENCIA: Anual		
METAS		
CUMPLE: 1 NO CUMPLE: 0		
OBSERVACIONES		

INDICADOR 11 – IMPLEMENTACIÓN DE LOS PROCESOS DE REGISTRO Y AUDITORÍA		
IDENTIFICADOR	ID-11	
DEFINICIÓN		
Grado de implementación de los mecanismos encaminados a la detección de anomalías e irregularidades.		
OBJETIVO		
Busca medir el nivel de mecanismos encaminados a la detección de anomalías e irregularidades		
TIPO DE INDICADOR		
Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
V21: ¿La entidad ha implementado mecanismos para detectar periódicamente vulnerabilidades de seguridad en el funcionamiento de?: a) Infraestructura, b) Redes, c) Sistemas de información, d) Aplicaciones, e) Uso de los servicios	VX = 1 (Sí se evidencia) VX = 0 (NO se evidencia)	Usuarios Internos, no conformidades
RESPONSABLE Y FRECUENCIA		
RESPONSABLE: Oficina de Tecnologías de la Información		
FRECUENCIA: Anual		
METAS		
CUMPLE: 1 NO CUMPLE: 0		
OBSERVACIONES		



INDICADOR 12 – POLÍTICAS DE DISPONIBILIDAD DEL SERVICIO Y LA INFORMACIÓN		
IDENTIFICADOR	ID-12	
DEFINICIÓN		
Grado de cumplimiento de las políticas de disponibilidad del servicio y la información.		
OBJETIVO		
Busca identificar el nivel de implementación de políticas de disponibilidad del servicio y la información.		
TIPO DE INDICADOR		
Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
V22: ¿La entidad verifica que los lineamientos, normas y/o estándares orientados a la continuidad en la prestación de los servicios se cumplan?	VX = 1 (Sí se evidencia)	Usuarios Internos.
V23: ¿La entidad ha implementado mecanismos para que los servicios de Gobierno en línea tengan altos índices de disponibilidad?	VX = 0 (NO se evidencia)	Usuarios Internos.
RESPONSABLE Y FRECUENCIA		
RESPONSABLE: Oficina de Tecnologías de la Información		
FRECUENCIA: Anual		
METAS		
CUMPLE: 1 NO CUMPLE: 0		
OBSERVACIONES		

INDICADOR 13 – PORCENTAJE DE DISPONIBILIDAD DE LOS SERVICIOS DE GOBIERNO EN LINEA QUE PRESTA LA ENTIDAD		
IDENTIFICADOR	ID-13	
DEFINICIÓN		
Porcentaje de disponibilidad de los servicios que presta la entidad		
OBJETIVO		
Busca identificar el nivel de disponibilidad del servicio y la información.		
TIPO DE INDICADOR		
Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
V24: La entidad tiene definidos ANS (acuerdo de nivel de servicio) para los servicios de Gobierno en Línea que presta	VX = 1 (Sí se evidencia)	Usuarios Internos.
V25: Porcentaje de disponibilidad de los servicios de Gobierno en línea que presta la entidad en base a los ANS del punto anterior.	VX = 0 (NO se evidencia)	Usuarios Internos.
RESPONSABLE Y FRECUENCIA		
RESPONSABLE: Oficina de Tecnologías de la Información		
FRECUENCIA: Anual		
METAS		
CUMPLE: 1 NO CUMPLE: 0		
OBSERVACIONES		

4.1.4 Gestión de roles y responsabilidades

El documento presenta los roles y responsabilidades que se requieren para la implementación del Sistema de Gestión de Seguridad de la Información en el MVCS, tomando como referencia lo establecido en la NTP/ISO 27001:2014, a través del cual se busca el logro de los objetivos de la seguridad de la información en el Ministerio.

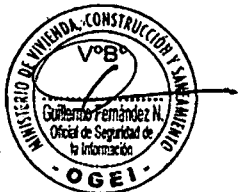


Definiciones:

- **Activo:** Cualquier elemento que tiene valor para la institución y para la Gestión de Riesgo de Seguridad de la Información se consideran los siguientes tipos: información, actividades y procesos del negocio, software, hardware, personal, redes, institución y ubicación.
- **Amenaza:** Causa potencial de incidente no deseado, el cual puede resultar en daño al sistema o la institución.
- **Confidencialidad:** Propiedad de la información que hace que no esté disponible o que sea revelada a individuos no autorizados, procesos o instituciones.
- **Disponibilidad:** Propiedad de ser accesible y utilizable ante la demanda de una entidad autorizada. [Fuente: ISO 27000].
- **Integridad:** Propiedad de precisión y completitud [Fuente: ISO 27000].
- **Monitoreo:** Verificación, supervisión, observación crítica o determinación continua del estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado.
- **Propietario del activo:** Persona o cargo que administra, autoriza el uso, regula o gestiona el activo de información. El propietario del activo aprueba el nivel de protección requerido frente a confidencialidad, integridad y disponibilidad.
- **Riesgo:** Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen, medio ambiente) y se pueden aplicar a niveles diferentes (estratégico, operacional, toda la organización). [Fuente: ISO 31000].
- **Vulnerabilidad:** Debilidad identificada sobre un activo y que puede ser aprovechado por una amenaza para causar una afectación sobre la confidencialidad, integridad y/o disponibilidad de la información.

A nivel general los colaboradores del MVCS asumirán las siguientes responsabilidades, una vez se formalice el SGSI al interior de la institución.

- a) **Alta Dirección:** Es el responsable por la dirección estratégico e impulso del SGSI. Requiere el compromiso, recursos y asignación de responsabilidades para la gestión de seguridad de la información. De la misma forma debe contar con el direccionamiento y los resultados por parte del Comité de Seguridad de la Información.
- b) **Comité de Gestión de Seguridad de la Información:** Encargado de participar en el proceso de implementación y/o adecuación, operación y monitoreo del Sistema de Gestión de Seguridad de la Información (SGSI) en el MVCS.
- c) **Oficial de Seguridad de la Información:** Es el responsable por el SGSI, reportando a la Oficina General de Estadística e Informática sobre las políticas, objetivos y su cumplimiento.



- d) **Propietario del Activo:** Es el funcionario asignado de gestionar que el activo asignado bajo su responsabilidad esté protegido con los controles definidos en el SGSI y que le apliquen a dicho activo; de esta manera este rol es quien debe responder por la afectación de la confidencialidad, integridad y disponibilidad del mismo, en cualquiera de los procesos que se encuentre involucrado.
- e) **Custodio del Activo:** Es el usuario final a quien se asigna el activo para el cumplimiento de las actividades diarias.
- f) **Responsable del Riesgo:** Esta gestión será asumida por el dueño del proceso.

Existe un nivel de responsabilidades, agrupados de la siguiente forma:

- Responsabilidades generales:
Oficina: Todos los afectados por el SGSI
Responsable: Alta dirección
- Gestión de cumplimiento de normativa:
Oficina: Todos los afectados por el SGSI
Responsable: Oficial de Seguridad de la Información
- Gestión de riesgo:
Oficina: Todos los afectados por el SGSI
Responsable: Directores afectados por el SGSI y el Oficial de Seguridad de la Información
- Revisión y medición del SGSI:
Oficina: Todos los afectados por el SGSI
Responsable: Oficial de Seguridad de la Información y Auditor interno
- Gestión de activos:
Oficina: Todos los afectados por el SGSI
Responsable: Director de la Oficina de Tecnología de la Información y el Oficial de Seguridad de la Información
- Gestión de incidencias:
Oficina: Todos los afectados por el SGSI
Responsable: Director de la Oficina de Tecnología de la Información y el Oficial de Seguridad de la Información

4.1.5 Metodología de análisis de riesgos

El análisis de riesgos, como pueden ser la pérdida de confidencialidad, integridad o disponibilidad de los activos del Ministerio ha de seguir una metodología que define los criterios que influyen en el riesgo global,



escalas de impacto, criterios de aceptación de riesgo y tipos de impacto, entre otros elementos a analizar.

4.1.5.1 Proceso de análisis de riesgos

El primer paso es definir la metodología que utilizará el Ministerio para valorar o calcular los riesgos. Se ha de ser coherente con la estrategia de la empresa.

- **Escala de valoración de activos:** se toma el valor máximo de un activo dentro de la empresa y se crea la siguiente escala a partir de ella:

Valoración de activos	
Valoración	Rango (en S/)
Muy alta	Entre 300,000 y 100,000
Alta	Entre 99,999 y 50,000
Media	Entre 49,000 y 10,000
Baja	Entre 9,999 y 1,000
Muy baja	Entre 999 y 1

- **Clasificación de vulnerabilidades:** se toma como máximo el valor 1, que quiere decir que la vulnerabilidad está presente al 100% de días del año (365 días). Partiendo de esto, se crea la siguiente escala:

Clasificación de vulnerabilidades		
Valoración	Rango (en iteraciones)	Código
Muy alta	1 (cada día)	F-1
Alta	0,0712 (cada 2 semanas)	F-2
Media	0,0164 (cada 2 meses)	F-3
Baja	0,0054 (cada semestre)	F-4
Muy baja	0,0027 (cada año)	F-5

- **Escala de valoración del impacto:** se toma como máximo 100%, que corresponde a que impacta a la totalidad de activos de la empresa. Partiendo de esto, se crea la siguiente escala:

Valoración del impacto	
Valoración	Rango (en %)
Muy alto	Entre 100 y 75
Alto	Entre 74 y 50
Medio	Entre 49 y 25
Bajo	Entre 25 y 5
Muy bajo	Entre 4 y 1

- **Dimensiones de seguridad:** a continuación, se presenta la escala con la que se mide la criticidad de las amenazas a las cinco dimensiones de la seguridad, que son:
 - ✓ Autenticidad (A): garantías de identidad de los usuarios.
 - ✓ Confidencialidad (C): accesos a información sensible.
 - ✓ Integridad (I): garantía de que los métodos de acceso a la información son completos.
 - ✓ Disponibilidad (D): garantía de disponibilidad máxima de la información.
 - ✓ Trazabilidad (T): garantía de revisión de acciones sobre la información.

La escala de valoración es:



Dimensiones de la seguridad	
Valoración	Criterio / daño
10	Muy grave
9 – 7	Grave
6 – 4	Importante o considerable
3 – 1	Menor
0	Irrelevante

Clasificación de amenazas		
Origen	Amenaza	Identificación
Natural	Inundación	A-NAT1
Natural	Incendio	A-NAT2
Natural	Terremoto	A-NAT3
No intencionado	Accidente laboral	A-NOINT1
No intencionado	Avería	A-NOINT2
No intencionado	Pérdida / hurto	A-NOINT3
Intencionado	Ataque SQL / DDoS	A-INT1
Intencionado	Robo	A-INT2
Intencionado	Intrusión	A-INT3

4.1.6 Declaración de aplicabilidad

En la NTP-ISO/IEC 27001:2014 se establece que la aplicabilidad de los controles puede deberse por una obligación contractual, por un requerimiento regulatorio o por un requerimiento del negocio. De igual modo, se estipula que alguno de los controles puede ser excluido de la aplicabilidad de la norma.

A continuación, se muestra la matriz de aplicabilidad por dominio y control:

Declaración de Aplicabilidad NTP ISO 27001-2014			
ID	Control		Registro de implementación
A.5 Políticas de Seguridad de la Información			
A.5.1 Dirección de la gerencia para la seguridad de la información			
A.5.1.1	Políticas para la seguridad de la información	Aplica	Actualmente se ha actualizado la Política de Seguridad de la Información del MVCS con la RM N° 374-2017-VIVIENDA
A.5.1.2	Revisión de las políticas para la seguridad de la información	Aplica	Actualmente se ha actualizado la Directiva General N° 005-2017-VIVIENDA-SG de Correo Electrónico e Internet, el cual no ha sido actualizada desde el 2011 con RSG N° 056-2017-VIVIENDA/SG "Lineamientos para el uso del correo electrónico e internet en el MVCS"
A.6 Aspectos organizativos para la seguridad			
A.6.1 Organización interna			
A.6.1.1	Roles y Responsabilidades para la seguridad de la información	Aplica	En el MVCS nombró el Comité de Gestión de Seguridad de la Información con RM N° 072-2016-VIVIENDA, así como un oficial de Seguridad de la Información RM N° 166-2016-VIVIENDA, los cuales los cuales se reúnen de manera periódica para la aprobación de documentos y revisión de avances referente a la Seguridad de la Información y al SGSI.
A.6.1.2	Segregación de funciones	Aplica	En la Resolución Ministerial N° 072-2016-VIVIENDA se designó como miembros de comité a las siguientes personas: - El Ministro - El Director General de la Oficina General de Administración - El Director General de la Oficina General de Planeamiento y Presupuesto - El Director General de Estadística e Informática - El Director General de la Oficina General de Asesoría Jurídica - Oficial de Seguridad de la Información



A.6.1.3	Contacto con autoridades	Aplica	Cesar Vilchez Inga - Subsecretario de Tecnologías Digitales Maurice Frayssinet - Secretaria de Gobierno Digital - SeGDI
A.6.1.4	Contacto con grupos especial de interés	Aplica	Conectados al Grupo de WhatsApp "CISO Perú" (SeGDI)
A.6.1.5	Seguridad de la información en la gestión de proyectos.	Aplica	Actualmente se puede evidenciar la existencia de acuerdos de confidencialidad en los contratos con los proveedores, trabajadores y locadores de la organización para evitar la divulgación de información. Sin embargo, se debe emitir una normativa adecuada en la cual se indique cada cuanto se debe revisar y actualizar estos acuerdos de confidencialidad con los trabajadores
A.6.2	Dispositivos móviles y teletrabajo		
A.6.2.1	Política de dispositivos móviles	Aplica	Documento con recomendaciones y guías para el uso de dispositivos
A.6.2.2	Teletrabajo	No aplica	En el MVCS no ha establecido el teletrabajo
A.7	Seguridad de los recursos humanos		
A.7.1	Antes del empleo		
A.7.1.1	Selección	Aplica	Proceso de revisión de antecedentes dentro del ministerio y en redes
A.7.1.2	Términos y condiciones del empleo	Aplica	Inclusión de elementos de seguridad sobre los procesos de selección de personal
A.7.2	Durante el empleo		
A.7.2.1	Responsabilidades de la gerencia	Aplica	Responsabilidad asignada al equipo de la OGGRH
A.7.2.2	Concientización, educación y capacitación sobre la seguridad de la información	Aplica	Plan de formación y capacitación continua (intranet y e-learning)
A.7.2.3	Proceso disciplinario	Aplica	Existe proceso de apertura y seguimiento de procesos disciplinarios
A.7.3	Terminación y cambio de empleo		
A.7.3.1	Terminación o cambio de responsabilidades del empleo.	Aplica	Existe proceso de cese o cambio de puesto de trabajo
A.8	Gestión de activos		
A.8.1	Responsabilidad por los activos		
A.8.1.1	Inventario de activos	Aplica	Existe inventario en herramienta de gestión
A.8.1.2	Propiedad de los activos	Aplica	Propiedad reflejada en inventario de activos
A.8.1.3	Uso aceptable de los activos	Aplica	Política de uso aceptable de activos pendientes de firma por parte de los usuarios
A.8.1.4	Retorno de activos	Aplica	Incluido en procedimiento existente de uso de activos
A.8.2	Clasificación de la información		
A.8.2.1	Clasificación de la información	Aplica	Incluido en procedimiento existente de uso de activos
A.8.2.2	Etiquetado de la información	Aplica	Incluido en procedimiento existente de uso de activos
A.8.2.3	Manejo de activos	Aplica	Incluido en procedimiento existente de uso de activos
A.8.3	Manejo de los medios		
A.8.3.1	Gestión de medios removibles	Aplica	Incluido en procedimiento existente de uso de activos
A.8.3.2	Devolución de medios	Aplica	Incluido en procedimiento existente de uso de activos
A.8.3.3	Transferencia de medios físicos	Aplica	Incluido en procedimiento existente de uso de activos
A.9	Control de acceso		
A.9.1	Requisitos de la empresa para el control de acceso		
A.9.1.1	Política de control de acceso	Aplica	En proceso de implementación
A.9.1.2	Acceso a redes y servicios de red	Aplica	Existe procedimiento implementado por la Oficina de Tecnología de la Información



A.9.2	Gestión de acceso de usuarios		
A.9.2.1	Registro y baja de usuarios	Aplica	Existe procedimiento implementado por la Oficina de Tecnología de la Información
A.9.2.2	Aprovisionamiento de acceso a usuario	Aplica	Inventario de accesos mantenido por la Oficina de Tecnología de la Información
A.9.2.3	Gestión de derechos de acceso privilegiados	Aplica	Inventario de accesos mantenido por la Oficina de Tecnología de la Información
A.9.2.4	Gestión de información de autenticación secreta de usuarios	Aplica	Inventario de accesos mantenido por la Oficina de Tecnología de la Información
A.9.2.5	Revisión de derechos de acceso de usuarios	Aplica	Procedimiento de revisión periódica de accesos pendientes de implementar
A.9.2.6	Remoción o ajuste de derechos de acceso	Aplica	Procedimiento de revisión periódica de accesos pendientes de implementar
A.9.3	Responsabilidades de los usuarios		
A.9.3.1	Uso de información de autenticación secreta	Aplica	Procedimiento para el control de acceso implementado
A.9.4	Control de acceso a sistema y aplicación		
A.9.4.1	Restricción de acceso a la información	Aplica	Procedimiento para el control de acceso implementado
A.9.4.2	Procedimientos de ingreso seguro	Aplica	Pendiente de integrar en aplicaciones de sistema que permita inicio seguro de sesión único
A.9.4.3	Sistema de gestión de contraseñas	Aplica	Procedimiento de autogestión de contraseñas implementado y comunicado
A.9.4.4	Uso de programas utilitarios privilegiados	Aplica	Herramientas implementadas y en uso por la OTI
A.9.4.5	Control de acceso al código fuente de los programas	Aplica	Inventario de accesos mantenido por la Oficina de Tecnología de la Información
A.10	Criptografía		
A.10.1	Controles criptográficos		
A.10.1.1	Política sobre el uso de controles criptográficos	Aplica	Procedimientos implementado por la OTI
A.10.1.2	Gestión de claves	Aplica	Inventario de accesos mantenido por la Oficina de Tecnología de la Información
A.11	Seguridad física y ambiental		
A.11.1	Áreas seguras		
A.11.1.1	Perímetro de seguridad física	Aplica	Medidas físicas de seguridad en perímetro del ministerio implementadas
A.11.1.2	Controles de ingreso físico	Aplica	Medidas de control de acceso físico implementadas
A.11.1.3	Asegurar oficinas, áreas e instalaciones	Aplica	Medidas de control de acceso físico implementadas
A.11.1.4	Protección contra amenazas externas y ambientales	Aplica	Medidas de control de acceso físico implementadas
A.11.1.5	Trabajo en áreas seguras	Aplica	Auditorías de cumplimiento de normativa de seguridad en el puesto de trabajo realizadas por terceros
A.11.1.6	Áreas de despacho y carga	Aplica	Áreas delimitadas
A.11.2	Equipos		
A.11.2.1	Emplazamiento y protección de los equipos	Aplica	Ubicación y seguridad física de equipos reglamentadas
A.11.2.2	Servicios de suministro	Aplica	Suministro instalado e inventariado
A.11.2.3	Seguridad del cableado	Aplica	Cableado implementado de forma ordenada y segura
A.11.2.4	Mantenimiento de equipos	Aplica	Equipos revisados de forma periódica según procedimiento
A.11.2.5	Remoción de activos	Aplica	Equipos son retirados de su lugar con autorización



A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Aplica	Política de uso aceptable de activos pendientes de firma por parte de los usuarios
A.11.2.7	Disposición o reutilización segura de equipos	Aplica	Política de uso aceptable de activos pendientes de firma por parte de los usuarios
A.11.2.8	Equipos de usuario desatendidos	Aplica	Política de uso aceptable de activos pendientes de firma por parte de los usuarios
A.11.2.9	Política de escritorio limpio y pantalla limpia.	Aplica	Política de uso aceptable de activos pendientes de firma por parte de los usuarios
A.12 Seguridad de las operaciones			
A.12.1 Procedimientos y responsabilidades operativas			
A.12.1.1	Procedimientos operativos documentados	Aplica	Documentos y manuales de operación
A.12.1.2	Gestión del cambio	Aplica	Documentos y procedimientos para la gestión del cambio
A.12.1.3	Gestión de la capacidad	Aplica	Documento con la inclusión de las responsabilidades, funciones o en los cargos o en los procesos implementados
A.12.1.4	Separación de los entornos de desarrollo, pruebas y operaciones	Aplica	Documento de arquitectura de red y entornos mantenido por la OTI
A.12.2 Protección contra códigos maliciosos			
A.12.2.1	Controles contra códigos maliciosos	Aplica	Procesos de ejecución de software de análisis
A.12.3 Respaldo			
A.12.3.1	Respaldo de la información	Aplica	Procedimientos de realización de copias de seguridad existente
A.12.4 Registros y monitoreo			
A.12.4.1	Registro de eventos	Aplica	Documentos de procedimientos de uso de entornos mantenido por OTI
A.12.4.2	Protección de información de registros	Aplica	Documentos de procedimientos de uso de entornos mantenido por OTI
A.12.4.3	Registros del administrador y del operador	Aplica	Documentos de procedimientos de uso de entornos mantenido por OTI
A.12.4.4	Sincronización de reloj	Aplica	Documentos de procedimientos de uso de entornos mantenido por OTI
A.12.5 Control del software operacional			
A.12.5.1	Instalación de software en sistemas operacionales	Aplica	Documentos de procedimientos de uso de entornos mantenido por OTI
A.12.6 Gestión de vulnerabilidad técnica			
A.12.6.1	Gestión de vulnerabilidades técnicas	Aplica	Documentos de procedimientos de uso de entornos mantenido por OTI
A.12.6.2	Restricciones sobre la instalación de software	Aplica	Documentos de procedimientos de uso de entornos mantenido por OTI
A.12.7 Consideraciones para la auditoría de los sistemas de información			
A.12.7.1	Controles de auditoría de sistemas de información	Aplica	Documentos de procedimientos de uso de entornos mantenido por OTI
A.13 Seguridad de las comunicaciones			
A.13.1 Gestión de seguridad de la red			
A.13.1.1	Controles de la red	Aplica	Documento de uso aceptable de recursos existente
A.13.1.2	Seguridad de servicios de red	Aplica	Documento de procedimientos de uso de entornos mantenido por la OTI
A.13.1.3	Segregación en redes	Aplica	Documento de procedimientos de uso de entornos mantenido por la OTI
A.13.2 Transferencia de información			



A.13.2.1	Políticas y procedimientos de transferencia de la información	Aplica	Documento de uso aceptable de recursos existente
A.13.2.2	Acuerdo sobre transferencia de información	Aplica	Documento de uso aceptable de recursos existente
A.13.2.3	Mensajes electrónicos	Aplica	Documento de uso aceptable de recursos existente
A.13.2.4	Acuerdos de confidencialidad o no divulgación	Aplica	Contratos suscritos por diversos proveedores y contratantes. Documento de uso aceptable de recursos existente
A.14 Adquisición, desarrollo y mantenimiento de sistemas			
A.14.1 Requisitos de seguridad de los sistemas de información			
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Aplica	Procedimientos de especificaciones de seguridad implantado por la OTI
A.14.1.2	Aseguramiento de servicios de aplicaciones sobre redes públicas	Aplica	Procedimientos de especificaciones de seguridad implantado por la OTI
A.14.1.3	Protección de transacciones en servicios de aplicación	Aplica	Procedimientos de especificaciones de seguridad implantado por la OTI
A.14.2 Seguridad en los procesos de desarrollo y soporte			
A.14.2.1	Política de desarrollo seguro	Aplica	Procedimientos de especificaciones de seguridad implantado por la OTI
A.14.2.2	Procedimientos de control de cambio del sistema	Aplica	Procedimientos de especificaciones de seguridad implantado por la OTI
A.14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	Aplica	Procedimientos de especificaciones de seguridad implantado por la OTI
A.14.2.4	Restricciones sobre cambios a los paquetes de software	Aplica	Procedimientos de especificaciones de seguridad implantado por la OTI
A.14.2.5	Principios de ingeniería de sistemas seguros	Aplica	Procedimientos de especificaciones de seguridad implantado por la OTI
A.14.2.6	Ambiente de desarrollo seguro	Aplica	Procedimientos de especificaciones de seguridad implantado por la OTI
A.14.2.7	Desarrollo contratado externamente	Aplica	Procedimientos de especificaciones de seguridad implantado por la OTI
A.14.2.8	Pruebas de seguridad del sistema	Aplica	Procedimientos de especificaciones de seguridad implantado por la OTI
A.14.2.9	Pruebas de aceptación del sistema	Aplica	Procedimientos de especificaciones de seguridad implantado por la OTI
A.14.3 Datos de prueba			
A.14.3.1	Protección de datos de prueba	Aplica	Procedimientos de especificaciones de seguridad implantado por la OTI
A.15 Relaciones con los proveedores			
A.15.1 Seguridad de la información en las relaciones con los proveedores			
A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores	Aplica	Procedimientos de especificaciones de seguridad implantado por la OGEI
A.15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	Aplica	Procedimientos de especificaciones de seguridad implantado por la OGEI
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Aplica	Procedimientos de especificaciones de seguridad implantado por la OGEI



A.15.2	Seguridad de la información en las relaciones con los proveedores		
A.15.2.1	Monitoreo y revisión de servicios de los proveedores	Aplica	Procedimientos de especificaciones de seguridad implantado por la OGEI
A.15.2.2	Gestión de cambios a los servicios de proveedores	Aplica	Responsabilidades asignadas y procedimiento de seguridad implementado
A.16	Gestión de incidentes de seguridad de la información		
A.16.1	Gestión de incidentes de seguridad de la información y mejoras		
A.16.1.1	Responsabilidades y procedimientos	Aplica	Responsabilidades asignadas a los distintos grupos creados
A.16.1.2	Reporte de eventos de seguridad de la información	Aplica	Procedimiento de notificación de eventos de seguridad a la OTI y a la dirección por implantar
A.16.1.3	Reporte de debilidades de seguridad de la información	Aplica	Resultado de la auditoria de seguridad interna
A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	Aplica	Resultado de la auditoria de seguridad interna
A.16.1.5	Respuesta a incidentes de seguridad de la información	Aplica	Pendiente de realizar auditoria de seguridad interna
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Aplica	Resultado de la auditoria de seguridad interna
A.16.1.7	Recolección de evidencia	Aplica	Procedimientos para la identificación, recolección, embalaje y tratamiento de las evidencias
A.17	Aspectos de seguridad de la información en la gestión de continuidad del negocio		
A.17.1	Continuidad de seguridad de la información		
A.17.1.1	Planificación de continuidad de seguridad de la información	Aplica	Procedimiento de continuidad a estar preparados
A.17.1.2	Implementación de continuidad de seguridad de la información	Aplica	Sistemas preparados para asegurar la continuidad
A.17.1.3	Verificación, revisión y evaluación de continuidad de seguridad de la información	Aplica	Sistemas preparados para asegurar la continuidad
A.17.2	Redundancias		
A.17.2.1	Instalaciones de procesamiento de la información	Aplica	Sistemas preparados para asegurar la continuidad pero falta validación
A.18	Cumplimiento		
A.18.1	Cumplimiento con requisitos legales y contractuales		
A.18.1.1	Identificación de requisitos contractuales y de legislación aplicable	Aplica	Documento de normativa vigente aplicable y procedimientos de verificación de cumplimiento
A.18.1.2	Derechos de propiedad intelectual	Aplica	Documento de normativa vigente aplicable y procedimientos de verificación de cumplimiento
A.18.1.3	Protección de registros	Aplica	Documento de normativa vigente aplicable y procedimientos de verificación de cumplimiento
A.18.1.4	Privacidad y protección de datos personales	Aplica	Documento de normativa vigente aplicable y procedimientos de verificación de cumplimiento
A.18.1.5	Regulación de controles criptográficos	Aplica	Documento de normativa vigente aplicable y procedimientos de verificación de cumplimiento



A.18.2	Revisiones de seguridad de la información		
A.18.2.1	Revisión independiente de la seguridad de la información	Aplica	Documento de normativa vigente aplicable y procedimientos de verificación de cumplimiento
A.18.2.2	Cumplimiento de políticas y normas de seguridad	Aplica	Documento de normativa vigente aplicable y procedimientos de verificación de cumplimiento
A.18.2.3	Revisión del cumplimiento técnico	Aplica	Documento de normativa vigente aplicable y procedimientos de verificación de cumplimiento

5. ANÁLISIS DEL RIESGO

5.1 Caracterización de los activos

Antes de realizar el plan a implementar en el Ministerio para mitigar ciertas amenazas o riesgos, primero es necesario evaluar, dentro del marco del SGSI, los activos y valorando los distintos riesgos y amenazas que los afectan.

A continuación, se detalla el análisis de los activos del Ministerio, los riesgos asociados y el impacto potencial sobre los activos, a partir de la metodología definida en el punto "4.1.5 Metodología de Análisis de Riesgos".

La metodología MAGERIT propone que las actividades del análisis de riesgos se realicen a través de las siguientes tareas:

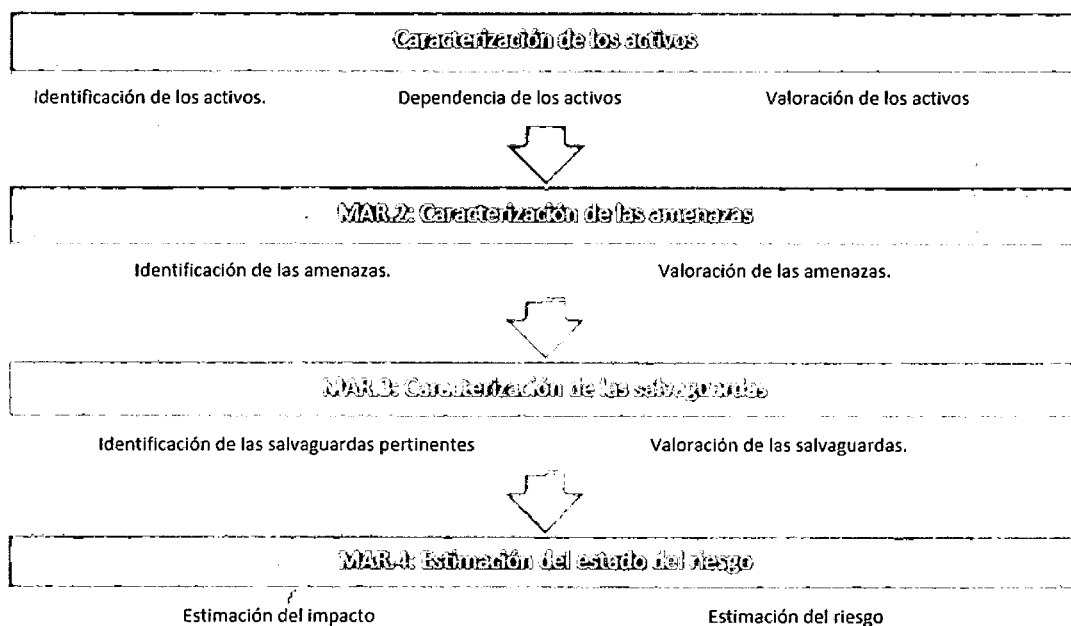


Figura 7. Método de análisis del riesgo. Tomado de MAGERIT

5.1.1 Identificación de los activos

Antes de empezar a valorar los activos, sus amenazas y vulnerabilidades, debemos identificar los activos, objeto del Sistema de Seguridad de la Información, dentro del ministerio.

En el caso de del MVCS, tenemos los siguientes activos:



Redes de comunicación			
Nombre	Cantidad	Tipo	Ubicación
Cableado de datos para puesto de trabajo	-	Cat5e	Edificio (pisos 2,3,5,6) y en todas las sedes
Cableado de datos para servidores	-	Cat5e	Centro de Datos - OGEI
Cableado de datos entre todas las sedes	-	Cat5e	Miraflores, Olacocha, Callao, Blondet, Vitrina Inmobiliaria, Cisnes, Baltazar y San Isidro
Switch	83	Cisco, Alcatel, 3com, TP-Link, HPE, TRENDnet, D-Link, TP-Link	Edificio (pisos 2,3,5,6) y en todas las sedes
Access Point (WiFi)	14	Cisco, D-Link	Piso 2, 3, 5 y 6
Firewalls	2	Palo Alto	Sede Central

Nombre	Cantidad	Ubicación
PCs	1262	En todas las sedes
Portátiles	125	En todas las sedes
Impresoras	114	En todas las sedes
Teléfonos anexos	551	En todas las sedes
Multifuncionales	116	En todas las sedes
Escáneres	37	En todas las sedes
Faximil	7	En todas las sedes
Fotocopiadora	1	En todas las sedes
Plotter	11	En todas las sedes
Servidores	35	En el Centro de Datos (San Isidro)

Aplicaciones			
Nombre	Cantidad	Tipo	Ubicación
Webs	6	No aplica	AWS
Servidor de licencias	2	RLM	AWS

Datos			
Nombre	Cantidad	Tipo	Ubicación
Repositorio de código	3	GIT, SVN, HG	CPD
Base de datos de clientes	1	No aplica	AWS
Base de datos de proveedores	1	No aplica	CPD
Base de datos de recursos humanos	1	No aplica	AWS

Personal			
Nombre	Cantidad	Tipo	Ubicación
Empleados	2900	No aplica	En todas las sedes

Intangibles			
Nombre	Cantidad	Tipo	Ubicación
Satisfacción del ciudadano	No aplica	No aplica	No aplica
Imagen corporativa de la empresa	No aplica	No aplica	No aplica

5.1.2 Valoración de los activos

Para realizar la valoración de los activos se toma en consideración tanto las dimensiones en que el activo es relevante, como su estimación de la valoración de cada dimensión.

Las dimensiones a considerar son:

- ✓ (C)onfidencialidad de los datos
- ✓ (I)ntegridad de los datos



- ✓ (D)isponibilidad de los servicios
- ✓ (A)utenticidad de la información y los usuarios
- ✓ (T)razabilidad del uso del servicio y los datos

Aplicando las escalas anteriores a los activos del ministerio, tenemos:

Valoración de activos						
Nombre	Valoración	Criticidad				
		C	I	D	A	T
Redes de comunicación						
Cableado de datos para puestos de trabajo	Baja	8	5	10	8	8
Cableado de datos para servidores	Baja	8	5	10	8	8
Cableado de datos entre dispositivos de red	Baja	8	5	10	8	8
Switch	Media	8	5	10	8	8
Access Point	Baja	8	5	10	8	8
Firewalls	Media	10	8	10	8	10
Routers	Media	1	2	8	2	2
Hardware (PCs, servidores, consumo)						
PCs	Alta	2	5	1	2	5
Portátiles	Media	2	5	1	2	5
Impresoras	Media	2	5	0	0	4
Teléfonos	Baja	3	5	0	1	2
Servidores	Alta	4	5	3	3	7
Software						
Ofimática	Media	1	5	5	2	5
Aplicaciones de desarrollo	Media	1	5	5	2	5
Aplicaciones de administración	Media	5	5	5	2	5
Motores de base de datos	Media	7	7	7	7	10
Aplicaciones						
Webs	Alta	10	10	10	8	8
Servidor de licencias	Media	7	7	7	8	7
Datos						
Repositorio de código	Muy alta	8	10	10	10	10
Base de datos de clientes	Muy alta	8	10	8	7	8
Base de datos de proveedores	Muy alta	8	10	8	7	8
Base de datos de recursos humanos	Muy alta	8	10	8	7	8
Personal						
Empleados	Muy alta	0	0	5	5	5
Socios directivos	Muy alta	0	0	5	5	5
Intangibles						
Satisfacción de clientes	Muy alta	8	8	0	8	0
Imagen corporativa del ministerio	Muy alta	8	0	0	8	0

Tabla 4. Valoración de los activos

5.2 Caracterización de las amenazas

Con los activos ya identificados y valorados en el numeral anterior, el siguiente paso consiste en determinar las amenazas que puede afectar a cada activo de acuerdo con las siguientes categorías:

1. Desastres naturales [N]
2. De origen industrial [I]
3. Errores y fallos no intencionados [E]
4. Ataques intencionados [A]

Las amenazas pueden centrarse en un activo en particular y por una reacción en cadena afectar el resto de activos de acuerdo a sus relaciones de dependencia.

La actividad de caracterización de amenazas se puede diferenciar en dos tareas: la identificación de las amenazas que afectan a los activos y la valoración de las mismas.



Clasificación de amenazas		
Origen	Amenazas	Identificación
Natural	Inundación	A-NAT1
Natural	Tormenta eléctrica	A-NAT2
Natural	Incendio	A-NAT3
Industrial	Baja médica	A-IND1
Industrial	Bajo rendimiento	A-IND2
No intencionado	Accidente laboral	A-NOINT1
No intencionado	Avería	A-NOINT2
No intencionado	Pérdida / hurto	A-NOINT3
Intencionado	Ataque SQL / DDoS	A-INT1
Intencionado	Robo	A-INT2
Intencionado	Intrusión	A-INT3

Tabla 5: Clasificación de amenazas

Cruzando esta información junto con las frecuencias indicadas en el documento de metodología de análisis y las dimensiones de seguridad, obtenemos el análisis del impacto que tiene cada incidencia sobre los activos de la empresa:

Valoración del Impacto							
Nombre	Amenaza	Frecuenc.	Impacto				
			C	I	D	A	T
Redes de comunicación							
Cableado de datos para puestos de trabajo	A-NAT3	F-5			100%		
Cableado de datos para puestos de trabajo	A-NOINT2	F-5			100%		
Cableado de datos para servidores	A-NAT3	F-5			100%		
Cableado de datos para servidores	A-NOINT2	F-5			100%		
Cableado de datos entre dispositivos de red	A-NAT3	F-5			100%		
Cableado de datos entre dispositivos de red	A-NOINT2	F-5			100%		
Switch	A-NAT3	F-5			100%		
Switch	A-NOINT2	F-5			100%		
Switch	A-INT3	F-5	100%	80%	80%	80%	80%
Access Points	A-NAT3	F-5			100%		
Access Points	A-NOINT2	F-5			100%		
Access Points	A-INT3	F-5	100%	80%	80%	80%	80%
Firewall	A-NAT3	F-5			100%		
Firewall	A-NOINT2	F-5			100%		
Firewall	A-INT3	F-5	100%	80%	80%	80%	80%
Routers	A-NAT3	F-5			100%		
Routers	A-NOINT2	F-5			100%		
Routers	A-INT3	F-5	80%	80%	100%	80%	80%
Hardware (PCs, servidores, consumo)							
PCs	A-NAT1	F-5			100%		
PCs	A-NAT2	F-5			75%		
PCs	A-NAT3	F-5			100%		
PCs	A-NOINT2	F-5			100%		
PCs	A-INT1	F-5			50%		
PCs	A-INT3	F-5	80%	50%			80%
Portátiles	A-NAT1	F-5			100%		
Portátiles	A-NAT2	F-5			75%		
Portátiles	A-NAT3	F-5			100%		
Portátiles	A-NOINT2	F-5	100%		100%		100%
Portátiles	A-INT1	F-5			100%		
Portátiles	A-INT2	F-5	100%		100%		100%
Portátiles	A-INT3	F-5	80%	50%			80%
Impresoras	A-NAT1	F-5					
Impresoras	A-NAT2	F-5			100%		
Impresoras	A-NAT3	F-5			75%		
Teléfonos	A-NAT3	F-5			100%		
Teléfonos	A-NOINT2	F-5			100%		
Servidores	A-NAT1	F-5			100%		
Servidores	A-NAT2	F-5			75%		
Servidores	A-NAT3	F-5			100%		
Servidores	A-NOINT2	F-5			100%		
Servidores	A-INT1	F-5	100%	75%	50%	50%	50%
Servidores	A-INT3	F-5	80%	50%	80%	50%	100%
Software							
Ofimática	A-INT2	F-5			100%		
Aplicaciones de desarrollo	A-INT2	F-5			100%		
Aplicaciones de administración	A-INT2	F-5			100%		



Motores de base de datos	A-INT2	F-5			100%		
Aplicaciones							
Webs	A-NOINT2	F-4	50%	75%	100%	50%	50%
Webs	A-INT1	F-4	75%	80%	100%	75%	100%
Webs	A-INT3	F-5	100%	100%	80%	80%	100%
Servidor de licencias	A-NOINT2	F-4	50%	75%	100%	50%	50%
Servidor de licencias	A-INT1	F-4	75%	80%	100%	75%	100%
Servidor de licencias	A-INT3	F-5	100%	100%	80%	80%	100%
Datos							
Repositorio de código	A-NOINT2	F-4			100%		
Repositorio de código	A-INT1	F-5	100%	75%	50%	50%	50%
Repositorio de código	A-INT3	F-5	80%	50%	80%	50%	100%
Base de datos de clientes	A-NOINT2	F-4			100%		
Base de datos de clientes	A-INT1	F-5	100%	75%	50%	50%	50%
Base de datos de clientes	A-INT3	F-5	80%	50%	80%	50%	100%
Base de datos de proveedores	A-NOINT2	F-4			100%		
Base de datos de proveedores	A-INT1	F-5	100%	75%	50%	50%	50%
Base de datos de proveedores	A-INT3	F-5	80%	50%	80%	50%	100%
Base de datos de recursos humanos	A-NOINT2	F-4			100%		
Base de datos de recursos humanos	A-INT1	F-5	100%	75%	50%	50%	50%
Base de datos de recursos humanos	A-INT3	F-5	80%	50%	80%	50%	100%
Personal							
Empleados	A-IND1	F-3			50%		
Empleados	A-IND2	F-3			50%		
Empleados	A-NOINT1	F-5			50%		
Socios directivos	A-IND1	F-3			50%		
Socios directivos	A-IND2	F-3			50%		
Socios directivos	A-NOINT1	F-5			50%		
Intangibles							
Satisfacción de clientes	A-NOINT2	F-5			50%		
Imagen corporativa del ministerio	A-NOINT2	F-5			50%		

Tabla 6: Valoración del impacto

En cuanto al impacto potencial, para determinar el coste que implicaría a la empresa que se materialice las amenazas, se realiza la siguiente estimación, a partir de la escala de valores definida en el documento de metodología de análisis de riesgos:

Valoración del Riesgo	
Nombre	Valoración
Redes de comunicación	
Cableado de datos para puestos de trabajo	Baja
Cableado de datos para servidores	Baja
Cableado de datos entre dispositivos de red	Baja
Switch	Media
Access Points	Baja
Firewalls	Baja
Routers	Media
Hardware (PCs, servidores, consumo)	
PCs	Alta
Portátiles	Media
Impresoras	Media
Teléfonos	Baja
Servidores	Alta
Software	
Ofimática	Media
Aplicaciones de desarrollo	Media
Aplicaciones de administración	Media
Motores de bases de datos	Media
Aplicaciones	
Webs	Alta
Servidor de licencias	Media
Datos	
Repositorios de código	Muy alta
Base de datos de clientes	Muy alta
Base de datos de proveedores	Muy alta
Base de datos de recursos humanos	Muy alta
Personal	
Empleados	Muy alta
Socios directivos	Muy alta
Intangibles	



Satisfacción del ciudadano	Muy alta
Imagen corporativa del ministerio	Muy alta

Tabla 7: Valoración del Riesgo

El cálculo del riesgo intrínseco, teniendo en cuenta los activos de la empresa, las vulnerabilidades detectadas y el impacto que tendría su materialización, se realiza mediante la siguiente fórmula:

$$\text{Riesgo_Intrínseco} = \text{Valor_activo} \times \text{Vulnerabilidad} \times \text{Impacto}$$

De esta forma tenemos el riesgo intrínseco. Para obtener el riesgo efectivo, aplicando atenuantes que hacen más realista el cálculo, se emplea la fórmula siguiente:

$$\text{Riesgo_Efectivo} = \text{Riesgo_Intrínseco} \times$$

$$\%_disminución_vulnerabilidad \times \%_disminución_impacto$$

6. PROPUESTA DEL PLAN

De acuerdo a los resultados del análisis diferencial realizado en el capítulo 2 y los resultados del plan de tratamiento de riesgos del capítulo 5, en este capítulo se proponen un conjunto de proyectos para poder mejorar el estado de seguridad de la información en el Ministerio de Vivienda, Construcción y Saneamiento.

6.1 Cartera de Proyectos Estratégicos del Plan Estratégico de Tecnología de la Información y Comunicaciones (PETIC) 2017-2021

NOMBRE DEL PROYECTO	CÓDIGO DEL PROYECTO	NTP ISO/IEC 27001
Implementación de un Sistema de Gestión de Seguridad de la Información sostenible: La meta es poder obtener la certificación internacional ISO 27001	PE1	27001 y 27002
Elaboración y aprobación de políticas y procedimientos sectoriales y/o ministeriales en materia tecnología: Estos documentos de gestión deben estar alineados a las normas y estándares actuales nacionales e internacionales, así como también a las buenas prácticas de la industria. Se deben oficializar mediante Resoluciones Ministeriales o de Secretaría General, y deben ser socializados y explicados a todo el personal del sector.	PE2	A.5.1.1 y A.5.1.2
Digitalización de documentos físicos y virtuales con valor legal mediante microformas: Este proceso debe aplicarse tanto a los documentos que ingresan por mesa de partes como para ele partes como para el acervo documentario sectorial. El proceso debe ir acompañado con una reingeniería del sistema de trámite documentario y una adecuada gestión documental.	PE3	A.8.1.3, A.8.2.1, A13.2.2
Integración de los sistemas de información: Los sistemas de información del Ministerio y del sector deben estar integrados entre sí, con una base de información válida y actualizada, apoyándose en información geoespacial y en la recopilación de información realizada con las unidades ejecutoras. La integración de los sistemas busca mejorar la calidad de vida de nuestros servidores y funcionarios para que puedan registrar, evaluar, monitorear y tomar decisiones haciendo uso de un solo sistema seguro, amigable y rápido.	PE4	A.14.1.1, A.14.1.2, A.14.1.3
Implementación de iniciativas de gobierno abierto (datos abiertos) y gobierno electrónico: Los sistemas de gobierno abierto y gobierno electrónico buscan mejorar la calidad de vida de nuestros ciudadanos y de las unidades ejecutoras con las que trabajamos de la mano en los servicios e intervenciones del sector. Dichos sistemas fortalecen la transparencia y simplificar los procedimientos administrativos del Ministerio.	PE5	A.8.2.1
Implementación de sistemas estratégicos para la toma de decisiones: Teniendo sistemas de información integrados entre sí e interoperables con		



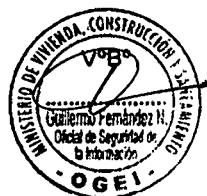
otros sistemas de los diferentes niveles de gobierno se busca mejorar la toma de decisiones en el sector para mejorar la gestión del mismo y disminuir las brechas existentes en beneficio de los ciudadanos de las poblaciones urbanas y rurales.	PE6	A.8.2.1
Convergencia de la infraestructura tecnológica: Realizar un esfuerzo para clasificar, inventariar y estandarizar una infraestructura tecnológica flexible, contingente y seguro que pueda apoyar las comunicaciones tecnológicas del Ministerio. La convergencia es una buena práctica de TI que busca tener el menor número posible de fabricantes y proveedores de equipos tecnológicos para facilitar la administración, soporte y mantenimiento de los mismos.	PE7	A.8.2.1, A.8.2.2, A.8.2.3
Migración de sistemas críticos a la nube pública: Para mejorar la contingencia, rendimiento y escalabilidad de los sistemas críticos del Ministerio, estos deben migrar a un entorno de nube pública donde se puedan administrar de manera sostenida y rentable.	PE8	A.12.3.1
Migración de servicios tecnológicos a la nube pública: Para mejorar la contingencia, capacidad, facilidad de uso, rendimiento y escalabilidad de los servicios tecnológicos del Ministerio, estos deben migrar a un entorno de nube pública donde se pueden administrar de manera centralizada, sostenida y rentable.	PE9	A.12.3.1
Aplicación de tecnologías RFID: Se debe aplicar este tipo de tecnologías para mejorar el control de visitas y activos tecnológicos.	PE10	A.11.1.2, A.11.1.3
Explotación de aplicaciones y dispositivos móviles: Aprovechar las facilidades que los dispositivos nos brindan como la portabilidad, georreferenciación, captura de imágenes, alertas, entre otros.	PE11	A.6.2.1
Implementación de tecnologías para prevención de desastres.	PE12	A.17.11
Implementación de un servicio de acceso a Internet rápido, seguro y contingente.	PE13	A.9.1.2
Implementación de tecnologías de prevención y corrección de ataques informáticos.	PE14	A.12.2.1
Fortalecimiento de capacidades del personal de la OGEI a través de capacidades continuas en tendencias tecnológicas y estadísticas, estándares internacionales y buenas prácticas reconocidas en la industria.	PE15	A.7.2.2
Implementación de un geoportal y reportes georreferenciados dentro de los sistemas de información del MVCS incluyendo información de los principales actores de los sectores agua, saneamiento y vivienda.	PE16	A.9.4.1
Implementación de Minería de Datos, Inteligencia de Negocios y Big Data dentro de los sistemas de información del MVCS.	PE17	A.9.4.1, A.9.4.2
Implementación de un Centro de Servicios Tecnológicos: Abarca todo lo referente a la ISO 20000 y las buenas prácticas de ITIL.	PE18	A.14.1.1, A.14.1.2, A.14.1.3

Tabla 8. Cartera de Proyectos Estratégicos del PETIC del MVCS 2017-2021

6.2 Proyectos propuestos

En la siguiente tabla se enumeran las propuestas de proyectos a ejecutar, así como el control al cual soportan:

Proyecto		Dominio Control SGSI
6.1.1	Plan de capacitación sobre SGSI a distintos estamentos que tratan la información	7.2, A.9.2, A11.2.8, A11.2.9, A13.2.4, A16.1.2, A16.1.3, A16.1.6, A18.1.4, A18.2.2
6.1.2	Reorganización de la Oficina de Tecnologías de la Información	5.3, 7.2, A6.1.1, A6.1.2, A7.2.2
6.1.3	Cifrado de discos duros de dispositivos móviles (portátiles, tabletas y móviles) de personal que maneje información sensible.	8.3, A6.2.1, A11.2.6
6.1.4	Plan de Contingencia de OGEI.	A12.3, A.17.1.1, A17.1.2, A17.1.3
6.1.5	Selección, adquisición e implementación de un sistema gestor de incidentes y seguridad de la información (SIEM).	A16.1



6.1.6	Selección, adquisición e implementación de un sistema de prevención y detección de intrusos (IDS e IPS) para la red de datos del MVCS.	A16.1, A12.2.1
6.1.7	Selección e implementación de un servicio de Ethical Hacking para la detección de vulnerabilidades para la red de datos del MVCS.	6.1.2, 6.1.3, A.12.6.1
6.1.8	Parametrización del sistema de mesa de ayuda para que incluya la gestión de incidentes.	A16.1
6.1.9	Selección, adquisición e implementación de un DLP (Data Loss Prevention).	A18.1.2, A18.1.3, A18.1.4
6.1.10	Plan de auditorías al SGSI del ministerio.	9.2, A18.1.2, A18.2.2, A18.2.3
6.1.11	Compra de memorias USB cifradas para uso en el Centro de Datos y dependencias que manejan información sensible.	8.3, A6.2.1, A11.2.6
6.1.12	Hardening de servidores del MVCS.	A11.5
6.1.13	Proceso de archivado y backup en la nube	A12.3, A.17.1, A.17.1.1, A17.1.2, A17.1.3

Tabla 9. Proyectos propuestos y su impacto en NTP-ISO/IEC 27001:2014 y Matriz de riesgo a mitigar

Para desarrollar los proyectos relacionados con sistemas de información o aplicativos nuevos, se trabajará una metodología con las siguientes fases:

1. Investigación del mercado y selección de soluciones para el proyecto.
2. Pruebas de concepto de cada una de las selecciones consideradas.
3. Selección de unas métricas para la toma de decisión de la mejor solución o herramienta de software más ajustada a las necesidades del SGSI del Ministerio.
4. Selección de la solución de acuerdo a la valoración, a cada una de las métricas.
5. Adquisición de la solución, con las condiciones evaluadas.
6. Implementación de la solución.
7. Pruebas de la solución.
8. Puesta en producción.

Adicionalmente a las soluciones resultado de los proyectos mencionados, es necesario el estudio, aprobación y puesta en marcha de los siguientes procedimientos:

Procedimiento		Dominio / Control SGSI
6.2.1	Procedimiento de borrado seguro para equipos que son cambiados de dependencia y/o son dados de baja.	A11.2.7
6.2.2	Procedimiento de gestión de incidentes de seguridad de la información.	6.1.3, A.16.1
6.2.3	Procedimiento para la configuración de alarmas para gestión de las capacidades de los servidores del Centro de Cómputo.	A12.1.3
6.2.4	Procedimiento de revisión de políticas de seguridad de la información.	9.3, A18.2, A18.2.3
6.2.5	Procedimiento de tratamiento de no conformidades en materia de seguridad de la información.	10.1
6.2.6	Procedimiento de revisión del estado del SGSI en el Ministerio.	10.2, A18.2.2

Tabla 10: Procedimientos nuevos a elaborar para soportar el SGSI del MVCS

6.1.1 Plan de capacitación sobre seguridad de la información y SGSI a todos los responsables que tratan la información

OBJETIVO

Mejorar las competencias de los responsables del tratamiento de la información en el Ministerio, respecto a la confidencialidad, integridad y disponibilidad de la misma y los riesgos que corre dicha información.



ALCANCE	
Todos los trabajadores del Ministerio	
RESPONSABLE	AREAS INVOLUCRADAS
OGGRH	Todos los responsables
COSTO APROXIMADO	
PLAZO DE EJECUCIÓN	Corto plazo
TIEMPO ESTIMADO DE EJECUCIÓN	6 meses
ACTIVIDADES	
- Elaboración de un plan de capacitación (se debe involucrar al proveedor de antivirus) - Aprobación de recursos y actividades de formación (enseñanza digital) - Ejecución del plan de formación (enseñanza digital) - Evaluación de las actividades de capacitación por parte de los participantes.	

6.1.2 Revisión de nuevos roles y funciones de seguridad en la Oficina de Tecnología de la Información.

OBJETIVO	
Gestionar en forma adecuada la seguridad de la información, según los roles y nuevas funciones resultantes de los nuevos proyectos y la puesta en marcha del SGSI.	
ALCANCE	
Únicamente a la Oficina de Tecnologías de la Información	
RESPONSABLE	AREAS INVOLUCRADAS
Director de la Oficina de Tecnologías de la Información	Dirección de la Oficina de Tecnologías de la Información
COSTO APROXIMADO	
PLAZO DE EJECUCIÓN	Corto plazo
TIEMPO ESTIMADO DE EJECUCIÓN	3 meses
ACTIVIDADES	
- Revisión de las nuevas funciones de seguridad de la información para la dirección y los nuevos roles de acuerdo al desarrollo de los proyectos propuestos. - Identificación de los nuevos cargos a cubrir. - Caracterización de los cargos nuevos y actuales y reestructuración del manual de funciones. - Contratación del personal nuevo. - Entrenamiento del personal nuevo.	

6.1.3 Cifrado de discos duros de dispositivos móviles (portátiles, tabletas y móviles) de personal que maneje información sensible.

OBJETIVO	
Proteger la información almacenada en dispositivos móviles de ataques contra la confidencialidad e integridad y secuestro de información.	
ALCANCE	
Equipos móviles (portátiles, tabletas, celulares) de los directores y personal que manejen información sensible.	
RESPONSABLE	AREAS INVOLUCRADAS
Director de la Oficina de Tecnologías de la Información	Dirección de la Oficina de Tecnologías de la Información
COSTO APROXIMADO	
PLAZO DE EJECUCIÓN	Mediano plazo
TIEMPO ESTIMADO DE EJECUCIÓN	3 meses
ACTIVIDADES	
- Evaluación de los dispositivos móviles cuyos dispositivos de almacenamiento amerita ser cifrado. - Realización del proceso de cifrado. - Capacitación al personal que usará dichos equipos.	

6.1.4 Actualización del Plan de Contingencia de OGEI.

OBJETIVO	
Evitar la interrupción de los servicios de misión crítica y restablecer el pleno funcionamiento en el menor tiempo posible.	



ALCANCE	
Sistema de información de OGEI	
RESPONSABLE	AREAS INVOLUCRADAS
Oficial de Seguridad de la Información	OGEI
COSTO APROXIMADO	
PLAZO DE EJECUCIÓN	Mediano plazo
TIEMPO ESTIMADO DE EJECUCIÓN	1 año
ACTIVIDADES	
- Identificación y priorización de las amenazas. - Análisis de impacto del MVCS. - Creación del plan de respuesta y recuperación. - Adecuación de la solución. - Pruebas. - Refinamiento del Plan de Contingencia de OGEI.	

6.1.5 Selección, adquisición e implementación de un sistema gestor de eventos y seguridad de la información (SIEM).

OBJETIVO	
Centralizar el almacenamiento y la interpretación de los datos relevantes de seguridad (logs), facilitando la detección de tendencias y patrones no habituales	
ALCANCE	
Sede San Isidro	
RESPONSABLE	AREAS INVOLUCRADAS
Director de la Oficina de Tecnologías de la Información	Dirección de la Oficina de Tecnologías de la Información
COSTO APROXIMADO	
PLAZO DE EJECUCIÓN	Mediano plazo
TIEMPO ESTIMADO DE EJECUCIÓN	6 meses
ACTIVIDADES	
- Investigación del mercado y selección de soluciones para el proyecto. - Pruebas de concepto de cada una de las selecciones consideradas. - Selección de unas métricas para la toma de decisión de la mejor solución o herramienta de software más ajustada a las necesidades del SGSI del MVCS. - Selección de una solución de acuerdo a la valoración, de acuerdo a cada una de las métricas. - Adquisición de la solución, con las condiciones evaluadas. - Implementación de la solución. - Pruebas de solución. - Puesta en producción.	

6.1.6 Selección, adquisición e implementación de un sistema de prevención y detección de intrusos para la red de datos del MVCS (IDS e IPS).

OBJETIVO	
Detectar las actividades anormales, que puedan evidenciar la explotación de alguna vulnerabilidad de la infraestructura de red o la materialización de un riesgo de un activo.	
ALCANCE	
Sede San Isidro	
RESPONSABLE	AREAS INVOLUCRADAS
Director de la Oficina de Tecnologías de la Información	Dirección de la Oficina de Tecnologías de la Información
COSTO APROXIMADO	
PLAZO DE EJECUCIÓN	Largo plazo
TIEMPO ESTIMADO DE EJECUCIÓN	6 meses
ACTIVIDADES	
- Investigación del mercado y selección de soluciones para el proyecto. - Pruebas de concepto de cada una de las selecciones consideradas. - Selección de unas métricas para la toma de decisión de la mejor solución o herramienta de software más ajustada a las necesidades del SGSI del MVCS. - Selección de una solución de acuerdo a la valoración, de acuerdo a cada una de las métricas. - Adquisición de la solución, con las condiciones evaluadas.	



- Implementación de la solución.
- Pruebas de solución.
- Puesta en producción.

6.1.7 Selección e implementación de un servicio de Ethical Hacking para la detección de vulnerabilidades en el centro de datos y la red de datos del MVCS.

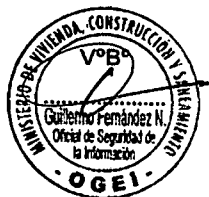
OBJETIVO	
Detectar las vulnerabilidades de sistemas, redes y servicios y realizar actividades de Pentesting al momento de implementar soluciones nuevas para el manejo de información.	
ALCANCE	
Centro de Datos y red del MVCS en la Sede San Isidro	
RESPONSABLE	AREAS INVOLUCRADAS
Director de la Oficina de Tecnologías de la Información	Dirección de la Oficina de Tecnologías de la Información
COSTO APROXIMADO	
PLAZO DE EJECUCIÓN	Mediano plazo
TIEMPO ESTIMADO DE EJECUCIÓN	6 meses
ACTIVIDADES	
- Investigación del mercado y selección de soluciones para el proyecto. - Pruebas de concepto de cada una de las selecciones consideradas. - Selección de unas métricas para la toma de decisión de la mejor solución para el servicio de Ethical Hacking para las necesidades del SGSI del MVCS. - Selección de una solución de acuerdo a la valoración, de acuerdo a cada una de las métricas. - Adquisición de la solución, con las condiciones evaluadas. - Implementación del servicio. - Puesta en ejecución del servicio.	

6.1.8 Parametrización del sistema de mesa de ayuda para que incluya la gestión de incidentes.

OBJETIVO	
Realizar la gestión de incidentes haciendo uso de la plataforma de Mesa de Ayuda implementado para soporte técnico.	
ALCANCE	
Sede San Isidro	
RESPONSABLE	AREAS INVOLUCRADAS
Director de la Oficina de Tecnologías de la Información	Dirección de la Oficina de Tecnologías de la Información
COSTO APROXIMADO	
PLAZO DE EJECUCIÓN	Mediano plazo
TIEMPO ESTIMADO DE EJECUCIÓN	6 meses
ACTIVIDADES	
- Revisión de requerimientos para la gestión de incidentes. - Adecuación de los requerimientos y activación de módulos que soporten dichos requerimientos. - Implementación de la solución. - Pruebas de la solución. - Puesta en producción.	

6.1.9 Selección, adquisición e implementación de un DLP (Data Loss Prevention).

OBJETIVO	
Disminuir los riesgos asociados con fuga de información sensible y confidencial del MVCS.	
ALCANCE	
Sede San Isidro	
RESPONSABLE	AREAS INVOLUCRADAS
Director de la Oficina de Tecnologías de la Información	Dirección de la Oficina de Tecnologías de la Información



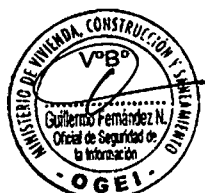
COSTO APROXIMADO	
PLAZO DE EJECUCIÓN	Largo plazo
TIEMPO ESTIMADO DE EJECUCIÓN	6 meses
ACTIVIDADES	
- Investigación del mercado y selección de soluciones para el proyecto. - Pruebas de concepto de cada una de las selecciones consideradas. - Selección de una métrica para la toma de decisión de la mejor solución o herramienta de software más ajustada a las necesidades del SGSI del MVCS. - Selección de la solución de acuerdo a la valoración, de acuerdo a cada una de las métricas. - Adquisición de la solución, con las condiciones evaluadas. - Implementación de la solución. - Pruebas de la solución. - Puesta en producción.	

6.1.10 Compra de memorias USB cifradas para uso en el Centro de Datos y dependencias que manejan información sensible.

OBJETIVO	
Mitigar el riesgo de pérdida de dispositivos de almacenamiento externo con información sensible o información de carácter personal, para cumplir con la Ley de Protección de Datos Personales.	
ALCANCE	
Sede San Isidro	
RESPONSABLE	AREAS INVOLUCRADAS
Director de la Oficina de Tecnologías de la Información	Dirección de la Oficina de Tecnologías de la Información
COSTO APROXIMADO	
PLAZO DE EJECUCIÓN	Largo plazo
TIEMPO ESTIMADO DE EJECUCIÓN	3 meses
ACTIVIDADES	
- Investigación del mercado y selección de soluciones para el proyecto. - Pruebas de concepto de cada una de las selecciones consideradas. - Selección de unas métricas para la toma de decisión de la mejor solución o herramienta de software más ajustada a las necesidades del SGSI del ministerio. - Adquisición de la solución, con las condiciones evaluadas. - Implementación de la solución. - Pruebas de la solución. - Puesta en producción.	

6.1.11 Hardening (fortalecimiento) de servidores del MVCS.

OBJETIVO	
Mitigar el riesgo relacionado por errores en las configuraciones, instalaciones por defecto, puertos abiertos innecesarios, mal uso de mecanismos de autenticación y vulnerabilidades en los sistemas operativos, servicios y protocolos.	
ALCANCE	
Sede San Isidro	
RESPONSABLE	AREAS INVOLUCRADAS
Director de la Oficina de Tecnologías de la Información	Áreas que manejan información sensible
COSTO APROXIMADO	
PLAZO DE EJECUCIÓN	Mediano plazo
TIEMPO ESTIMADO DE EJECUCIÓN	6 meses
ACTIVIDADES	
- Desarrollar cronograma de actividades de hardening de servidores. - Configuraciones necesarias para protegerse de posibles ataques físicos o de hardware de la máquina. - Instalación segura del sistema operativo. - Activación y/o configuración adecuada de servicios de actualizaciones automáticas. - Instalación, configuración y mantención de programas de seguridad tales como Antivirus, Antispyware, y un filtro Antispam según las necesidades del sistema. - Configuración de la política local del sistema.	



- Configuración de opciones de seguridad generales.
- Restricciones de software.
- Activación de auditorías de sistema.
- Configuración de servicios de sistema.
- Configuración de los protocolos de Red.
- Configuración adecuada de permisos de seguridad en archivos y carpetas del sistema.
- Configuración de opciones de seguridad de los distintos programas.
- Configuración de acceso remoto.
- Configuración adecuada de cuentas de usuario.
- Cifrado de archivos o unidades según las necesidades del sistema.
- Realizar y programar un sistema de respaldos frecuente a los archivos y al estado de sistema.
- Eliminación de usuarios que no sean los que se requieren.
- Configuración de credenciales más robustas.
- Configuración el bloqueo de pantalla luego de cierto tiempo de uso.
- Configuración para que solo admita protocolos robustos.
- Realizar un documento a manera de Check List que sería la guía a seguir para "hardenizar" los servidores y así no perder alguna configuración importante a tener en cuenta en beneficio de la seguridad de la información.
- Pruebas.

6.1.12 Proceso de archivado, backup y recuperación en la nube.

OBJETIVO	
Permitir completar la estrategia de disponibilidad de la información de manera transparente y extremadamente simple con backup's y recuperación ante desastres asociados a la nube como una manera de reducir costes sin incrementar los RPOs y RTOs.	
ALCANCE	
Sede San Isidro	
RESPONSABLE	AREAS INVOLUCRADAS
Director de la Oficina de Tecnologías de la Información	Áreas que manejan información sensible
COSTO APROXIMADO	
PLAZO DE EJECUCIÓN	Mediano plazo
TIEMPO ESTIMADO DE EJECUCIÓN	6 meses
ACTIVIDADES	
- Desarrollar cronograma de actividades del proceso. - Realización de dichas actividades. - Configuración simple de backup y recuperación de la información en la nube. - Pruebas de la solución. - Puesta en producción de la solución.	

6.1.13 Políticas de Seguridad de la Información.

OBJETIVO	
Proteger adecuadamente la información del MVCS, definiendo las medidas esenciales y directivas generales de seguridad de la información, que garanticen el tratamiento adecuado de los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información, implementando un Sistema de Gestión de Seguridad de la Información en el Ministerio.	
ALCANCE	
Sede San Isidro	
RESPONSABLE	AREAS INVOLUCRADAS
Oficial de Seguridad de la Información	Todo el Ministerio, incluyendo aquellos programas que sean unidades ejecutoras
COSTO APROXIMADO	
PLAZO DE EJECUCIÓN	Mediano plazo
TIEMPO ESTIMADO DE EJECUCIÓN	1 año
ACTIVIDADES	
- Desarrollar cronograma de actividades del proceso incluyendo las políticas a realizar. - Realización de dichas actividades. - Monitoreo de las actividades hasta que se conviertan en Resolución de Secretaría General.	



7. AUDITORÍA DE CUMPLIMIENTO

7.1 Metodología

En este capítulo se realiza la evaluación del SGSI del Ministerio, evaluando el grado de madurez alcanzado haciendo uso de NTP-ISO/IEC 27002:2017. En el numeral 1, 2, 3 y 4 del presente documento se encuentra ampliamente explicado este manual de buenas prácticas para la gestión de la seguridad de la información, que cuenta con 14 capítulos de control de seguridad que en su conjunto contienen un total de 35 categorías principales de seguridad y 114 controles.

El modelo de madurez CMM (Capability Maturity Model) fue creado por el Software Engineer Institute y tiene un conjunto de procedimientos para la evaluación y mejora de los procesos de desarrollo, implementación y mantenimiento de software (Mary Beth Chrissis, 2009). Este modelo puede ser extendido a sistemas de gestión para evaluar el nivel de madurez de dicho sistema.

Los niveles del CMM que se aplicarán para evaluar la madurez del sistema de gestión son los siguientes:

Efectividad	CMM	Nivel	Descripción
0%	L0	Inexistente	- Carencia completa de cualquier proceso reconocible. - No se ha reconocido siquiera que existe un problema a resolver.
10%	L1	Inicial / Ad-hoc	- Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. - Los procedimientos son inexistentes o localizados en áreas concretas. - No existen plantillas definidas a nivel corporativo.
50%	L2	Reproducible, no intuitivo	- Los procesos similares se realizan de forma similar por distintas personas con la misma tarea. - Se normalizan las buenas prácticas en base a la experiencia y el método. - Se depende del grado de conocimiento de cada individuo.
90%	L3	Proceso definido	- La organización entera participa en el proceso. - Los procesos están implantados, documentados y comunicados mediante entrenamiento.
95%	L4	Gestionado y medible	- Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. - Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100%	L5	Optimizado	- Los procesos están en constante mejora. - En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

Tabla 11: Criterios de evaluación del modelo de madurez del SGSI

Las fuentes de información utilizadas para la realización del estado de madurez fueron las siguientes:



- Análisis de la documentación soporte aplicable al SGSI:
 - ✓ Política de seguridad de la información aprobada.
 - ✓ Política de correo, Internet y backup aprobada.
 - ✓ Procedimiento aplicable a seguridad de la información.
 - ✓ Reglamentos internos del MVCS.
 - ✓ Documentación de gestión de activos.
 - ✓ Documentación de soporte de los sistemas de información.
- Inspección visual en oficinas
- Revisión de registros que soportan los distintos procesos

7.2 Nivel de madurez del SGSI en el MVCS.

De acuerdo a la evaluación de los controles de la NTP-ISO/IEC 27001, se sintetizan por medio de tablas las conformidades mayores, menores, observaciones y el estado de madurez de cada uno de los controles. Dicha información se encuentra concentrada en el anexo.

Los resultados obtenidos por dominio se resumen en la siguiente tabla:

Dominio	No conformidades			Madurez	
	Mayores	Menores	Observaciones	%	CMM
A.5. Políticas de seguridad de la información	0	1	0	00.5%	L5
A.6. Organización de la seguridad de la información	4	1	0	64.3%	L2
A.7. Seguridad de los recursos humanos	4	2	0	5.0%	L1
A.8. Gestión de activos	10	0	0	10.0%	L1
A.9. Control de acceso	5	8	0	18.0%	L1
A.10. Criptografía	2	0	0	2.0%	L1
A.11. Seguridad física y ambiental	0	12	0	21.0%	L2
A.12. Seguridad de las operaciones	8	6	0	17.0%	L2
A.13. Seguridad de las comunicaciones	2	5	0	9.5%	L2
A.14. Adquisición, desarrollo y mantenimiento de sistemas	10	3	0	14.5%	L2
A.15. Relaciones con los proveedores	5	0	0	5.0%	L1
A.16. Gestión de incidentes de seguridad de la información	4	3	0	8.5%	L1
A.17. Aspectos de seguridad de la información en la gestión de continuidad del negocio	0	4	0	6.0%	L3
A.18. Cumplimiento	1	7	0	11.5%	L2

Tabla 12. Modelo de madurez SGSI de acuerdo con los controles NTP-ISO/IEC 27002:2017

Se tendrá en cuenta los valores obtenidos en cada apartado para determinar de forma orientativa la madurez inicial de cada control y dominio de la seguridad con respecto a los valores CMM representados en la tabla anterior. Esta clasificación inicial de los controles contempla varios estados:

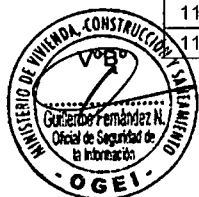
- ✓ Planificado.
- ✓ Iniciado.
- ✓ Implantado – sin documentar.
- ✓ Implantado – sin auditar.
- ✓ Auditado.

Los estados representan el grado de madurez, empezando por el menos maduro y finalizando por el que mayor grado de madurez presenta al inicio de este estudio.

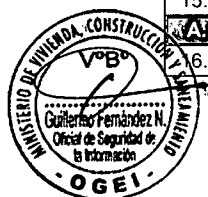
Con respecto a continuación, se muestra la valoración de madurez inicial y CMM tras la implantación de los proyectos propuestos:



ID	Dominio / Control	Aplicabilidad	Madurez inicial	Madurez CMM %
A.6	Políticas de Seguridad de la Información			
5.1.1	Políticas para la seguridad de la información	Aplica	Auditado	00.5%
5.1.2	Revisión de las políticas para la seguridad de la información	Aplica	Implantado – sin auditar	
A.6	Aspectos organizativos para la seguridad			
6.1.1	Roles y Responsabilidades para la seguridad de la información	Aplica	Implantado – sin documentar	64.3 %
6.1.2	Segregación de funciones	Aplica	Iniciado	
6.1.3	Contacto con autoridades	Aplica	Implantado – sin documentar	
6.1.4	Contacto con grupos especial de interés	Aplica	Implantado – sin documentar	
6.1.5	Seguridad de la información en la gestión de proyectos.	Aplica	Iniciado	
6.2.1	Política de dispositivos móviles	Aplica	Planificado	
6.2.2	Teletrabajo	No aplica	No aplica	
A.7	Seguridad de los recursos humanos			
7.1.1	Selección	Aplica	Iniciado	5.0%
7.1.2	Términos y condiciones del empleo	Aplica	Iniciado	
7.2.1	Responsabilidades de la gerencia	Aplica	Iniciado	
7.2.2	Concientización, educación y capacitación sobre la seguridad de la información	Aplica	Implantado – sin auditar	
7.2.3	Proceso disciplinario	Aplica	Implantado – sin auditar	
7.3.1	Terminación o cambio de responsabilidades del empleo.	Aplica	Implantado – sin documentar	
A.8	Gestión de activos			
8.1.1	Inventario de activos	Aplica	Iniciado	10.0%
8.1.2	Propiedad de los activos	Aplica	Iniciado	
8.1.3	Uso aceptable de los activos	Aplica	Iniciado	
8.1.4	Retorno de activos	Aplica	Iniciado	
8.2.1	Clasificación de la información	Aplica	Iniciado	
8.2.2	Etiquetado de la información	Aplica	Iniciado	
8.2.3	Manejo de activos	Aplica	Iniciado	
8.3.1	Gestión de medios removibles	Aplica	Iniciado	
8.3.2	Devolución de medios	Aplica	Iniciado	
8.3.3	Transferencia de medios físicos	Aplica	Iniciado	
A.9	Control de acceso			
9.1.1	Política de control de acceso	Aplica	Iniciado	18.0%
9.1.2	Acceso a redes y servicios de red	Aplica	Implantado – sin documentar	
9.2.1	Registro y baja de usuarios	Aplica	Implantado – sin documentar	
9.2.2	Aprovisionamiento de acceso a usuario	Aplica	Implantado – sin documentar	
9.2.3	Gestión de derechos de acceso privilegiados	Aplica	Iniciado	
9.2.4	Gestión de información de autenticación secreta de usuarios	Aplica	Implantado – sin documentar	
9.2.5	Revisión de derechos de acceso de usuarios	Aplica	Implantado – sin documentar	
9.2.6	Remoción o ajuste de derechos de acceso	Aplica	Implantado – sin auditar	
9.3.1	Uso de información de autenticación secreta	Aplica	Implantado – sin documentar	
9.4.1	Restricción de acceso a la información	Aplica	Iniciado	
9.4.2	Procedimientos de ingreso seguro	Aplica	Iniciado	
9.4.3	Sistema de gestión de contraseñas	Aplica	Iniciado	
9.4.4	Uso de programas utilitarios privilegiados	Aplica	Implantado – sin auditar	
9.4.5	Control de acceso al código fuente de los programas	Aplica	Implantado – sin auditar	
A.10	Criptografía			
10.1.1	Política sobre el uso de controles criptográficos	Aplica	Iniciado	2.0%
10.1.2	Gestión de claves	Aplica	Iniciado	
A.11	Seguridad física y ambiental			
11.1.1	Perímetro de seguridad física	Aplica	Implantado – sin documentar	21.0%
11.1.2	Controles de ingreso físico	Aplica	Implantado – sin documentar	
11.1.3	Asegurar oficinas, áreas e instalaciones	Aplica	Implantado – sin documentar	
11.1.4	Protección contra amenazas externas y ambientales	Aplica	Implantado – sin auditar	
11.1.5	Trabajo en áreas seguras	Aplica	Implantado – sin documentar	
11.1.6	Áreas de despacho y carga	Aplica	Implantado – sin documentar	



11.2.1	Emplazamiento y protección de los equipos	Aplica	Implantado – sin documentar	
11.2.2	Servicios de suministro	Aplica	Implantado – sin documentar	
11.2.3	Seguridad del cableado	Aplica	Implantado – sin documentar	
11.2.4	Mantenimiento de equipos	Aplica	Implantado – sin documentar	
11.2.5	Remoción de activos	Aplica	Implantado – sin documentar	
11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Aplica	Implantado – sin documentar	
11.2.7	Disposición o reutilización segura de equipos	Aplica	Implantado – sin auditar	
11.2.8	Equipos de usuario desatendidos	Aplica	Implantado – sin documentar	
11.2.9	Política de escritorio limpio y pantalla limpia.	Aplica	Implantado – sin documentar	
A.12 Seguridad de las operaciones				
12.1.1	Procedimientos operativos documentados	Aplica	Implantado – sin documentar	17.0%
12.1.2	Gestión del cambio	Aplica	Planificado	
12.1.3	Gestión de la capacidad	Aplica	Implantado – sin documentar	
12.1.4	Separación de los entornos de desarrollo, pruebas y operaciones	Aplica	Iniciado	
12.1.1	Controles contra códigos maliciosos	Aplica	Implantado – sin documentar	
12.3.1	Respaldo de la información	Aplica	Implantado – sin auditar	
12.4.1	Registro de eventos	Aplica	Planificado	
12.4.2	Protección de información de registros	Aplica	Planificado	
12.4.3	Registros del administrador y del operador	Aplica	Iniciado	
12.4.4	Sincronización de reloj	Aplica	Implantado – sin auditar	
12.5.1	Instalación de software en sistemas operacionales	Aplica	Planificado	
12.6.1	Gestión de vulnerabilidades técnicas	Aplica	Iniciado	
12.6.2	Restricciones sobre la instalación de software	Aplica	Implantado – sin documentar	
12.7.1	Controles de auditoría de sistemas de información	Aplica	Iniciado	
A.13 Seguridad de las comunicaciones				
13.1.1	Controles de la red	Aplica	Implantado – sin auditar	9.5%
13.1.2	Seguridad de servicios de red	Aplica	Implantado – sin auditar	
13.1.3	Segregación en redes	Aplica	Implantado – sin auditar	
13.2.1	Políticas y procedimientos de transferencia de la información	Aplica	Planificado	
13.2.2	Acuerdo sobre transferencia de información	Aplica	Planificado	
13.2.3	Mensajes electrónicos	Aplica	Iniciado	
13.2.4	Acuerdos de confidencialidad o no divulgación	Aplica	Implantado – sin documentar	
A.14 Adquisición, desarrollo y mantenimiento de sistemas				
14.1.1	Análisis y especificación de requisitos de seguridad de la información	Aplica	Implantado – sin documentar	14.5%
14.1.2	Aseguramiento de servicios de aplicaciones sobre redes públicas	Aplica	Planificado	
14.1.3	Protección de transacciones en servicios de aplicación	Aplica	Planificado	
14.2.1	Política de desarrollo seguro	Aplica	Implantado - sin documentar	
14.2.2	Procedimientos de control de cambio del sistema	Aplica	Planificado	
14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	Aplica	Planificado	
14.2.4	Restricciones sobre cambios a los paquetes de software	Aplica	Planificado	
14.2.5	Principios de ingeniería de sistemas seguros	Aplica	Planificado	
14.2.6	Ambiente de desarrollo seguro	Aplica	Planificado	
14.2.7	Desarrollo contratado externamente	Aplica	Planificado	
14.2.8	Pruebas de seguridad del sistema	Aplica	Planificado	
14.2.9	Pruebas de aceptación del sistema	Aplica	Planificado	
14.3.1	Protección de datos de prueba	Aplica	Planificado	
A.15 Relaciones con los proveedores				
15.1.1	Política de seguridad de la información para las relaciones con los proveedores	Aplica	Planificado	5.0%
15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	Aplica	Planificado	
15.1.3	Cadena de suministro de tecnología de información y comunicación	Aplica	Planificado	
15.2.1	Monitoreo y revisión de servicios de los proveedores	Aplica	Planificado	
15.2.2	Gestión de cambios a los servicios de proveedores	Aplica	Planificado	
A.16 Gestión de incidentes de seguridad de la información				
16.1.1	Responsabilidades y procedimientos	Aplica	Implantado – sin auditar	8.5%



16.1.2	Reporte de eventos de seguridad de la información	Aplica	Implantado – sin auditar	
16.1.3	Reporte de debilidades de seguridad de la información	Aplica	Implantado – sin documentar	
16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	Aplica	Planificado	
16.1.5	Respuesta a incidentes de seguridad de la información	Aplica	Planificado	
16.1.6	Aprendizaje de los incidentes de seguridad de la información	Aplica	Planificado	
16.1.7	Recolección de evidencia	Aplica	Planificado	
A.17	Aspectos de seguridad de la información en la gestión de continuidad del negocio			
17.1.1	Planificación de continuidad de seguridad de la información	Aplica	Implantado – sin auditar	6.0%
17.1.2	Implementación de continuidad de seguridad de la información	Aplica	Implantado – sin auditar	
17.1.3	Verificación, revisión y evaluación de continuidad de seguridad de la información	Aplica	Implantado – sin auditar	
17.2.1	Instalaciones de procesamiento de la información	Aplica	Implantado – sin auditar	
A.18	Cumplimiento			
18.1.1	Identificación de requisitos contractuales y de legislación aplicable	Aplica	Iniciado	11.5%
18.1.2	Derechos de propiedad intelectual	Aplica	Implantado – sin documentar	
18.1.3	Protección de registros	Aplica	Implantado – sin documentar	
18.1.4	Privacidad y protección de datos personales	Aplica	Implantado – sin documentar	
18.1.5	Regulación de controles criptográficos	Aplica	Planificado	
18.2.1	Revisión independiente de la seguridad de la información	Aplica	Implantado	
18.2.2	Cumplimiento de políticas y normas de seguridad	Aplica	Implantado – sin auditar	
18.2.3	Revisión del cumplimiento técnico	Aplica	Implantado – sin auditar	

Tabla 13: Controles de seguridad NTP-ISO/IEC 27001:2014

Como resultado, tenemos la siguiente cantidad de controles por tipo de madurez inicial:

Madurez inicial	Nº de controles
Planificado	28
Iniciado	27
Implantado – sin documentar	34
Implantado – sin auditar	21
Auditado	1

Tabla 14: Síntesis de cumplimiento de dominios, objetivos de control y controles NTP-ISO/IEC 27001:2014

Representando de forma gráfica la madurez CMM de todos los controles ISO anteriores, tenemos:

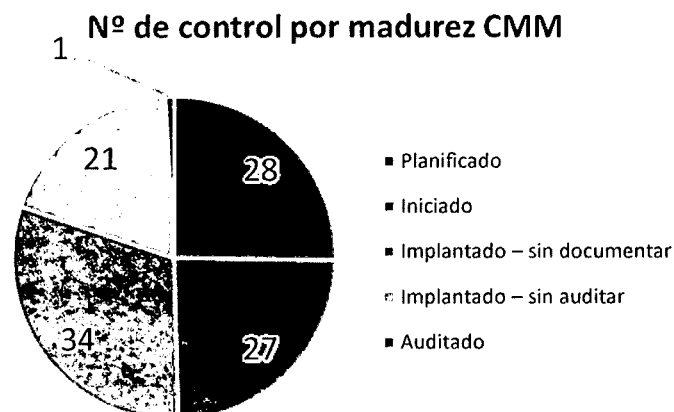


Figura 8: Nivel de Madurez de los controles NTP-ISO/IEC 27001:2014



7.3 Revisión

El presente plan debe ser revisado y evaluado anualmente por el Comité de Gestión de Seguridad de la Información y/o el Oficial de Seguridad de la Información para el enfoque de mejora continua y la preservación de la confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento.

8. CONCLUSIONES

El Plan de Seguridad de la Información para el MVCS, genera en el Ministerio un ambiente de concientización de la importancia de abordar proyectos y programas en materia de seguridad de la información a corto, mediano y largo plazo.

En esta primera etapa se plantea disminuir la brecha que se tiene en seguridad de la información en el MVCS enfocado al riesgo. Además el registro de incidencias sigue siendo necesario para disminuir las brechas existentes con la valoración de los activos (Tabla 4) y la valoración del impacto (Tabla 6).

Los resultados de las propuesta de proyectos a desarrollar en materia de seguridad de la información, serán evaluados por la Oficina de Tecnología de la Información, para ser considerados dentro de los Planes Operativos Informáticos anuales y alineados al Plan Estratégico de Tecnologías de la Información, como parte de los planes de acción con miras a la certificación NTP-ISO/IEC 27001:2014 que se está proyectando conseguir en un período de 3 años.

Finalmente, las auditorias de cumplimiento contribuirán a alcanzar un nivel de madurez idóneo en materia de seguridad de la información de acuerdo a los controles de NTP-ISO/IEC 27002:2017, insumo base para el desarrollo de buenas prácticas en materia de seguridad de la información. Asimismo, podemos complementar estos logros con marcos de trabajo considerados estándares a nivel mundial como ITIL y CMMI para promover un mejor gobierno de la seguridad y tecnología de la información. Todo esto permitirá que el MVCS gestione la información de una forma segura, con un manejo adecuado del riesgo, en cumplimiento de la normatividad legal peruana pertinente y orientado a salvaguardar la confidencialidad, integridad y disponibilidad de la información que se genera, almacena, transporta e intercambia con su entorno.

