

**MINISTERIO DE ECONOMÍA Y FINANZAS
POLÍTICAS DE SEGURIDAD INFORMÁTICA
POLITICA DE CLASIFICACION DE LA INFORMACION**

PROPÓSITO

Este documento cubre la identificación, clasificación, etiquetado y responsables de los activos de información asociados a los procesos organizacionales que hacen uso los funcionarios del MEF, terceros operando en función del MEF.

OBJETIVOS

- a. Definir la información sensible para el Ministerio de Economía y Finanzas.
- b. Identificar y clasificar los activos de información según su criticidad en términos de confidencialidad, integridad y disponibilidad.
- c. Etiquetar los activos de información del MEF.
- d. Conocer quiénes son los dueños y administradores de los activos de información.
- e. Servir de insumo para el análisis del riesgo informático a partir de este inventario.

ALCANCE

Para todo el personal del MEF y los proveedores que presten servicios a este organismo que estén directa o indirectamente relacionados con activos de información de alta o mediana criticidad.

DIRECTRICES

Se entiende por información sensible para el MEF lo siguiente:

- a. Cualquier información que su divulgación, publicidad, comunicación o conocimiento pueda afectar, los derechos de las personas (salud, seguridad, privacidad o derechos de carácter comercial o económico), la seguridad de La Nación (defensa nacional o mantener el orden público o seguridad pública) o el interés Nacional (salud pública, relaciones internacionales o intereses económicos o comerciales del país).
- b. Todos los activos de información asociados a los procesos de negocio, deben ser identificados y estar registrados en el Inventario de activos de Información.
- c. La información del MEF o terceros dependientes, deben ser clasificados en una de las tres categorías siguientes: información confidencial, información de acceso restringido e información pública o de acceso libre, de conformidad a la Ley 6 de 22 de enero del 2002, que dicta normas para la transparencia en la gestión pública.
- d. Todos los activos de información deben tener identificado un Propietario o Responsable, ya sea a través del cargo, rol, o nombre particular. Dentro de sus responsabilidades está instruir o actualizar el inventario de activos de información, controlar quién o quienes deben tener acceso, la modificación de los accesos y la autorización para la divulgación.
- e. Todos los activos registrados en el Inventario de activos de Información asociados a los procesos de negocio, deben tener una Valorización de Criticidad basada en el nivel de resguardo que deben tenerse en relación a la integridad, disponibilidad y confidencialidad de estos activos.
- f. Todos los activos de Información tienen que estar debidamente etiquetados:
 1. Todos los activos de información asociados a los procesos institucionales (cuando corresponda), deben estar debidamente identificados por el nombre o identificador y su clasificación.
 2. La información del etiquetado debe ser realizada independiente del medio físico de manejo. El Propietario es el responsable del etiquetado de la información.

Código:	SI-PLT-05-2015	Elaborado por:	Fecha:	Página
Versión:	3.0	DTI – Departamento de Seguridad de Sistemas Informáticos	Marzo 2018	1 de 4

**MINISTERIO DE ECONOMÍA Y FINANZAS
POLÍTICAS DE SEGURIDAD INFORMÁTICA
POLITICA DE CLASIFICACION DE LA INFORMACION**

- g. Los funcionarios que hagan uso de la información sensible deben cumplir y haber firmado los acuerdos de no divulgación de la información o acuerdos de confidencialidad.
- h. Toda solicitud de información acerca de las operaciones del MEF deberá ser remitida al Comité Operativo de Seguridad de la Información, sin incluir la información de uso público.
- i. Las actividades que requieran acceso a la información sensible solo podrán ser realizadas por funcionarios autorizados por el Comité Operativo de Seguridad de la Información a menos que el Propietario así lo autorice, para casos calificados y puntuales.
- j. En las reuniones donde se trate información sensitiva de uso interno, sólo podrán asistir las personas que hayan sido previamente invitadas, las que en todo caso deberán ser validadas por el Propietario.
- k. Si se divulga oralmente información sensitiva de uso interno en una reunión, el expositor deberá exponer la clasificación de la información y exigir discreción, y eliminar cualquier información usada en la reunión.
- l. El copiado o reproducción de los activos de Información sean estos independientes del medio (papel, electrónico, etc.) deben aplicar las mismas políticas y normas de seguridad definidas para los activos de información originales.
- m. La eliminación o destrucción de los activos de Información sean estos independientes del medio (papel, electrónico, etc.), deberá efectuarse de acuerdo a las normativas vigentes.
- n. El traslado de los activos de Información, debe efectuarse aplicando medidas de control acordes con la clasificación del activo y el impacto del proceso relacionado.

RESPONSABILIDADES

Propietario de la información.

- Clasificar la información, de acuerdo al esquema de clasificación definido en este documento.
- Autorizar la divulgación de la información y cambios en los controles respectivos.
- Instruir o actualizar el inventario de activos de información y controlar quién o quienes deben tener acceso a los activos de información a su cargo.

Representante del Comité de Seguridad de la Información.

- Designar los propietarios de la información.
- Verificar junto con informática los controles adecuados para garantizar la confidencialidad, integridad y disponibilidad del activo de información.
- Tomar el inventario como insumo para realizar el análisis de riesgo informático correspondiente.

Departamento de Seguridad de Sistemas Informáticos.

- Implantar e implementar de manera coordinada con los propietarios de la información los controles a aplicar.
- Definir las herramientas respectivas en conjunto con el representante asignado de Seguridad de la Información y explicar su uso a los propietarios de los activos de información.

Código:	SI-PLT-05-2015	Elaborado por:	Fecha:	Página
Versión:	3.0	DTI – Departamento de Seguridad de Sistemas Informáticos	Marzo 2018	2 de 4

**MINISTERIO DE ECONOMÍA Y FINANZAS
POLÍTICAS DE SEGURIDAD INFORMÁTICA
POLITICA DE CLASIFICACION DE LA INFORMACION**

Unidades Informáticas del MEF

- Hacer cumplir en sus áreas todas las políticas, normas y controles que el Comité de Seguridad Informática establezca.

Dirección de Auditoría y Fiscalización Interna

- Revisar las normas, políticas, procedimientos y controles que el Comité presente respecto a esta política y recomendar cambios y adecuaciones según las normas y estándares vigentes.

Oficina Institucional de Recursos Humanos

- Notificará la existencia de esta las políticas de seguridad informática a todos los funcionarios de la Institución.
- Aplicará las sanciones que, de acuerdo con el Reglamento Interno del MEF y el Código Uniforme de Ética de los Servidores Públicos, corresponda a aquellos funcionarios que incumplan esta política.

Directores y Jefes de Unidades del MEF

- Comunicarán esta política y todas aquellas que el Comité apruebe entre los funcionarios de sus unidades administrativas.

Usuarios

- Cumplirán las normas, políticas, directrices, procedimientos y controles que el Comité establezca.
- Reportarán a los Directores y Jefes de unidades del MEF, cualquier anomalía posible y que pueda convertirse en una vulnerabilidad o contravenga esta política.

Código:	SI-PLT-05-2015	Elaborado por:	Fecha:	Página
Versión:	3.0	DTI – Departamento de Seguridad de Sistemas Informáticos	Marzo 2018	3 de 4

**MINISTERIO DE ECONOMÍA Y FINANZAS
POLÍTICAS DE SEGURIDAD INFORMÁTICA
POLITICA DE CLASIFICACION DE LA INFORMACION**

HISTORIAL DE REVISIONES Y MODIFICACIONES

Actualizado / Revisado Por:

	Nombre	Cargo	Firma
Actualizado por	Zulma M. de Rivera	Jefe del Departamento de Seguridad de Sistemas	

Histórico de Revisiones

Listas de Cambios		
Fecha de Revisión	Cambios Realizados	Versión
Mayo/2015	Reunión: Revisión de Contenido y Redacción	1.0
Dic/2015	Correcciones Contenido y redacción	2.0
Mayo/2016	Correcciones de contenido y redacción / Inclusión de diagrama de autorizaciones	3.0
Agosto/2016	Reordenamiento de numeración de las políticas	3.0
Marzo 2018	Resolución MEF-RES-2018-629	3.0

Flujo de Aprobación

Aprobado por		
Nombre	Cargo	Firma
Zulma de Rivera	Jefe del Departamento de Seguridad de Sistemas	
Jorge Ramos	Subdirector de Tecnología e Informática	
Robin Arjona	Director de Tecnología e Informática	

Distribuido / Publicado Por:

Nombre	Medio	Fecha Publicación	Versión
Departamento de Seguridad de Sistemas Informáticos	Documento impreso / Intranet / Política General de Seguridad /	Abril 2018	3.0

Clasificación:

Confidencial

Código:	SI-PLT-05-2015	Elaborado por:	Fecha:	Página
Versión:	3.0	DTI – Departamento de Seguridad de Sistemas Informáticos	Marzo 2018	4 de 4