Resolución Ministerial

N° 004-2016-PCM

Lima, - 8 ENE. 2016

CONSIDERANDO:

Que, mediante Resolución Ministerial N° 246-2007-PCM se aprobó el uso 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 del Sistema Nacional de Informática;

Que, mediante Resolución Ministerial N° 197-2011-PCM, se estableció el plazo para que determinadas entidades de la Administración Pública implementen el Plan de Seguridad de la Información dispuesto en la Norma Técnica Peruana antes señalada; posteriormente, mediante Resolución Ministerial N° 129-2012-PCM se estableció un nuevo cronograma y la incorporación del rol del oficial de seguridad para el proceso de implementación de la Norma Técnica Peruana "NTP-ISO /IEC 27001:2008;

Que, 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", aprobada mediante Resolución N° 42-2008/INDECOPI-CNB, por 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) ha sido reemplazada por la nueva versión de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos.2ª Edición" aprobada por Resolución N° 129-2014/DNB-INDECOPI;

Que, de acuerdo a lo establecido en el numeral 4.8 del artículo 4 y el artículo 49 del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por el Decreto Supremo N° 063-2007-PCM, la Presidencia del Consejo de Ministros actúa como ente rector del Sistema Nacional de Informática a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), siendo ésta la encargada de implementar la Política Nacional de Gobierno Electrónico e Informática;

Que, el "Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0" aprobado mediante Decreto Supremo N° 066-2011-PCM, establece en su Objetivo N° 7, la necesidad de promover una Administración Pública de calidad orientada a la población, determinando como parte de su Estrategia N° 4, la implementación de mecanismos para mejorar la seguridad de la información, la necesidad de contar con una Estrategia Nacional de Ciberseguridad con el objetivo de minimizar los riesgos en caso de sufrir algún tipo de incidente en los recursos informáticos del Estado, así como, la disuasión del crimen cibernético, que se producen mediante el uso de redes teleinformáticas, entre otros;

Que, la actual Política Nacional de Gobierno Electrónico 2013 – 2017, aprobada mediante el Decreto Supremo N° 081-2013-PCM, prevé determinados Lineamientos

Estratégicos para el Gobierno Electrónico en el Perú, entre otros, el relacionado con la Seguridad de la Información, el mismo que busca velar por la integridad, seguridad y disponibilidad de los datos debiendo establecerse lineamientos de seguridad de la información a fin de mitigar el riesgo de exposición de información sensible del ciudadano, correspondiendo que en uso de las funciones atribuidas al ente rector del Sistema Nacional de Informática, para el caso ONGEI-PCM, a cargo de implementar dicha Política Nacional, articular la implementación efectiva del acotado lineamiento por parte de los distintos entes del sector público;

Que, estando a lo indicado en los considerando precedentes la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros a través del Memorando Nº 152-2015-PCM/ONGEI, recomienda la aplicación y uso de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades del Sistema Nacional de Informática, con la finalidad de coadyuvar con la infraestructura de Gobierno Electrónico, por considerar a la seguridad de la información, como un componente crucial para dicho objetivo;

De conformidad con lo dispuesto en la Ley Nº 29158, Ley Orgánica del Poder Ejecutivo; la Ley Nº 27658, Ley Marco de Modernización de la Gestión del Estado; y, el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros aprobado mediante Decreto Supremo Nº 063-2007-PCM y sus modificatorias;

SE RESUELVE:

Artículo 1.- De la aprobación

Apruébese el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

Artículo 2.- Publicación

La Norma Técnica Peruana NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición" será publicada en el Portal de la Presidencia del Consejo de Ministros (www.pcm.gob.pe) y en el Portal de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) (www.ongei.gob.pe) el mismo día de la publicación de la presente resolución en el Diario Oficial El Peruano.

Artículo 3.- De la implementación

Las entidades integrantes del Sistema Nacional de Informática, tendrán un plazo máximo de dos (2) años para la implementación y/o adecuación de la presente norma.

Dichas entidades públicas tendrán un plazo de 60 días contados a partir de la fecha de publicación de la presente norma, para la presentación del cronograma de

Resolución Ministerial

implementación y/o adecuación del sistema de gestión de la Seguridad de la Información, que deberá ser presentado a la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros.

La ONGEI brindará asistencia técnica a las entidades que lo requieran. Las entidades públicas que a la fecha cuenten con la certificación ISO 27001, están exoneradas del presente proceso de implementación.

Artículo 4.- De la certificación de la norma

Las entidades que requieran certificarse de acuerdo a lo establecido en la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2 Edición"; podrán realizar dicha certificación de forma opcional y con recursos propios de cada entidad.

Artículo 5.- Del Comité de Gestión de Seguridad de la Información

Cada entidad designará un Comité de Gestión de Seguridad de la Información, conformado por:

- El/la titular de la entidad;
- El/la responsable de administración o quien haga sus veces;
- El/la responsable de planificación o quien haga sus veces;
- El/la responsable del área de informática o quien haga sus veces;
- El/la responsable de área legal o quien haga sus veces y
- El/la oficial de seguridad de la información.

Las funciones del Comité de Gestión de Seguridad de la Información, serán establecidas por cada entidad de acuerdo a la norma que se aprueba mediante el Artículo 1° de la presente Resolución Ministerial.

Artículo 6.- De la responsabilidad de la implementación

La responsabilidad de la implementación de la presente norma será del titular de cada entidad.

Artículo 7.- Déjese sin efecto

Deróguese la Resolución Ministerial N° 129-2012-PCM.

Regístrese, comuníquese y publíquese

PEDRO CATERIANO BELLIDO
Presidente del Consejo de Ministros

USO DE LA NTP ISO/IEC 27001:2014 EN LAS ENTIDADES INTEGRANTES DEL SISTEMA NACIONAL DE INFORMATICA

2015

Contenido

INTRODUCCION

ISO (la Organización Internacional para la Normalización) e IEC (la Comisión Electrotécnica Internacional) forman el sistema especializado para la normalización mundial. Los órganos nacionales que son miembros de ISO o de IEC participan en el desarrollo de las Normas Internacionales a través de comités técnicos establecidos por la respectiva organización para ocuparse de campos particulares de actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en enlace con ISO y con IEC, también participan en el trabajo. En el campo de la tecnología de la información, ISO e IEC han establecido un comité técnico conjunto, ISO/IEC JTC 1.

Se redactan las Normas Internacionales en concordancia con las reglas proporcionadas en las Directivas ISO/IEC, Parte 2.La tarea principal del comité técnico conjunto es preparar los proyectos de normas internacionales adoptadas por el comité técnico conjunto, se circulan a los órganos nacionales para su votación. La publicación como una Norma Internacional requiere la aprobación de al menos 75% de los órganos nacionales que emiten un voto.

Se señala la posibilidad de que alguno de los elementos de este documento pueda estar sujeto a derechos de patentes. No se hará responsable a ISO e IEC de identificar cualquiera o todos los mencionados derechos de patentes.

ISO/IEC 27001 fue preparada por el Comité Técnico conjunto ISO/IEC JTC 1, Tecnología de la información, Sub-comité SC 27, Técnicas de seguridad de la TI.

La nueva norma NTP ISO/IEC 27001:2014 cancela y reemplaza la primera edición (NTP-ISO/IEC 27001:2008), la cual se ha revisado técnicamente.

PARTE I Norma NTP ISO/IEC 27001:2014

1.-OBJETO Y CAMPO DE APLICACIÓN

Este Proyecto de Norma Técnica Peruana especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización. Este Proyecto de Norma Técnica Peruana también incluye requisitos para la evaluación y tratamiento de los riesgos de seguridad de la información orientados a las necesidades de la organización. Los requisitos establecidos en este Proyecto de Norma Técnica Peruana son genéricos y están hechos para aplicarse a todas las organizaciones, sin importar su tipo, tamaño o naturaleza. Excluir cualquiera de los requisitos especificados en las Cláusulas 4 a 10 no es aceptable cuando una organización declara conformidad con este Proyecto de Norma Técnica Peruana.

2.- REFERENCIAS NORMATIVAS

Los siguientes documentos, en parte o en su totalidad, se referencian normativamente en este documento y son indispensables para su aplicación. Para referencias fechadas sólo se aplica la edición citada. Para referencias no fechadas se aplica la edición más reciente del documento referenciado (incluida cualquier enmienda).

ISO/IEC 27000, Information Technology. Security Technology Techniques. Information Security Management Systems. Overview and Vocabulary

3.- TÉRMINOS Y DEFINICIONES

Para propósitos de este documento, se aplican los términos y definiciones proporcionados en ISO/IEC 27000.

4.- CONTEXTO DE LA ORGANIZACION

4.1 Comprender la organización y su contexto

La organización debe determinar los aspectos externos e internos que son relevantes para este propósito y que afectan su capacidad de lograr el(los) resultado(s) deseados de este sistema de gestión de seguridad de la información.

> NOTA Determinar estos aspectos se refiere a establecer el contexto externo e interno de la organización considerado en la Cláusula 5.3 de ISO 31000:2009[].

4.2 Comprender las necesidades y expectativas de las partes interesadas

La organización debe determinar:

a) las partes interesadas relevantes al sistema de gestión de seguridad de la información; y

b) los requisitos de estas partes interesadas relevantes a la seguridad de la información.

NOTA los requisitos de las partes interesadas pueden incluir requisitos legales, regulatorios y obligaciones contractuales.

4.3 Determinar el alcance del sistema de gestión de seguridad de la información

La organización debe determinar los límites y la aplicabilidad del sistema de gestión de seguridad de la información para establecer su alcance.

Cuando se determina este alcance la organización debe considerar:

a) los aspectos externos e internos referidos en 4.1;

b) los requisitos referidos en 4.2; y

c) las interfaces y dependencias entre actividades realizadas por la organización y las que son realizadas por otras organizaciones.

El alcance debe estar disponible como información documentada.

4.4 Sistema de gestión de seguridad de la información

La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, en conformidad con los requisitos de este Proyecto de Norma Técnica Peruana.

5.- LIDERAZGO

5.1 Liderazgo y compromiso

La alta dirección debe demostrar liderazgo y compromiso respecto del sistema de gestión de seguridad de la información:

a) asegurando que la política de seguridad de la información y los objetivos de seguridad de la información son establecidos y compatibles con la dirección estratégica de la organización;

b) asegurando la integración de los requisitos del sistema de gestión de seguridad de la información en los procesos de la organización;

c) asegurando que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles;

d) comunicando la importancia de una efectiva gestión de seguridad de la información y en conformidad con los requisitos del sistema de gestión de seguridad de la información;

e) asegurando que el sistema de gestión de seguridad de la información logre su(s) resultado(s) previsto(s);

f) dirigiendo y apoyando a las personas para que contribuyan con la efectividad del sistema de gestión de seguridad de la información;

g) promoviendo la mejora continua; y

h) apoyando a otros roles relevantes de gestión para demostrar su liderazgo tal como se aplica a sus áreas de responsabilidad.

5.2 Política

La alta dirección debe establecer una política de seguridad de la información que:

a) es apropiada al propósito de la organización;

b) incluye objetivos de seguridad de la información (ver 6.2) o proporciona el marco de referencia para fijar los objetivos de seguridad de la información;

c) incluye un compromiso de satisfacer requisitos aplicables relacionados a la seguridad de la información; e

d) incluye un compromiso de mejora continua del sistema de gestión de seguridad de la información.

La política de seguridad de la información debe:

e) estar disponible como información documentada;

f) estar comunicada dentro de la organización; y

g) estar disponible a las partes interesadas, según sea apropiado.

5.3 Roles, autoridad y responsabilidades organizacionales

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

La alta dirección debe asignar la responsabilidad y la autoridad para:

a) asegurar que el sistema de gestión de seguridad de la información esté conforme a los requisitos de este Proyecto de Norma Técnica Peruana; y

b) reportar sobre el desempeño del sistema de gestión de seguridad de la información a la alta dirección.

NOTA la alta dirección también puede asignar responsabilidades y la autoridad para reportar desempeño del sistema de gestión de seguridad de la información dentro de la organización.

6.- PLANIFICACIÓN

6.1 Acciones para tratar los riesgos y las oportunidades

6.1.1 Generalidades

Cuando se planifica para el sistema de gestión de seguridad de la información, la organización debe considerar los asuntos referidos en el numeral 4.1 y los requisitos referidos en el numeral 4.2 y determinar los riesgos y oportunidades que necesitan ser tratados para:

a) asegurar que el sistema de gestión de seguridad de la información pueda lograr su(s) resultado(s) esperado(s);

b) prevenir, o reducir, efectos indeseados; y
c) lograr la mejora

continua. La organización

debe planificar:

d) acciones que traten estos riesgos y oportunidades; y

e) como

1) integrar e implementar estas acciones en sus procesos del sistema de gestión de seguridad de la información; y

2) evaluar la efectividad de estas acciones.

6.1.2 Valoración del riesgo de seguridad de la información

La organización debe definir y aplicar un proceso de valoración del riesgo de seguridad de la información que:

a) establezca y mantenga criterios de riesgo de seguridad de la información que incluyan;

1) los criterios de aceptación de los riesgos; y

2) los criterios para realizar valoraciones de riesgo de seguridad de la información;

b) asegure que las valoraciones repetidas de riesgos de seguridad de la información produzcan resultados consistentes, válidos y comparables;

c) identifique los riesgos de seguridad de la información

1) aplicando el proceso de valoración de riesgos de seguridad de la información para identificar riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad para la información dentro del alcance del sistema de gestión de seguridad de la información; e

2) identificando a los propietarios de riesgos;

d) analice los riesgos de seguridad de la información:

1) valorando las consecuencias potenciales que resultarían si los riesgos identificados en 6.1.2 c) 1) fueran a materializarse;

2) valorando la probabilidad realista de la ocurrencia de los riesgos identificados en 6.1.2 c) 1); y

3) determinando los niveles de riesgo;

e) evalúe los riesgos de seguridad de la información:

1) comparando los resultados del análisis de riesgo con los criterios de riesgo establecidos en 6.1.2 a); y

2) priorizando los riesgos analizados para el tratamiento de riesgos.

La organización debe retener información documentada sobre el proceso de valoración de riesgos de seguridad de la información.

6.1.3 Tratamiento de riesgos de seguridad de la información

La organización debe definir y aplicar un proceso de tratamiento de riesgos de seguridad de la información para:

a) seleccionar opciones de tratamiento de riesgos de seguridad de la información apropiadas, tomando en cuenta los resultados de la valoración de riesgos;

b) determinar todos los controles que son necesarios para implementar la(s) opción(es) elegida(s) de tratamiento de riesgos de seguridad de la información;

NOTA Las organizaciones pueden diseñar controles según se requiera, o identificarlos de cualquier fuente.

c) Comparar los controles determinados en 6.1.3 b) con aquellos del Anexo A y verificar que no se ha omitido ningún control necesario;

NOTA 1 El Anexo A contiene una lista integral de objetivos de control y controles. Los usuarios de este Proyecto de Norma Técnica Peruana pueden dirigirse al Anexo A para asegurar que no se deje de lado ningún control necesario.

NOTA 2 Los objetivos de control están incluidos implícitamente en los controles escogidos. Los objetivos de control y los controles listados en el Anexo A no son exhaustivos y pueden ser necesarios objetivos de control y controles adicionales.

d) producir una Declaración de Aplicabilidad que contenga los controles necesarios (ver 6.1.3 b) y c)) y la justificación de las inclusiones ya sea que se implementen o no, así como la justificación de excluir controles del Anexo A;

e) formular un plan de tratamiento de riesgos de seguridad de la información; y

f) obtener la aprobación, por parte de los propietarios de riesgos, del plan de tratamiento de riesgos de la seguridad de la información y la aceptación de los riesgos residuales de la seguridad de la información.

La organización debe retener información documentada sobre el proceso de tratamiento de riesgos de seguridad de la información.

NOTA El proceso de valoración y tratamiento de riesgos de seguridad de la información en este Proyecto de Norma Técnica Peruana se alinea con los principios y lineamientos genéricos proporcionados en ISO 31000

6.2 Objetivos de seguridad de la información y planificación para conseguirlos

La organización debe establecer objetivos de seguridad de la información a niveles y funciones relevantes.

Los objetivos de seguridad de la información deben:

a) ser consistentes con la política de seguridad de la información;

b) ser medibles (si es práctico);

c) tomar en cuenta requisitos aplicables de seguridad de la información y resultados de la valoración y tratamiento de riesgos;

d) ser comunicados; y

e) ser actualizados según sea apropiado.

La organización debe retener información documentada sobre los objetivos de seguridad de la información.

Cuando planifique cómo lograr sus objetivos de seguridad de la información, la organización debe determinar:

f) qué se hará;

g) qué recursos serán requeridos;

h) quién será responsable;

i) cuándo se culminará;

j) cómo los resultados serán evaluados.

7.- SOPORTE

7.1 Recursos

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información.

7.2 Competencia

La organización debe:

a) Determinar la competencia necesaria de la(s) persona(s) que trabajan bajo su control que afecta su desempeño en seguridad de la información;

b) Asegurar que estas personas son competentes sobre la base de educación, capacitación, o experiencia adecuados;

c) Cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la efectividad de las acciones tomadas; y

d) Retener información documentada apropiada como evidencia de competencia.

NOTA Las acciones aplicables pueden incluir, por ejemplo: la provisión de capacitación a, mentoría a, o reasignación de los actuales empleados; o la contratación de personas competentes.

7.3 Concientización

Las personas que trabajan bajo el control de la organización deben ser conscientes de:

a) la política de seguridad de información;

b) su contribución a la efectividad del sistema de gestión de seguridad de la información, incluyendo los beneficios de un mejor desempeño de la seguridad de la información; y

c) las implicancias de no tener conformidad con los requisitos del sistema de gestión de seguridad de la información.

7.4 Comunicación

La organización debe determinar la necesidad de comunicaciones internas y externas relevantes al sistema de gestión de seguridad de la información incluyendo:

a) qué comunicar;

b) cuándo comunicar;

c) a quién comunicar;

d) quién debe comunicar; y

e) los procesos por los cuales la comunicación debe ser efectuada.

7.5 Información documentada

7.5.1 Generalidades

El sistema de gestión de seguridad de la información de la organización debe incluir:

a) información documentada requerida por este Proyecto de Norma Técnica Peruana; e

b) información documentada determinada por la organización como necesaria para la efectividad del sistema de gestión de seguridad de la información.

NOTA La extensión de la información documentada para un sistema de gestión de seguridad de la información puede diferir de una organización a otra debido a:

1) el tamaño de la organización y su tipo de actividades, procesos, productos y servicios;

2) la complejidad de los procesos y sus interacciones; y

3) la competencia de las personas.

7.5.2 Creación y actualización

Cuando se crea y actualiza información documentada, la organización debe asegurar:

a) identificación y descripción apropiados (por ejemplo, un título, fecha, autor, o número de referencia);

b) formato (por ejemplo el lenguaje, versión de software, gráficos) y medios (por ejemplo papel, electrónico) apropiados; y

c) revisión y aprobación apropiadas para su conveniencia y adecuación.

7.5.3 Información documentada

La información documentada requerida por el sistema de gestión de seguridad de la información y por este Proyecto de Norma Técnica Peruana se debe controlar para asegurar:

a) que esté disponible y sea conveniente para su uso donde y cuando sea necesaria; y

b) que esté protegida adecuadamente (por ejemplo de pérdida de confidencialidad, uso impropio, o pérdida de integridad).

Para el control de la información documentada, la organización debe realizar las siguientes actividades, según sea aplicable:

c) distribución, acceso, búsqueda y uso;

d) almacenamiento y preservación, incluyendo la preservación de legibilidad;

e) control de cambios (por ejemplo control de versiones); y

f) retención y disposición.

La información documentada de origen externo, determinada por la organización como necesaria para la planificación y operación del sistema de gestión de seguridad de la información, debe ser identificada según sea apropiado y controlarse.

NOTA El acceso implica una decisión respecto de la autorización de solamente ver la información documentada, o el permiso y la autoridad de ver y cambiar la información documentada, etc.

8.- OPERACION

8.1 Planificación y control operacional

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información e implementar las acciones determinadas en 6.1. La organización debe también implementar planes para lograr los objetivos de seguridad de la información determinados en 6.2.

La organización debe mantener información documentada en la medida necesaria para estar segura de que los procesos se han llevado a cabo tal como fueron planificados.

La organización debe controlar los cambios planeados y revisará las consecuencias de cambios no intencionados, actuando para mitigar cualquier efecto adverso, según sea necesario.

La organización debe asegurar que los procesos tercerizados son determinados y controlados.

8.2 Evaluación de riesgos de seguridad de la información

La organización debe realizar evaluaciones de riesgos de seguridad de la información en intervalos planificados o cuando cambios significativos se propongan u ocurran, tomando en cuenta los criterios establecidos en 6.1.2 a).

La organización debe retener información documentada de los resultados de las evaluaciones de riesgos de seguridad de la información.

8.3 Tratamiento de riesgos de seguridad de la información

La organización debe implementar el plan de tratamiento de riesgos de seguridad de la información.

La organización debe retener información documentada de los resultados del tratamiento de riesgos de seguridad de la información.

9.- EVALUACION DEL DESEMPEÑO

9.1 Monitoreo, medición, análisis y evaluación

La organización debe evaluar el desempeño de la seguridad de la información y la efectividad del sistema de gestión de seguridad de la información.

La organización debe determinar:

a) qué necesita ser monitoreado y medido, incluyendo procesos y controles de seguridad de la información;

b) los métodos para monitoreo, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos;

NOTA Los métodos seleccionados deberían producir resultados comparables y reproducibles para ser considerados válidos.

c) cuándo el monitoreo y medición debe ser realizado;

d) quién debe monitorear y medir;

e) cuándo los resultados del monitoreo y medición deben ser analizados y evaluados; y

f) quién debe analizar y evaluar estos resultados.

La organización debe retener información documentada apropiada como evidencia del monitoreo y los resultados de la medición.

9.2 Auditoría interna

La organización debe conducir auditorías internas en intervalos planificados para proporcionar información sobre si el sistema de gestión de seguridad de la información:

a) está en conformidad con

1) los requisitos de la propia organización para su sistema de gestión de seguridad de la información; y

2) los requisitos de este Proyecto de Norma Técnica Peruana;

b) está efectivamente implementado y mantenido.

La organización debe:

c) planificar, establecer, implementar y mantener uno o varios programas de auditoría, incluyendo la frecuencia, métodos, responsabilidades, requisitos e informes de planificación. Los programas de auditoría deben tomar en consideración la importancia de los procesos concernientes y los resultados de auditorías previas;

d) definir los criterios y el alcance de cada auditoría;

e) seleccionar a los auditores y conducir auditorías que aseguren objetividad e imparcialidad del proceso de auditoría;

f) asegurar que los resultados de las auditorías se reporten a los gerentes relevantes; y

g) retener información documentada como evidencia del (de los) programa(s) de auditoría y los resultados de la auditoría.

9.3 Revisión por la gerencia

La alta dirección debe revisar el sistema de gestión de seguridad de la información de la organización a intervalos planificados para asegurar su conveniencia, adecuación y efectividad continua.

La revisión por la gerencia debe incluir consideraciones de:

a) el estado de las acciones con relación a las revisiones anteriores por parte de la gerencia;

b) cambios en asuntos externos e internos que son relevantes al sistema de gestión de seguridad de la información;

c) retroalimentación sobre el desempeño de seguridad de la información, incluyendo tendencias en:

   1) no conformidades y acciones correctivas;

   2) resultados del monitoreo y medición;

   3) resultados de auditoría; y

   4) cumplimiento de los objetivos de seguridad de la información;

d) retroalimentación de partes interesadas;

e) resultados de la evaluación de riesgo y estado del plan de tratamiento de riesgos; y oportunidades para la mejora continua.

Los productos de la revisión por la gerencia deben incluir decisiones relacionadas a oportunidades de mejora continua y cualquier necesidad de cambios al sistema de gestión de seguridad de la información.

La organización debe retener información documentada como evidencia de los resultados de revisiones por parte de la gerencia.

10.- Mejoras

10.1 No conformidades y acción correctiva

Cuando ocurre una no conformidad, la organización debe:

a) reaccionar a la no conformidad y, según sea aplicable:

   1) tomar acción para controlarla y corregirla; y

   2) ocuparse de las consecuencias;

b) evaluar la necesidad de la acción para eliminar las causas de la no conformidad con el fin de que no recurra u ocurra en otro lugar de las

siguientes maneras:

1) revisando la no conformidad;

2) determinando las causas de la no conformidad; y

3) determinando si existen no conformidades similares o si podrían ocurrir potencialmente;

c) implementar cualquier acción necesaria;

d) revisar la efectividad de cualquier acción correctiva tomada; y.

e) hacer cambios al sistema de gestión de seguridad de la información, si fuera necesario.

Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas.

La organización debe retener información documentada como evidencia de:

f) la naturaleza de las no conformidades y cualquier acción subsiguiente tomada; y

g) los resultados de cualquier acción correctiva.

10.2 MEJORA CONTINUA

La organización debe mejorar continuamente la conveniencia, adecuación y efectividad del sistema de gestión de seguridad de la información

PARTE 2 INFORME TÉCNICO

1.- ANTECEDENTES

Resolución Ministerial Nº 246-2007-PCM, mediante la cual 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. 2da. Edición" en todas las entidades integrantes del Sistema Nacional de Informática".

"NTP ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos." Aprobada mediante Resolución Nº 42-2008/INDECOPI-CNB del 11 de Enero de 2009, por 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).

Resolución Ministerial Nº 197-2011-PCM, mediante la cual establecen fecha límite para que las diversas entidades de la Administración Pública implementen el plan de seguridad de la información dispuesto en la NTP ISO/IEC17799:2007EDI.Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información.

Resolución Ministerial Nº 129-2012-PCM, mediante la cual se aprueba el uso obligatorio de la Norma Técnica Perùana "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.

2.- BASE LEGAL

- Constitución Política del Perú.
- Ley Nº 29158 - Ley Orgánica del Poder Ejecutivo.
- Ley Nº 27658 - Ley Marco de Modernización de la Gestión del Estado.
- Decreto Supremo 063-2007-PCM, y sus modificatorias, que aprueba el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros.
- Resolución Ministerial Nº 274-2006-PCM, que aprueba la Estrategia Nacional de Gobierno Electrónico.
- Resolución Ministerial Nº 246-2007-PCM, mediante la cual 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. 2da. Edición" en todas las entidades integrantes del Sistema Nacional
- Resolución Ministerial Nº 197-2011-PCM, mediante la cual establecen fecha límite para que las diversas entidades de la Administración Pública implementen el plan de seguridad de la información dispuesto en la NTP ISO/IEC17799:2007EDI.Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información.
- Resolución Ministerial Nº 129-2012-PCM, mediante la cual 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.

3.- ANALISIS

La Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros (PCM), tiene entre sus funciones, de acuerdo a lo dispuesto en su Reglamento de Organización y Funciones, aprobado mediante Decreto Supremo Nº 063-2007-PCM, dirigir como ente rector, el Sistema Nacional de Informática, y de implementar la Política Nacional de Gobierno Electrónico e Informática.

Coordinadamente, mediante Resolución Ministerial Nº 274-2006-PCM, se aprobó la Estrategia Nacional de Gobierno Electrónico, la misma que tiene entre sus objetivos, la emisión de normatividad, que sobre la integración funcional entre instituciones públicas, permita la definición de compromisos y responsabilidades asociadas a mejores prácticas referidas a procesos de innovación, rediseño de procesos y mejora de calidad en los servicios, con el objetivo, entre otros, de salvaguardar la seguridad de la información, relacionada a esos servicios públicos.

Para el desarrollo del Gobierno Electrónico en el Perú, se han definido un conjunto de políticas sobre las que se implementan acciones para el logro de la estrategia desarrollada. Estas políticas son de aplicación dentro de lo que constituye la Ley Marco de Modernización de la Gestión del Estado, Ley 27658, las mismas que se enmarcan dentro de los alcances de las Políticas del Acuerdo Nacional.

De otro lado, la Ley Nº 29158, Ley Orgánica del Poder Ejecutivo, establece que las entidades deben asegurar que sus actividades se realicen, entre otros, con arreglo a la eficacia, eficiencia, continuidad, y celeridad de la gestión.

Es así 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. Sin embargo se observa que desde la

publicación de la norma mencionada, existen entidades que no han implementado las medidas de seguridad de la información establecidas; más aún para poder implementarlas adecuadamente, se requiere adoptar una política clara, un esquema de certificación internacional, que defina procesos, y que permita establecer un sistema de gestión de seguridad de la información.

En el orden de ideas de la nueva norma se requiere desarrollar una política de gestión, evaluación de riesgos y el tratamiento de los mismo conformando esto el modelo a implementar. Establecidos los riesgos y su tratamiento, se establece con claridad la declaración de aplicabilidad. Por lo que es necesario aprobar mediante norma, la nueva versión 2014 de la ISO 27001 e implementar como parte de nuestra legislación los controles y/o los objetivos de control, y posteriormente definir en cada caso, su aplicabilidad y el por que.

De otro lado, siendo que a la fecha ya se encuentra publicada la nueva versión de la norma es decir la NTP-ISO/IEC 27001:2014, se recomienda la derogación de la Resolución Ministerial Nº 129-2012-PCM, toda vez que esta apunta a la versión anterior es decir la NTP-ISO/IEC 27001:2008

Finalmente, a fin de desarrollar una implementación progresiva coordinada y eficiente, se adjuntan se presentara un cronograma de Implementación acompañado de una pequeña guía metodológica Incremental de la NTP-ISO/IEC 27001:2014, con plazos máximos de cumplimiento por cada fase, pudiendo las entidades realizarlos en menor tiempo, según los avances previamente realizados. Dicho cronograma será publicado en el Portal de la ONGEI y de PeCERT.

4.- CONCLUSIONES

La propuesta de norma mediante la cual se establece el uso obligatorio por parte de las entidades de la Administración Pública de la "NTP ISO/IEC 27001:20014 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos", permitirá establecer en cada entidad pública, un sistema de gestión de seguridad de la información que permita conocer y manejar los riesgos asociados a los activos der información.

La implementación de la norma propuesta permitirá garantizar el adecuado tratamiento de la información, elevando la calidad en los procesos internos/externos y los servicios públicos que brinden las entidades del Estado.

La implementación de la norma propuesta apoyará los esfuerzos que se vienen realizando a través de la Coordinadora de Emergencia de Redes Teleinformáticas (PeCERT) y en los CSIRT, de cada entidad pública, manteniendo una red de información de prevención en temas de seguridad, al estar incorporada como uno de los hitos de control en la NTP ISO/IEC 27001:2014 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos".

El presente proyecto se encuentra enmarcado dentro de los objetivos y estrategias de la Agenda Digital 2.0 aprobada mediante RM 066-2011-PCM, en lo que respecta a la implementación de servicios públicos por medios electrónicos seguros, así como con lo establecido en la Estrategia Nacional de Gobierno Electrónico e Informática, aprobado mediante Resolución Ministerial Nº 274-2006-PCM.

A fin de lograr el éxito en la implementación de la NTP- ISO/IEC 27001:2014, se ha establecido un cronograma de implementación apoyado en una

metodología de implementación, el cual se adjunta al presente, y que será publicado en el Portal de ONGEI.

Es necesaria la derogatoria de la Resolución Ministerial Nº Resolución Ministerial Nº 129-2012-PCM, mediante la cual 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.

Finalmente, se adjunta el proyecto de Resolución Ministerial para su etapa de discusión y modificaciones por parte de la OGAJ y ONGEI de PCM.

5.- RECOMENDACIONES

Por las razones expuestas se recomienda la aprobación del proyecto de norma, mediante el cual se aprueba el uso de la "NTP ISO/IEC 27001:2014 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos", y la derogación de la Resolución Ministerial Nº 129-2012-PCM, procediendo con su tramitación y publicación en el Diario Oficial "El Peruano" a la brevedad.

PRESIDENCIA DEL CONSEJO DE MINISTROS
Caballero