DGPIP

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es
"COPIA FIEL DEL ORIGINAL"
que he tenido a la vista
03 MAR. 2014
Lic. JUAN RAÚL LÓPEZ TORRES
FEDATARIO

REPUBLICA DEL PERU

Resolución Ministerial

No. 081-2014-EF/44

Lima, 28 de febrero de 2014

CONSIDERANDO:

Que, mediante Resolución Ministerial Nº 246-2007-PCM, se aprobó 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, con la finalidad de establecer un modelo integral para el desarrollo de los planes de seguridad de la información en la Administración Pública;

Que, la referida Norma Técnica Peruana señala que la Política de Seguridad de Información, tiene como objeto dirigir y dar soporte a la gestión de seguridad de la información en concordancia con los requerimientos de la institución, las leyes y las regulaciones, correspondiendo a la Alta Dirección establecer las líneas de la política de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo una Política de Seguridad en toda la organización;

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, cuyo control deberá ser implementado de acuerdo a las recomendaciones de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información";

Que, mediante Resolución Ministerial N° 649-2012-EF/10 se conformó el Grupo de Trabajo denominado "Comité de Gestión de Seguridad de la Información", como instancia administrativa responsable de dirigir, coordinar y revisar la puesta en práctica de la seguridad de la información en el Ministerio de Economía y Finanzas; teniendo como una de sus funciones, proponer políticas y normatividad de seguridad de la información para su aprobación;

Que, en tal sentido, dicho Grupo de Trabajo ha formulado la "*Política de Seguridad de la Información del Ministerio de Economía y Finanzas*", que tiene por objetivo establecer el marco general de gestión para proteger adecuadamente la

040918
032973

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es
"COPIA FIEL DEL ORIGINAL"
que he tenido a la vista

03 MAR. 2014

Lic. JUAN RAÚL LÓPEZ TORRES
FEDATARIO

información y que define un conjunto de principios, lineamientos y responsabilidades para tal propósito;

De conformidad con lo dispuesto en la Ley Nº 29158, Ley Orgánica del Poder Ejecutivo y el Reglamento de Organización y Funciones del Ministerio de Economía y Finanzas, aprobado con Resolución Ministerial Nº 223-2011-EF/43 y sus modificatorias;

SE RESUELVE:

Artículo 1.- Aprobar el documento de gestión interna denominado: "*Política de Seguridad de la Información del Ministerio de Economía y Finanzas*", cuyo texto se presenta en anexo adjunto y que forma parte integrante de la presente Resolución.

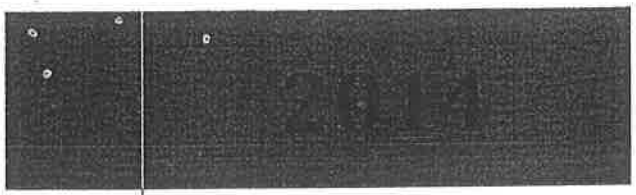
Artículo 2.- Disponer que lo establecido en la "*Política de Seguridad de la Información del Ministerio de Economía y Finanzas*", a que se refiere el artículo precedente, es de cumplimiento obligatorio por los funcionarios y servidores del Ministerio de Economía y Finanzas.

Artículo 3.- Disponer la publicación de la presente Resolución y su Anexo, en el portal institucional del Ministerio de Economía y Finanzas (www.mef.gob.pe) y en el Portal de Transparencia.

Regístrese y comuníquese.

LUIS MIGUEL CASTILLA RUBIO
Ministro de Economía y Finanzas

9



Ministerio de Economía y Finanzas

Oficina General de Tecnologías de la Información

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es
"COPIA FIEL DEL ORIGINAL"
que he tenido a la vista

03 MAR. 2014

Lic. JUAN RAÚL LÓPEZ TORRES
FEDATARIO

Política de Seguridad de la Información del Ministerio de Economía y Finanzas

V. S.

MINISTERIO DE ECONOMÍA Y FINANZAS
SECRETARÍA GENERAL

99

PERÚ | Ministerio de Economía y Finanzas

MINISTERIO DE ECONOMÍA Y FINANZAS
Secretaría General
El presente documento es
"COPIA FIEL DEL ORIGINAL"
que he tenido a la vista
03 MAR. 2014
Lic. JUAN RAÚL LÓPEZ TORRES
FEDATARIO

INDICE

V.S.

MINISTERIO DE ECONOMÍA Y FINANZAS
SECRETARÍA GENERAL

99

1. Declaración

El Ministerio de Economía y Finanzas reconoce que la información generada, procesada o administrada en el ejercicio de sus funciones constituye un recurso de valiosa importancia para el eficaz desempeño institucional, siendo necesario resguardar y proteger dicha información así como los diversos medios físicos y electrónicos de soporte, almacenamiento, tratamiento, transporte y transmisión, de modo que se garantice el normal desarrollo de las labores del Ministerio.

Se declara de absoluta relevancia la seguridad de la información en el quehacer diario del Ministerio, por medio de la cual se preservan la confidencialidad, la integridad y la disponibilidad de los activos críticos de información en niveles adecuados que aseguren la prosecución confiable de las operaciones, contribuyendo así al efectivo cumplimiento de la misión y objetivos estratégicos institucionales.

El Ministerio de Economía y Finanzas debe conducir un Sistema de Gestión de Seguridad de la Información bajo un esquema de evaluación de los riesgos pertinentes y de permanente adaptación a los cambios en las necesidades y objetivos institucionales, los requisitos de seguridad identificados, los procesos empleados y el tamaño y estructura organizacional del Ministerio, con el fin de establecer, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información en concordancia con las recomendaciones contenidas en normas técnicas peruanas, estándares internacionales y mejores prácticas de la industria en seguridad de la información que sean pertinentes.

2. Objetivo

La presente ***Política de Seguridad de la Información del Ministerio de Economía y Finanzas*** tiene como objetivo establecer el marco general de gestión para proteger adecuadamente la información del Ministerio, definiendo las directrices generales de actuación que aseguren el tratamiento adecuado de los riesgos y que conduzcan al fortalecimiento de una cultura en seguridad de la información.

3. Alcance

La presente Política de Seguridad de la Información y las disposiciones emanadas en el marco de la misma son de cumplimiento obligatorio por parte de todo el personal del Ministerio de Economía y Finanzas (MEF), sin distingo de régimen laboral o contractual o de nivel jerárquico, al que en adelante se denominará "trabajador del MEF", así como de las personas naturales o jurídicas que prestan servicios en general, en adelante "terceros", que tengan acceso a la información del MEF.

4. Base legal

a) Ley Nº 27806, Ley de Transparencia y Acceso a la Información Pública, del 03 de agosto de 2002.

b) Ley Nº 27927, Ley que modifica la Ley 27806, Ley de Transparencia y Acceso a la Información Pública, del 04 febrero de 2003.

MINISTERIO DE ECONOMÍA Y FINANZAS SECRETARÍA GENERAL

99

c) Resolución Ministerial Nº 246-2007-PCM, que 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.

d) Resolución Ministerial N° 129-2012-PCM, que 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.

e) Resolución Ministerial N° 512-2012-EF/10, que designa al Coordinador que hará las veces de Oficial de Seguridad de la Información del Ministerio de Economía y Finanzas, de conformidad con lo dispuesto por la R.M. Nº 129-2012-PCM.

f) Resolución Ministerial N° 649-2012-EF/10, que aprueba la conformación del grupo denominado "*Comité de Gestión de la Seguridad de la Información*" en el Ministerio de Economía y Finanzas.

g) Resolución de Contraloría General Nº 320-2006-CG, que aprueba las Normas de Control Interno de aplicación en las entidades del Estado.

5. Principios

Los siguientes principios constituyen los fundamentos sobre los que se basará cualquier acción en materia de seguridad de la información.

a. Protección

Los activos de información deben ser protegidos con el nivel de seguridad necesario, guardando proporción entre el valor y el riesgo de pérdida para el MEF. La protección debe enfocarse en la confidencialidad, integridad y disponibilidad de estos activos.

b. Uso apropiado

Los activos de información disponibles en el MEF deben ser utilizados en forma adecuada, eficiente, racional y exclusivamente para el desarrollo de las actividades institucionales.

c. Acceso autorizado

Todos los usuarios de sistemas de información del MEF deben ser identificados individualmente, y sus permisos de acceso deben concederse en forma específica de acuerdo a su rol y responsabilidades. Los métodos de acceso de los usuarios deben exigir un proceso de autenticación, autorización y auditoría.

d. Auditabilidad

Se debe asegurar que los sistemas informáticos, de acuerdo a su criticidad, registren eventos pertinentes a la seguridad de la información para su control posterior. Las evidencias de auditoría generadas deben permitir identificar usuarios y documentar las situaciones relacionadas con dichos eventos.

e. ***Disponibilidad***
Los activos de información deben estar disponibles para su uso por parte de los usuarios autorizados toda vez que lo requieran, garantizando el acceso oportuno a la información y a los recursos relacionados con la misma.

f. ***Integridad***
Los activos de información deben estar adecuadamente protegidos para asegurar su integridad. Las medidas de validación definidas deben permitir detectar la modificación inadecuada, adulteración o eliminación de los activos de información.

g. ***Confidencialidad***
Los activos de información deben mantenerse protegidos para asegurar la confidencialidad y privacidad entre usuarios con acceso autorizado a los mismos. En todo momento deben mantenerse esquemas de seguridad que prevengan la divulgación no autorizada de información.

h. ***Colaboración***
La conservación de la seguridad de la información es un esfuerzo de equipo en el que participan los trabajadores del MEF y terceros que tengan acceso a los activos de información del Ministerio, por el cual estas personas deben desempeñar un papel activo en el cumplimiento y divulgación de las políticas y normas vigentes de seguridad de la información.

i. ***Supervisión***
Periódicamente se deben revisar las plataformas tecnológicas (hardware y software) disponibles en el MEF, a fin de verificar el cumplimiento de las políticas de seguridad y la implementación de los estándares de configuración establecidos.

j. ***Propiedad***
La información registrada, almacenada y procesada por las operaciones de la organización es propiedad del MEF, a menos que en una relación contractual se establezca lo contrario, y la facultad de otorgar acceso a ella es del propietario de la información.

6. Lineamientos

6.1 Sobre la seguridad de la información

1. **Política de seguridad de la información**
La Política de Seguridad de la Información, contenida en el presente documento, define las líneas de acción y dirección a observar para la gestión adecuada de la seguridad de la información. Es necesario revisar y actualizar periódicamente esta política cuando surjan nuevas exigencias regulatorias en la materia o en caso de un cambio significativo dentro del MEF.

2. **Organización de la seguridad**
El MEF debe administrar la seguridad de la información dentro del Organismo y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades en forma adecuada.

Se debe conformar el Comité de Gestión de la Seguridad de la Información (CGSI) del MEF para la atención de temas en materia de seguridad de la información que requieran de una definición o aprobación institucional.

Se debe designar a un Oficial de Seguridad de la Información, o quien haga sus veces, con el perfil técnico adecuado para garantizar el cumplimiento de la política de seguridad de la información.

3. **Gestión de los activos**

El MEF debe elaborar y mantener un inventario de sus activos de información para el proceso de evaluación de riesgos de seguridad, asignando responsables de velar por la protección de dichos activos.

Se deben identificar, documentar e implementar reglas para el uso aceptable de la información y de los activos relacionados con su procesamiento.

4. **Seguridad de los recursos humanos**

Se debe verificar la idoneidad de las personas a contratar para laborar en la entidad, e incluir la firma de acuerdos de cumplimiento de seguridad de la información para trabajadores del MEF y terceros que puedan tener acceso a información sensible.

Se deben realizar programas de concientización y entrenamiento para asegurar que los trabajadores del MEF asuman sus responsabilidades relacionadas con la seguridad de la información, estableciéndose procesos disciplinarios para casos de incumplimiento. Los terceros que incumplan las políticas de seguridad se sujetarán a lo establecido en los respectivos contratos.

Al término de la vinculación laboral o contractual, debe asegurarse la devolución de activos de información asignados y el retiro de los accesos a sistemas informáticos del MEF que se hayan otorgado.

5. **Seguridad física y ambiental**

Las áreas e instalaciones de procesamiento, gestión o almacenamiento de información del MEF deben contar con mecanismos de control de acceso y protecciones físicas y ambientales apropiadas para prevenir el daño o pérdida de los activos de información. Se deben establecer procedimientos de mantenimiento de los equipos de procesamiento de información con el fin de asegurar su continua disponibilidad e integridad.

6. **Gestión de las comunicaciones y las operaciones**

En resguardo de la operación correcta y segura de las instalaciones de tecnologías de la información, se deben mantener documentados y actualizados los procedimientos operativos informáticos, controlar y documentar los cambios previamente autorizados sobre la plataforma tecnológica, y efectuar una separación de tareas y áreas de responsabilidad.

Se deben aplicar medidas efectivas de protección para el software utilizado en los sistemas de cómputo, la información que estos procesan, y la información transmitida por sistemas de comunicación de datos en la red interna del Ministerio, incluyendo la mensajería electrónica y los intercambios de información con cualquier entidad externa.

Se debe monitorear el uso de las redes y sistemas de información a fin de detectar actividades no autorizadas de procesamiento de información. Se deben generar evidencias de auditoría (*logs*) sobre sistemas críticos o sensibles cuya revisión periódica permita el análisis de eventos anómalos.

7. **Control de acceso**
   Deben establecerse mecanismos para prevenir el acceso no autorizado a los sistemas de información, servicios de la red interna y plataformas de tecnología informática del MEF, así como garantizar la seguridad de la información de la entidad en entornos computacionales móviles, instalaciones de trabajo remoto y conexiones de redes externas.

   Todo usuario autorizado debe poseer un identificador único para el acceso a los sistemas y servicios de información del MEF, debiéndose controlar la asignación y retiro de los correspondientes privilegios de uso.

8. **Adquisición, desarrollo y mantenimiento de sistemas de información**
   Se deben determinar los requisitos de seguridad para los nuevos sistemas de información del MEF o para los cambios en los existentes, ya sean desarrollados internamente o por terceros, que incluyan las verificaciones del procesamiento correcto de las aplicaciones y la protección del código y datos en producción.

   Todo sistema de información nuevo o actualizado debe cumplir con el ciclo de vida establecido para el desarrollo, desde su requerimiento hasta la validación y aceptación formal por parte de los usuarios solicitantes antes de su puesta en producción, respetando la normativa correspondiente.

   Los cambios en las aplicaciones y en el entorno de producción deben ser controlados adecuadamente, a fin de minimizar el riesgo de daños en la información o en los sistemas en donde se procesa la información.

9. **Gestión de incidentes de seguridad de la información**
   Se deben establecer medidas para asegurar que las vulnerabilidades y eventos detectados que afecten negativamente a la seguridad de la información o procesos de negocio del MEF sean reportados, registrados y gestionados de manera que permita la adopción de acciones preventivas y correctivas oportunas.

10. **Gestión de la continuidad de negocio u operativa**
    El proceso de gestión de la continuidad de negocio u operativa debe tomar en cuenta los aspectos necesarios para el tratamiento de los riesgos en seguridad de la información. Se debe contar con planes de continuidad operativa y contingencia que cubran los recursos informáticos e infraestructuras tecnológicas que dan soporte a los procesos esenciales del MEF, a fin de garantizar la continua disponibilidad de estos.

11. **Cumplimiento de las normas legales y técnicas**
    Se deben establecer mecanismos para garantizar el cumplimiento de toda norma legal, directiva, regulación técnica u obligación contractual y de los requisitos de seguridad aplicables a los sistemas y activos de información del MEF.

6.2 Sobre el Sistema de Gestión de Seguridad de la Información

1. El Sistema de Gestión de la Seguridad de la Información (SGSI) del MEF está conformado por la estructura organizativa, políticas, actividades de planeamiento, responsabilidades, prácticas, procesos, procedimientos y recursos destinados a la preservación de la seguridad de la información.
2. El Sistema de Gestión de Seguridad de la Información está sujeto a un proceso de mejora continua basado en los resultados de evaluaciones periódicas de riesgos, la respuesta ante incidentes que afecten la seguridad, o por la revisión periódica de las políticas vigentes.
3. Todo proceso de gestión del riesgo relacionado con la seguridad de la información se implementa con la metodología establecida por la unidad orgánica responsable de la gestión de riesgos del MEF y aprobada por la Alta Dirección, en el ámbito de sus competencias, asegurándose así que dichos procesos se encuentren alineados con la gestión del riesgo institucional.
4. El Sistema de Gestión de Seguridad de la Información del MEF establece los requisitos de seguridad tomando en cuenta los resultados de la evaluación metódica de los riesgos relevantes, los dispositivos legales pertinentes y los métodos y mecanismos de procesamiento de la información desarrollados en el MEF para el apoyo a sus operaciones, entre otros aspectos.

7. Responsabilidades

Para el cumplimiento de la presente Política de Seguridad de la Información en el MEF, se establecen las siguientes responsabilidades:

a) **Despacho Ministerial:** Aprobar la política de seguridad y sus futuras modificaciones con la asesoría del Comité de Gestión de Seguridad de la Información del MEF.

b) **Comité de Gestión de Seguridad de la Información (CGSI):** Dirigir, coordinar y revisar la puesta en práctica de la seguridad de la información en el MEF, comprometiendo el apoyo de la Alta Dirección.

c) **Oficial de Seguridad de la Información:** Supervisar el cumplimiento de la presente política en coordinación con las distintas dependencias del MEF, y liderar el establecimiento, implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información.

d) **Directivos:** Aplicar las políticas de seguridad de la información al interior de cada órgano o unidad orgánica, en los ámbitos funcional, técnico y administrativo, según corresponda.

e) **Propietario de la información:** Determinar el grado de confidencialidad y criticidad de la información, definir a cuáles usuarios se les otorgará el acceso y autorizar las peticiones sobre las distintas formas de utilizar la información.

f) **Custodio de la información:** Preservar y proteger la información que le ha sido confiada en custodia.

g) **Usuario:** Responder por los resultados derivados del uso de los activos de información a los que tiene acceso autorizado.

8. Glosario de Términos

a) **Activo de Información:** sistemas de información, aplicaciones o herramientas de tipo software, base de datos, equipos computacionales, dispositivos móviles, archivos físicos, documentos electrónicos o cualquier otro activo que por su naturaleza registre, procese, almacene o transmita información considerada relevante para los procesos esenciales del Ministerio.

b) **Confidencialidad:** característica por la cual se garantiza que la información sea accesible solo por las personas debidamente autorizadas para su acceso.

c) **Custodio de la información:** persona o grupo que, para efectos de custodia, detenta la posesión física de la información generada en el MEF o de aquella confiada al Ministerio.

d) **Determinación de riesgos:** evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatividad del MEF.

e) **Disponibilidad:** característica por la cual se garantiza que los usuarios autorizados tengan acceso a la información cuando se requiera y previene contra intentos de denegar su uso autorizado.

f) **Evento de seguridad:** ocurrencia identificada de un estado de un sistema, servicio o red que indica una posible violación de la política de la seguridad de la información o falla de salvaguardas, o una situación previamente desconocida que puede ser pertinente a la seguridad.

g) **Incidente de seguridad:** uno o varios eventos de seguridad de información, no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones esenciales y de amenazar la seguridad de la información.

h) **Integridad:** característica por la cual se garantiza que la información y los correspondientes métodos de procesamiento sean exactos y estén completos, asegurando que la información no es transformada ni modificada de forma no autorizada durante su procesamiento, transporte o almacenamiento.

i) **Propietario de la información:** persona o grupo bajo cuya autoridad la información es producida y que dispone las reglas de uso de la misma. Toda información del MEF contenida en activos o sistemas en producción debe tener un propietario designado.

j) **Usuario:** persona que utiliza directamente los activos de información a los que tiene acceso autorizado.

k) **Seguridad de la información:** conjunto de acciones destinadas a asegurar la confidencialidad, integridad y disponibilidad de los activos de información y tecnologías para su procesamiento, apoyando finalmente a la continuidad de las operaciones del MEF.