UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA DE SISTEMAS Y ADMINISTRACIÓN DE EMPRESAS

CARRERA PROFESIONAL INGENIERÍA DE SISTEMAS

"PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NTP-ISO/IEC 27001:2014 PARA LA PROTECCIÓN DE LA INFORMACIÓN EN LA OFICINA TÉCNICA DE INFORMÁTICA DE UNA ENTIDAD DEL ESTADO"

TRABAJO DE SUFICIENCIA PROFESIONAL
Para optar el Título Profesional de

INGENIERO DE SISTEMAS

PRESENTADO POR EL BACHILLER

MONTENEGRO JULCAPOMA, KATHERINE

Villa El Salvador
2016

DEDICATORIA

Dedico el presente trabajo a Dios que me dio la vida y ha guiado mis pasos, siendo mi compañía y fortaleza en cada momento de mi vida. A mis padres, por brindarme su apoyo incondicional y motivación cuando más lo necesité.

AGRADECIMIENTO

Agradezco a la Universidad Nacional Tecnológica de Lima Sur por su formación y hacer posible que cumpla con mis metas profesionales.

A la Oficina Técnica de Informática del INEI por permitirme ser parte del equipo en la generación del Sistema de Gestión de Seguridad de la Información.

A mis asesores, que supieron motivarme y orientarme en el desarrollo de mi proyecto.

A mis compañeros de universidad y trabajo, que me brindaron palabras de aliento para seguir adelante y no rendirme.

ÍNDICE DE CONTENIDOS

LISTADO DE GRÁFICOS Y FIGURAS

LISTADO DE TABLAS

LISTADO DE ANEXOS

INTRODUCCIÓN

Actualmente, las instituciones y sus sistemas de información están expuestos, progresivamente, a riesgos e inseguridades provenientes de diversas fuentes; la mayoría de incidencias ocurren debido a que los usuarios, por parte de la organización, hacen uso de los sistemas de información de la manera incorrecta o indebida (fraudes informáticos, espionaje, sabotaje, vandalismo, etc.). Y ya no por fallos técnicos, por ejemplo, que los equipos dejen de funcionar.

Esas malas acciones no se pueden prevenir con sólo medidas de seguridad técnicas; también se necesita políticas claras y procedimientos para la seguridad de la información, formación y sensibilización dirigida a todos los empleados, protección legal, medidas de disciplina, etc.

La elaboración de un Plan de Gestión para la mejora de la Seguridad de la Información es una decisión estratégica la cual tiene un impacto positivo sobre toda la institución, y debe ser guiada y apoyada desde la dirección de la misma.

El diseño va a depender de los objetivos y carencias de la institución así como de su estructura, estos elementos son los que definirán el alcance del Plan de Gestión de Seguridad de la Información, es decir los componentes (áreas, unidades, direcciones, departamentos, etc.) que se verán involucrados en el cambio; en ocasiones no es necesario que el Plan de Gestión de Seguridad de la Información abarque a toda la institución, se puede dar el caso que solo abarque a una dirección u oficina técnica, una sede en concreto o una unidad de negocio.

El tiempo de implementación del Plan de Gestión de Seguridad de la Información va a depender del tamaño de la institución, los recursos con los que cuenta y la situación actual; pero se podría estimar que la duración del Plan varía de seis (06) meses a un (01) año.

En el Capítulo I de este Proyecto de Tesis denominado "PLANTEAMIENTO DEL PROBLEMA" se describirá la realidad problemática de la institución, la justificación del problema, el alcance del proyecto así como los objetivos específicos y el objetivo general que se buscó alcanzar.

En el Capítulo II "MARCO TEÓRICO" se encuentran las investigaciones anteriores realizadas referentes al proyecto, los fundamentos, teoremas o teorías empleadas, los tecnicismos y un glosario de términos respectivamente.

Para finalizar en el Capítulo III "CONSTRUCCIÓN DEL MODELO" se desarrollará el Proyecto de Tesis, el cual refleja el análisis y construcción del modelo empleado, culminando con la consolidación de resultados de los cuales se obtienen las conclusiones y recomendaciones.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la Realidad Problemática

La Organización Internacional de Normalización (ISO) ha publicado normas estándar internacionales referidas a la Gestión de la Seguridad de la Información; el Perú ha definido leyes y normas que se alinean a éstos estándares internacionales logrando que las empresas, instituciones y entidades del país públicas o privadas puedan aplicarlas de acuerdo a la realidad existente.

En Enero del 2016 por Resolución Ministerial N°004-2016-PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana ISO NTP/IEC 27001:2014, dando como plazo máximo de dos (02) años a las entidades integrantes del Sistema Nacional de Informática para la implementación y/o adecuación de la norma.[1]

El especialista en Seguridad de la Información de la Oficina Técnica de Informática (OTIN), en la entrevista realizada a principios del presente año, indicó que actualmente la OTIN viene implementando nuevos

Notas:

[1] La Resolución Ministerial publicada el 08 de enero del 2016 se puede encontrar en la siguiente dirección: http://www.pcm.gob.pe/wp-content/uploads/2016/01/RM_N_04-2016-PCM.pdf

software, teniendo como activos críticos a las aplicaciones desarrolladas y almacenadas, la documentación de las mismas, los datos sensibles, las bases de datos, los equipos que se encuentran en el Centro de datos, entre otros; lo que hace que las actividades que se realizan para la institución dependan, en mayor grado, de los sistemas de información más que de otros servicios informáticos brindados, como los servicios de soporte técnico.

En julio del presente año la ONGEI (Oficina Nacional de Gobierno Electrónico e Informático) envió un Oficio múltiple al INEI, en el cual manifiesta que la entidad presenta vulnerabilidad severa ante posibles ataques cibernéticos, lo que quiere decir que se pueden suscitar incidentes de pérdida de información, accesos no autorizados, ataques de ciber delincuentes, y demás.

A causa de ello, se realizó una auditoría interna a las unidades funcionales de la OTIN a cargo de la Unidad de Seguridad y Calidad de la Información de la misma. El resultado de dicha auditoría evidenció que existe un control informal de los procesos de TI de los servicios que brinda la OTIN; es decir no se cuenta con procedimientos formalizados ni con controles internos de seguridad, generando que no se tenga un completo control de la seguridad de la información.

1.2. Justificación del Proyecto

Debido a que la institución no cuenta con lineamientos definidos referentes al resguardo de la Seguridad de la Información y teniendo en cuenta que, la información es uno de los activos más importantes dentro de una organización (Berrueta, 2015). Es necesario que la institución

demuestre que sus sistemas y servicios son diligenciados de manera fiable, eficaz y eficiente.

La implantación de un Plan de Gestión de Seguridad de la Información basado en la NTP-ISO/IEC 27001:2014, particularmente para la OTIN, permitirá un enfoque claro y conciso de las actividades que realiza, especificando los documentos y plazos que se tomarán en cuenta dentro del Plan, y cumpliendo con las recomendaciones dadas por el especialista en Seguridad de la Información de la OTIN.

Además, como entidad pública perteneciente al Sistema Nacional de Informática, la institución está obligada a cumplir las regulaciones establecidas por la Presidencia del Consejo de Ministros – PCM mediante la ONGEI.[2]

Los beneficios que se obtienen al implantar un Plan de Gestión de Seguridad de la Información tomando como referencia los lineamientos de la ISO 27001 son los siguientes (Honan, 2010, p.42):

- Optimización de la Seguridad, productividad y eficiencia en la Gestión organizacional.
- Confianza y satisfacción de los usuarios.
- Mejorar la Gestión ante alguna amenaza o incidente de Seguridad en contra los sistemas de información la institución.
- Incrementar el nivel de protección de los activos críticos de información de la institución.

Notas:

[2] En el siguiente link se puede ver las entidades que integran el Sistema Nacional de Informática: ttp://www.ongei.gob.pe/quienes/ongei_quienes.asp?pk_id_entidad=1878&opciones=S

- Contar con controles y procedimientos basados en un estándar internacional con los cuales se minimizan los riesgos y se puede alcanzar la excelencia.

1.3. Delimitación del Proyecto

El Plan de Gestión de Seguridad de la Información ha sido elaborado el presente año entre los meses de enero y agosto para la Oficina Técnica de Informática (OTIN) del INEI, localizada en el segundo piso de la Sede Central del INE, ubicada en la Av. General Garzón N° 654 – 658, Jesús María, Lima – Perú, tal y como se muestra en la siguiente figura:

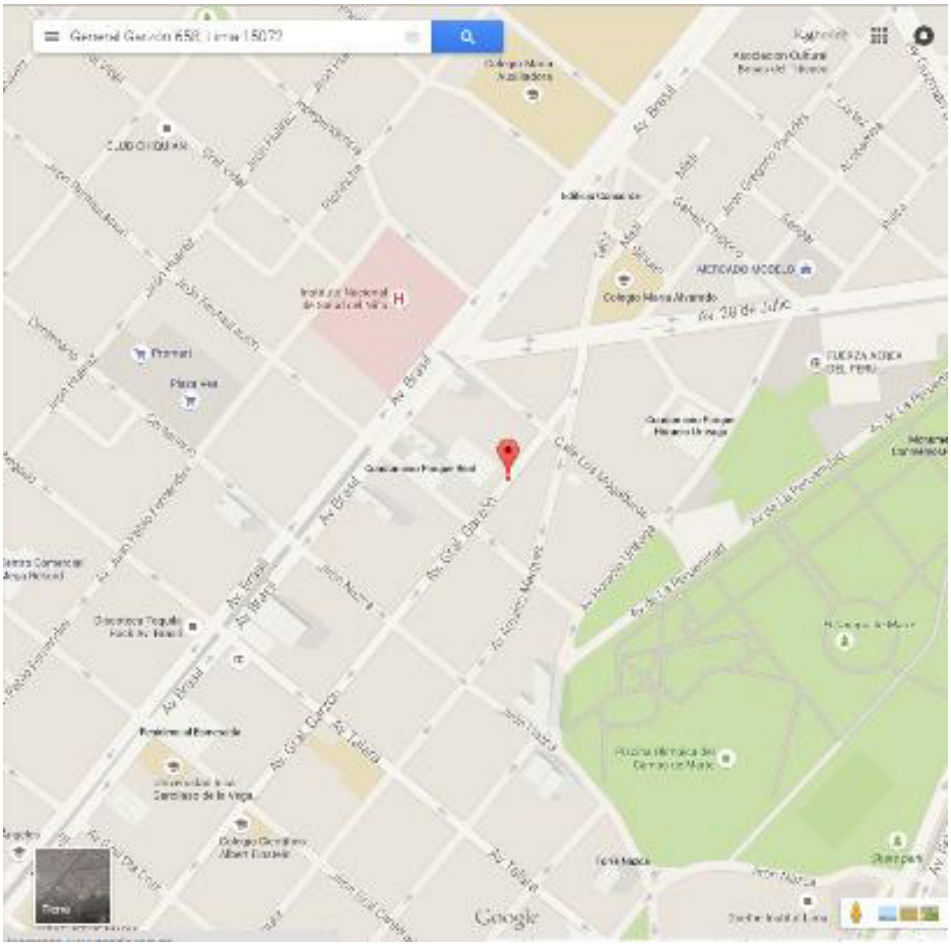


Figura N°01. Mapa de ubicación del INEI.

Fuente: Google Maps.

Se aplica a todas las actividades realizadas para la mejora de la Seguridad de la Información.

Especifica los documentos necesarios y plazos para la mejora de la Seguridad de la Información tomando como base los lineamientos de la NTP-ISO/IEC 27001:2014, aplicando como metodología el Ciclo de Deming.

1.4. Formulación del Problema

Problema Principal

¿De qué manera un Plan de Gestión de Seguridad de la Información basado en la NTP-ISO/IEC 27001:2014 permite la protección de la información en la Oficina Técnica de Informática de una entidad del estado?

1.5. Objetivos

1.5.1. Objetivo General

Elaborar un Plan de Gestión de Seguridad de la Información bajo los conceptos de la NTP-ISO/IEC 27001:2014 para la protección de la información en la Oficina Técnica de Informática de una entidad del estado.

1.5.2. Objetivos Específicos

- Desarrollar el Plan del Proyecto según lo establecido por la ONGEI.
- Realizar el inventario de procesos y activos de información críticos de la Oficina Técnica de Informática del INEI.

- Tener un marco de referencia a través del cual se gestione continuamente la Seguridad de la Información dentro de la Oficina Técnica de Informática.
- Elevar los niveles de protección de los activos de información críticos de información de la Institución.

CAPÍTULO II: MARCO TEÓRICO

2.1. Antecedentes de la Investigación

A nivel nacional se pudieron encontrar los siguientes antecedentes

2.1.1. Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013

Presentado por Vasco Rodrigo Talavera Álvarez (2015), en el cual realiza el Análisis y Diseño de un Sistema de Gestión de Seguridad de la Información del Instituto Nacional Materno Perinatal de acuerdo al cumplimiento de la normativa vigente relativa a Seguridad de la Información. Verificó que existe un gran retraso respecto a la programación establecida por la ONGEI con respecto al proceso de implementación de la NTP ISO/IEC 27001:2008. Llegando a la conclusión de que en la institución sobre la cual se realizó el proyecto existe una brecha considerable respecto a seguridad de la información, considera que la principal falencia que debe ser resuelta es involucrar a la dirección en el proceso de implementación del Sistema de Gestión de Seguridad de la

Información institucional para así se pueda contar con el apoyo de las diferentes direcciones y áreas de la institución.

2.1.2. Diseño de procedimientos de auditoría de cumplimiento de la norma NTP-ISO/IEC 17799:2007 como parte del proceso de implantación de la norma técnica NTP-ISO/IEC 27001:2008 en instituciones del estado peruano.

Presentado por Huamán Monzón, Fernando Miguel. (2014).

En el cual elabora procedimientos basados en COBIT 5.0 para realizar auditorías que verifiquen el cumplimiento de la NTP-ISO/IEC 27001 en las empresas del estado peruano.

Define los controles a ser establecidos e implementados por la institución, el inventario de activos de información y realiza un mapeo del marco COBIT 5.0 versus la NTP 17799. Luego de realizar las pruebas de los procedimientos, concluye que los procedimientos representan una herramienta muy útil en el proceso de evaluación del cumplimiento de la NTP-ISO/IEC 1779 y NTP-ISO/IEC 27001. Ya que los procedimientos están enfocados para escenarios de empresas del estado peruano, recomienda que puedan ser trasladados a empresas del sector privado para que se cuente con una mejor calidad en lo que respecta a Seguridad de la Información en ambos sectores beneficiando así a los ciudadanos y por ende a las empresas y/u organizaciones.

2.1.3. Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo.

Presentado por Espinoza Aguinaga, Hans Ryan. (2013). Toma en cuenta los aspectos más importantes de la ISO/IEC 27001:2005 y desarrolla las etapas del diseño de un Sistema de Gestión de Seguridad de la Información a ser aplicados por una empresa dedicada a la producción de alimentos de consumo masivo en Perú para cumplir con las normas de regulación vigentes en lo que respecta a Seguridad de la Información. Llega a la conclusión de que es necesario el apoyo de la alta gerencia como promotor activo para el logro de una adecuada gestión de la seguridad de la información.

Recomienda la concientización hacia los empleados sobre seguridad de la información y su importancia así como también recomienda ejecutar evaluaciones periódicas a los indicadores de seguridad de la empresa de los riesgos que fueron encontrados.

2.1.4. Elaboración y aplicación de un Sistema de Gestión de la Seguridad de la Información (SGSI) para la realidad tecnológica de la USAT.

Presentado por De la Cruz Guerrero, César Wenceslao y Vasquez Montenegro, Juan Carlos. (2008).

Elaboran y aplican un Sistema de Gestión de Seguridad de la Información (SGSI) para mejorar la seguridad de las tecnologías de

información y las comunicaciones en la Universidad Católica Santo Toribio de Mogrovejo efectuando un diagnóstico de la situación actual de la seguridad de información en la organización, evaluando las áreas encargadas del cuidado y distribución de la información y realizando un análisis de riesgos de los puntos fuertes. Logrando desarrollar en la organización el modelo de Sistema de Gestión de Seguridad de la Información (SGSI) protegiendo la información y los activos de la USAT a través de la confidencialidad, integridad y disponibilidad de los datos.

2.1.5. Diseño e implementación de un Sistema de Gestión de Seguridad de Información en procesos tecnológicos.

Presentado por Barrantes Porras, Carlos Eduardo y Hugo Herrera, Javier Roberto. (2012).

En el cual bajo una metodología de análisis y evaluación de riesgos, desarrollada por los autores, buscan la implementación de un Sistema de Gestión de Seguridad de la Información utilizando como referencia las normas ISO 27001:2005 e ISO 17799:2005. La implementación logró aumentar la seguridad de los activos de información de la empresa Card Perú S. A. garantizando que los riesgos de seguridad de la información sean administrados de una forma óptima. Concluyen que cuando se quiere implementar cualquier sistema de gestión en una empresa, implementar una política de seguridad e interiorizarla por los trabajadores es de gran utilidad. Y que la documentación de los procesos es una poderosa

herramienta para la mejora y mantenimiento de cualquier sistema de gestión organizacional.

A nivel internacional se pudieron encontrar los siguientes antecedentes:

2.1.6. Proyecto CAMERSEC.

Iniciativa de la Cámara de Comercio, Industria y Navegación de Málaga, empresa Nexus Consultores y Auditores y empresa Tecnotur 3000. (2006).

Orientado a la Implantación de Sistemas de Gestión de Seguridad de la Información según ISO 27001 especialmente en PyMEs que cuenten con equipos de procesos de datos para su gestión. Está orientado para aquellas empresas cuyos activos de información representen un alto valor dentro de la actividad organizacional ya que la implementación de un Sistema de Gestión de Seguridad de la Información apoya a la gestión de la seguridad de sus activos de información implicando políticas y estrategias del negocio constituyendo un aporte de indiscutible valor.

2.1.7. Proyecto PYMETICA

ETICOM, asociación de Empresarios de Tecnologías de la Información y Comunicaciones de Andalucía. (2002).

Dirigido a la implementación y certificación de un Sistema de Gestión de Seguridad de la Información en las PYMES de Andalucía según la norma ISO 27001, busca introducir elementos de Continuidad de Negocio buscando mejorar la gestión interna de la seguridad de la información. Representó la primera experiencia

agrupada en España orientada a la implementación de un Sistema de Gestión de Seguridad de la Información en las PYMES TICs.

2.2. Bases Teóricas

La ISO/IEC 27000

Es un conjunto de estándares desarrollados por la ISO (Organización Internacional de Normalización) y la IEC (Comisión Internacional Electrotécnica), las cuales brindan un marco de gestión sobre la Seguridad de la Información dirigido a todo tipo de organización. (López Neira y Ruiz Spohr, 2016).

La ISO 27001

Es un estándar internacional emitido por la ISO el cual describe la forma de administrar la Seguridad de la Información dentro de una empresa.

La primera revisión, publicada en el 2005, fue elaborada en base a la norma británica BS 7799-2. Y en el 2013 se publicó la ISO/IEC 27001:2013 (su última revisión).

Se ha convertido en la norma principal a nivel mundial referente a la Seguridad de la Información motivo por el cual muchas empresas han certificado su cumplimiento.

En el gráfico 01 se puede ver la Evolución de los certificados ISO/IEC 27001 en Perú en los últimos años:

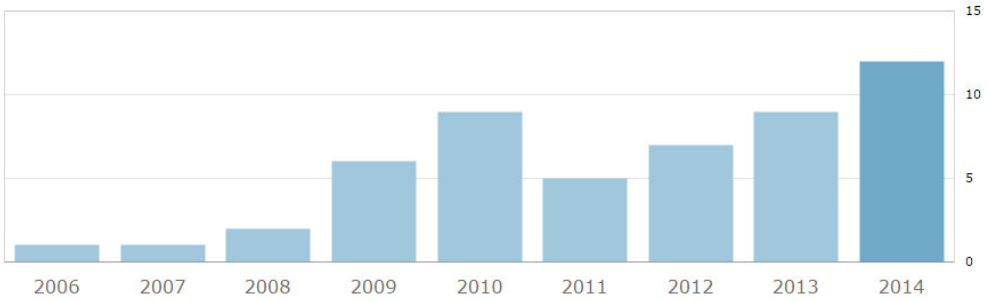


Gráfico 01. Cantidad de certificados.

Fuente: Encuesta ISO sobre certificaciones de la norma para sistemas de gestión.

¿Cómo funciona?

La ISO 27001 vela por la protección de la confidencialidad, integridad y disponibilidad de la información en una organización realizando una evaluación de riesgos y definiendo las acciones necesarias para la mitigación o tratamiento del riesgo. De ahí que la ISO 27001 esté basada en la Gestión de riesgos.

Figura N° 02. Estructura ISO 27001.

Fuente: Advisera.

Por lo general las empresas cuentan con el hardware y software para la implementación de la norma; sin embargo la utilizan de una forma no segura. Es por ello

Las políticas, procedimientos y la implementación técnica son los controles que se van a implementar. (Advisera, 2012).

La Norma Técnica Peruana ISO/IEC 27001

Ha sido elaborada por el Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos y describe cómo gestionar un Sistema de Gestión de Seguridad de la Información.

La edición más reciente de esta norma fue publicada el 2016 y ahora su nombre completo es NTP-ISO/IEC 27001:2014. La primera versión se publicó en el 2007 y fue desarrollada en base a la norma ISO/IEC 17799:2005. Está alineada al estándar internacional ISO/IEC 27001:2013.

La NTP-ISO/IEC 27001 se puede ser adoptada por cualquier tipo de organización, con o sin fines de lucro, pública o privada, pequeña, mediana o grande. Está redactada por especialistas en el tema y ofrece los requisitos para implantar, implementar, mantener y optimizar continuamente un Sistema de Gestión de Seguridad de la Información en una organización. (NTP-ISO/IEC 27001: 2014).

Ciclo de Deming

Metodología, mayormente conocida como el ciclo o espiral de mejora continua PHVA (Plan, Do, Check, Act), las siglas son traducidas al español como Planificar, Hacer, Verificar y Actuar.

El primer paso (Planificar) consiste en realizar un análisis del estado inicial de la organización para identificar las necesidades y evaluar las medidas a implementarse. El segundo paso (Hacer) consiste en implementar los controles, análogamente se capacita y concientiza al personal de la organización sobre lo que se está desarrollando y el por qué.

Luego que el modelo se ha implantado y esté funcionando, se debe ejecuta el tercer paso (Verificar) consiste en realizar el monitoreo, mediante los registros e indicadores de los controles previamente implementados, evaluando el nivel de eficacia y éxito de los mismos. Por último se procede al cuarto paso (Actuar) se realiza el mantenimiento del Plan de Gestión corrigiendo las debilidades encontradas en el paso anterior mediante medidas correctivas, preventivas y de mejora. (Mora Martínez, 2003).

En la figura 03 se presenta lo que se ha explicado:

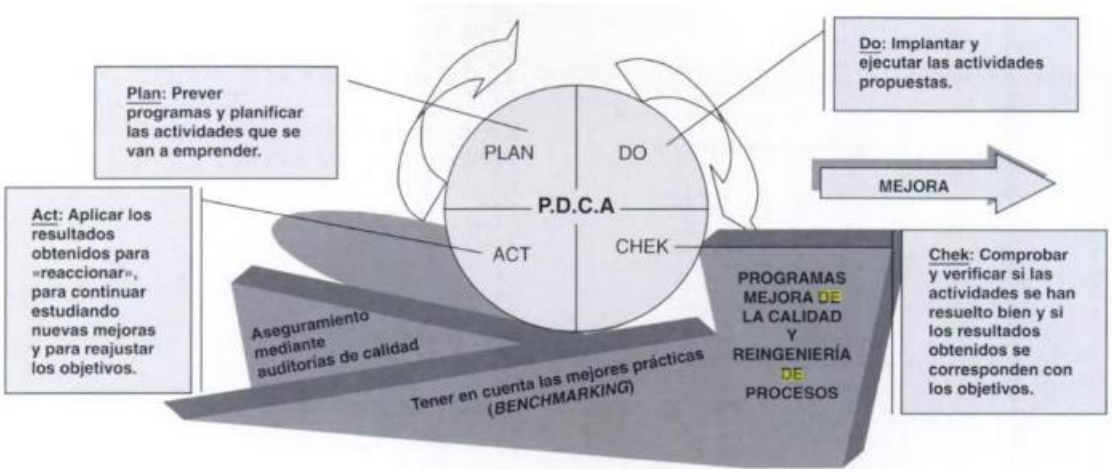


Figura N°03. Diagrama de fases del PDCA.

Fuente: Guía Metodológica para la Gestión clínica por procesos.

2.3. Marco Conceptual

Activo de Información

Son recursos que poseen valor o utilidad para la organización. Para que la organización funcione y logre los objetivos que plantea la dirección, son necesarias sus operaciones comerciales y su continuidad. (Fernandez, Medina, Moya y Plattini, 2003).

Amenaza

Es todo aquello que pueda causar un incidente no deseado generando daños a la organización y a sus activos como por ejemplo la pérdida de información, de la privacidad o un fallo en los equipos físicos. (Tupia, 2011).

Centro de Datos

Es aquella ubicación donde se encuentran todos los recursos necesarios para el procesamiento de información de una institución. Se usa para mantener en él equipos informáticos (servidores, equipos de comunicaciones, sistemas de almacenamiento de datos, entre otros). (Ferrer, 2009)

Control

Un control es lo que permite garantizar que cada aspecto que se valoró con un cierto riesgo quede cubierto y auditable, abarca todo el conjunto de acciones, documentos, medidas a adoptar, procedimientos, medidas técnicas, etc…(Corletti, 2006).

Política de Seguridad de la Información

Es un conjunto de leyes, reglas y prácticas que definen lo que está permitido y lo prohibido regulando la forma de dirigir, proteger y distribuir los recursos en una organización. Permiten definir procedimientos y herramientas necesarias para llevar a cabo los objetivos en cuanto a seguridad informática respecta dentro de la organización. (López, 2016).

Riesgo

Cualquier cosa que amenace el progreso de un proyecto; algo que bajo ciertas circunstancias puede interferir o interrumpir la buena marcha

del proyecto. Está relacionado con algún evento que podría ocurrir y que en caso ocurriese tendría un impacto negativo para el progreso del proyecto. (Llorens, 2005).

Seguridad de la Información

Es el conjunto de acciones reactivas y provisorias de las organizaciones, que posibilitan el resguardo y protección de la información con el fin de mantener los parámetros (confidencialidad, disponibilidad e integridad) de la misma. (Frayssinet, 2013).

Sistema de Gestión de Seguridad de la Información (SGSI)

Para que una empresa proteja sus activos de información es necesario seguir algunos pasos. Lo primero es identificar aquellos activos de información que tengan algún impacto significativo en el negocio, después realizar un análisis y evaluación de riesgos de cada activo identificado y finalmente determinar las alternativas más óptimas a implementar para el tratamiento del riesgo y minimizar las posibilidades de que las amenazas puedan causar daño.(Alexander G., 2007).

Vulnerabilidad

Es una debilidad asociada con los activos de la organización. Las debilidades pueden ser explotadas por una amenaza causando incidentes no deseados. La vulnerabilidad no causa daño, es una condición que permite que una amenaza afecte a un activo. (Alexander, 2005).

CAPÍTULO III: CONSTRUCCIÓN DEL MODELO

3.1. Análisis del Plan de Gestión de Seguridad de la Información

3.1.1. Descripción de la Organización

El INEI es el organismo central y rector del SEN (Sistema Estadístico Nacional), responsable de normar, planear, dirigir, coordinar y supervisar las actividades estadísticas oficiales del país. (Web INEI, 2016).

3.1.2. La Oficina Técnica de Informática (OTIN)

Es el órgano responsable de la incorporación de las tecnologías de información, así como de la sistematización, planificación, innovación tecnológica, procesamiento automático, organización y explotación de la información. (INEI, 2004).

Unidades funcionales:

3.1.2.1. Unidades Funcionales

- Unidad de Desarrollo de Sistemas[3]
- Unidad de Producción

Notas:

[3] Esta unidad se subdivide en 4: SI de Proyectos Especiales, SI para Censos, SI para Encuestas y Registros, y la Unidad de Desarrollo, Investigación e Innovación Tecnológica

- Unidad de Operaciones
- Unidad de Infraestructura TIC
- Unidad de Calidad y Seguridad de la Información
- Unidad de Planificación TIC

3.1.3. Descripción del Plan de Gestión de Seguridad de la Información

Durante el desarrollo del Proyecto se han definido los documentos que se iban a redactar, los plazos, y las funciones y responsabilidades del proyecto.

3.1.3.1. Entregables del Proyecto

- Plan del Proyecto
- Inventario de Procesos
- Alcance del Proyecto
- Política de Seguridad de la Información
- Procedimiento para control de documentos y registros
- Procedimiento para identificación de requisitos
- Inventario de activos de información
- Metodología de evaluación y tratamiento de riesgos

3.1.4. Riesgos del Plan de Gestión de Seguridad de la Información

- Falta de compromiso del equipo del proyecto.
- Ampliación de los plazos en los entregables.
- Inadecuada definición del alcance.
- Selección de demasiados controles y/o muy caros.
- Posibilidad que la imagen de la Institución se afecte por servicios interrumpidos, frente a amenazas contra algún activo crítico de información.

- Falta de recursos asignados al proyecto
- Posibilidad que las políticas de información no se cumplan por falta de difusión o porque los controles no están efectivamente implementados.
- Cambios en los integrantes del equipo del proyecto

3.1.5. Presupuesto

Materiales y equipos utilizados	**Costo (S/.)**
Licencia Microsoft Office 2010	S/. 95.00
ISO 27001 & 22301 Premium DocumentationToolkit	S/. 5,745.00
Materiales de impresión	S/. 869.00
Equipo de cómputo	
• Pantalla	S/. 314.67
• CPU	S/. 2,500.00
• Teclado	S/. 40.00
• Mouse	S/. 20.00
Otros Servicios	
• Agua	S/. 39.00
• luz	S/. 75.00
• Internet	S/. 110.00
TOTAL :	**S/. 9,807.67**

3.1.6. Financiamiento

El 100% del presente proyecto ha sido financiado por la institución.

3.1.7. Evaluación de cumplimiento de la Gestión TIC

Se tomó como referencia las buenas prácticas de control que brinda COBIT.

Los resultados de la auditoría interna realizada a las unidades de la OTIN, mostraron que:

- La planificación de la Oficina es una práctica muy débil y deficiente, existiendo una escaza capacidad de organización.
- No existe ningún procedimiento formal para la gestión adecuada de la Seguridad de la información.
- No existe un registro de control de acceso a la información sensible de la OTIN.

Lo cual conllevaba a los siguientes riesgos:

- Gestión ineficiente, trayendo consigo una insatisfacción y disconformidad de los servicios TIC en la organización en perjuicio de los usuarios.
- No tener identificados a los usuarios formalmente generando entropía de los mismos y desgobierno de los sistemas y usuarios.
- La información, al encontrarse accesible, puede ser manipulada por cualquier persona sin autorización previa.

Las recomendaciones tras la auditoría fueron:

- Dar mayor énfasis al planeamiento estratégico, operativo y táctico de las TIC en la OTIN.

- Definir un Plan que contenga procedimientos para la formalización y gestión de la seguridad de la información en OTIN.
- Las políticas de seguridad de la información necesitan ser documentadas.

3.2. Diseño del Plan de Gestión de Seguridad de la Información

3.2.1. Etapas

Planificar.-

Se realizó un análisis del estado inicial de la organización, identificandolas necesidades y vulnerabilidades con el fin de realizar una evaluación de las medidas a implementarse. Además se realizó el inventario de procesos de la OTIN con el fin de tener documentada de forma detallada y secuencial las operaciones que se desarrollan dentro de la OTIN, y las entradas, procesos y salidas que implicada cada una de ellas, y la Unidad funcional responsable. (Ver Anexo01).

En esta etapa se elaboró el Plan del Proyecto, según la plantilla de la ONGEI[4], definiendo la estructura del Plan de Gestión de Seguridad de la Información, identificando a las partes interesadas, los plazos y actividades a seguir, y validando el alcance.

Notas:
[4] La plantilla del SGSI publicada por la ONGEI se puede encontrar en la siguiente dirección web: http://www.ongei.gob.pe/entidad/ongei_tematicos.asp?cod_tema=4552

Hacer.-

Se realizó una auditoría interna a las Bases de datos del INEI. Utilizando las preguntas (checklist) del Anexo 02.

Se elaboró la Política General de Seguridad de la Información estableciendo las funciones y responsabilidades de la OTIN, de los propietarios de los activos de la información, de los usuarios y los custodios de la información. Además se establecieron formalmente las Políticas en base a los 14 controles de la NTP-ISO 27001:2014 que son:

- Política de Seguridad de la Información
- Organización de la Seguridad de la Información
- Seguridad de los Recursos Humanos
- Gestión de activos
- Control de acceso
- Criptografía
- Seguridad Física y ambiental:
- Seguridad de las Operaciones
- Seguridad de las comunicaciones:
- Adquisición, desarrollo y mantenimiento de sistemas
- Relación con los proveedores
- Gestión de Incidentes de Seguridad de la información:
- Aspectos de la Seguridad de la información en la Gestión de Continuidad del negocio
- Cumplimiento

Estableciendo formatos de “Declaración de Confidencialidad” tanto para proveedores, como para personal CAS (Contrato Administrativo de Servicios) y Nombrados.

Se implementaron los siguientes procedimientos:

- Procedimiento para control de documentos y registros
- Procedimiento para identificación de requisitos

Y se capacitó al personal de la OTIN, mediante Talleres Informáticos, sobre lo que se estaba desarrollando y el por qué.

Verificar.-

Se realizó una encuesta de seguridad a la OTIN, tomando de referencia el Cuestionario de Seguridad de la Información en la Administración Publica del 2010 (ver Anexo 03), para evaluar el nivel aplicación de las políticas y procedimientos implementados para la optimización de la Seguridad de la Información.

Además, se elaboró un inventario de activos de información, siguiendo la planilla del Anexo 04, para poder tenerlos identificados, y así contar con un mejor control de la seguridad de la información.

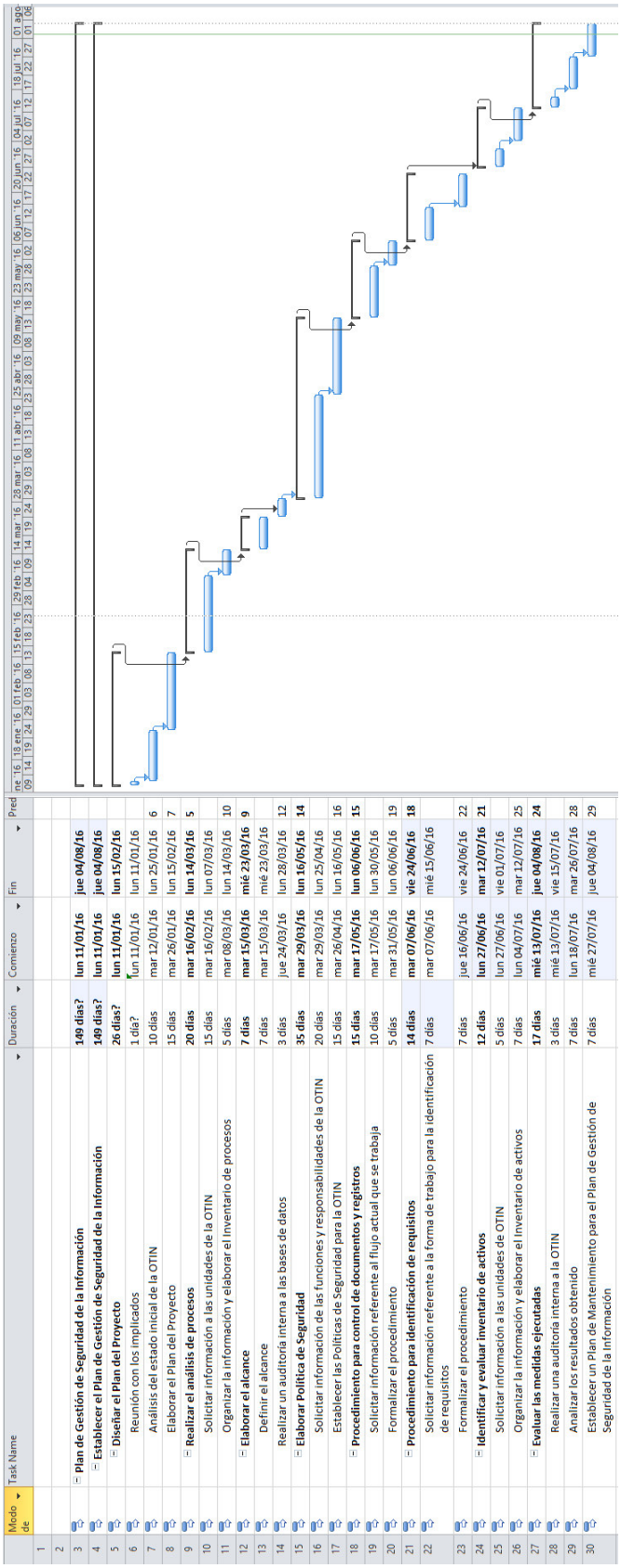
Actuar.-

Se ha elaborado una metodología de evaluación y tratamiento de riesgos que se aplica a todos los activos de información que se utilizan dentro de la institución o que pueden tener un impacto sobre la seguridad de la información. También se ha establecido un Plan de Mantenimiento para el Plan de Gestión de Seguridad de la información, que se ejecutará de forma anual, en el cual se verificará el cumplimiento de los controles, corrigiendo las debilidades

encontradas mediante las acciones que sean necesarias para asegurar una mejora permanente.

3.2.2. Cronograma

Se muestra el cronograma realizado del Plan de Gestión de Seguridad de la Información en el cual se detalla las etapas y los entregables correspondientes. Teniendo como fecha de inicio el 11 de enero del 2016 y fecha fin en agosto del 2016.



	Modo de	Task Name	Duración	Comienzo	Fin	Pred
1						
2						
3		**Plan de Gestión de Seguridad de la Información**	**149 días?**	**lun 11/01/16**	**jue 04/08/16**	
4		**Establecer el Plan de Gestión de Seguridad de la Información**	**149 días?**	**lun 11/01/16**	**jue 04/08/16**	
5		**Diseñar el Plan del Proyecto**	**26 días?**	**lun 11/01/16**	**lun 15/02/16**	
6		Reunión con los implicados	1 día?	lun 11/01/16	lun 11/01/16	
7		Análisis del estado inicial de la OTIN	10 días	mar 12/01/16	lun 25/01/16	6
8		Elaborar el Plan del Proyecto	15 días	mar 26/01/16	lun 15/02/16	7
9		**Realizar el análisis de procesos**	**20 días**	**mar 16/02/16**	**lun 14/03/16**	**5**
10		Solicitar información a las unidades de la OTIN	15 días	mar 16/02/16	lun 07/03/16	
11		Organizar la información y elaborar el Inventario de procesos	5 días	mar 08/03/16	lun 14/03/16	10
12		**Elaborar el alcance**	**7 días**	**mar 15/03/16**	**mié 23/03/16**	**9**
13		Definir el alcance	7 días	mar 15/03/16	mié 23/03/16	
14		Realizar un auditoria interna a las bases de datos	3 días	jue 24/03/16	lun 28/03/16	12
15		**Elaborar Política de Seguridad**	**35 días**	**mar 29/03/16**	**lun 16/05/16**	**14**
16		Solicitar información de las funciones y responsabilidades de la OTIN	20 días	mar 29/03/16	lun 25/04/16	
17		Establecer las Políticas de Seguridad para la OTIN	15 días	mar 26/04/16	lun 16/05/16	16
18		**Procedimiento para control de documentos y registros**	**15 días**	**mar 17/05/16**	**lun 06/06/16**	**15**
19		Solicitar información referente al flujo actual que se trabaja	10 días	mar 17/05/16	lun 30/05/16	
20		Formalizar el procedimiento	5 días	mar 31/05/16	lun 06/06/16	19
21		**Procedimiento para identificación de requisitos**	**14 días**	**mar 07/06/16**	**vie 24/06/16**	**18**
22		Solicitar información referente a la forma de trabajo para la identificación de requisitos	7 días	mar 07/06/16	mié 15/06/16	
23		Formalizar el procedimiento	7 días	jue 16/06/16	vie 24/06/16	22
24		**Identificar y evaluar inventario de activos**	**12 días**	**lun 27/06/16**	**mar 12/07/16**	**21**
25		Solicitar información a las unidades de OTIN	5 días	lun 27/06/16	vie 01/07/16	
26		Organizar la información y elaborar el Inventario de activos	7 días	lun 04/07/16	mar 12/07/16	25
27		**Evaluar las medidas ejecutadas**	**17 días**	**mié 13/07/16**	**jue 04/08/16**	**24**
28		Realizar una auditoria interna a la OTIN	3 días	mié 13/07/16	vie 15/07/16	
29		Analizar los resultados obtenido	7 días	lun 18/07/16	mar 26/07/16	28
30		Establecer un Plan de Mantenimiento para el Plan de Gestión de Seguridad de la Información	7 días	mié 27/07/16	jue 04/08/16	29

Figura N°04 Cronograma del Plan

Fuente: Propia

3.2.3. Alcance

Se definieron los límites correspondientes de la OTIN dentro del Plan de Gestión de Seguridad de la Información para decidir qué información quiere proteger

3.2.3.1. Procesos

- **Proyectos de Sistemas de Información**

  Subprocesos:

  - ✓ Desarrollo de Sistemas de Información
  - ✓ Mantenimiento de Sistemas de Información
  - ✓ Actualización y/o Modificación de Base de Datos

- **Producción de Sistemas y Aplicaciones**

  Subprocesos:

  - ✓ Publicación y Administración de la Página Web
  - ✓ Publicación y Administración del Portal de Transparencia
  - ✓ Actualización de Sistemas y/o Aplicaciones en los Servidores de Producción
  - ✓ Monitoreo de Sistemas y/o Aplicaciones de Publicaciones en el Portal
  - ✓ Nuevos Sistemas y/o Aplicativos en Producción

- **Operaciones e Infraestructura**

  Subprocesos:

Operaciones:

- ✓ Soporte Técnico Informático de Hardware y Software
- ✓ Inventario y actualización de Software base en los equipos informáticos

Infraestructura:

- ✓ Mantenimiento Lógico de Comunicaciones de Redes, Servidores y PC'S
- ✓ Mantenimiento Físico Preventivo y Correctivo de los equipos de Servidores y Redes
- ✓ Monitoreo y Solución de Conexiones
- ✓ Implementación de Servidores
- ✓ Creación de Cuentas de Redes
- ✓ Respaldo de Información de base de datos
- ✓ Informe de Verificación y Procesos de Respaldo de Información
- ✓ Restauración de Backup
- ✓ Mantenimiento y Revisión de los Dispositivos de Backup
- ✓ Monitoreo de los Servicios de las ODEI

- **Gestión de Seguridad de la Información**

Subprocesos:

- ✓ Formulación y Evaluación del Plan Operativo Informático
- ✓ Seguridad Perimetral Informática
- ✓ Seguridad de la Información

- **Gestión de la Calidad**

  Subprocesos:

  - ✓ Medición, Análisis y Mejora
  - ✓ Auditoria y Paso a Certificación

- **Gestión de Proyectos Estratégicos**

  Subprocesos:

  - ✓ Formulación y Seguimiento de Estrategias de las Tecnologías de la Información (PETI)
  - ✓ Formulación y Seguimiento de Estrategias de Gobierno Electrónico (PEGE)
  - ✓ Formulación y Seguimiento del Plan de Contingencias

3.2.3.2. Redes de Infraestructura de TI

En la figura 05 se muestra el Diagrama Topológico de Red de todo el INEI y entorno de Instalación de equipos. El Centro de datos de la Sede Central se encuentra ubicado en la OTIN.

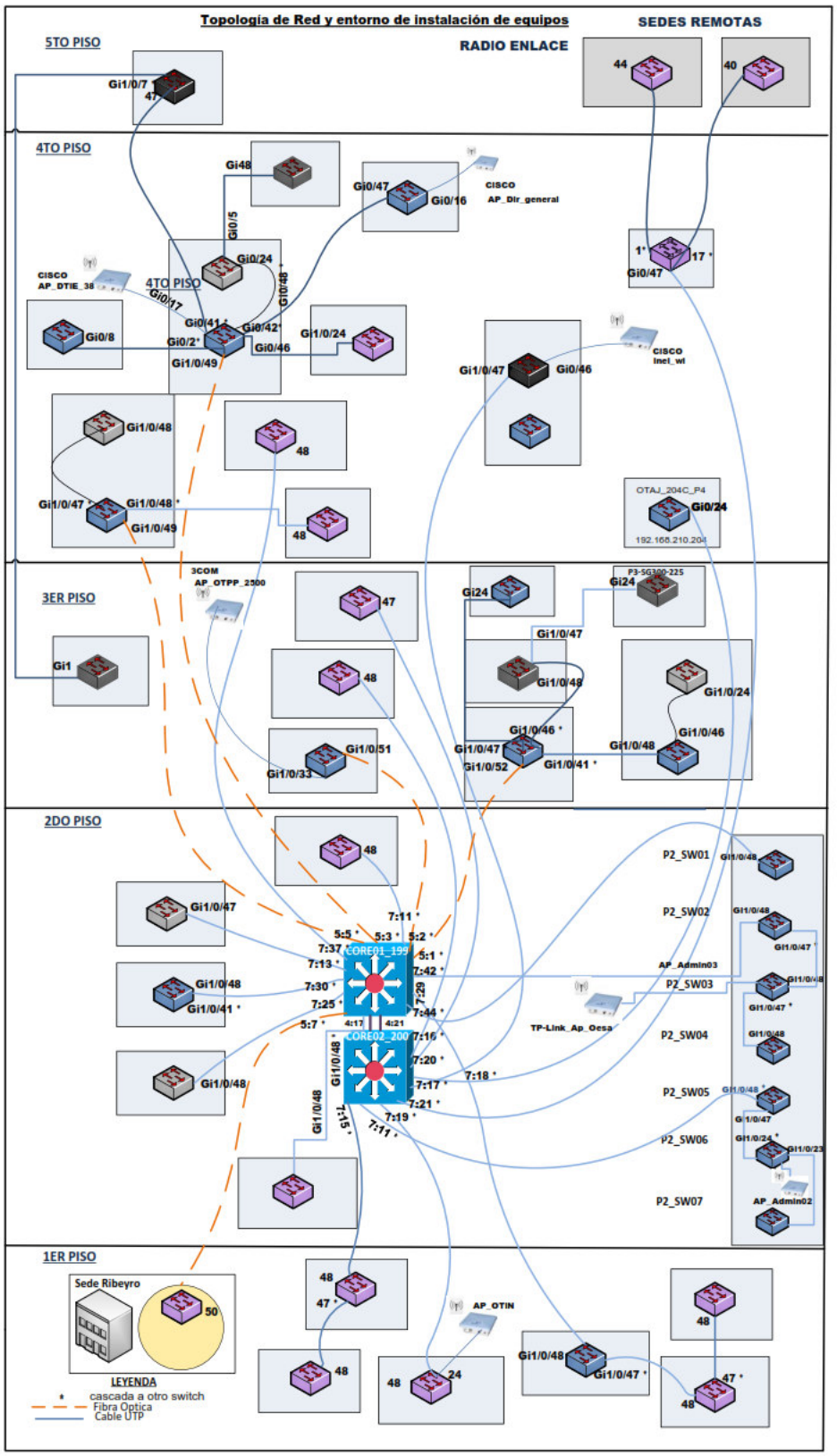


Figura N°05. Topología de Red y entorno de instalación de equipo

Fuente: INEI

En la figura N°06 se muestra el Diagrama Topológico de Seguridad Perimetral de todo el INEI y entorno de Instalación de equipos.

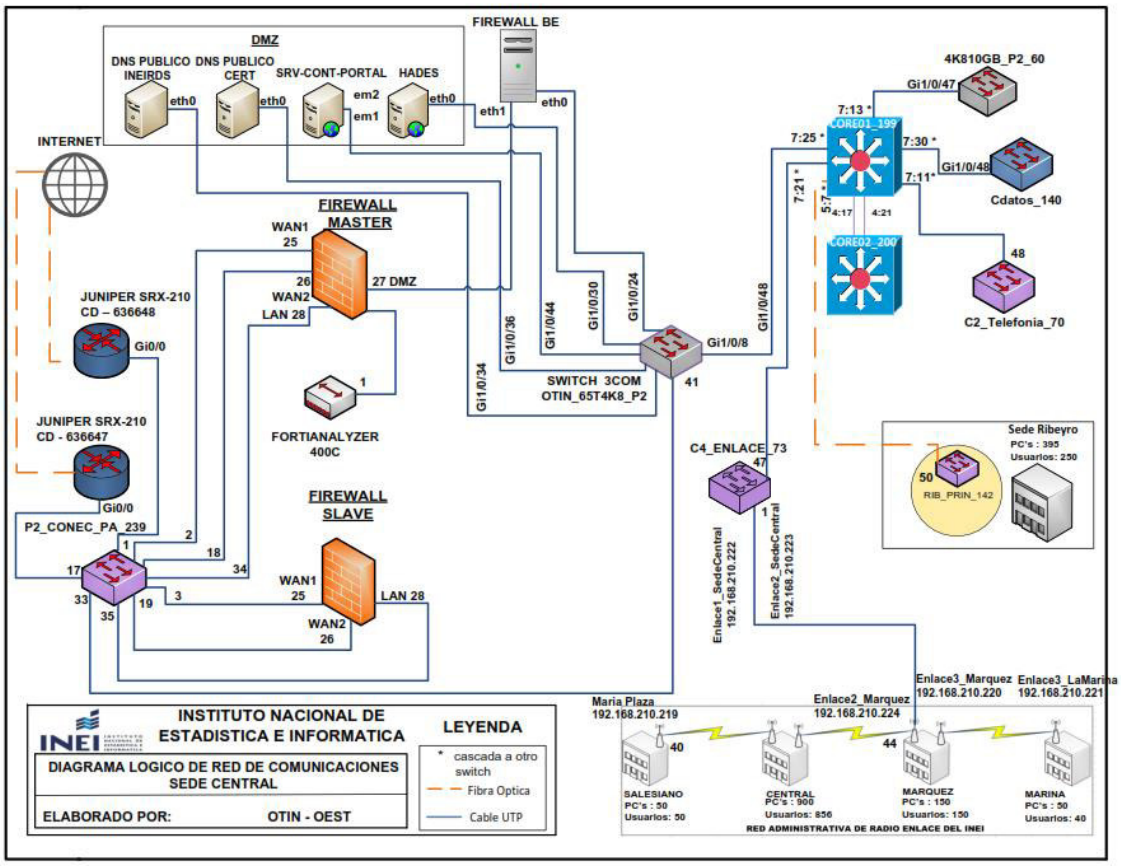


Figura N°06. Diagrama lógico de red de comunicaciones de la Sede Central del INEI

Fuente: INEI

La Unidad funcional de Infraestructura de la OTIN se encarga de la administración de la Red perimetral (firewall, ids, ips, routers y enlaces WAN, y acceso remoto) y el Networking (switches core y switches de distribución) de toda la institución.

3.2.3.3. Exclusiones

No se consideró dentro del Plan de Gestión de Seguridad de la Información los siguientes elementos:

- ✓ Toda información que no sea de manipulación de la OTIN.
- ✓ El Plan de Continuidad, que se desarrollará posteriormente.
- ✓ Las capacitaciones del personal INEI, fuera de OTIN.

3.2.3.4. Metodología de evaluación y tratamiento de riesgos

Se ha definido una metodología para evaluar y tratar los riesgos de la información en la OTIN y definir el nivel aceptable de riesgo según la norma NTP-ISO/IEC 27001:2014.

Activos, vulnerabilidades y amenazas

Como primer paso se ha definido la identificación de todos los activos de información dentro del alcance de la OTIN; es decir, todos los activos que pueden afectar la confidencialidad, integridad y disponibilidad de la información en la OTIN. También se identificó a sus propietarios: la unidad funcional responsable de cada activo.

El siguiente paso que se ha definido en la metodología es la identificación de todas las amenazas y vulnerabilidades relacionadas con cada activo.

Identificación de los propietarios de riesgos

Para cada riesgo se identificó un propietario: la persona o unidad organizativa responsable de cada riesgo.

Consecuencias y probabilidad

Una vez identificados los riesgos, se ha fijado que se evaluarán las consecuencias para cada combinación de amenazas y vulnerabilidades de un activo específico en caso que ello se pueda producir:

Tabla 01. Escala de evaluación de riesgos

Baja consecuencia	0	La pérdida de confidencialidad, disponibilidad o integridad no afecta las finanzas, las obligaciones legales o contractuales o el prestigio de la organización.
Consecuencia moderada	1	La pérdida de confidencialidad, disponibilidad o integridad causa gastos y tiene consecuencias bajas o moderadas sobre obligaciones legales o contractuales o sobre el prestigio de la organización.
Alta consecuencia	2	La pérdida de confidencialidad, disponibilidad o integridad tiene consecuencias importantes y/o inmediatas sobre las finanzas, las operaciones, las obligaciones legales o contractuales o el prestigio de la organización.

Fuente: ISO 27001 & 22301 Premium DocumentationToolkit

Para los riesgos de alta consecuencia se ha dispuesto que se deberán seleccionar una o más opciones de tratamiento. (Aplicación de controles de seguridad)

Revisiones periódicas

Se ha dispuesto que los propietarios de los riesgos deben revisar y actualizar los riesgos vigentes. Ésta revisión se realizará una vez al año, o cada que sea necesaria.

Informes

Se han documentado los resultados de la evaluación y del tratamiento de riesgos, y se documentarán todas las revisiones subsiguientes.

3.3. Revisión y consolidación de resultados

Tras la ejecución del Plan, la OTIN cuenta con un inventario de procesos y de activos de información, además de políticas de seguridad. Cada documento y registro lleva un control y se identifican los requisitos legales, normativos, contractuales y de otra índole relacionados con la seguridad de la información. También la OTIN cuenta con una metodología para identificar y evaluar los riesgos de los activos de información, así como de un Plan de mantenimiento para el Plan de Gestión de seguridad de la Información, el cual garantiza la continuidad de los controles y procedimientos aplicados.

3.3.1. Resultados de la auditoría realizada a las Unidades funcionales de OTIN

La metodología de trabajo que se aplicó fue reuniones de trabajo y encuestas a los jefes de unidad de la OTIN.

Tabla 02. Nivel de cumplimiento, proceso: Definir los procesos, organización y relaciones

PROCESO	Objetivo de Control evaluado	Cumplimiento	Observaciones y comentarios
Definir los procesos, organización y Relaciones	**TOTAL**	**46.29%**	
	Marco de trabajo de procesos de TI	0.00%	En proceso.
	Estructura Organizacional	50.00%	Se requiere formalizar el documento de la organización de la oficina.
	Establecimiento de Roles y Responsabilidades	100.00%	
	Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento	14.29%	En proceso.
	Supervisión	100.00%	Se efectúan las reuniones de comité donde se asignan las tareas.
	Segregación de Funciones	100.00%	Se requiere formalizar el documento de la organización de la oficina.
	Personal de TI	100.00%	Se requiere formalizar el documento de la organización de la oficina. No hay políticas.
	Personal Clave de TI	50.00%	Se requiere formalizar el documento de la organización de la oficina. No hay políticas.
	Políticas y Procedimientos para el Personal Contratado	0.00%	

Fuente: Propia

Se observa que la OTIN presentaba un 46.29% de cumplimiento ratificando que no existe un marco de trabajo de procesos de TI y no se encuentran definidas las responsabilidades sobre el riesgo, la seguridad y el cumplimiento de controles.

Tabla 03. Nivel de cumplimiento, procesos: Garantizar la seguridad de los sistemas y Administrar el ambiente físico

PROCESO	OBJETIVO DE CONTROL	CUMPLIMIENTO	OBSERVACIONES Y COMENTARIOS
Garantizar la seguridad de los sistemas	**TOTAL**	**43%**	
	Administración de la Seguridad de TI	0%	Se cuenta con un plan de seguridad en proceso.
	Plan de Seguridad de TI	50%	
	Administración de Identidad	100%	
	Administración de Cuentas del Usuario	100%	
	Pruebas, Vigilancia y Monitoreo de la Seguridad	0%	
	Definición de Incidente de Seguridad	0%	No hay un proceso de gestión de incidentes.
	Protección de la Tecnología de Seguridad	0%	
	Administración de Llaves Criptográficas	0%	
	Prevención, Detección y Corrección de Software Malicioso	100%	
	Seguridad de la Red	100%	Se requiere la implementación de aseguramiento de las redes a través de VLAN que garanticen accesos seguros.
	Intercambio de Datos Sensitivos	25%	Se requiere un procedimiento y herramienta de software para intercambio de datos.
Administrar el ambiente físico	**TOTAL**	**67%**	
	Selección y Diseño del Centro de Datos	100%	
	Medidas de Seguridad Física	100%	
	Acceso Físico	0%	
	Protección	33%	
	Administración de Instalaciones Físicas. Contra Factores Ambientales	100%	

Fuente: Propia

Se observa que la OTIN presentaba un 55% en el cumplimiento de la seguridad de los sistemas y la administración del ambiente físico demostrando que no se contaba con un plan de seguridad de la información y la protección del acceso al ambiente físico era nula.

Tabla 04. Nivel de cumplimiento, proceso: Monitorear y Evaluar el Control Interno

PROCESO	OBJETIVO DE CONTROL	CUMPLIMIENTO	OBSERVACIONES Y COMENTARIOS
Monitorear y Evaluar el Control Interno	**TOTAL**	**15.28%**	
	Monitorización del Marco de Trabajo de Control Interno	0.00%	No existe dicho ambiente.
	Revisiones de Auditoría	0.00%	
	Excepciones de Control	25.00%	
	Control de Auto Evaluación	66.67%	
	Aseguramiento del Control Interno	0.00%	
	Control Interno para Terceros	0.00%	
	Acciones Correctivas	75.00%	

Fuente: Propia

Se observa que la OTIN presentaba un 15.28% en el monitoreo y la evaluación del control interno, la OTIN no realizaba auditorías internas ni tenía políticas de seguridad para asegurar el control interno.

3.3.2. Resultados de la encuesta de seguridad realizada a los trabajadores de la OTIN luego del establecimiento del Plan de Gestión de Seguridad de la Información

Se han seleccionado 4 preguntas, ya que estos dominios son los que se han trabajado y mejorado dentro del Proyecto.

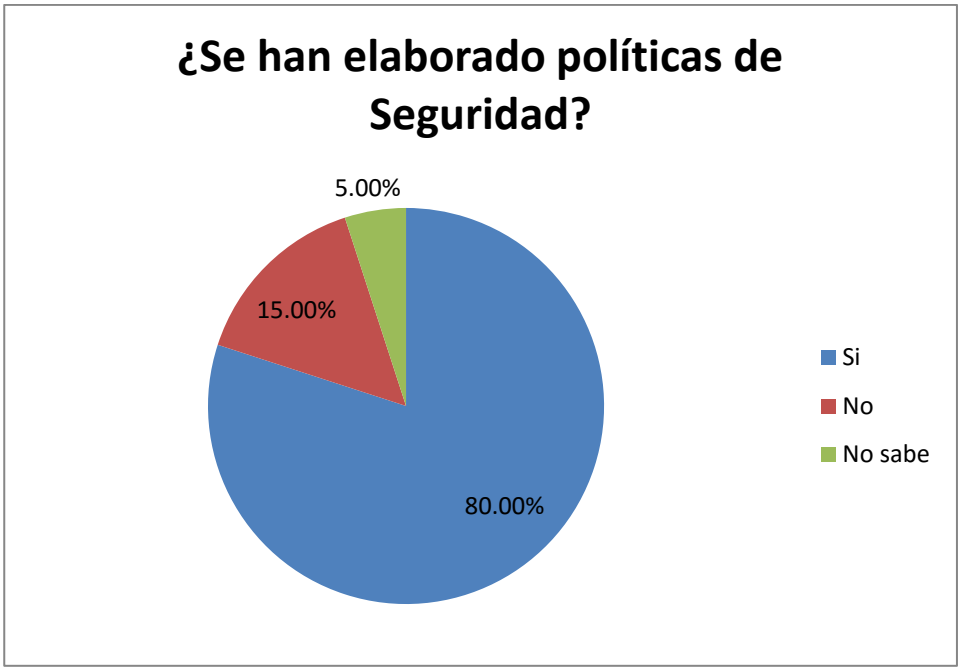


Gráfico 02. Pregunta 1.a y 1.b Cuestionario de seguridad

Se puede observar que el 80% de empleados conoce de la existencia de políticas de seguridad y acerca de su aplicación, un 15% considera que no están siendo aplicadas y un 5% desconoce la elaboración y aplicación de las mismas.

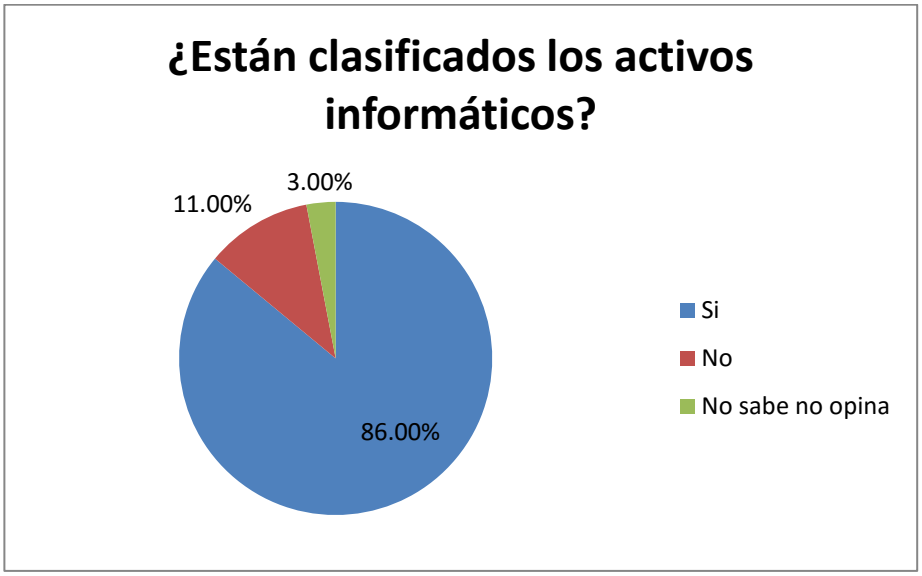


Gráfico 03. Pregunta 3.a Cuestionario de seguridad

Se puede observar que un 86% de empleados está informado y considera que si están clasificados los activos de información (hardware y software) de la OTIN.

Gráfico 04. Pregunta 4.b Cuestionario de seguridad

Se puede observar que el total de empleados de la OTIN conoce la existencia de acuerdos de confidencialidad de seguridad de la información.

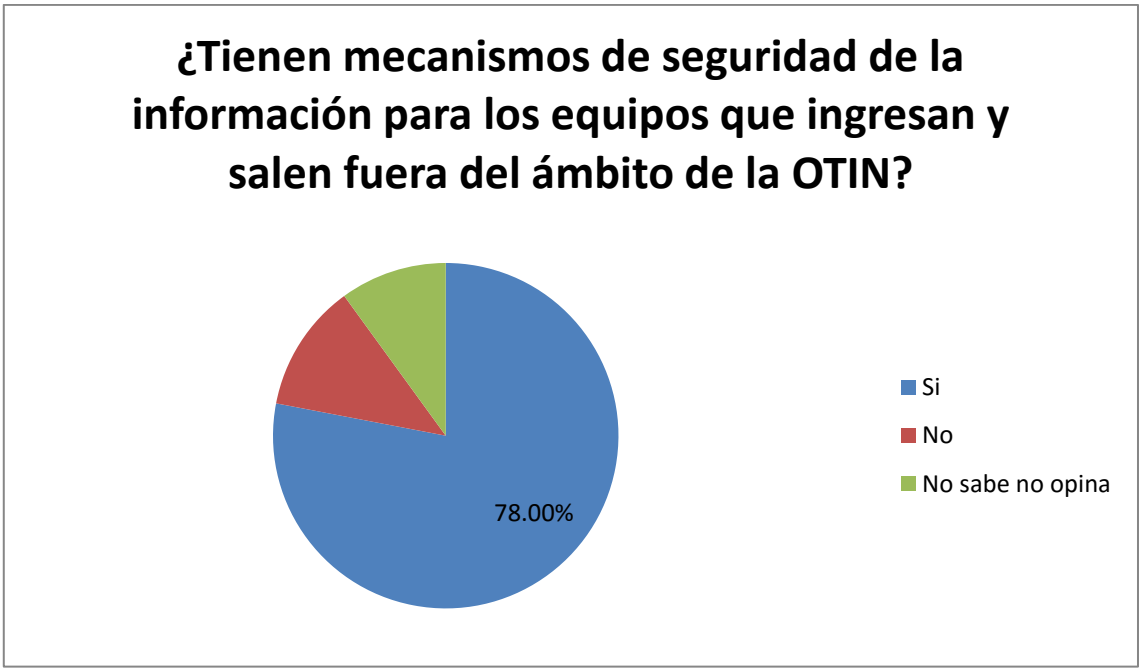


Gráfico 05. Pregunta 5.e Cuestionario de seguridad

El 78% de los encuestados indican que sí existen mecanismos de seguridad de la información de los equipos que ingresan y salen de la OTIN. De ellos la mayoría pertenece a la unidad funcional de Operaciones (Soporte Técnico).

CONCLUSIONES

El Plan de Gestión de Seguridad de la Información ha conseguido que la OTIN cuente con documentación y registros formales de los activos de información, y de la organización de los procesos de la OTIN, haciendo más factible una efectiva adecuación a la NTP-ISO/IEC 27001:2014.

Luego de la ejecución del Plan de Gestión de Seguridad de la Información, la OTIN posee un mejor control y una administración más efectiva de los datos debido a la formalizaron las políticas de seguridad de la Información, las cuales cuentan con estrategias de alto nivel.

Para un ágil proceso de implementación del Plan de Gestión de Seguridad de la Información es necesario el compromiso de la Alta Dirección y la participación de todo el personal.

Un Plan de Gestión de Seguridad de la Información ofrece la metodología necesaria para implantar la seguridad en la gestión de la información en una organización reduciendo el riesgo de que se produzcan pérdidas de información.

Un nivel de protección total de la información es imposible, pero un Plan de Gestión de Seguridad de la Información garantiza que los riesgos de la seguridad de la información sean conocidos y minimizados.

RECOMENDACIONES

Se recomienda dar mayor énfasis al planeamiento estratégico, táctico y operativo de las TIC en la OTIN, con la finalidad de reducir la brecha en el porcentaje de cumplimiento de controles de seguridad de la información.

Se recomienda implementar el Plan de Continuidad de Negocio para definir de forma precisa cómo la OTIN gestionará los incidentes en caso de un desastre o de otro incidente disruptivo y cómo recuperará sus actividades dentro de plazos establecidos.

Se recomienda mantener una continua revisión de la Política de Seguridad de la Información, verificando su cumplimiento por parte de los trabajadores de la OTIN.

Se recomienda continuar con las capacitaciones al personal en temas de seguridad de la información con el fin de que puedan familiarizarse y aplicar los conocimientos adquiridos.

Se recomienda realizar evaluaciones de riesgos periódicamente para minimizar los mismos y priorizar aquellos que sean catalogados como riesgos de alta consecuencia.

BIBLIOGRAFÍA

- Advisera. (2012). Your simple introduction to the basic facts. Recuperado de http://advisera.com/27001academy/what-is-iso-27001/
- Agustín López Neira y Javier Ruiz Spohr. ISO 27000.ES El portal de ISO 27001 en Español. Recuperado de http://www.iso27000.es/iso27000.html
- Alberto G. Alexander. (2005). *Análisis del Riesgo y el Sistema de Gestión de Seguridad de Información: El Enfoque ISO 27001:2005*. Lima.
- Alejandro Corletti Estrada. (2006). ISO-27001: *LOS CONTROLES (Parte I)*. Madrid.
- Alexander G., Alberto. (2007). *Diseño de un Sistema de Gestión de Seguridad de Información/Óptica ISO/ IEC 27001:2005. Primera edición.* Bogotá: Alfaomega Colombiana S.A.
- Barrantes Porras, Carlos Eduardo y Hugo Herrera, Javier Roberto. (2012). *DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN EN PROCESOS TECNOLÓGICOS.* (Proyecto de Tesis para optar el Título profesional de ingeniero de computación y sistemas). Universidad de San Martín de Porres, Lima, Perú.
- Berrueta García, Eduardo. (2015). *Transmisión de información por medios convencionales e informáticos.* España: Ediciones Nobel S. A.
- Cámara de Comercio, Industria y Navegación de Málaga, empresa Nexus Consultores y Auditores y empresa Tecnotur 3000. *Proyecto CAMERSEC*. (2006). Málaga, España.

- De la Cruz Guerrero, César Wenceslao y Vasquez Montenegro, Juan Carlos. (2008). *ELABORACIÓN Y APLICACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACION (SGSI) PARA LA REALIDAD TECNOLÓGICA DE LA USAT*. (Proyecto de tesis para optar el título de Ingeniero de Sistemas y Computación). Universidad Católica Santo Toribio de Mogrovejo, Chiclayo, Perú.
- De pablos Carmen, López José, Romo Santiago y Medina Sonia. (2004). INFORMÁTICA Y COMUNICACIONES EN LA EMPRESA. Madrid: ESIC Editorial.
- Eduardo Fernandez, Medina Paton, Roberto Moya Quiles, Mario Gerardo Plattini Velthuis. (2003). *Seguridad de las tecnologías de la información. La construcción de la confianza para una sociedad conectada.*Madrid: Ediciones Aenor.
- Erika López López. Universidad Nacional Autónoma de México. Esquemas de Seguridad Informática. Recuperado de http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/DefinicionPolitica.php
- Espinoza Aguinaga, Hans Ryan. (2013). *Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo*. (Proyecto de tesis de fin de carrera, Pontificia Universidad Católica del Perú). Recuperado de http://tesis.pucp.edu.pe/repositorio/handle/123456789/4957

- ETICOM, asociación de Empresarios de Tecnologías de la Información y Comunicaciones de Andalucía. *Proyecto PYMETICA.* (2002). Andalucía, España.
- Ferrer Quintana, José Damián. (2009). *CENTRO DE PROCESO DE DATOS: EL CEREBRO DE NUESTRA SOCIEDAD*. Discurso en Academia de Ciencias e Ingeniería de Lanzarote, España.
- Google Maps. (2016). Recuperado de https://www.google.com.pe/maps/place/Av.+Gral.+Garz%C3%B3n+658,+Jes%C3%BAs+Mar%C3%ADa+15072/@-12.066466,-77.0475487,17z/data=!3m1!4b1!4m5!3m4!1s0x9105c8e7d3722aa7:0x50e3e8f4a344faf9!8m2!3d-12.066466!4d-77.04536
- Huamán Monzón, Fernando Miguel. (2014). *Diseño de procedimientos de auditoría de cumplimiento de la norma NTP-ISO/IEC 17799:2007 como parte del proceso de implantación de la norma técnica NTP-ISO/IEC 27001:2008 en instituciones del estado peruano*. (Tesis para optar por el Título de Ingeniero Informático, Pontificia Universidad Católica del Perú). Recuperado de http://tesis.pucp.edu.pe/repositorio/handle/123456789/5582
- J. Llorens Fabregas. (2005). *Gerencia de Proyectos de Tecnología de Información*. Venezuela: Editorial CEC, SA.
- José Ramón Mora Martínez. (2003). *GUÍA METODOLÓGICA PARA LA GESTIÓN CLÍNICA POR PROCESOS*. Madrid: Ediciones Díaz de Santos, S. A.
- Manuel Tupia. (2011). Principios de auditoría y control de sistemas de información. Segunda edición. Lima: Tupia Consultores y Auditores.

- Maurice Frayssinet Delgado. *Taller de Implementación de la norma ISO 27001*. ONGEI. Recuperado de http://www.ongei.gob.pe/docs/ISO_27001_v011.pdf
- NTP-ISO/IEC 27001: 2014. TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de Gestión de seguridad de la información. Requisitos.
- Soy Aumatell, Cristina. (2003). *Auditoría de la información*. Barcelona: Editorial UDC.
- Talavera Álvarez, Vasco Rodrigo. (2015). *Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013*. (Tesis para optar por el Título de Ingeniero Informático, Pontificia Universidad Católica del Perú). Recuperado de http://tesis.pucp.edu.pe/repositorio/handle/123456789/6092
- Web INEI https://www.inei.gob.pe/nosotros/

ANEXOS

Anexo 01

Inventario de procesos de la Oficina Técnica de Informática

MACROPROCESO		UNIDADES	PROCESO		SUBPROCESO	
10	Tecnologías de Información y Comunicaciones	**UNIDAD DE DESARROLLO DE SISTEMAS**	10.01	Proyectos de Sistemas de Información	10.01.01	Desarrollo de Sistemas de Información
					10.01.02	Mantenimiento de Sistemas de Información
					10.01.03	Actualización y/o Modificación de Base de Datos
		UNIDAD DE PRODUCCION	10.02	Producción de Sistemas y Aplicaciones	10.02.01	Publicación y Administración de la Página Web
					10.02.02	Publicación y Administración del Portal de Transparencia
					10.02.03	Actualización de Sistemas y/o Aplicaciones en los Servidores de Producción
					10.02.04	Monitoreo de Sistemas y/o Aplicaciones de Publicaciones en el Portal
					10.02.05	Nuevos Sistemas y/o Aplicativos en Producción
		UNIDAD DE OPERACIONES	10.03	Operaciones e Infraestructura	10.03.01	Soporte Técnico Informático de Hardware y Software
					10.03.02	Inventario y actualización de Software base en los equipos informáticos
		UNIDAD DE INFRAESTRUCTURA	10.04		10.04.01	Mantenimiento Lógico de Comunicaciones de Redes, Servidores y PC'S
					10.04.02	Mantenimiento Físico Preventivo y Correctivo de los equipos de Servidores y Redes
					10.04.03	Monitoreo y Solución de Conexiones
					10.04.04	Implementación de Servidores
					10.04.05	Creación de Cuentas de Redes
					10.04.06	Respaldo de Información de base de datos
					10.04.07	Informe de Verificación y Procesos de Respaldo de Información
					10.04.08	Restauración de Backup
					10.04.09	Mantenimiento y Revisión de los Dispositivos de Backup
					10.04.10	Monitoreo de los Servicios de las ODEI
		UNIDAD DE CALIDAD Y SEGURIDAD	10.05	Gestión de Seguridad de la Información	10.05.01	Formulación y Evaluación del Plan Operativo Informático
					10.05.02	Seguridad Perimetral Informática
					10.05.03	Seguridad de la Información
				Gestión de la Calidad	10.05.04	Medición, Análisis y Mejora
					10.05.05	Auditoria y Paso a Certificación
		UNIDAD DE PLANIFICACIÓN TIC	10.06	Gestión de Proyectos Estratégicos	10.06.01	Formulación y Seguimiento de Estrategias de las Tecnologías de la Información (PETI)
					10.06.02	Formulación y Seguimiento de Estrategias de Gobierno Electrónico (PEGE)
					10.06.03	Formulación y Seguimiento del Plan de Contingencias

Fichas técnicas de los procesos:

INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA				
FICHA DEL PROCESO NIVEL 1				
1) Nombre	10.01 Ingeniería de Software			
2) Objetivo	Desarrollar e implementar los diversos sistemas de información para los diversos proyectos que lo soliciten.			
3) Descripción	Desarrollar sistemas de información y dar mantenimiento a los diversos proyectos y plataformas que lo requieran y respaldar la base de datos para su resguardo.			
4) Alcance	Oficina Ejecutiva de Desarrollo de Sistemas.			
5) Proveedor	**6) Entrada**	**7) Listado de procesos de nivel 2**	**8) Salida**	**9) Destinatario de los bienes y servicios**
Entidades solicitantes	Solicitud	10.01.01. Desarrollo de Sistemas de Información	Sistema implementado, manuales de usuario	Entidades Solicitantes
Áreas de INEI			Sistema implementado, manuales de usuario, manuales técnicos	Áreas del INEI
Áreas de INEI	Solicitud de modificación	10.01.02. Mantenimiento de Sistemas de Información	Sistema implementado, manuales de usuario, manual de capacitación	Área usuaria
Área usuaria	Requerimiento de actualización y/o modificación de base de datos	10.01.03. Actualización y/o Modificación de Base de Datos	Base de Datos actualizada	Área usuaria
10) Indicadores				
11) Registros				
Aprobado por:	**Nombres y apellidos**		**Oficina - Cargo**	**Firma**

INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA

FICHA DEL PROCESO NIVEL 1				
1) Nombre	10.02. Producción de Sistemas y Aplicaciones			
2) Objetivo	Brindar el mantenimiento y soporte a los sistemas y aplicativos en producción			
3) Descripción	Se encarga de administrar la página web, portal de transparencia, actualización y monitoreo de los sistemas de consultas del INEI.			
4) Alcance	Oficina Ejecutiva de Producción			
5) Proveedor	**6) Entrada**	**7) Listado de procesos de nivel 2**	**8) Salida**	**9) Destinatario de los bienes y servicios**
Usuario INEI	Solicitud de modificación de la página web o un nuevo módulo	10.02.01. Publicación y Administración de la Página Web	Modificaciones efectuadas	Usuario INEI
Usuario INEI	Solicitud (Solicitud de personal, directorio telefónico, directorio de funcionarios, responsables del INEI, otros documentos)	10.02.02. Publicación y Administración del Portal de Transparencia	Confirmación de atención a solicitud (Solicitud atendida por la ONGEI)	Usuario INEI
			Confirmación de atención a solicitud	Usuario INEI
Usuario INEI	Solicitud de actualización	10.02.03. Actualización de Sistemas y/o consultas en los servidores de publicaciones	Actualización de los diversos sistemas y/o aplicaciones en los servidores de publicaciones.	Usuario INEI
Usuario INEI	Solicitud de verificación	10.02.04. Monitoreo de Sistemas y/o Aplicaciones de Publicaciones en el Portal	Solicitud de verificación inválida	Solicitante
			Error solucionado	Solicitante
OTIN	Solicitud de pase a producción	10.02.05. Publicación de Sistemas y/o Aplicativos Nuevos	Publicación de aplicativo correcta	OTIN
10) Indicadores				
11) Registros				
Aprobado por:	**Nombres y apellidos**		**Oficina - Cargo**	**Firma**

INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA

FICHA DEL PROCESO NIVEL 1				
1) Nombre	10.03. Gestión de Operaciones			
2) Objetivo	Implementar y ejecutar la actualización, respaldo, implementación y soporte técnico tanto a nivel de equipos, redes, conexiones, servidores y otros del INEI.			
3) Descripción	Se encarga de administrar, monitoreo y soluciones de las conexiones a nivel INEI y del soporte técnico a todos los equipos informáticos a nivel nacional.			
4) Alcance	Oficina Ejecutiva de Operaciones			
5) Proveedor	**6) Entrada**	**7) Listado de procesos de nivel 2**	**8) Salida**	**9) Destinatario de los bienes y servicios**
Solicitante - INEI	Solicitud de atención	10.02.09. Soporte Técnico Informático de Hardware y Software	Registro en HelpDesk	Solicitante - INEI
Usuario INEI	Inventario de Hardware y Software	10.03.02. Inventario y actualización de Software base en los equipos informáticos	Inventario de Hardware y Software Actualizado	Usuario INEI
10) Indicadores				
11) Registros				
Aprobado por:	**Nombres y apellidos**		**Oficina - Cargo**	**Firma**

INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA

FICHA DEL PROCESO NIVEL 1				
1) Nombre	10.04. Gestión de Infraestructura			
2) Objetivo	Implementar y ejecutar la actualización, respaldo, implementación y soporte técnico tanto a nivel de equipos, redes, conexiones, servidores y otros del INEI.			
3) Descripción	Se encarga de administrar, monitoreo y soluciones de las conexiones a nivel INEI y del soporte técnico a todos los equipos informáticos a nivel nacional.			
4) Alcance	Oficina Ejecutiva de Infraestructura			
5) Proveedor	**6) Entrada**	**7) Listado de procesos de nivel 2**	**8) Salida**	**9) Destinatario de los bienes y servicios**
OTIN	Necesidad de monitorear los equipos	10.04.01. Mantenimiento Lógico de Comunicaciones de Redes, Servidores y PC's	Mantenimiento lógico finalizado	Usuario de INEI
			Reporte de equipo con fallas de actualización	Soporte Técnico Informático de Hardware y Software.
			Verificación de actualización	Usuario de INEI
OTIN	Solicitud de mantenimiento	10.04.02. Mantenimiento Físico Preventivo y Correctivo de los equipos de Servidores y Redes	Comunicado del análisis realizado	Director Técnico I - OTIN
Sede Central	Monitoreo de conexiones	10.04.03. Monitoreo y Solución de Conexiones	Conexión restablecida	Usuarios INEI.
Oficinas Departamentales			Conexión restablecida	Oficinas Departamentales
Usuario - INEI	Solicitud de implementación de servidores	10.04.04. Implementación de Servidores	Comunicar atención de servidor implementado y respaldo realizado	Solicitante - INEI
OEPER	Solicitud de creación de cuenta	10.04.05. Creación de Cuentas de Redes	Cuenta creada	Soporte Técnico Informático de Hardware y Software
Áreas Solicitantes	10.04.06. Solicitar respaldo de información de base de datos y aplicaciones	10.04.06. Respaldo de Información de Base de Datos y Aplicaciones	Respaldo validado	Administrador de Base de Datos
Supervisor Informático - ODEIS	10.04.07. Enviar el cuadro de respaldo de información actual para su revisión	10.04.07. Informe de Verificación y Procesos de Respaldo de Información	Informe de respaldo de información revisado	OTIN
Analista de Sistemas, Analista de Sistemas, Analista de Sistemas / Usuario - INEI	10.04.08. Solicitar restauración de Información	10.04.08. Restauración de Backup	Respaldo de información	Analista de Sistemas, Analista de Sistemas, Analista de Sistemas / Usuario - INEI

5) Proveedor	6) Entrada	7) Listado de procesos de nivel 2	8) Salida	9) Destinatario de los bienes y servicios
OTIN	10.04.09. Verificar los job (diario, quincenal y mensual). ¿Hay incidencias? SI no hay incidencias, fin del subproceso; si hay incidencias ir a la siguiente actividad.	10.04.09. Mantenimiento y Revisión de los Dispositivos de Backup	Reporte de incidencias identificadas en el proceso	Verificación y Procesos de Respaldo de Información
OTIN	Solicitar información sobre estado situacional de las ODEI	10.04.10. Monitoreo de los Servicios de las ODEI	Confirmación de solución a incidencia	Informe de Verificación y Respaldo de Información
10) Indicadores				
11) Registros				
Aprobado por:	**Nombres y apellidos**		**Oficina - Cargo**	**Firma**

INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA

FICHA DEL PROCESO NIVEL 1				
1) Nombre	10.05. Seguridad Informática			
2) Objetivo	Establecer los lineamientos, implementación y ejecución de seguridad de información.			
3) Descripción	Encargada de la formulación y evaluación del Plan Operativo informático para la planificación de actividades y la seguridad perimetral informática.			
4) Alcance	Oficina de Calidad y Seguridad			
5) Proveedor	**6) Entrada**	**7) Listado de procesos de nivel 2**	**8) Salida**	**9) Destinatario de los bienes y servicios**
OTIN	Necesidad del Plan Operativo Informático	10.05.01. Formulación y Evaluación del Plan Operativo Informático	Evaluación del Plan Operativo Informático	OTIN
OTIN	Registros de equipos de seguridad	10.05.02. Seguridad Perimetral Informática	Informe del incidente	Director Técnico I - OTIN
OTIN	Necesidad del Plan del SGSI	10.05.03. Seguridad de la Información	Verificación del cumplimiento de los planes	INEI
OTIN	Implementar Aplicativo Alertas de Indicadores ISO	10.05.04. Medición, Análisis y Mejora de los productos de tecnologías de información.	Verificar el cumplimiento de los indicadores	OTIN
OTIN	Necesidad de contratar Auditor	10.05.05. Auditoria y Paso a Certificación	Memo a los responsables de las observaciones o no conformidades	Usuarios INEI
10) Indicadores				
11) Registros				
Aprobado por:	**Nombres y apellidos**		**Oficina - Cargo**	**Firma**

INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA

FICHA DEL PROCESO NIVEL 1				
1) Nombre	10.05. Seguridad Informática			
2) Objetivo	Establecer los lineamientos, implementación y ejecución de seguridad de información.			
3) Descripción	Encargada de la formulación y evaluación del Plan Operativo informático para la planificación de actividades y la seguridad perimetral informática.			
4) Alcance	Oficina de Calidad y Seguridad			
5) Proveedor	**6) Entrada**	**7) Listado de procesos de nivel 2**	**8) Salida**	**9) Destinatario de los bienes y servicios**
OTIN	Solicitud de necesidades de Sistemas de Información de todas las unidades orgánicas del INEI	10.06.01. Formulación y Seguimiento de Estrategias de las Tecnologías de la Información (PETI)	PETI actualizado	Coordinador de Desarrollo de Sistemas
OTIN	Necesidad de implementación del E-government	10.06.02. Formulación y Seguimiento de Estrategias de Gobierno Electrónico (PEGE)	PEGE actualizado	Ciudadanos, empresas, entidades públicas y personal del INEI
OTIN	Necesidad de implementar planes de contingencia	10.06.03. Formulación y Seguimiento del Plan de Contingencias	Cumplimiento del plan verificado	Usuarios del INEI
10) Indicadores				
11) Registros				
Aprobado por:	**Nombres y apellidos**		**Oficina - Cargo**	**Firma**

Anexo 02

CheckList de auditoría de la Base de Datos Microsoft SQL Server

1. PLANIFICACIÓN Y ALCANCE DE LA AUDITORÍA		Cumple		Sustento y/o Comentario
		Si	No	
	Definir los objetivos de auditoría/aseguramiento			
1.1.0.	¿Conoce sobre los controles de seguridad de bases de datos Microsoft SQL Server?			
1.1.1.	¿Se aplica en el INEI controles de seguridad de Bases de datos?			
		Si	No	Sustento y/o Comentario
	Definir límites de revisión.			
1.2.1.	¿Existe procedimiento de seguridad del sistema de la base de datos?			
1.2.2.	¿Existe procedimiento de seguridad de las políticas de Gestión de la base de datos?			
1.2.3.	¿Existe documentación sobre el entorno de base de datos Microsoft SQL Server?			
1.2.4.	¿Está registrado el total de número de usuarios de la Base de datos?			
1.2.5.	¿Está registrado el número de instancias de la base de datos?			
1.2.6.	¿Se cuenta con documentación de la versión, reléase del Sistema Operativo que soporta la Base de Datos?			
1.2.7.	¿Se cuenta con una lista de Servidores de Base de datos en la cual se indica el número de versión, su ubicación y las aplicaciones que contiene cada uno?			
1.2.8.	¿Se cuenta con información sobre los actuales grupos locales de Windows Server y los miembros de cada grupo que acceden a la base de datos?			
		Si	No	Sustento y/o Comentario
	Definir seguridad			
1.3.0	¿Conoce sobre los estándares corporativos de seguridad para base datos Microsoft SQL Server?			
1.3.1.	¿Existe implementada algún estándar corporativo de seguridad de base datos en el INEI?			
1.3.2.	¿Existen mejores prácticas que ayuden a emplear las normas de control de seguridad de la base de datos?			
1.3.3.	¿Conoce sobre las configuraciones de seguridad para base de datos, según las publicaciones de Microsoft?			
1.3.4.	¿Existe implementada alguna configuración de seguridad de base datos en la institución?			
1.3.5.	¿Conoce las políticas de configuración de la Base de Datos de Microsoft SQL Server?			

2. PREPARATIVOS		Cumple		Sustento y/o Comentario
		Si	No	
	Definir el entorno de base de datos de Microsoft SQL Server.			
2.1.0.	¿Conoce y comprende el entorno de Base de Datos de Microsoft SQL Server de la institución?			
2.1.1.	¿Existe evaluación de riesgos claves que puedan afectar directamente a las bases de datos y su continuidad?			
2.1.2.	¿Existe una cultura de controles de la empresa? (Se ejerce juicio propio para determinar los controles claves durante el proceso)			
2.2.3.	¿Conoce sobre las sentencias de triggers respecto a seguridad de base de datos?			
2.2.4.	¿Las sentencias de triggers de la base de datos se encuentran documentadas?			
2.2.5.	¿Las sentencias de triggers están identificadas según su nivel de prioridad e importancia? Mencione			
2.2.6.	¿Existen triggers que monitoreen los cambios a las tablas de la base de datos?			
2.2.7.	¿Existen triggers que alerten sobre malos procedimientos dentro de las base de datos? (acciones raras o altamente riesgosas)			
		Si	No	Sustento y/o Comentario
	Instalaciones físicas y el acceso a bases de datos están asegurados.			
2.2.0.	¿Existe políticas establecidas de control de acceso físico al datacenter?			
2.2.1.	¿El acceso físico al datacenter se encuentra limitado solo a personal autorizado?			
2.2.2.	¿Los servidores de base de datos se encuentran en un ambiente seguro?			
2.2.3.	¿El acceso a la configuración de la consola de servidores se encuentran protegidos por contraseña?			
2.2.4.	¿Existen procedimiento de bitácora de acceso a las instalaciones del datacenter?			
2.2.5.	¿Se ha efectuado anteriormente alguna auditoria de seguridad física y/o datos al datacenter?			
2.2.6.	¿Existe actualmente activa alguna auditoria de seguridad física?			

3. ACCESO Y AUTORIZACIÓN		Cumple		Sustento y/o Comentario
		Si	No	
	El acceso apropiado y autorizaciones están en su lugar.			
3.1.0.	¿Existe controles respecto al acceso y las autorizaciones de acceso a la Base de Datos?			
3.1.1.	¿El acceso de DBA tienen diferentes procedimientos para iniciar sesión en los sistemas de base de datos SQL Server? (SQL autentication, cuentas de Active Directory o ambos)			
3.1.2.	¿Se documenta la aprobación de usuarios que pueden acceder directamente a las bases de datos SQL?			
3.1.3.	¿Se evalúan y verifican los permisos a todos los usuarios/miembros asignados a la función db_owner?			
3.1.4.	¿Se tiene programado algún procedimiento para obtener la lista de usuarios activos de la base de datos SQL ejecutando el comando sp_helplogins?			
3.1.5.	¿Se hace revisión a la lista de usuarios de SQL Server para asegurarse que no se utilicen cuentas genéricas (pruebas, huésped o cuentas compartidas)?			
3.1.6.	¿Se verifica que las cuentas y contraseñas por defecto no se utilizan al tratar de iniciar sesión en la base de datos utilizando valores conocidos?			
3.1.7.	¿Se revisa y evalúa la idoneidad de los perfiles de acceso asignado a los usuarios de la bases de datos SQL Server?			
3.1.8.	En el proceso para establecer una contraseña. ¿Se utilizan contraseñas genéricas o contraseñas que no pueden ser fácilmente adivinadas?			
3.1.9.	¿Se hace controles sobre los atributos de las contraseñas asignadas a los usuarios de la Base de datos SQL Server?			
3.1.9.1.	¿Se cumple historia de contraseña? (Recomendado 24)			
3.1.9.2.	¿Se cumple edad máxima de contraseña? (Recomendado 42)			
3.1.9.3.	¿Se cumple edad mínima de contraseña? (Recomendado 1)			
3.1.9.4.	¿Se cumple longitud de la contraseña mínima? (Se recomienda 8)			
3.1.9.5.	¿Se cumple requisitos de complejidad de contraseña? (Recomendado SI)			
3.1.9.6.	¿Se almacenan las contraseñas usando cifrado reversible para todos los usuarios de dominio?			
3.1.10.	¿Existen procedimientos para el acceso a las bases de datos en caso de emergencia?			
3.1.10.1.	¿Existe definido los métodos y los controles sobre el acceso de emergencia?			
3.1.10.2.	¿Se requiere documentación para cada uso de emergencia que se presente?			
3.1.10.3.	¿Se requiere terminación después que se resuelva la cuestión de negocios?			

3. ACCESO Y AUTORIZACIÓN		Cumple		Sustento y/o Comentario
		Si	No	
3.1.10.4.	¿Se requiere acceso posterior revisión y aprobación del administrador para la autorización previa?			
		Si	No	Sustento y/o Comentario
	El acceso remoto a la base de datos			
3.2.0.	¿Existe algún control respecto al acceso remoto a la base de datos SQL Server?			
3.2.1.	¿Se encuentra activo el acceso remoto a la base de datos SQL Server?			
3.2.2.	¿El DBA evalúa los requisitos de negocio para brindar el acceso remoto a la base de datos?			

4. SEGURIDAD Y VIGILANCIA		Cumple		Sustento y/o Comentario
		Si	No	
	Acceso de los usuarios es acorde con sus responsabilidades de trabajo.			
4.1.0.	¿Existe control respecto al acceso de los usuarios acorde a sus responsabilidades de trabajo?			
4.1.1.	¿Existe procesos de revisión para la concesión, actualización y terminación de acceso de los usuarios de la base de datos?			
4.1.2.	¿Se cuenta con información sobre los usuarios actuales de base de datos y administradores y sus funciones?			
4.1.3.	¿Está determinado los privilegios de acceso a objetos o Estados directamente de los usuarios?			
4.1.3.1.	¿Se cuenta con información sobre los usuarios con privilegios individuales y los objetos relacionados a los que tienen acceso?			
4.1.3.2.	¿Se designa los accesos basado en las descripciones de tareas y el acceso concedido?			
4.1.3.3.	¿Se efectúan las solicitudes relacionadas con el acceso de carácter razonable y posterior autorización?			
4.1.3.4.	¿Se realiza evaluación y discusión sobre los posibles derechos de acceso excesivo con los administradores, oficiales de seguridad de información y dueños de negocio?			
4.1.4.	¿Se cumple responsablemente con la asignación de privilegios de revisión asignados a usuarios y roles?			
4.1.5.	¿Existe algún control periódico de roles y privilegios asignados que garanticen que el acceso este acorde con sus responsabilidades de trabajo?			
4.1.6.	¿Se realiza alguna constatación de la lista de los empleados despedidos con los usuarios activos de la base de datos?			

4. SEGURIDAD Y VIGILANCIA		Cumple		Sustento y/o Comentario
		Si	No	
4.1.7.	¿Existe control sobre la asignación de funciones fijas de servidor (Adm de sistemas, Server admin u otro) para que estas solo se utilicen como apoyo de la actividad del DBA?			
4.1.8.	¿Existe algún informe o documento que se procede a realizar para asignar crear, alterar o privilegios de las cuentas de usuarios de la base de datos?			
4.1.9.	¿Existe algún tipo de procedimiento de evaluación para dar privilegios de administrador de sistemas?			
4.1.10.	¿Se verifica que los usuarios invitados o temporales de la base de datos son deshabilitados inmediatamente acabado su función?			
4.1.11.	¿Se hace verificación que los usuarios invitados de la base de datos no tengan acceso a ningún objeto?			
		Si	No	Sustento y/o Comentario
	Resolver casos de inadecuado acceso y procesamiento de problemas y anomalías de SQL Server.			
4.2.0.	¿Existe algún control o procedimientos para resolver casos de inadecuado acceso y procesamiento de problemas y anomalías de SQL Server?			
4.2.1.	¿Existen precedentes de algunos informes, consultas, ajustes de alarma y salida de la herramienta utilizadas por el DBA, el personal de seguridad de la información o demás personal operativo de vigilancia?			
		Si	No	Sustento y/o Comentario
	Base de datos comunicado en una red está protegido.			
4.3.0.	¿Existe control para la protección de la red que permita tener acceso a las bases de datos?			
4.3.1.	¿Existe algún diagrama de arquitectura de red que describa la relación lógica entre la base de datos y otros sistemas y redes de la institución?			
4.3.2.	¿La base de datos está protegida por un firewall que protege su salida a internet?			
4.3.3.	¿La base de datos se encuentra protegida de cualquier red externa?			
4.3.4.	¿Los servidores se encuentra en una DMZ? (Servidores de Aplicaciones y bd)			

5. RESPALDO Y RECUPERACIÓN		Cumple		Sustento y/o Comentario
		Si	No	
	Una estrategia de backup y recuperación existe y se prueba.			
5.1.0.	¿Existe estrategia de backup y recuperación y posteriores pruebas de operatividad?			
5.1.1.	¿Existe algún plan de continuidad del negocio para la base de datos SQL Server?			
5.1.2.	¿Las copias del archivo de respaldo se almacenan en una ubicación independiente de la ubicación de los servidores?			
5.1.3.	¿Los procedimientos de backup y los datos son examinados regularmente?			
5.1.4.	¿Existe documentación de los procedimientos de backup?			
5.1.5.	¿Se registra el historial más reciente de las copias de seguridad?			
5.1.6.	¿El sistema de base de datos Server Maestro y el modelo están siendo respaldados?			
5.1.7.	¿Los archivos de registro de transacciones están respaldados?			
5.1.8.	¿Existen procedimientos que efectúan cifrado de datos sensibles y confidenciales sobre los medios de copia de seguridad?			
5.1.9.	¿Los datos de Microsoft SQL Server y registro de archivos tienen distinta ubicación en el disco físico al de las copias de seguridad y ambos se encuentran debidamente protegidos?			
5.1.10.	¿Existe documentación sobre el programa de backup y el registro de todas las copias de seguridad realizadas?			
5.1.11.	¿La ejecución de los backup se efectúa cuando las actividades en la base de datos son bajas?			

6. CIFRADO		Cumple		Sustento y/o Comentario
		Si	No	
	Una estrategia de cifrado existe y se implementa para proteger la información confidencial apropiadamente.			
6.1.0	¿Existe alguna estrategia de cifrado implementada para proteger la información confidencial apropiadamente de la base de datos?			
6.1.1.	¿Se utiliza un paquete o el paquete nativo para implementar la encriptación?			
6.1.2.	¿Existe alguna norma de clasificación de cifrado de datos de la empresa?			
6.1.3.	¿Existe alguna exigencia del uso de encriptación para proteger la información de la base de datos?			

6. CIFRADO		Cumple		Sustento y/o Comentario
		Si	No	
6.1.4.	¿Existe alguna verificación periódica de que los registros que contienen información sensible estén correctamente cifrados?			

7. CONFIANZA RELACIONES		Cumple		Sustento y/o Comentario
		Si	No	
	Relaciones de confianza son restringidas y protegidas.			
7.1.0.	¿Existe algún control de restricción y protección sobre las relaciones de confianza de acceso a la base de datos SQL Server?			

Anexo 03

CUESTIONARIO DE SEGURIDAD DE LA INFORMACION EN LA ADMINISTRACION PUBLICA

PERÚ | Presidencia del Consejo de Ministros | Oficina Nacional de Gobierno Electrónico e Informática

INFORMACION GENERAL	
1. Nombre de la Institución :	
2. Poder, Sector, Gobierno Regional, Gobierno Local u otro pertinente :	
3. Departamento :	
4. Provincia :	
5. Distrito :	
6. Centro Poblado Urbano :	
7. Apellidos y Nombres del Informante :	
8. Teléfono del Informante :	
9. Correo Electrónico del informante :	

(Responder con **X** en la columna Si o No a cada pregunta)

		SI	NO
1.	**Con relación a las Políticas de seguridad de la información**		
a.	¿Se han elaborado políticas de seguridad de la información?		
b.	¿Se están aplicando las políticas de seguridad de la información?		
c.	¿Se hacen de conocimiento al personal de la institución las políticas de seguridad de la información?		
d.	¿Realizan evaluaciones y actualizaciones constantes de las políticas de seguridad de la información?		
e.	¿Las políticas de seguridad de la información están basadas en algún estándar nacional o internacional?		
2.	**Con relación a la organización para la seguridad de la información**	SI	NO
a.	¿Tiene la institución un área o una persona asignada para labores exclusivas de seguridad de la información?		
b.	¿El área de seguridad de la información está formalizada dentro del organigrama de la institución?		
c.	¿Tienen un comité de seguridad de la información a nivel de alta dirección?		
d.	¿Tienen asesoramiento especializado en materia de seguridad de la información?		
e.	¿Tienen algún mecanismo de cooperación con organizaciones públicas o privadas referidas a seguridad de la información?		
f.	¿Realizan evaluaciones de seguridad de la información a través de otras entidades públicas o privadas?		
g.	¿Al realizar contratos con empresas externas exige requerimientos de seguridad de la información?		
3.	**Con relación a la clasificación y control de activos informáticos**	SI	NO
a.	¿Están clasificados los activos informáticos (hardware, software)?		
b.	¿Cuenta esta clasificación, con un sistema software que la automatice?		
c.	¿Realizan periódicamente la actualización de su inventario de activos informáticos?		
d.	¿Actualizan las etiquetas con nombres de contenidos, fechas, ubicación, versiones y responsables de los activos informáticos?		
4.	**Con relación a las políticas del personal respecto a la seguridad Informática**	SI	NO
a.	¿Están preparados los usuarios para reportar los incidentes de seguridad de los sistemas de información?		
b.	¿La institución tiene acuerdos con el personal sobre la confidencialidad de la información?		
c.	¿Reciben los usuarios capacitación actualizada en temas de seguridad de la información?		
d.	¿Tienen procedimientos de respuesta a incidentes y anomalías en materia de seguridad informática para ser aplicados por los usuarios?		
e.	¿Los empleados,contratistas y terceros tienen una guía que establezca expectativas de seguridad de su rol?		
5.	**Con relación a la seguridad física y ambiental de los sistemas de Información**	SI	NO
a.	¿Tienen identificadas las áreas físicas seguras donde se encuentran los sistemas de información?		
b.	¿Tienen controles de ingreso del personal a las áreas físicas donde se encuentran los sistemas de información?		
c.	¿Están preparados para mantener el correcto funcionamiento del suministro eléctrico en caso del alguna falla?		

d.	¿Están preparados para mantener el correcto funcionamiento del cableado de datos en caso del alguna falla?		
e.	¿Tienen mecanismos de seguridad de la información para los equipos que ingresan y salen fuera del ámbito de la institución?		
f.	¿Cuentan con mantenimiento periódico del hardware y software en los equipos informáticos?		
g.	¿Se usan técnicas para que la información de dispositivos de almacenamiento con data sensible no sea recuperable?		
6.	**Con relación a la gestión de las comunicaciones de datos y operaciones de los sistemas informáticos**	**SI**	**NO**
a.	¿Cuentan con procedimientos y responsabilidades operativas del uso y acceso a los sistemas informáticos?		
b.	¿Cuentan con documentación de los procedimientos operativos del uso y acceso de los sistemas informáticos?		
c.	¿Tienen procedimientos para afrontar incidentes de las comunicaciones de datos y operaciones de los sistemas informáticos?		
d.	¿Tienen establecidos controles en la red de datos contra software malicioso (antivirus, antispyware, etc)?		
e.	¿Tienen un registro de acceso y uso de las aplicaciones y servicios de la red de datos del personal operativo?		
f.	¿Tienen un registro de fallas de las comunicaciones de datos?		
g.	¿Tienen un control documentado de toda la información referida a la red de datos, es decir direcciones IP de las maquinas de los usuarios, distribución de las IP, diagrama de la red de datos, entre otros?		
h.	¿Tienen mecanismos de seguridad para proteger la documentación de los sistemas de información?		
i.	¿Tienen establecidos controles de seguridad de los medios de almacenamiento de información en tránsito?		
j.	¿Tienen establecidos controles de seguridad para el sistema de correo electrónico de la institución?		
7.	**Con relación al control de acceso a los sistemas informáticos**	**SI**	**NO**
a.	¿Tienen políticas de control de acceso a los sistemas informáticos de los usuarios en la red de datos?		
b.	¿Se están aplicando las políticas de control de acceso a los sistemas informáticos de los usuarios en la red de datos?		
c.	¿Cuentan con un registro permanente de acceso a los sistemas informáticos de los usuarios en la red de datos?		
d.	¿Cuentan con una administración de los privilegios para acceder a los sistemas informáticos?		
e.	¿Cuentan con una administración de las contraseñas de usuarios para los sistemas informáticos?		
f.	¿Tienen políticas de uso, de los servicios de la red de datos de su institución?		
g.	¿Tienen establecidos mecanismos de autenticación de usuarios para las conexiones externas a la red de datos?		
h.	¿Tienen establecido limitaciones de horario para la conexión a la red de datos?		
i.	¿Están aislados los sistemas informáticos críticos de personal no autorizado?		
j.	¿Tienen mecanismos de monitoreo del uso de los sistemas informáticos?		
k.	¿Tienen controles de seguridad informática de los usuarios que usan computadoras portátiles?		
8.	**Con relación al desarrollo y mantenimiento de sistemas informáticos**	**SI**	**NO**
a.	¿Realiza el análisis y define especificaciones de los requerimientos de seguridad informática cuando desarrolla sistemas informáticos?		
b.	¿Tienen mecanismos de validación de datos de entrada y de salida los sistemas de información?		
c.	¿Se han establecido controles criptográficos en su red de datos, como por ejemplo el uso de certificados digitales u otros programas para la encriptación de datos?		
d.	¿Tienen políticas de uso de los controles criptográficos en su red de datos?		
e.	¿Tienen servicios de no repudio, es decir que el usuario no pueda negar las acciones realizadas en los sistemas informáticos?		
f.	¿Cuentan con una administración de llaves para los certificados digitales?		
g.	¿Mantienen un control del acceso a los programas fuente de las aplicaciones que utilizan en la red institucional?		
h.	¿Tienen procedimientos de control de los cambios que se realizan en las aplicaciones software y el sistema operativo de los servidores o las estaciones de trabajo?		
i.	¿Realizan revisiones a posibles códigos ocultos maliciosos o código troyano dentro de sus aplicaciones software?		

j. ¿Tienen mecanismos de protección cuando se desarrolla software por parte de personal que no pertenece a la institución?		

9. Con relación a la gestión de incidentes de sistemas informáticos	**SI**	**NO**
a. ¿Realiza algún procedimiento para reportar algún evento o debilidad ?		
b. ¿Usa algún sistema de registro de incidentes o software de Helpdesk?		
c. ¿Realiza la clasificación de incidentes?		
d. ¿Tienen elaborado un plan de respuesta ante incidentes?		
e. ¿Investigan y recolectan evidencias sobre el incidente ?		
f. ¿Evaluan el daño y costo de las incidencias?		

10. Con relación a la administración de la continuidad de los sistemas Informáticos	**SI**	**NO**
a. ¿Tienen elaborado planes de continuidad de las operaciones informáticas?		
b. ¿Están implementados los planes de continuidad de las operaciones informáticas?		
c. ¿Realizan pruebas, mantenimiento y evaluación constante de los planes de continuidad de las operaciones informáticas?		

11. Con relación al cumplimiento legal referido a los sistemas Informáticos	**SI**	**NO**
a. ¿Tienen identificada la normativa legal a la que pueda sujetarse las aplicaciones software que usan en la red de su institución?		
b. ¿Tienen políticas y mecanismos de protección de datos y privacidad de la información del personal de la institución?		
c. ¿Tienen controles de prevención del uso inadecuado de los recursos de procesamiento de información?		
d. ¿Tienen controles del cumplimiento de las políticas de seguridad informática?		
e. ¿Realizan auditoria a los sistemas informáticos de su institución?		

Anexo 04

INEI INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA	**INVENTARIO DE ACTIVOS DE INFORMACIÓN**										Edición N°01 Pág. 1 de 1
Área/Proceso/ Subproceso :											Fecha de la Consulta:
Responsable :											__/__/__
CÓDIGO ACTIVO	**CATEGORÍA DE ACTIVO**	**NOMBRE DEL ACTIVO**	**DETALLE DEL ACTIVO**	**UBICACIÓN FÍSICA**	**URL**	**PROPIETARIO**	**CUSTODIO**	**USUARIO**	**FRECUENCIA DE USO**	**TIPO DE USO DEL ACTIVO**	**VALOR DEL ACTIVO**