DESPACHO PRESIDENCIAL
Dirección de Tecnología de Información y Sistemas
15 JUN. 2015
Hora: 11:37 a.m.
Recibido por:

Resolución de la Subsecretaría General de la Presidencia de la República

N° 021 -2015-DP/SSGPR

Lima, 15 JUN. 2015

VISTOS; El Oficio N° 172-2015-DP/DGA del 19 de mayo de 2015 por el cual el Director General de Administración eleva la propuesta de "Plan de Proyecto para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en el Despacho Presidencial";

CONSIDERANDO:

Que, mediante Resolución de la Comisión de Reglamentos Técnicos y Comerciales Nº 001-2007-INDECOPI-CRT del 5 de enero de 2007 se aprobó la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª Edición";

Que, mediante Resolución Ministerial Nº 246-2007-PCM se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática;

Que, mediante Resolución N° 42-2008/CNB-INDECOPI de la Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias del Instituto Nacional de Defensa de la Competencia y de Protección de la Propiedad Intelectual (INDECOPI), se aprueba la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos";

Que, mediante Decreto Supremo Nº 066-2011-PCM se aprueba el "Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0" de aplicación para todas las entidades del Sistema Nacional de Informática, el cual plantea como Estrategia 4. "Implementar mecanismos para mejorar la seguridad de la información";

Que, mediante Resolución Ministerial Nº 129-2012-PCM se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos" en todas las entidades integrantes del Sistema Nacional de Informática cuyos controles deberán ser implementados de acuerdo a las recomendaciones de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición";

Que, mediante el documento del Visto, el Director General de Administración eleva la propuesta de "Plan de Proyecto para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en el Despacho Presidencial" sustentado en el Informe N° 007-2015-DP-DGA/DTIS-CISO-INFZ del 20 de marzo de 2015 de la coordinadora que hace las veces de Oficial de Seguridad de la Información de la entidad, designada mediante Resolución de la Secretaría General de la Presidencia de la República N° 007-2015-DP/SGPR, presentado mediante Oficio N° 071-2015-DP-DGA/DTIS de la Dirección de Tecnología de Información y Sistemas;

Que, mediante Memorando N° 051-2015-DP-DGA/DTIS, de la Dirección de Tecnología de Información y Sistemas se remiten los Informes N° 015-2015-DP-DGA/DTIS-CISO-INFZ y N° 016-2015-DP-DGA/DTIS-CISO-INFZ ambos del 08 de junio de 2015, emitidos por la coordinadora que hace las veces de Oficial de Seguridad de la Información de la entidad, a fin de complementar el sustento técnico de la propuesta formulada;

Que, de acuerdo a lo señalado en los informes antes citados, el "Plan de Proyecto para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en el Despacho Presidencial", responde a lo programado en el Plan Operativo Informático 2015 aprobado mediante Resolución de la Secretaría General de la Presidencia de la República N° 004-2015-DP/SGPR, que a su vez, implementa el Objetivo Específico 2 sobre reforzamiento de la seguridad de la información gestionada en la entidad según el Plan Estratégico Institucional 2012-2016 aprobado mediante Resolución N° 022-2012-DP/SSGPR;

Que, conforme con lo establecido en el numeral 1.1 del artículo 1 de la Resolución de la Secretaría General de la Presidencia de la República N° 014-2015-DP/SGPR, corresponde a la Subsecretaría General aprobar la propuesta de "Plan de Proyecto para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en el Despacho Presidencial" en virtud a la delegación de facultades dispuesta por la referida resolución;

Que, evaluada la propuesta, estando a las consideraciones expuestas y atendiendo a la propuesta realizada por el Director General de Administración y el sustento técnico formulado por la coordinadora que hace las veces de Oficial de Seguridad de la Información del Despacho Presidencial, es pertinente aprobar el "Plan de Proyecto para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en el Despacho Presidencial" y disponer las acciones pertinentes para su cumplimiento;

De conformidad con lo establecido en el Decreto Supremo N° 066-2011-PCM; la Resolución Ministerial N° 129-2012-PCM; y, el Reglamento de Organización y Funciones del Despacho Presidencial, aprobado mediante Decreto Supremo N° 066-2006-PCM, modificado por Decreto Supremo N° 082-2011-PCM;

Contando con los vistos de la Dirección General de Administración, la Dirección de Tecnologías de Información y Sistemas y la Oficina de Asesoría Jurídica;

SE RESUELVE:

Artículo 1.- Aprobación del Plan SGSI

Aprobar el "Plan de Proyecto para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en el Despacho Presidencial", que como anexo forma parte de la presente resolución.

Artículo 2.- Realización de coordinaciones y acciones necesarias

Disponer que la coordinadora que hace las veces de Oficial de Seguridad de la Información del Despacho Presidencial designada por Resolución de la Secretaría General de la Presidencia de la República N° 007-2015-DP/SGPR, está encargada de realizar las coordinaciones y acciones necesarias para el cumplimiento del Plan aprobado por la presente resolución.

Artículo 3.- Difusión

Encargar a la Dirección de Tecnología de la Información y Sistemas la publicación del documento "Plan de Proyecto para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en el Despacho Presidencial", en la intranet y el Portal web institucional.

Regístrese y comuníquese.

ING. JOSÉ ERNESTO MONTALVA DE FALLA
Subsecretario General de la
Presidencia de la Republica (e)

PERÚ | Presidencia del Consejo de Ministros | Despacho Presidencial

PLAN DEL PROYECTO PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL DESPACHO PRESIDENCIAL

Lima, Junio 2015

Datos del Documento

Código:	SGSI PL-001
Versión:	1.0
Fecha de aprobación:	
Creado por:	Ing. Isabel Neri Falla Zevallos Oficial de Seguridad de la Información
Aprobado por:	Secretaría General del Despacho Presidencial
Nivel de confidencialidad:	RESERVADO

Historial de revisiones y modificaciones

Fecha	Versión	Modificado/Revisado por	Descripción de la revisión o modificación
08/06/2015	1.0	Oficial de Seguridad de la Información	Creación del documento y propuesto a la Secretaría General para su aprobación.

TABLA DE CONTENIDO

1. OBJETIVO DEL PLAN

El objetivo del Plan del Proyecto es definir claramente el propósito del Proyecto de implementación del Sistema de Gestión de Seguridad de la Información para el Despacho Presidencial, los documentos que se redactarán, los plazos y las funciones y responsabilidades del proyecto.

2. ALCANCE

El presente Plan se aplica a todas las actividades realizadas en el Proyecto de implementación del Sistema de Gestión de Seguridad de la Información.

3. USUARIOS

Los usuarios de este documento son los miembros de la Alta Dirección, la Oficial de Seguridad de la Información y los miembros del equipo implementador, descrito en el numeral 5.4.

4. DOCUMENTOS DE REFERENCIA

- **Ley Marco de Modernización de la Gestión del Estado - Ley 27658.**
- La **Ley Nº 29733 – Ley de Protección de Datos Personales** para garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen.
- **Resolución Ministerial Nº 129-2012-PCM**, que establece la Implementación de un Sistema de Gestión de Seguridad de la Información usando la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la Información. Requisitos", en las Instituciones del Estado Peruano.
- **Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI.** Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos".
- **Reglamento de Organización y Funciones - ROF del Despacho Presidencial,** aprobado por Decreto Supremo N° 066-2006-PCM y modificado por Decreto Supremo N° 082-2011-PCM
- **Reglamento Interno de trabajo – RIT del Despacho Presidencial, aprobado con** Resolución N° 029-2007-DP/JCGOB
- **Manual de Organización y Funciones del Despacho Presidencial.**
- **Resolución de la Secretaría General de la República N° 007-2015-DP-SGPR** en la que se designa Oficial de Seguridad de la Información del Despacho Presidencial.

5. PROYECTO DE IMPLEMENTACIÓN DEL SGSI

5.1. Objetivo del proyecto

Administrar la seguridad de la información, en base a controles, monitoreo y mejora continua, estableciendo indicadores que midan la confidencialidad, integridad y disponibilidad de la información gestionada en la Institución.

Implementar un Sistema de Gestión de Seguridad de la Información en el Despacho Presidencial en conformidad con la NTP-ISO/IEC 27001:2008, para dar cumplimiento a la Resolución Ministerial N° 129-2012-PCM.

5.2. Entregables del Proyecto

Durante el proyecto de implementación del Sistema de Gestión de Seguridad de la Información - SGSI, se redactarán los siguientes documentos (algunos de los cuales contienen apéndices no mencionados aquí en forma expresa):

i. **Procedimiento para control de documentos y registros**: documento que establece las reglas básicas para la redacción, aprobación, distribución y actualización de documentos y registros.

ii. **Procedimiento para identificación de requisitos**: indicaciones para identificar obligaciones legales, normativas, contractuales y de otra índole.

iii. **Alcance del Sistema de Gestión de Seguridad de la Información**: documento que define en forma precisa los activos, ubicaciones, tecnología, etc. que forman parte del alcance.

iv. **Política de seguridad de la información**: documento clave que establece el marco normativo para controlar la gestión de la seguridad de la información.

v. **Metodología de gestión de riesgos**: documento que describe los métodos, procedimientos y parámetros que se deben emplear para la evaluación y tratamiento de riesgos de la información.

vi. **Cuadro de evaluación de riesgos**: documentación resultante de la evaluación del valor, de las amenazas y vulnerabilidades de los activos.

vii. **Cuadro de tratamiento de riesgos**: documentación que establece los controles de seguridad que se deben implementar para cada riesgo inaceptable.

viii. **Informe sobre evaluación de riesgos y tratamiento del riesgo**: un documento que incluye todos los documentos clave generados en el proceso de evaluación y tratamiento de riesgos.

ix. **Declaración de aplicabilidad**: documento que determina los objetivos y la necesidad u obligatoriedad de cada control establecido en el Anexo A de la norma ISO 27001.

x. **Procedimiento para Auditoría interna:** documento que define cómo se seleccionan los auditores, cómo se redactan los programas de auditoría, cómo se realizan las auditorías y cómo se informan los resultados de las mismas.

xi. **Procedimiento para acciones correctivas:** describe el proceso de implementación para acciones correctivas y preventivas.

xii. **Formulario la revisión por parte de la dirección:** formulario que se utiliza para crear minutas de las reuniones que la dirección realiza para revisar la adecuación del SGSI.

xiii. **Plan de tratamiento del riesgo:** documento que especifica los controles que se deben implementar, quién es responsable de la implementación, de los plazos y de los recursos.

En el Plan de tratamiento del riesgo se especifican otros documentos que deben redactarse durante la implementación del SGSI.

5.3. Fases, Actividades y Plazos

La Oficina Nacional de Gobierno Electrónico e Informática - ONGEI, órgano rector de todas las entidades integrantes del Sistema Nacional de Informática, ha establecido un programa de Implementación incremental de NTP-ISO/IEC 27001:2008; en función de dicho plan se han establecido actividades y entregables en el Despacho Presidencial, ver **ANEXO N° 1: ACTIVIDADES Y ENTREGABLES.**

El tiempo de implementación variará de acuerdo a la asignación de recursos humanos, para la función de seguridad de la información, el Despacho Presidencial, cuenta solamente con la Oficial de Seguridad de la Información (IN HOUSE), otra opción es tercerizar una o más fases de la implementación, con lo que los tiempos se acortarían.

Para la ejecución de las actividades que requieran de desembolso presupuestal, se harán modificaciones en el PAC 2015 de la Dirección de Tecnología de la Información y Sistemas, a fin de lograr los objetivos propuestos.

El presente documento es susceptible de mejoras durante su desarrollo, dado que este tipo de proyectos no han sido desarrollados anteriormente en la institución y en función de la aplicación de la metodología PHVA descrita en el título ***Metodología*** del presente documento, además es de esperar que durante el avance se presenten variables que no pueden ser consideradas desde el inicio, tales como la cultura organizacional, disponibilidad presupuestal y cumplimiento de disposiciones urgentes.

5.4. Organización del Proyecto

EL proyecto estará a cargo de un equipo implementador, organizado de la siguiente manera:

5.4.1. Patrocinador: Proveerá los recursos necesarios para la ejecución del proyecto. Esta función será desempeñada por el Subsecretario General de la Presidencia de la República.[1]

5.4.2. Gerente de Proyecto: Gestionará los recursos necesarios para la implementación del Sistema de Gestión de Seguridad de la Información y realizará las coordinaciones con los gerentes para la adopción de las medidas aprobadas por el Comité. Esta función será desempeñada por la Oficial de Seguridad de la Información.

5.4.3. Equipo del Proyecto: ayudarán en diversos aspectos de la implementación del proyecto, realizar tareas preestablecidas y tomar decisiones sobre diversos temas que requieren un enfoque multidisciplinario. El equipo del proyecto se reúne antes de completar cada versión final de un documento oficial y en otros casos, cuando el gerente del proyecto lo considere necesario. Está conformado por dos comités:

- ***Comité de Gestión de Seguridad de la Información.***- *Conformado por integrantes de la Alta dirección, quienes aprobarán las medidas a adoptarse como parte de la implementación.*
- ***Comité de Operativo de Seguridad de la Información.***- *Está conformado por un representante de cada área que comprende el alcance del proyecto, coordinarán con la Oficial de Seguridad de la Información.*

5.5. Principales riesgos del Plan

La implementación de un Sistema de Gestión de Seguridad de la Información, es un proyecto que conlleva a un cambio en la cultura organizacional en todos los niveles de la institución.

Los principales riesgos en la implementación del proyecto son los siguientes:

i. Falta de respaldo de la Alta Dirección.
ii. Falta de definición de Procesos de la áreas comprendidas en el alcance.

[1] Art. 11° del ROF del Despacho Presidencial: La Subsecretario General de la Presidencia de la República es quien secunda la Secretaría General, cumpliendo las funciones de máxima autoridad administrativa de la entidad, teniendo a su cargo el enlace de los diversos órganos del Despacho Presidencial con el Titular del Pliego y asumiendo la supervisión de la gestión técnica, administrativa y financiera del Despacho Presidencial.

iii. Extensión de los plazos porque la Institución no cuente con los requisitos básicos para la implementación de la NTP-ISO/IEC 27001:2008 y haya que formularlos.
- Planes de gestión y desarrollo de las áreas involucradas
- Inventario de activos (Hardware, Software, Bases de datos y registros)
- Documentación de la configuración de equipos y software
- Documentación de procesos
- Manuales de Procedimientos
- Definición y asignación formal de responsabilidades de las personas que laboran.

iv. Falta de compromiso del personal del Despacho Presidencial con la Seguridad de la Información.

v. Falta de capacitación del personal implementador en gestión de procesos, entrega de servicios, desarrollo seguro, y seguridad informática.

vi. Ampliación de los plazos en los entregables

Algunas medidas para reducir los riesgos mencionados anteriormente son las siguientes:

i. Se formará un Comité de Seguridad de la Información de Alta Dirección y un Comité Operativo, para darle seguimiento oportuno a las actividades del proyecto.

ii. Contratación de una consultoría para realizar una evaluación y mejora de procesos

iii. Se formulará y llevará a cabo planes y campañas de sensibilización en el Despacho Presidencial.

iv. El gerente del proyecto supervisa que todas las actividades sean realizadas dentro de los plazos definidos y solicita a tiempo la intervención del patrocinador del proyecto.

5.6. Requisitos

5.6.1. Para el inicio de la Implementación del Proyecto

i. Identificación y mejora de Procesos, los cuales son la base para la implementación del Sistema de Gestión de Seguridad de la Información

ii. Auditoría informática especializada, para establecer el nivel actual de vulnerabilidades y deficiencias del sistema informático que permitan trazar medidas inmediatas de mitigación y un análisis GAP de la seguridad informática.

iii. Fortalecimiento de Capacidades de los participantes clave del proyecto en los siguientes temas:

TEMA	DESCRIPCIÓN	PERSONAL
ITIL Foundations	Metodología de gestión de entrega de servicios informáticos.	Dirección de Tecnología de la Información y Sistemas

5.6.2. Para la Implementación del Proyecto

i. Auditoría informática especializada, en intervalos de mínimo tres meses, para determinar vulnerabilidades o intrusos informáticos.

ii. Software de Gestión de Seguridad de la Información, que permitirá establecer indicadores de cumplimiento y de gestión.

iii. Fortalecimiento de Capacidades de los participantes clave del proyecto en los siguientes temas:

TEMA	DESCRIPCIÓN	PERSONAL
Programación segura	Técnicas de programación para evitar vulnerabilidades en software	Área de Desarrollo de Sistemas
Ethical Hacking	Técnicas de identificación de vulnerabilidades y amenazas en la red	Área de Redes
Gestión por Procesos	Técnicas de administración por procesos medibles.	Comité Operativo

6. GESTIÓN Y VALIDEZ DE REGISTROS Y DOCUMENTOS.

Se definirán procedimientos y codificaciones estándar para la aprobación de documentos de gestión, lineamientos y directivas como resultado de la implementación del proyecto.

El presente documento podrá ser actualizado por la Secretaría General del Despacho Presidencial

7. METODOLOGÍA

Para la implementación del Proyecto, se empleará la metodología PDCA (Plan–Do-Check–Act), también llamado ciclo de DEMING, que impulsa al mejoramiento continuo de procesos y consiste en los siguientes pasos:

i. Planear (PLAN): Reconocer una oportunidad y planee el cambio.
ii. Hacer (DO) :Probar el cambio.
iii. Revisar (CHECK): Revisar la prueba, analizar los resultados e identificar lo aprendido.
iv. Actuar (ACT):Tomar acción basada en lecciones aprendidas. Si el cambio fue exitoso, incorporar lo aprendido. De lo contrario, intentar un plan diferente.

ANEXO N° 1 : ACTIVIDADES Y ENTREGABLES

FASE/OBJETIVO	ACTIVIDADES PROGRAMADAS POR PCM	ENTREGABLES COMO PRODUCTO DE LAS ACTIVIDADES	Tiempo de la implementación si es IN HOUSE	Tiempo de la implementación si es tercerizada
FASE I **ORGANIZACIÓN** Desarrollar las actividades principales para la dirección e inicio de la implantación del SGSI.	▪ Obtener el apoyo institucional ▪ Determinar el alcance del Sistema de Gestión de Seguridad de la Información ▪ Determinar la declaración de Política de Seguridad de la Información y objetivos ▪ Desarrollar documentos necesarios para la Fase II ▪ Determinar criterios para la evaluación y aceptación de riesgos	1. Proyecto de implementación del Sistema de Gestión de Seguridad de la Información en el Despacho Presidencial 2. Conformación del Comité de Gestión de Seguridad de la Infor. – CGSI 3. Procedimiento para control de documentos y registros 4. Alcance del Sistema de Gestión de Seguridad de la Información 5. Declaración de la Política de seguridad de la información 6. Informe de Análisis de Brecha o GAP 7. Plan de Sensibilización de Seguridad de la Información 8. Políticas Generales de Seguridad de la Información 9. Informe a ONGEI 10. Procedimiento para identificación de requisitos	3 meses (60 días hábiles)	2 meses
FASE II **PLANIFICACIÓN** Desarrollar las actividades de planificación requeridas por la norma de manera metodológica y en concordancia con la política y objetivos del SGSI dentro del alcance del mismo.	▪ Realizar evaluación de Riesgos ▪ Conducir un análisis entre los riesgos identificados y las medidas correctivas existentes ▪ Desarrollar un plan de tratamiento de riesgos ▪ Desarrollar documentos necesarios para la Fase III ▪ Desarrolla la declaración de Aplicabilidad	1. Documentos de gestión 2. Asignación de formal de responsabilidades. 3. Definición de procesos críticos 4. Metodología de Gestión de Riesgos 5. Cuadro de evaluación de riesgos 6. Cuadro de tratamiento de riesgos 7. Declaración de aplicabilidad	4 meses (80 días hábiles)	2 meses
FASE III **DESPLIEGUE** Desplegar las actividades de implementación del Sistema de Gestión de Seguridad de la Información	▪ Elaborar el plan de trabajo priorizado ▪ Desarrollar documentos y registros necesarios ▪ Implementar los controles seleccionados	1. Inventario de Activos de Información 2. Evaluación de riesgos 3. Informe sobre evaluación de riesgos y tratamiento del riesgo 4. Elaboración de Políticas Específicas 5. Plan de tratamiento del riesgo 6. Ejecución del Plan de tratamiento del riesgo 7. Despliegue del Plan de Sensibilización en Seguridad de la Inform.	13 meses (270 días hábiles)	3 meses
FASE IV **REVISIÓN** Realizar actividades de revisión del SGSI evidenciando el cumplimiento de los requisitos de la norma.	▪ Monitorear el desempeño del SGSI ▪ Fortalecer la gestión de incidentes ▪ Desarrollar documentos y registros necesarios ▪ Desarrollar las actividades para evidenciar la mejora continua	1. Procedimiento para Auditoría interna 2. Plan de Auditoría interna 3. Procedimiento para acciones correctivas 4. Plan de pruebas 5. Procedimiento de Atención de incidentes	4 meses (80 días hábiles)	2 meses
FASE V **AUDITORIA** Auditar e implementar las mejoras y correcciones del SGSI a fin de cumplir con los requisitos de la norma.	▪ Auditar internamente el SGSI ▪ Implementar las acciones correctivas ▪ Implementar las acciones preventivas pertinentes ▪ Desarrollar, corregir y mejorar documentación nueva o existente.	1. Ejecución de Auditoría interna 2. Informe de Auditoría Interna 3. Plan de Acciones Correctivas 4. Plan de Acciones Preventivas 5. Seguimiento a las no conformidades	3 meses (60 días hábiles)	2 meses