Dirección Administración y Finanzas
GAC /MBV /XGM
E11965/2015

MINISTERIO DE HACIENDA
29 DIC 2015
TOTALMENTE TRAMITADO
DOCUMENTO OFICIAL

ACTUALIZA Y ESTABLECE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA SECRETARIA Y ADMINISTRACIÓN GENERAL DEL MINISTERIO DE HACIENDA Y DEJA SIN EFECTO RESOLUCIÓN EXENTA N° 1504 DE 08.11.2012

RESOLUCIÓN EXENTA Nº 461

SANTIAGO, 24 DICIEMBRE 2015

VISTOS:

En lo dispuesto en la Ley N° 19.880 que establece Bases de los Procedimientos Administrativos; la Ley N° 19.799, sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma; la Ley N° 19.223, que tipifica figuras penales relativas a la informática; la Ley N° 20.285 sobre Acceso a la Información Pública; el Decreto Supremo N° 83, del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los Órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos, de 2004; Res. Ex. 1504, de 08 de Nov de 2012, que Establece Política de Seguridad de los activos de Información Institucional de la Secretaría y Administración General del Ministerio de Hacienda.

CONSIDERANDO:

La conveniencia de actualizar la Política de Seguridad de la Información Institucional, que en función del marco legal y tecnológico, proporcione a la Secretaría y Administración General del Ministerio de Hacienda la dirección y soporte para la Seguridad de la Información, en concordancia con las necesidades del Servicio, las leyes y regulaciones correspondientes.

RESUELVO:

APRUÉBESE la Política de Seguridad de la Información de la Secretaría y Administración General del Ministerio de Hacienda.

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

DE LA SECRETARÍA Y ADMINISTRACIÓN GENERAL DEL MINISTERIO DE HACIENDA

I. DECLARACION INSTITUCIONAL

La Secretaría y Administración General del Ministerio de Hacienda considera la Seguridad de la Información Institucional como una actividad prioritaria dentro de la organización y declara el interés y compromiso en apoyar el fomento y desarrollo del Sistema de Gestión de Seguridad de la Información Institucional.

1. Objetivo General de la Política de Seguridad de la Información

El objetivo central es proteger los activos de información de la Secretaría y Administración General del Ministerio de Hacienda, que permita lograr niveles adecuados de **integridad** (asegurando que la información y sus métodos de proceso son exactos y completos), **confidencialidad** (asegurando que sólo quienes estén autorizados pueden acceder a la información) y **disponibilidad** (asegurando que los usuarios autorizados tengan acceso a la información y a sus activos asociados cuando lo requieran) para todos los activos de información institucional considerados relevantes, de manera tal que se asegure la continuidad operacional de los procesos institucionales y la entrega de productos y servicios a los usuarios.

Para lograr este objetivo, se gestionarán los recursos que permiten una adecuada implementación de un sistema de seguridad de información (SGSI).

La información es un activo primordial para la actividad de una organización por lo que es necesario protegerla de manera adecuada. La información se puede almacenar de manera digital, en forma material (papel) o en forma de conocimiento de los integrantes de la institución, por cuanto se debe procurar que cada uno de esos soportes cumpla a cabalidad con el resguardo de la información.

Adicionalmente, los riesgos asociados a la seguridad de la información de una organización se necesitan abordar para contribuir a la continuidad en la prestación de los servicios ofrecidos a la ciudadanía.

2. Alcance e importancia

Esta Política se aplica a los activos de información de los procesos identificados en el Inventario de Activos de Información de la Secretaría y Administración General del Ministerio de Hacienda y su importancia radica en asegurar la integridad, confidencialidad y disponibilidad de los activos de información necesarios para permitir la continuidad del negocio.

3. Responsabilidad

Todos los funcionarios incluyendo a autoridades o personal, no importando su escalafón y sea cual fuere su nivel jerárquico, son responsables de la implementación de esta Política General de Seguridad de los activos de Información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha Política por parte de su equipo de trabajo.

La Política General de Seguridad de los activos de información es de aplicación obligatoria para todos los funcionarios independiente del área actual de desempeño.

La máxima autoridad de la Subsecretaría aprueba esta Política y es responsable de aprobar futuras modificaciones y validar el proceso de gestión de Seguridad de la Información, además debe aprobar las estrategias y mecanismos de control para el tratamiento de riesgos que afecten a los activos de información institucionales, que se generen como resultado de los reportes o propuestas del comité de seguridad de la información, así como los recursos necesarios para su ejecución.

4. Aprobación de la Política

La Política General de Seguridad de la Información se aprueba mediante resolución exenta del Jefe de Servicio, en consideración a propuesta del Comité de Seguridad de la Información. De igual manera, cada modificación realizada a la Política deberá ser aprobada por el Jefe de Servicio o Subsecretario de Hacienda.

5. Difusión de las Políticas

La política será difundida a todos(as) los(as) funcionarios(as) a través de su publicación en la Intranet Institucional; también a través del envío de mail a todos(as) los(as) funcionarios(as) y partes externas pertinentes.

6. Revisión de las Políticas

Se debe mantener la Política General de Seguridad de los activos de Información actualizada, a efectos de asegurar su vigencia, conveniencia, suficiencia y nivel de eficacia continua.

Se deben revisar las políticas de seguridad de la información a intervalos planificados, o si se producen cambios significativos, para asegurar su conveniencia, suficiencia y eficacia continúa.

La Política General de Seguridad de la Información se revisará cada 3 años y se reevaluará su cumplimiento también cada 3 años.

II RIESGOS DE ACUERDO A LA NORMATIVA VIGENTE EN LA INSTITUCIÓN

La gestión de riesgos en materia de Seguridad de los activos de información es realizada conforme lo establecido por la Política de Gestión de Riesgos del Servicio y en base a la metodología de Gestión de Riesgos dispuesta por el Consejo de Auditoría Interna General de Gobierno (CAIGG).

III DOMINIOS CONSIDERADOS EN BASE A LA NORMA Nch-ISO 27001:2013.:

Esta Política se conforma de una serie de pautas sobre aspectos específicos de la Seguridad de los activos de Información y define el marco para fijar objetivos de control y controles definidos en procedimientos y políticas del sistema de Seguridad de la Información de la Secretaría y Administración General del Ministerio de Hacienda, que incluyen los siguientes tópicos:

1. Política de Seguridad de la Información
La finalidad de este dominio es establecer un marco de trabajo de la dirección para controlar la implementación y funcionamiento de la seguridad de la información dentro de la organización.

2. Organización de la Seguridad de la Información
Este Tópico consiste en establecer un marco de trabajo de la dirección para controlar la implementación y funcionamiento de la seguridad de la información dentro de la organización y fuera de ésta.

3. Seguridad ligada a los recursos humanos
El objetivo de este dominio es asegurar que los empleados y contratistas entiendan sus responsabilidades, y que sean aptos para los roles que están siendo considerados; por otra parte este tópico busca asegurar que los empleados y contratistas cumplan con sus responsabilidades de seguridad de la información.

4. Administración de Activos
Este dominio consiste en identificar los activos de información de la organización y definir las responsabilidades de protección pertinentes, una vez identificados dichos activos se deben clasificar asegurando que la información reciba el nivel adecuado de protección, según su importancia para la organización, previniendo la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los medios.

5. Control de acceso
Este dominio pretende restringir el acceso a la información y a las instalaciones de procesamiento de la información, asegurando el acceso de usuarios autorizados y evitando el acceso sin autorización a los sistemas, aplicaciones y servicios. Además busca concientizar a los usuarios de su responsabilidad frente al cuidado de su información de autenticación.

6. Criptografía
La finalidad de este dominio es asegurar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad o integridad de la información.

7. Seguridad física y del ambiente
Lo que busca este tópico es evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones de procesamiento de la información y de la información misma de la organización, previniendo pérdidas, daños, hurtos o el compromiso de los activos, así como la interrupción de las actividades de la organización.

8. Seguridad de las operaciones
Este dominio tiene como finalidad la operación correcta y segura de las instalaciones de procesamiento de la información (definir), además debe asegurar que las instalaciones de procesamiento de la información estén protegidas contra código malicioso. Por otra parte busca protección contra pérdida de datos, y generación de evidencia y registro de eventos. Además asegura la integridad de los sistemas operacionales evitando la explotación de las vulnerabilidades técnicas. Finalmente minimiza el impacto de las actividades de auditoría en los sistemas operacionales

9. Seguridad de las comunicaciones
Este domino consiste en establecer y asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo, además de mantener la seguridad de la información transferida dentro de una organización y con cualquier otra entidad externa.

10. Adquisición, desarrollo y mantenimiento del sistema
El objetivo de este dominio es asegurar que la seguridad de la información sea parte integral de los sistemas de información en todo el ciclo. Esto también incluye los requisitos para los sistemas de información que proporcionan servicios de las redes públicas, asegurar que la seguridad de la información está diseñada e implementada dentro del ciclo de desarrollo de los sistemas de información y asegurar la protección de los datos usados para prueba.

11. Relaciones con el proveedor
La finalidad de este dominio es asegurar la protección de los activos de la organización a los que tienen acceso los proveedores, manteniendo un nivel acordado de la seguridad de la información y entrega del servicio en línea con los acuerdos del proveedor.

12. Gestión de incidentes de seguridad de la información
Este dominio pretende asegurar un enfoque consistente y eficaz sobre la gestión de los incidentes de seguridad de la información incluida la comunicación sobre eventos de seguridad y debilidades.

13. Aspectos de seguridad de la información en la gestión de la continuidad del negocio de la organización
Esto tópico incorpora la continuidad de la seguridad de la información en los sistemas de gestión de continuidad de negocio de la organización, asegurando la disponibilidad de las instalaciones de procesamiento de información.

14. Cumplimiento
El dominio tiene por objetivo evitar el incumplimiento de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas con la seguridad de la información y todos los requisitos de seguridad. Además busca asegurar que la seguridad de la información se implemente y funcione de acuerdo a las políticas y procedimientos de la organización.

IV. ROLES DE LA SEGURIDAD DE LA INFORMACIÓN

• Encargado de Seguridad de la Información: tendrá toda la responsabilidad del desarrollo e implementación de las Políticas de Seguridad de la Información, formar parte del grupo tecnológico en la identificación de los controles y asesorar en materia de seguridad de la información a las autoridades y al Comité de Seguridad de los activos de Información. Será la persona que coordine el equipo que trabajará la seguridad de la información en el resto de las dependencias de la Subsecretaría de Hacienda.
La especificidad de sus funciones es declarada bajo resolución exenta N° 456 del 21 de Diciembre de 2015.

• Comité de Seguridad de la Información: es un cuerpo integrado por representantes de las diferentes áreas, destinado a asegurar la implantación del Sistema de Seguridad de la Información. Sus funciones principales son proponer, impulsar, promover, aprobar y revisar cada dos años las políticas de seguridad de la información, así como supervisar el desarrollo del Plan de Seguridad de la Información.
La segregación de las funciones y responsabilidades de cada miembro del comité están dictadas bajo resolución exenta N° 455 del 21 de Diciembre de 2015.

Otras Responsabilidades en especial sobre los Activos de Información:

Propietarios de la información:
El propietario de la información es el dueño del proceso que utiliza o genera dicha información y debe autorizar el acceso a esta, la designación de los dueños de la información, es realizada por el Comité de Seguridad de la Información.

Usuarios de la información:
El usuario de la información, es aquella persona, funcionario o proveedor, que con la debida autorización introduce, borra, cambia o lee información de la Institución. El propietario puede ser también usuario y por tanto estar sujeto a las mismas responsabilidades que éste.

Los usuarios sólo deben tener acceso a la información a la que están autorizados para ver o procesar, por tanto, a las autorizaciones que se otorguen deben limitar su capacidad, de forma que no puedan realizar actividades distintas de aquellas para las que se otorgó el permiso.

Custodios de la información:
Se denominan custodios de la información, al funcionario, departamento o proveedor, que recibe la responsabilidad de materializar las definiciones y disposiciones realizadas por el propietario de la información. Normalmente, los custodios no necesitan la información para la realización de su trabajo, sino sólo se limitan a procesarla, gestionar su almacenamiento y hacerla accesible.

El Departamento de Informática es el principal custodio de la información existente en soporte informático. En los casos de información que se gestione en forma de papel o digital, que no esté afecta a la gestión del Departamento de Informática, será responsable de custodiarla cada área propietaria de la misma.

Personal externo a la Institución:
La política de externalización de servicios que el MINISTERIO DE HACIENDA emita, debe incluir las cláusulas correspondientes por la que los proveedores de servicios se obligan a cumplir los requerimientos de la Política de Seguridad de la Información, normativas, estándares y procedimientos de la Institución. De esta forma, cualquier incumplimiento por su parte en este sentido, deberá permitir al amparo del contrato, tomar las medidas legales que se consideren oportunas. Esto se aplicará en el dominio Seguridad en las Relaciones con los Proveedores, el cual contendrá normativas y manuales de procedimientos que velarán por la correcta ejecución de los controles de seguridad definidos.

Responsabilidades del Departamento de Informática:
El Departamento de Informática, es responsable de velar por la seguridad física y lógica de las instalaciones en donde se localice el procesamiento centralizado de la información, y contar con las herramientas, sistemas y procedimientos que garanticen que tanto las instalaciones, los aplicativos como los archivos de datos tengan la protección adecuada que permita mantener razonablemente la integridad, confidencialidad y disponibilidad de los datos de la organización y sus usuarios.

V. INCUMPLIMIENTO

En caso de no cumplimiento de la presente Política de Seguridad de la Información y todas las normativas y manuales de procedimientos asociados, será reportado al Comité de Seguridad de la Información, por parte del Encargado de Seguridad de la Información, para que tome conocimiento y disponga las acciones correspondientes, de considerarlo necesario.

VI. GLOSARIO DE TERMINOS

Riesgo:
Posibilidad de que una amenaza pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Activos de Información
Los activos de información corresponden a todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución.

Seguridad de la Información
Preservación de la confidencialidad, integridad y disponibilidad de la información.

Confidencialidad: Propiedad de que la información no se pone a disposición o no es relevada a individuos, entidades o procesos no autorizados.

Integridad: se salvaguarda la precisión y exhaustividad de la información y los métodos de procesamiento.

Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

CONTROL DE VERSIONES

REVISIONES DEL DOCUMENTO DE POLITICA				
Nº Revisión	**Fecha Aprobación**	**Motivo de la revisión**	**Páginas Modificadas**	**Autor**
1	28/03/2011	Elaboración inicial	Todas	Miguel Ávila
2	19/05/2011	Dar cumplimiento a los requisitos técnicos de Sistema de Seguridad de la Información y a las observaciones recibidas	Todas	Macarena Jara
3	08/11/2012	Dar cumplimiento a los requerimientos de validación PMG 2012 y a las observaciones recibidas en el período	Todas	Macarena Jara
4	24/12/2015	Revisión y actualización de la Política de Seguridad de la Información, acorde con la Norma ISO 27.001/2013	Todas	Ximena Gutiérrez

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE

ALEJANDRO MICCO AGUAYO
SUBSECRETARIO DE HACIENDA