Firmado Digitalmente por TRINIDAD GUERRERO Kitty Elisa FAU 20131370645 soft
Fecha: 20/07/2022 17:06:56 COT
Motivo: Doy V° B°

Firmado Digitalmente por VARGAS MEDRANO Carlos Alberto FAU 20131370645 hard
Fecha: 20/07/2022 13:49:16 COT
Motivo: Doy V° B°

Resolución de Secretaría General

Lima, 20 de julio del 2022 N° 046-2022-EF/13

CONSIDERANDO:

Que, mediante el Decreto Supremo N° 004-2013-PCM, que aprueba la Política Nacional de Modernización de la Gestión Pública, se establece como objetivo específico, entre otros, "Implementar la gestión por procesos y promover la simplificación administrativa en todas las entidades políticas a fin de generar resultados positivos en la mejora de los procedimientos y servicios orientados a los ciudadanos y empresas";

Firmado Digitalmente por ALARCON ALVIZURI Bertha Patricia FAU 20131370645 soft
Fecha: 20/07/2022 14:22:50 COT
Motivo: Doy V° B°

Que, el literal g) del artículo 7 del Reglamento del Sistema Administrativo de Modernización de la Gestión Pública, aprobado con Decreto Supremo N° 123-2018-PCM, señala que la gestión por procesos tiene como propósito organizar, dirigir y controlar las actividades de trabajo de una entidad pública de manera transversal a las diferentes unidades de organización, para contribuir con el logro de los objetivos institucionales; así también, comprende acciones conducentes a la determinación de los procesos de la entidad, así como a su medición y análisis con el propósito de implementar mejoras en su desempeño, priorizando los procesos que contribuyan al logro de los objetivos de la entidad pública o aquellos que puedan afectar dicho logro;

Firmado Digitalmente por TAPIA DIAZ Vicente Raul FAU 20131370645 soft
Fecha: 20/07/2022 14:41:55 COT
Motivo: Doy V° B°

Que, mediante Resolución de Secretaría General N° 014-2020-EF/13, se aprueba el "Mapa de Procesos del Ministerio de Economía y Finanzas" y se establece el proceso "S03.03 Gestión de la Plataforma Tecnológica", que comprende las actividades de gestionar la contingencia informática y de las incidencias de la infraestructura y servicios de TI del Ministerio de Economía y Finanzas;

Que, el artículo 80 del Texto Integrado Actualizado del Reglamento de Organización y Funciones del Ministerio de Economía y Finanzas, aprobado por Resolución Ministerial N° 213-2020-EF/41, establece que la Oficina General de Tecnologías de la Información es el órgano de apoyo encargado de planificar, implementar y gestionar sistemas de información, infraestructura tecnológica de cómputo y de comunicaciones;

Firmado Digitalmente por MELGAREJO CASTILLO Juan Carlos FAU 20131370645 soft
Fecha: 20/07/2022 14:46:46 COT
Motivo: Doy V° B°

Que, asimismo, el inciso d) del artículo 81 del citado Texto Integrado Actualizado establece como función de la Oficina General de Tecnologías de la Información, la de formular y proponer políticas y normas de seguridad informática, e implementar soluciones de protección de las redes, equipos y sistemas de información del Ministerio, en concordancia con las políticas de seguridad establecidas;

Firmado Digitalmente por RAMOS PARADA Doris FAU 20131370645 soft
Fecha: 20/07/2022 16:34:14 COT
Motivo: Doy V° B°

MEF

Firmado Digitalmente por MELGAREJO CASTILLO Juan Carlos FAU 20131370645 soft
Fecha: 20/07/2022 14:46:51 COT
Motivo: Doy V° B°

MEF

Firmado Digitalmente por VARGAS MEDRANO Carlos Alberto FAU 20131370645 hard
Fecha: 20/07/2022 13:49:37 COT
Motivo: Doy V° B°

Que, mediante Resolución Ministerial N° 053-2021-EF/41 se aprueba la Directiva N° 001-2021-EF/41.02 “Lineamientos para la elaboración, aprobación y modificación de Directivas en el Ministerio de Economía y Finanzas”, cuyo numeral 4.4 establece que la Secretaría General aprueba, directivas y otros documentos normativos, sobre materias de administración interna distintas a las señaladas en el numeral 4.5 de la indicada directiva, y que se efectúa mediante Resolución de Secretaría General;

Que, en tal sentido, se ha considerado necesario aprobar la Directiva denominada “Lineamientos para la Prevención de Fuga de Información en el Ministerio de Economía y Finanzas”; a fin de establecer disposiciones para regular la adopción de un modelo integral de gestión para prevenir incidentes de fuga de información sensible en el Ministerio de Economía y Finanzas;

MEF

Firmado Digitalmente por ALARCON ALVIZURI Bertha Patricia FAU 20131370645 soft
Fecha: 20/07/2022 14:23:21 COT
Motivo: Doy V° B°

De conformidad con lo dispuesto en el Texto Integrado Actualizado del Reglamento de Organización y Funciones del Ministerio de Economía y Finanzas, aprobado por Resolución Ministerial N° 213-2020-EF/41;

SE RESUELVE:

Artículo 1. Aprobar la Directiva N° 001-2022-EF/44.04 denominada “Lineamientos para la Prevención de Fuga de Información en el Ministerio de Economía y Finanzas”, que como anexo forma parte integrante de la presente Resolución.

Artículo 2. Publicar la presente resolución en la sede digital del Ministerio de Economía y Finanzas (www.gob.pe/mef), en el Intranet del Ministerio de Economía y Finanzas y disponer su difusión a todo el personal del MEF mediante correo electrónico.

MEF

Firmado Digitalmente por TAPIA DIAZ Vicente Raul FAU 20131370645 soft
Fecha: 20/07/2022 14:42:01 COT
Motivo: Doy V° B°

Regístrese y comuníquese.

Ministerio de Economía y Finanzas

Firmado Digitalmente por TRINIDAD GUERRERO Kitty Elisa FAU 20131370645 soft
Fecha: 20/07/2022 17:06:51 COT
Motivo: Firma Digital

Documento firmado digitalmente
KITTY TRINIDAD GUERRERO
Secretaria General
Ministerio de Economía y Finanzas

MEF

Firmado Digitalmente por RAMOS PARADA Doris FAU 20131370645 soft
Fecha: 20/07/2022 16:34:23 COT
Motivo: Doy V° B°

DIRECTIVA N° 001-2022-EF/44.04

LINEAMIENTOS PARA LA PREVENCIÓN DE FUGA DE INFORMACIÓN EN EL MINISTERIO DE ECONOMÍA Y FINANZAS

1. OBJETO

Establecer disposiciones para regular la adopción de un modelo que permita prevenir incidentes de fuga de información sensible en el Ministerio de Economía y Finanzas (MEF).

2. BASE LEGAL

2.1 Ley N° 29733 – Ley de Protección de Datos Personales.

2.2 Decreto Legislativo Nº 1412, que aprueba la Ley de Gobierno Digital.

2.3 Decreto de Urgencia Nº 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

2.4 Decreto Supremo N° 021-2019-JUS, TUO de la Ley N° 27806 – Ley de Transparencia y Acceso a la Información Pública.

2.5 Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley N° 29733. Ley de Protección de Datos Personales.

2.6 Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.

2.7 Resolución Ministerial N° 004-2016-PCM, que aprueba 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.

2.8 Resolución Ministerial N° 210-2020-EF/44, que aprueba la "Política de Seguridad de la Información del Ministerio de Economía y Finanzas".

2.9 Resolución Ministerial N° 213-2020-EF/41, que aprueba el Texto Integrado actualizado del Reglamento de Organización y Funciones - ROF del Ministerio de Economía y Finanzas.

2.10 Resolución Ministerial N° 053-2021-EF/41, que aprueba la Directiva N° 001-2021-EF/41.02 "Lineamientos para la elaboración, aprobación y modificación de Directivas en el Ministerio de Economía y Finanzas".

2.11 Resolución Directoral N° 478-2016-EF/43.01, que modifica el "Manual de Políticas de Gestión de Tecnologías de la Información del MEF".

Las normas incluyen sus respectivas disposiciones ampliatorias, modificatorias y conexas, de ser el caso.

3. ALCANCE

Las disposiciones establecidas en la presente Directiva son de cumplimiento obligatorio por los servidores civiles del Ministerio de Economía y Finanzas, sin distinción de su régimen laboral o contractual al que estén sujetos.

4. DISPOSICIONES GENERALES

4.1 DEFINICIONES

a) *Confidencialidad:* La confidencialidad es la garantía de que la información sensible será protegida para que no sea divulgada sin consentimiento de la entidad. Dicha garantía se lleva a cabo por medio de un grupo de reglas que limitan el acceso a esta información.

b) *Dato sensible:* sinónimo de información sensible (ver definición f).

c) *Datos personales:* Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados. Incluye a los datos personales considerados sensibles que se refieren a aspectos raciales, étnicos, ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales, afiliación sindical e información relacionada a la salud o a la vida íntima.

d) *Fuga de datos:* Expresión sinónima de *Fuga de información*.

e) *Fuga de información:* Incidente de origen interno o externo que de manera intencional o no, pone información sensible en poder de una persona no autorizada para su acceso o uso.

f) *Información sensible:* En el ámbito de la presente directiva, es el conjunto de datos que incluye a la información secreta, confidencial y reservada según las normas nacionales de transparencia, así como a los datos personales **protegidos en el ámbito de la Ley de Protección de Datos Personales** y a la información de propiedad intelectual.

g) *Propiedad intelectual:* La propiedad intelectual brinda "derechos de exclusividad" a las instituciones públicas o privadas para utilizar y beneficiarse de lo que han protegido. Esto quiere decir que, si la institución patenta una nueva tecnología, será la única que pueda fabricar y comercializar dicha tecnología en el mercado.

h) Si una institución registra una marca para un determinado producto o servicio, entonces será la única que pueda utilizar dicha denominación en el mercado.[1]

i) *Dashboard:* También conocido como tablero o cuadro de mando, referido a un documento que refleja mediante gráficas, las principales métricas que intervienen en la consecución de los objetivos de una estrategia.

j) *DLP:* Término en inglés *Data Leak Prevention* referido a la protección de fuga de información.

MEF

Firmado Digitalmente por RAMOS PARADA Doris FAU 20131370645 soft
Fecha: 30/06/2022 20:55:45 COT
Motivo: Doy V° B°

MEF

Firmado Digitalmente por JARA HUALLPATUERO Maria Ysabel FAU 20131370645 soft
Fecha: 11/07/2022 14:10:15 COT
Motivo: Doy V° B°

[1] Definido a partir de lo señalado en: INDECOPI: "IMPORTANCIA DE PROTEGER LOS DESARROLLOS EN LAS EMPRESAS: EL VALOR DE LA PROPIEDAD INTELECTUAL.", 2021, https://www.patenta.pe/publicaciones.

4.2 SOBRE LA PREVENCIÓN DE FUGA DE INFORMACIÓN

4.2.1 La fuga de información es la salida de información sensible sin la autorización respectiva, poniendo en riesgo al propietario de dicha información de que su información sea mal utilizada, con las consiguientes consecuencias o daños tales como: consecuencia legal, económica y social.

4.2.2 El origen del riesgo de fuga de información sensible puede darse en el ámbito interno y externo. Entendiendo el interno al producido dentro del MEF, accionado por los/las servidores/as civiles que laboran o prestan servicios directa o indirectamente con la información que produce la entidad, y el externo, que son generados por personas u organizaciones criminales interesadas en obtener la información sensible. Las causas suelen ser: internas que son por falta de formación o desconocimiento; y las externas por ataques de entidades ajenas al MEF o piratas informáticos (*hackers*).

4.2.3 Los objetivos de la prevención de la fuga de información en el MEF son:

a) Ubicar donde está almacenada y catalogar el activo de información sensitiva declarada por el MEF.
b) Monitorear y controlar el movimiento del activo de información sensitiva a través de sus redes o procesos en el MEF.
c) Monitorear y controlar el movimiento del activo de información sensible administrada, procesada y almacenada por los/las servidores/as civiles que laboran o prestan servicios en el MEF.

4.3 SOBRE LOS DATOS O INFORMACIÓN A PROTEGER

Los estados posibles de la información sensible donde puede ocurrir fuga de información son los mostrados en la siguiente figura:

Fig. 1: Fuente Propia: Of. Gobierno de TI

4.3.1 <u>Dato en reposo.</u>

Referido a la información que no está siendo accedida, usada, ni procesada y que se encuentra almacenada en un medio físico o lógico, tales como: Ficheros almacenados en servidores de archivos, registros en bases de datos, documentos en unidades flash, discos duros etc.

4.3.2 Dato en movimiento / tránsito

Referido a la Información que viaja a través de la red informática del MEF a través de: correo electrónico (*email*), web (internet), aplicaciones de trabajo colaborativo, mensajería instantánea, o cualquier tipo de canal privado o público de comunicación.

4.3.3 Dato en uso

Referido a la información que está siendo accedida por los usuarios mediante aplicaciones para su tratamiento, pudiendo ser procesado en medios como: unidades USB, correos electrónicos, web, etc., por lo que el diseño de políticas o reglas de uso, deben estar claramente establecidas para la protección del activo de información y que a su vez no dificulten el accionar de las operaciones, lo que dejaría brechas de seguridad significativas. Este estado de información es el más desafiante para la protección de fuga de información.

MEF

Firmado Digitalmente por RAMOS PARADA Doris FAU 20131370645 soft
Fecha: 30/06/2022 20:55:54 COT
Motivo: Doy V° B°

4.4 SOBRE LAS CAUSAS DE LA FUGA DE DATOS

Las causas de la fuga de datos se clasifican en organizativas y técnicas.

4.4.1 Causas organizativas

a) Desconocimiento de la existencia e identificación de aquellos datos sensibles que constituyen activos de información que el MEF debe proteger.

b) Falta de clasificación de la información sensible, esto es, no se tiene una categorización de la propia información institucional en cuanto a su nivel de confidencialidad requerido y el valor que le representa, por lo que se hace difícil diseñar medidas de prevención adecuadas.

c) Deficiencias en la formación y niveles de conocimiento, por parte de los/las servidores/as civiles del MEF, en el uso seguro de los equipos y medios informáticos proporcionados por el MEF, lo que hace más propicia la fuga de datos por errores o procedimientos no seguros al emplear tecnologías digitales.

d) Ausencia de acuerdos de confidencialidad entre el MEF y sus propios servidores civiles, o de programas de inducción por los que se puede brindar un conocimiento y apreciación de las medidas de seguridad institucionales que se hayan establecido.

MEF

Firmado Digitalmente por JARA HUALLPATUERO Maria Ysabel FAU 20131370645 soft
Fecha: 11/07/2022 14:10:22 COT
Motivo: Doy V° B°

4.4.2 Causas técnicas

a) Exposición a código malicioso o malware, mediante técnicas diseñadas para mantener oculto su código en sistemas mientras va recogiendo o recolectando y transmitiendo la información sensible obtenida por este mecanismo.

b) Acceso no autorizado que deriva en robo o apropiación de datos, lo que ocurre cuando no existe o son muy débiles los mecanismos de seguridad para el control de acceso a la información sensible que se quiere proteger.

c) Uso indebido de las tecnologías móviles como dispositivos de comunicación y de almacenamiento, que permiten almacenar y transportar toda información, incluyendo la información sensible, de manera no autorizada.

4.5 SOBRE EL IMPACTO DE LA FUGA DE INFORMACIÓN

Se debe considerar la siguiente categorización de las consecuencias de la fuga de información a fin de tener claridad y criterios sobre el impacto que pueda ocasionar y las acciones que se deban tomar:

CATEGORÍAS	IMPACTOS
Consecuencia legal	Podrían conllevar a sanciones administrativas o a acciones legales.
Consecuencia económica-social	Impacto negativo en lo económico y social
Consecuencias en otros ámbitos	Impacto de imagen institucional.

Elaboración propia

4.6 SOBRE EL MODELO DE PREVENCIÓN DE LA FUGA DE INFORMACIÓN

4.6.1 El proceso integral para prevenir la fuga de información sensible en el MEF se alinea con las políticas de seguridad que se apliquen a la información que el MEF recibe, almacena, procesa y produce.

4.6.2 Se establece un Modelo de Prevención de la Fuga de Información para describir el proceso integral mencionado mediante seis (6) fases: Identificación y recopilación, Inventario y clasificación, Diagnóstico y planificación, Gestión de la prevención, Gestión de incidentes, Mejora continua.

Fig. 2: Fuente Propia-Of. Gobierno de TI

4.6.3 En este modelo se busca primero determinar cuál es la información sensible que el MEF considera como tal, a fin de planificar y adoptar las medidas necesarias para gestionar el riesgo de fuga o pérdida que pueda existir sobre dicha información. Para efectos de la implementación de este modelo, es necesario que los órganos del MEF que recopilan, producen, procesan, analizan, publican, almacenan y distribuyen información, en coordinación con el órgano responsable de las tecnologías de información, establezcan los mecanismos, acciones, apoyo técnico y presupuesto necesarios para planificar e implementar el proceso integral de prevención de fuga de datos o información.

4.6.4 El flujo que comprende el modelo integral para el monitoreo y fuga de la información se muestra en el **Anexo N° 01 Flujo del Modelo de prevención de la fuga de información en el MEF.**

MEF

Firmado Digitalmente por RAMOS PARADA Doris FAU 20131370645 soft
Fecha: 30/06/2022 20:56:02 COT
Motivo: Doy V° B°

4.7 FASE DE IDENTIFICACIÓN Y RECOPILACIÓN

4.7.1 En esta fase se identifica la información sensible que el MEF recibe, procesa, produce y almacena, como productos de sus procesos y procedimientos.

4.7.2 Para recopilar la información sensible existente a nivel organizacional se emplearán métodos y técnicas de revisión de documentación, entrevistas, encuestas y reuniones de trabajo que permitan ampliar el espectro de la identificación de la información

4.7.3 Los órganos del MEF, como propietarios de la información o custodios de la misma y tal como está establecido en los procesos o procedimientos, están obligados a proporcionar la información necesaria para esta etapa inicial.

4.8 FASE DE INVENTARIO Y CLASIFICACIÓN

4.8.1 En esta fase se realiza el inventario de la información recopilada, teniendo especial atención en el detalle de cómo se clasifica, ordena, describe y anota la información obtenida.

MEF

Firmado Digitalmente por JARA HUALLPATUERO Maria Ysabel FAU 20131370645 soft
Fecha: 11/07/2022 14:10:30 COT
Motivo: Doy V° B°

4.8.2 La clasificación de la información debe responder a las normas vigentes y se deben desarrollar los criterios necesarios de clasificación de la información, según las valoraciones de criticidad o importancia que se le atribuya en los procesos organizacionales que la utilizan[2].

4.8.3 El proceso de clasificación de la información debe establecerse de forma transparente y eficiente, y no estar sujeto a criterio propio o ajeno al objetivo o fin del MEF.

4.8.4 Los órganos del MEF, como propietarios de la información de sus procesos, deben delinear inicialmente la característica del tipo de información que poseen, utilizan y producen. De ser necesario, esta clasificación y/o criterio de clasificación del activo de información, debe

[2] La Ley de Transparencia y Acceso a la Información Pública clasifica la información de la administración pública en secreta, confidencial y reservada. La valoración indicada se realizará sobre la información confidencial que se genera o procesa internamente en los distintos órganos de la entidad, considerando las excepciones contempladas en el artículo Nº 17 de dicha ley.

estar respaldado por una política o directiva que establezca el criterio de clasificación de información.

4.8.5 En esta fase también debe determinar con precisión, los criterios de controles de seguridad del que debe estar sujeto el activo de información.

4.9 FASE DE DIAGNÓSTICO Y PLANIFICACIÓN

Una vez obtenida, inventariada y clasificada la información, y en base a:

a) Normas legales establecidas para el tratamiento de la información y otros procesos que reserven o limiten la información pública.
b) Normas técnicas de tratamiento y seguridad de la información.
c) Hallazgos obtenidos en el levantamiento de información.
d) Opinión y aportes de expertos sobre tratamiento de información.
e) Otros elementos que contribuyan a diagnosticar la situación real.

Se deben realizar las siguientes acciones:

4.9.1 Establecer las brechas correspondientes sobre el tratamiento de la información sensible en el MEF, así como la seguridad de información correspondiente.

4.9.2 Utilizar cuadros de mandos (Dashboard) que permitirán visualizar la situación real del tratamiento de información sensible en el MEF y cómo está alineado según las normativas emanadas al respecto.

4.9.3 El diagnóstico de la situación real del tratamiento de la información sensible en el MEF, debe ser de conocimiento por los órganos del MEF para que estén consciente de la situación real, así como de los riesgos que pueden ocurrir y de los impactos a los que estarían expuestos.

4.9.4 Establecer la planificación del tratamiento del activo de información sensible del MEF teniendo en cuenta lo siguiente:

a) Establecer los objetivos, metas a lograr y alcance.
b) Establecer o diseñar medidas: organizativas, técnicas y legales, que serán implementadas, y que tendrán una relación directa con los controles que se establezcan.
c) Establecer los indicadores para dar el seguimiento a la Planificación tanto en el desempeño, el resultado del plan, y su efectividad. Con el objetivo de establecer una gestión de control y supervisión de la Planificación.
d) La planificación del tratamiento del activo de información debe ser aprobado por todos los órganos del MEF.
e) Sensibilizar y difundir en el MEF, la conceptualización de la Fuga de Información, así como la planificación para su tratamiento.

4.10 FASE DE GESTIÓN DE LA PREVENCIÓN

Durante esta fase se pone en ejecución las actividades planificadas para el tratamiento del activo de información sensible del MEF. Algunas de estas medidas están clasificadas en: Organizativas, Técnicas y Legales.

4.10.1 Medidas organizativas

a) Buenas Prácticas.
b) Política de seguridad.
c) Procedimientos.
d) Clasificación de la información, establecimiento de roles y niveles de acceso.
e) Formación e información interna.
f) Sistema de Gestión de Seguridad de la Información.
g) Inducción y sensibilización sobre el tratamiento de la información sensible al personal del MEF.

MEF

Firmado Digitalmente por RAMOS PARADA Doris FAU 20131370645 soft
Fecha: 30/06/2022 20:56:10 COT
Motivo: Doy V° B°

4.10.2 Medidas técnicas

a) Control de acceso o identidad y a recursos.
b) Soluciones anti-malware y anti-fraude.
c) Seguridad perimetral y protección de las comunicaciones.
d) Control de contenidos y control de tráfico.
e) Copias de seguridad.
f) Actualizaciones de seguridad y parches.
g) Otras medidas de seguridad derivadas del cumplimiento de legislación.
h) Gestión de incidentes e inteligencia de seguridad.
i) Administración de dispositivos móviles dentro y fuera de una red
j) Detección y respuestas de puntos finales.
k) Defensa contra ataques avanzados y persistentes.
l) Detección de amenazas de descarga de direcciones IP y URL con protocolo HTTP y HTTPS.
m) Detección de amenazas mediante el contenido copiado y adjuntando en los correos electrónicos.

MEF

Firmado Digitalmente por JARA HUALLPATUERO Maria Ysabel FAU 20131370645 soft
Fecha: 11/07/2022 14:10:37 COT
Motivo: Doy V° B°

4.10.3 Medidas legales

a) Elaboración y aprobación de política de seguridad.
b) Elaboración y aceptación de la política de confidencialidad.
c) Otras medidas de carácter disuasorio en base a legislación o normativas.
d) Medidas relativas a la adecuación y cumplimientos de normativas, por ejemplo: Normas Técnicas Peruana, Ley de Transparencia de la Información Pública, Ley de Protección de los Datos Personales, Ley de la Transparencia Económica, Ley de la Transparencia Económica, Ley de las Adquisiciones del Estado, y otros que tenga directa o indirectamente con la limitación de acceso a la información, entre otros.

4.11 FASE DE GESTIÓN DE INCIDENTES

En esta fase se da seguimiento y se resuelve los incidentes relacionados a la fuga de la información sensible detallando las acciones que se deben de desarrollar como respuesta ante tales incidentes y alineados al marco de la seguridad de la información.

Se debe tener en cuenta lo siguiente:

4.11.1 Todo servidor civil del MEF ante el conocimiento de cualquier incidente que ponga en riesgo el activo de la información sensible del MEF, debe reportar a la instancia correspondiente del procedimiento de gestión de incidentes.

4.11.2 Todo incidente informado que ponga en riesgo el activo de información sensible del MEF debe ser anotado para mantener un control que permita: identificar su trazabilidad, dar respuesta inmediata y establecer la solución correspondiente, y la respuesta debe quedar registrada para el análisis, evaluación posterior y para tener una fuente importante de conocimiento de los incidentes que se presentan.

4.11.3 En el ***Anexo N° 02 Gestión de Incidencias de Fuga de Información en el MEF*** se muestra el flujo con las fases para la gestión de las incidencias.

MEF

Firmado Digitalmente por RAMOS PARADA Doris FAU 20131370645 soft
Fecha: 30/06/2022 20:56:14 COT
Motivo: Doy V° B°

4.12 FASE DE MEJORA CONTINUA

4.12.1 Definir, diseñar, establecer e implementar la mejora continua en la gestión de incidente de fuga de información sensible de forma permanente. En la siguiente figura se aprecia que, en base a algunos elementos, se debe implementar la mejora continua.

Fig. 3: Fuente Propia-Of. Gobierno de TI

MEF

Firmado Digitalmente por JARA HUALLPATUERO Maria Ysabel FAU 20131370645 soft
Fecha: 11/07/2022 14:10:40 COT
Motivo: Doy V° B°

4.12.2 Las medidas de prevención que se deben tener en cuenta para una mejora continua en la prevención de los riesgos y en especial de la fuga de información sensible, son las siguientes:

a) Medidas a través de Políticas y Normativas.
b) Medidas Organizacionales.
c) Medidas sobre los Recursos Humanos.
d) Medidas Tecnológicas.

5. DISPOSICIONES ESPECÍFICAS

5.1 La implementación del Modelo de Prevención de la Fuga de Información en el MEF, estará a cargo por la Oficina General de Tecnología de Información en coordinación permanente con los órganos que correspondan.

5.2 El Modelo de Prevención de la Fuga de Información en el MEF abarca el control a todos los órganos del MEF, a sus procesos definidos y a la tecnología utilizada en el almacenamiento, procesamiento y seguridad de los activos de información digital.

5.3 La OGTI, ante el hecho de una posible fuga de información procede a verificar con los órganos respectivos del MEF la importancia o nivel de reserva o de confidencialidad de la información involucrada a fin de identificar si corresponde activar las alertas o acciones preventivas correspondientes.

6. RESPONSABILIDADES

6.1 La Oficina General de Tecnologías de la Información es responsable de la viabilidad y operatividad técnica de los lineamientos establecidos en la presente directiva.

MEF

Firmado Digitalmente por RAMOS PARADA Doris FAU 20131370645 soft
Fecha: 30/06/2022 20:56:18 COT
Motivo: Doy V° B°

7. DISPOSICIONES COMPLEMENTARIAS Y FINALES

7.1 La Oficina General de la Tecnologías de la Información propone las medidas en el ámbito preventivo (organizativas, técnicas y legales) y coordinará con los órganos del MEF competente para su evaluación y posible implementación en el ámbito de su competencia.

7.2 Establecido e implementado el Modelo de Prevención de la Fuga de Información en el MEF, la Oficina General de la Tecnologías de Información, debe propiciar la formulación de Políticas o Documentos Normativos respecto a la prevención y gestión de la Fuga de Información en el MEF.

8. ANEXOS

8.1 Anexo N° 01 "*Flujo del Modelo de prevención de la fuga de información en el MEF*".

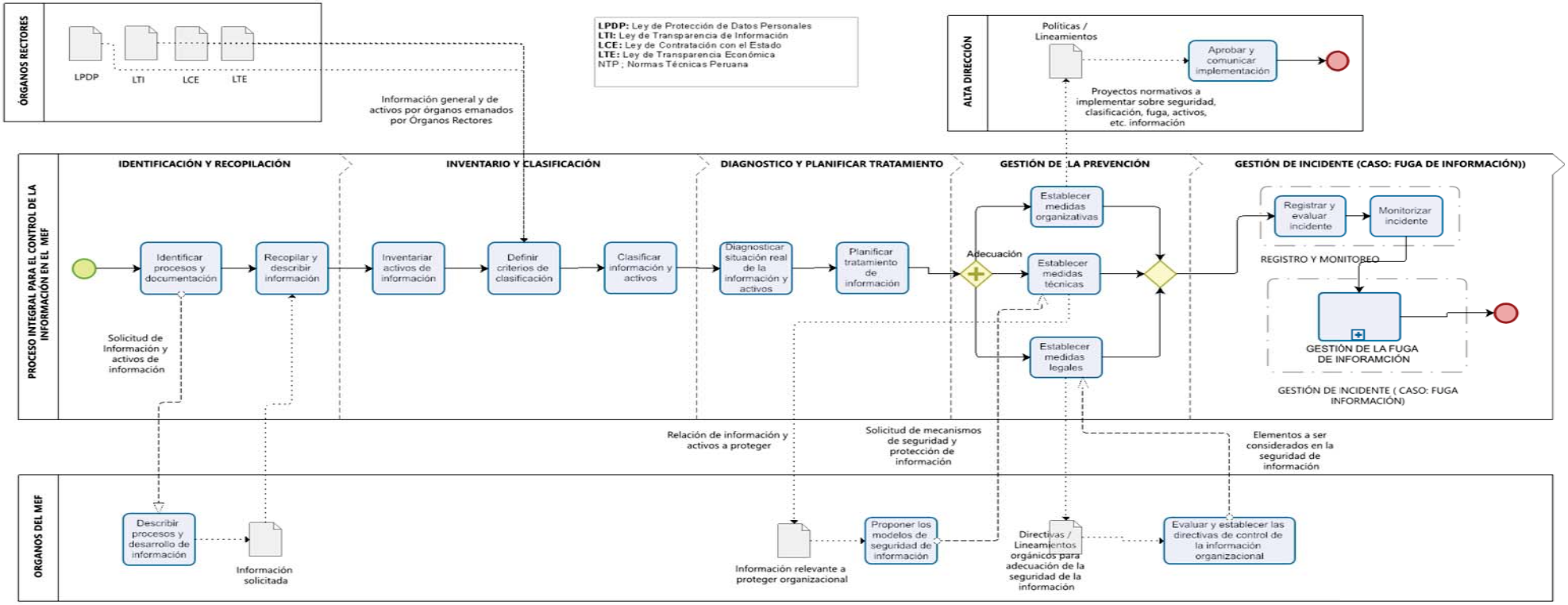
8.2 Anexo N° 02 "*Gestión de incidencias de fuga de información en el MEF*".

MEF

Firmado Digitalmente por JARA HUALLPATUERO Maria Ysabel FAU 20131370645 soft
Fecha: 11/07/2022 14:10:44 COT
Motivo: Doy V° B°

ANEXO N° 01

Flujo del Modelo de prevención de la fuga de información en el MEF



MEF

Firmado Digitalmente por RAMOS PARADA Doris FAU 20131370645 soft
Fecha: 30/06/2022 20:56:26 COT
Motivo: Doy V° B°

MEF

Firmado Digitalmente por JARA HUALLPATUERO Maria Ysabel FAU 20131370645 soft
Fecha: 11/07/2022 14:10:51 COT
Motivo: Doy V° B°

ANEXO N° 02

Gestión de Incidencias de Fuga de Información en el MEF

El MEF posee información sensible que de acuerdo **a la normativa vigente** debe ser protegida para evitar su divulgación sin las autorizaciones o permisos correspondientes. En tal sentido el MEF requiere tomar medidas e implementar controles para prevenir la posible **fuga de este tipo de** información.

Este modelo se alinea con la Política y Sistema de Gestión de la Seguridad de la Información del MEF, la que define, registra y procesa los incidentes de seguridad de la información en el MEF. Por tanto, el presente documento normativo tiene un alcance desde el inicio que se detecta el incidente de la fuga de información hasta su atención y acciones de control y prevención posterior.

Adicionalmente, el presente Modelo de Gestión de Incidencia de la Fuga de Información en el MEF, se constituye como apoyo a la Gestión de Riesgos Operativos y de Corrupción, ya que aporta a establecer el contexto del riesgo, identificar el riesgo, analizar el riesgo, valorar el riesgo y dar el tratamiento del riesgo que plasma las acciones de respuesta para una correcta gestión de riesgo de la fuga de información en el MEF.

Para esta gestión de incidencia de seguridad de información se adopta un proceso de respuesta a incidentes alineados a las fases establecidas en el procedimiento general de gestión de incidentes de seguridad de la información del MEF.

Fig. 4: Fuente Propia-Of. Gobierno de TI

MEF

Firmado Digitalmente por JARA HUALLPATUERO Maria Ysabel FAU 20131370645 soft
Fecha: 11/07/2022 14:10:57 COT
Motivo: Doy V° B°

1. Etapa: **INICIO**

El incidente de fuga de información sensible es un riesgo crítico y en ocasiones este se manifiesta cuando ya ocurrió el evento y a veces es detectado posteriormente al hecho por lo que es importante tomar medidas preventivas. Los pasos iniciales en la gestión de la fuga de información sensible son los siguientes:

MEF

Firmado Digitalmente por RAMOS PARADA Doris FAU 20131370645 soft
Fecha: 30/06/2022 20:56:34 COT
Motivo: Doy V° B°

1.1. El/La servidor/a civil del MEF que ha tomado conocimiento de una posible fuga de información sensible, debe reportar a la brevedad posible a su

Jefe/a inmediato/a o al Oficial de la Seguridad de Información, a fin de que tomen las medidas que corresponda.

1.2. Tanto el/la Jefe/a Inmediato/a y el Oficial de Seguridad de Información deben recopilar la mayor cantidad de información o evidencia posible sobre el hecho presentado, tanto en lo legal como en lo organizativo y técnico.

1.3. Se debe constituirse un grupo de trabajo especializado con el propósito de coordinar el manejo inicial del incidente desde el momento que se ha notificado en el punto 1.2. Este grupo especializado está conformado inicialmente por: la Jefatura del Órgano encargado del procesamiento de dicha información, el/la Oficial de Seguridad de Información o el que haga sus veces y el responsable de la Infraestructura Tecnológica de la OGTI.

1.4. De ser necesario y de existir un sistema de gestión de seguridad de la información, el incidente de fuga de información es registrado de acuerdo al procedimiento de gestión de incidentes de la seguridad de información del MEF, y se debe recopilar la mayor cantidad de información posible o evidencias posibles sobre el hecho.

1.5. Desarrollar un protocolo y establecer la coordinación y consulta a los Órganos del MEF cuya fuga de información sensible las involucre. De ser necesario y de acuerdo a la magnitud preliminar que se pueda establecer, estas coordinaciones pueden tener la condición de permanente y de clasificada o reservada.

1.6. De ser necesario, el grupo de trabajo especializado incorpora a un responsable el cual canaliza las comunicaciones y órdenes preliminares que éstos establezcan, debido a la importancia de guardar prudencia para el tratamiento del incidente presentado.

2. Etapa: **EJECUCIÓN**

Reconocido el incidente como riesgo de información, es necesario que las decisiones a tomar para gestionar el riesgo sean las oportunas, reconocidas y analizadas coherentemente de forma colegiada por el grupo de trabajo especializado.

Para ello se debe seguir los siguientes pasos que permitan manejar esta situación:

MEF

Firmado Digitalmente por JARA HUALLPATUERO Maria Ysabel FAU 20131370645 soft
Fecha: 11/07/2022 14:11:01 COT
Motivo: Doy V° B°

2.1. El grupo de trabajo especializado se reunirá para evaluar la situación actual, como producto de la fuga de la información. Para ello es importante tener recopilada, previamente, toda la información posible de los hechos presentados.

2.2. Se debe continuar ejecutando las actividades del protocolo diseñado en el punto 1.5, con miras a ir mitigando el riesgo.

2.3. De ser necesario, el grupo de trabajo especializado, puede incorporar a otras personas según el alcance del impacto del riesgo presentado, y

MEF

Firmado Digitalmente por RAMOS PARADA Doris FAU 20131370645 soft
Fecha: 30/06/2022 20:56:38 COT
Motivo: Doy V° B°

también a especialistas que aporten para la detección y mitigación del riesgo.

2.4. El grupo de trabajo especializado, de forma colegiada, presenta un Informe de los hechos y de la incidencia o impacto presentado a las autoridades correspondientes del MEF, para su conocimiento y evaluación, de ser el caso.

3. Etapa: **AUDITORÍA**

Estando en marcha las primeras acciones para la atención del incidente de fuga de información sensible, es indispensable obtener la mayor cantidad de información posible para: detectar, identificar, ubicar, dimensionar y evaluar el grado de fuga de información ocasionado, tratando esto en el menor tiempo posible. Adicionalmente, con la mayor información obtenida se debe perfilar las acciones para mitigar el riesgo presentado de forma más efectiva y concreta.

Esta acción de auditoría o peritaje puede ser realizada por el **grupo de trabajo especializado**, si se cuenta con las competencias y recursos técnicos necesarios, o en su defecto mediante servicios especializados contratados para tal efecto.

La información recibida debe estar enfocada desde dos frentes: interno y externo al MEF, por lo que será necesario realizar peritajes para obtener mayor información posible. Se debe seguir las siguientes actividades:

3.1. PERITAJE INTERNO

El peritaje interno se establece como mecanismo para obtener información situacional de las causas y consecuencias que se han producido al interior del MEF, para lo cual se obtendrá, en el menor tiempo posible, los siguientes elementos:

3.1.1 La cantidad de información sensible que ha podido ser sustraída corroborando la naturaleza de información sensible. Se debe contemplar la información tanto digital como la escrita.

3.1.2 Determinar si el cuidado de la información sensible estaba a cargo del MEF o por terceros y cuál es su nivel de importancia y criticidad para el MEF.

3.1.3 Identificar y establecer la causa o las causas principales de la filtración o fuga de información en el MEF. Observando su tipo de origen pudiendo ser:

MEF

Firmado Digitalmente por JARA HUALLPATUERO Maria Ysabel FAU 20131370645 soft
Fecha: 11/07/2022 14:11:05 COT
Motivo: Doy V° B°

MEF

Firmado Digitalmente por RAMOS PARADA Doris FAU 20131370645 soft
Fecha: 30/06/2022 20:56:42 COT
Motivo: Doy V° B°

Técnico
Tecnológico
Humano
Procesos o procedimientos
Controles
Normativos
Funcionales, etc.

3.2. PERITAJE EXTERNO

El peritaje externo se establece como mecanismo para determinar el tamaño, gravedad y nivel de difusión de la fuga de información sensible al exterior del MEF. Se realiza un balance de la cantidad o volumen de información que ha sido sustraída. En el peritaje externo se obtiene la siguiente información:

a) Identificación de la información sensible sustraída y la forma en que pudo ser filtrada indebidamente.

b) La ruta posible que siguió la información sensible filtrada indebidamente.

c) El alcance de información sustraída, determinando si la información sensible filtrada ha sido digital o escrita.

d) El nivel de impacto producido en la ciudadanía con la información sensible sustraída.

3.3. INFORME SITUACIONAL

3.3.1 La importancia de obtener información respecto al contenido de lo sustraído, es vital. Y la forma de cómo se produjo la fuga de información sensible, es crítico a la vez, por lo que se debe realizar un informe situacional con los hechos obtenidos en los peritajes efectuados.

3.3.2 Para la preparación del informe situacional se debe tener en cuenta aspectos que puedan mitigar el riesgo de forma rápida y oportuna, tales como:

a) La elaboración del informe situacional no debe superar a las primeras 12 horas desde el reporte inicial del incidente en el MEF.

b) El informe situacional no debe contener información basada en hipótesis, conjeturas o suposiciones. Debe ser lo más exacto posible y ser fidedigno respecto a todos los hechos expuestos.

MEF

Firmado Digitalmente por JARA HUALLPATUERO Maria Ysabel FAU 20131370645 soft
Fecha: 11/07/2022 14:11:09 COT
Motivo: Doy V° B°

MEF

Firmado Digitalmente por RAMOS PARADA Doris FAU 20131370645 soft
Fecha: 30/06/2022 20:56:47 COT
Motivo: Doy V° B°

4. Etapa: **EVALUACIÓN**

En esta etapa, se busca evaluar la situación presentada en la fuga de información sensible, la cual permita establecer un plan donde se incorpore que mitiguen la brecha del impacto que éste hecho pudo haber presentado.

4.1. EVALUACIÓN

Con el informe situacional, el grupo de trabajo especializado realiza las siguientes acciones:

a) Evaluar y valorizar el incidente presentado, sopesando el grado de importancia, criticidad y volumen de la información sustraída, que puede ser desde lo muy general a lo muy específico.

   La evaluación debe realizarse lo más pronto posible, para no extender el tiempo entre el incidente de fuga de información presentada y la respuesta a ser implementada

b) Evaluar la situación en la medida en que los peritajes incorporen nuevos elementos y abarque a la totalidad del hecho de la fuga de información.

4.2. PLANIFICACIÓN

El grupo de trabajo especializado elabora el “Plan de Emergencia” para dar respuesta de mitigación ante la situación presentada, de acuerdo a la evaluación establecida.

Las acciones contenidas en el **Plan de Emergencia** deben describir los siguientes aspectos:

a) Acciones que permitan minimizar la difusión de la información sensible y mitigar la misma. Estas acciones deben tomar en cuenta el carácter personal o la información sensible que ha sido filtrada.

b) Acciones para cerrar la filtración de información sensible y evitar nuevas fugas que se puedan seguir presentando.

c) Acciones que permitan mitigar el impacto a los afectados por la fuga de información sensible, ya sean internos o externos.

d) Acciones para mitigar las acciones legales de los afectados o el incumplimiento de normativas vigentes.

e) Acciones para mitigar la seguridad de los activos de información afectados del MEF.

f) Acciones de coordinación con otros organismos públicos o cuerpos de seguridad para establecer acciones conjuntas, si el impacto de la fuga de información ha extrapolado hasta esos ámbitos.

g) La definición de la gestión de comunicaciones del incidente de fuga de información a nivel del MEF, para tener un único canal de comunicación tanto interno como externo.

MEF

Firmado Digitalmente por JARA HUALLPATUERO Maria Ysabel FAU 20131370645 soft
Fecha: 11/07/2022 14:11:13 COT
Motivo: Doy V° B°

4.3. MITIGACIÓN

La mitigación al incidente de la fuga de información sensible tiene los siguientes objetivos:

MEF

Firmado Digitalmente por RAMOS PARADA Doris FAU 20131370645 soft
Fecha: 30/06/2022 20:56:51 COT
Motivo: Doy V° B°

a) Reducir la brecha de seguridad afectada.

b) Evitar que se sigan produciendo nuevas fugas de información.

La mitigación al incidente de la fuga de información sensible implica las siguientes actividades:

a) Restablecer las acciones del MEF que hayan sido afectadas por la fuga de información en el menor tiempo posible.

b) Reforzar o acortar (temporalmente) todas las acciones tecnológicas contenidas en la infraestructura DLP (Protección de fuga de datos), hasta que esté controlado la fuga de información.

c) Establecer coordinación de comunicación con los órganos correspondientes para tomar las medidas preventivas o correctivas que ayuden a prevenir que ocurran nuevos incidentes.

d) Establecer contactos con los afectados para ser informados del incidente y de las acciones de mitigación que se viene realizando.

5. Etapa: **SEGUIMIENTO**

El grupo de trabajo especializado realiza el seguimiento de todas las acciones contenidas en el Plan de Emergencia y es el medio entre los actores que trabajan directamente con la mitigación y las altas autoridades del MEF, para evaluar el avance de las acciones de mitigación que se vienen realizando.

En la medida que se viene ejecutando el Plan de Emergencia ante el incidente de fuga de información sensible, el grupo de trabajo especializado debe realizar las siguientes acciones:

a) Evaluar permanentemente el resultado y la efectividad de las acciones realizadas, teniendo en cuenta en todo momento, las consecuencias y el impacto.

b) Informar del avance del plan a los funcionarios de la Alta Dirección del MEF afectados por la fuga de la información sensible.

c) Viabilizar obligatoriamente las acciones y proponer los efectos presupuestarios para que las actividades mitigadoras puedan llevarse a cabo de forma inmediata.

d) Realizar las acciones de estabilización del incidente, empezando por la evaluación y valoración global del mismo mediante un peritaje más completo que permitirá efectuar e implementar medidas técnicas, operativas y legales para evitar nuevas fugas de información sensible y restablecer el normal funcionamiento de los servicios e infraestructura que hubieran sido afectadas.

MEF

Firmado Digitalmente por JARA HUALLPATUERO Maria Ysabel FAU 20131370645 soft
Fecha: 11/07/2022 14:11:18 COT
Motivo: Doy V° B°

MEF

Firmado Digitalmente por RAMOS PARADA Doris FAU 20131370645 soft
Fecha: 30/06/2022 20:56:58 COT
Motivo: Doy V° B°

/OGTI