APRUEBA POLÍTICA DE GESTIÓN DE OPERACIONES DEL MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA.

RESOLUCIÓN EXENTA Nº 312 /

SANTIAGO, 30 ABR 2021

V I S T O S:

La Ley Nº 18.993, que crea este Ministerio; el Decreto Supremo Nº 7, de 1991, de esta Secretaría de Estado, que aprueba su Reglamento Orgánico; el Decreto con Fuerza de Ley Nº 1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la Ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; el Decreto con Fuerza de Ley Nº 29, de 2004, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la Ley Nº 18.834, sobre Estatuto Administrativo; el Decreto Supremo Nº 83, de 2004, 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; la Resolución Exenta Nº 785, de 2020, de este origen, que aprueba la Política General de Seguridad de la Información del Ministerio Secretaría General de la Presidencia; el Decreto Supremo Nº 2, de 2021, de esta Secretaría de Estado, que designa al Subsecretario General de la Presidencia; y la Resolución Nº 7, de 2019, de la Contraloría General de la República, que fija normas sobre exención del trámite de toma de razón.

C O N S I D E R A N D O:

1. Que, según la Ley Nº 18.993, que crea el Ministerio Secretaría General de la Presidencia, establece que dicha Secretaría de Estado, estará encargada de realizar funciones de coordinación y de asesoría directa al Presidente de la República, al Ministerio del Interior y Seguridad Pública y a cada uno de los Ministros, especialmente en materias políticas, jurídicas y administrativas, referentes a las relaciones del Gobierno con el Congreso Nacional, los Partidos Políticos y otras organizaciones sociales e instituciones de la vida nacional, así como propender al logro de una efectiva coordinación programática general de la gestión de gobierno.

2. Que, lo indicado precedentemente implica la generación, envío, recepción, almacenamiento y distribución de multiples y diversos activos de información que demandan requisitos de seguridad apropiados para garantizar los atributos esenciales de confidencialidad, integridad y disponibilidad de la misma.

3. Que, en relación con lo anterior, mediante Resolución Exenta Nº 785, de 20 de noviembre de 2020, se aprobó la Política General de Seguridad de la Información de este Ministerio, estableciendo los lineamientos generales de implementación del Sistema de Gestión de Seguridad de la Información, con el objeto de resguardar la seguridad de los activos de información de propiedad de esta Secretaría de Estado.

4. Que, en concordancia con lo expuesto, es preciso definir las directrices necesarias para gestionar los procedimientos operativos documentados, los controles en la instalación de software de los sistemas operacionales y la forma en que se gestionan las vulnerabilidades técnicas dentro de la institución.

5. Que, de acuerdo con lo indicado, el presente acto administrativo viene en aprobar la Política de Gestión de Operaciones del Ministerio Secretaría General de la Presidencia.

R E S U E L V O:

ARTÍCULO ÚNICO.- APRUÉBASE la Política de Gestión de Operaciones del Ministerio Secretaría General de la Presidencia, cuyo texto es el siguiente:

POLÍTICA DE GESTIÓN DE OPERACIONES

DEL

MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA

Controles NCH ISO 27001:2013 Relacionados

CONTROL	NOMBRE
A.12.01.01	Procedimiento de operación documentados
A.12.01.02	Gestión de cambios
A.12.01.03	Gestión de la capacidad
A.12.04.01	Registro de evento
A.12.04.02	Protección de la información de registros
A.12.04.03	Registro del administrador y el operador
A.12.05.01	Instalación del software en sistemas operacionales
A.12.06.01	Gestión de las vulnerabilidades técnicas

2021

1. Introducción

El Ministerio Secretaría General de la Presidencia dispone del presente documento, "Política de Gestión de Operaciones", como parte integrante del sistema de seguridad de la información. En específico, se enmarca en el cumplimiento de la NCH ISO 27001-2013, que propone como requisito de control:

Control A.12.01.01 Procedimiento de operación documentados

"Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que lo necesiten".

- Requisito de control A.12.01.01 NCH ISO 27001-2013

Control A.12.01.02 Gestión de cambios

"Se deben controlar los cambios a la organización, procesos del negocio, instalaciones de procesamiento de información y los sistemas que afecten la seguridad de la información".

- Requisito de control A.12.01.02 NCH ISO 27001-2013

Control A.12.01.03 Gestión de la capacidad

"Se debe supervisar y adaptar el uso de los recursos, y se deben hacer proyecciones de los futuros requisitos de la capacidad para asegurar el desempeño requerido del sistema".

- Requisito de control A.12.01.03 NCH ISO 27001-2013

Control A.12.04.01 Registro de evento

"Se deben generar, mantener y revisar con regularidad los registros de eventos de las actividades del usuario, excepciones, faltas y eventos de seguridad de la información".

- Requisito de control A.12.04.01 NCH ISO 27001-2013

Control A.12.04.02 Protección del registro de información

"Las instalaciones de registros y la información de registro deberían estar protegidas contra la adulteración y el acceso no autorizado".

- Requisito de control A.12.04.02 NCH ISO 27001-2013

Control A.12.04.03 Registros del administrador y el operador

"Se deben registrar las actividades del operador y del administrador del sistema, los registros se deben proteger y revisar con regularidad".

- Requisito de control A.12.04.03 NCH ISO 27001-2013

Control A.12.05.01 Instalación del software en sistemas operacionales

"Se deben implementar los procedimientos para controlar la instalación de software en los sistemas operacionales".

- Requisito de control A.12.05.01 NCH ISO 27001-2013

Control A.12.06.01 Gestión de las vulnerabilidades técnicas

"Se debe obtener la información acerca de las vulnerabilidades técnicas de los sistemas de información usados de manera oportuna, evaluar la exposición de la organización a estas vulnerabilidades y se deben tomar las medidas apropiadas para abordar el riesgo asociado".

2. Alcance.

El presente instrumento será aplicado a los funcionarios/as y colaboradores/as del Ministerio, independiente de su modalidad de contratación, en adelante "el personal".

3. Objetivo.

El objetivo de esta política es definir las directrices necesarias para gestionar las operaciones relacionadas a la Unidad de Tecnologías de la Información y otras áreas relacionadas, generando procedimientos operativos documentados, llevando una gestión de los cambios y de la capacidad, del registro de eventos, del administrador y operador y del aseguramiento del respaldo de esta información para futuras auditorías, además de controlar la instalación de *softwares* en sistemas operacionales y la forma en que se gestionan las vulnerabilidades técnicas dentro de la institución.

4. Roles y responsabilidades.

Independiente del cargo/rol que se desempeñe, del nivel jerárquico del que se goce y de la modalidad bajo la cual se esté contratado, es responsabilidad de todo el personal de este Ministerio conocer y llevar a cabo el debido cumplimiento de esta política. Asimismo, es responsabilidad:

- **De los Jefes/as de División, Comisión, Unidad**, dar a conocer la presente Política en sus dependencias, así como, dar cumplimiento a la misma.
- **Del Jefe UTI (Jefe de la Oficina de Computación, también "Unidad de Tecnología de la Información"),** mantener la documentación de las actividades operacionales y los cambios realizados, además de mantener los sistemas con la capacidad necesaria para el buen funcionamiento de los equipos y el resguardo de la información del Ministerio.
- **Del Encargado de Seguridad de la Información,** velar por el debido cumplimiento y apego de este documento en los usuarios del Ministerio, así como realizar revisiones periódicas a dicho cumplimiento.

5. Mecanismo de difusión.

Es responsabilidad del Comité de Seguridad de la Información, la difusión de esta Política, la que deberá ser enviada por correo electrónico a todo el personal y permanecer a disposición de todos los usuarios de este Ministerio en la Intranet institucional.

6. Evaluación y revisión.

El tiempo de evaluación y revisión estándar para este documento, será cada dos años. No obstante, podrá revisarse cuando la situación lo amerite o la autoridad lo disponga.

El Encargado de Seguridad de la Información informará en sesión del Comité de Seguridad de la Información los cambios y/o actualizaciones de esta política, la que deberá ser revisada, observada y aprobada por el Comité de Seguridad de la Información.

7. Definiciones.

- **Control A.12.01.01 Procedimientos de operación documentados.**

  Deberán existir procedimientos de operación documentados, con el fin de mantener la continuidad operativa, aplicable en la ausencia de un miembro que influye en la operatividad del proceso o actividad, en caso de emergencia o como lineamiento interno de la institución.

  Esta documentación deberá definir roles y responsabilidades, estar a disposición de los usuarios del área relacionada, contener un alcance, definición y una sección que detalle el procedimiento e instrucciones para la ejecución de cada operación:

  - Instalación y configuración de los sistemas.
  - Procesamiento y manipulación de la información tanto automática como manual.
  - Requisitos de programación incluyendo las interdependencias con otros sistemas, las horas de inicio del trabajo más temprano y de finalización del trabajo más tardía.
  - Reinicio del sistema y recuperación en caso de fallas.
  - Instrucciones para el manejo de errores u otras condiciones excepcionales, los que pueden surgir durante la ejecución del trabajo.
  - Contactos de apoyo y escalamiento, incluidos los contactos de soporte externos en el caso de presentarse dificultades operativas o técnicas inesperadas.
  - Administración del seguimiento de auditoría y de la información de registro del sistema.
  - Monitoreo.

  Los procedimientos de operación documentados para cualquier actividad del sistema deberán tratarse como documentos formales y cualquier cambio deberá ser autorizado por el Jefe de la Unidad de Tecnología de la Información.

- **Control A.12.01.02 Gestión de cambios.**

  Se deberán controlar los cambios que se realicen en la institución en relación a las instalaciones de procesamiento de información y los sistemas que afectan a la seguridad de la información.

  Los cambios aplicados deberán ser planificados, registrados y comunicados en caso de que se requiera a todas las personas pertinentes. Se deberá realizar una evaluación de los posibles impactos, incluidos los impactos de seguridad de dichos cambios, pruebas de cambios, procedimientos de retroceso, responsabilidades para abortar y recuperar los cambios incorrectos y eventos inesperados.

  Se deberán establecer las responsabilidades y procedimientos formales para garantizar el control satisfactorio de todos los cambios.

- **Control A.12.01.03 Gestión de la capacidad.**

  Se deberá asegurar que la capacidad de la infraestructura de tecnología esté acorde con las necesidades de la institución.

La Unidad de tecnología de la Información deberá asegurar que los servicios y recursos estén respaldados por una capacidad de procesamiento y almacenamiento asegurando que los usuarios puedan efectuar sus tareas conforme a las necesidades propias del cargo.

Se deberá monitorear el uso de los recursos y hacer una planificación de los requerimientos de capacidad, identificando dichos requerimientos de las actividades las que pueden ser nuevas o en proceso, aplicando un monitoreo al sistema para asegurar la disponibilidad y eficiencia de los sistemas, estableciendo controles para identificar los problemas de forma oportuna.

La Unidad de Tecnología de la Información deberá monitorear la utilización de recursos claves de las plataformas que administra. Para ellos podrá hacer uso de herramientas que permitan analizar la capacidad de rendimiento y almacenamiento.

Se deberá identificar potenciales deficiencias en la capacidad de almacenamiento. De ser necesario se deberán eliminar datos que estén obsoletos para dar espacio en los discos o bien migrar a otros ambientes de respaldo de información de forma segura.

- **Control A.12.04.01 Registro de evento.**

La Unidad de Tecnología de la Información deberá llevar un registro de los usuarios y sus desarrollos internos por cada evento / logs. Estos registros deberán monitorear periódicamente los sistemas y equipos para así, detectar o localizar fallas, mal funcionamiento, errores, entre otros, los que puedan generar alertas de la información contenida en la plataforma del Ministerio.

A través de los actos registrados se obtendrá información crítica del funcionamiento de los activos de información como, conexión de las redes, ejecución de los sistemas y de las aplicaciones, cambio en la configuración de los sistemas, alteraciones en los permisos de acceso, funcionamiento irregular de aplicativos, límites de uso en capacidades de discos, memoria, ancho de banda de red y actividades detectadas por los sistemas de antivirus.

El registro de evento deberá incluir información útil como identificador de usuario, identificador de dispositivos (IP, MAC ADDRESS y / o cualquier otro dato de identificación), fecha y hora en que ocurre el suceso.

- **Control A.12.04.02 Protección del registro de información.**

La Unidad de Tecnología de la Información deberá disponer de un repositorio para el almacenamiento de los registros de información del cortafuego Institucional, el cual se deberá encontrar en un ambiente separado y escalable. Los registros de información de cortafuego deberán ser copiados y almacenados de forma automática en este ambiente y se deberá contar con registros históricos de hasta 6 años.

Deberá existir una herramienta de auditoría para poder procesar y analizar los registros de información del cortafuego. Para ello, deberán ser extraídos como una copia e incorporados en el analizador de registros de información para poder dar respuesta a posibles auditorías.

Los registros de información almacenados no podrán ser adulterados y accedidos de forma no autorizada.

Se deberá verificar de manera periódica la conectividad y capacidad de almacenamiento del repositorio en donde se almacenarán la copia de los registros del cortafuego. Se deberán realizar los ajustes de ampliación de espacio en caso de ser necesario, este no deberá ser menor al 25%.

Deberá verificarse de manera periódica la integridad de una muestra de los registros de información almacenados.

- **Control A.12.04.03 Registros del administrador y el operador.**

La Unidad de Tecnología de la Información deberá realizar una revisión periódica de los registros de las actividades del personal del Ministerio, fallas y eventos de la información. Se deberá verificar la correcta generación de logs del administrador y el operador de los sistemas y plataformas con que cuenta la institución.

- **Control A.12.05.01 Instalación del software en sistemas operacionales.**

  El Jefe de la Unidad de Tecnología de la Información deberá elaborar e implementar procedimientos para el control de la instalación y actualización de software en los sistemas operativos del Ministerio, dado que, sólo las personas autorizadas, capacitadas y especializadas podrán realizar dicha instalación y actualización.

  Se deberá contar con un registro actualizado de las licencias existentes y software autorizados de uso dentro de la institución, así como la identificación de personas que cuentan con las competencias y autorizaciones para la instalación, actualización o en su eventualidad borrado de software, se deberá tener un repositorio de software con acceso restringido, implementar auditorías del software instalados, un control que impida la copia de software y una estrategia de reversión antes de que implemente una instalación. Las versiones anteriores del software de aplicación se deberían retener como medida de contingencia. Las actualizaciones del software operacional, las aplicaciones y las bibliotecas de programas sólo la deberá realizar la Unidad de Tecnología de la Información o quien designe.

- **Control A.12.06.01 Gestión de las vulnerabilidades técnicas.**

  La Unidad de Tecnología de la Información deberá tomar las medidas adecuadas y oportunas en respuesta a la identificación de las posibles vulnerabilidades técnicas. Una vez identificada la vulnerabilidad técnica, se deberían identificar los riesgos asociados y las medidas que se deberían tomar, dichas medidas podrían involucrar la aplicación de actualizaciones correctivas a los sistemas vulnerables o la aplicación de otros controles.

  Las actualizaciones correctivas podrán ser evaluadas y probadas antes de su instalación con el fin de garantizar su eficacia y que no involucran efectos colaterales. En ausencia de actualizaciones correctivas se deberá llevar a cabo:

  - Desactivación de todos los servicios o capacidades relacionadas a la vulnerabilidad.
  - Adaptar o agregar controles de acceso.
  - Suplementar el monitoreo con el fin de detectar ataques reales.
  - Concientizar sobre la vulnerabilidad al área correspondiente e institución en caso de ser necesario.

  Se deberá llevar una auditoría para todos los procedimientos que se realizan. El proceso de vulnerabilidad técnica se debería monitorear y evaluar regularmente para poder garantizar su efectividad y eficiencia, priorizando los sistemas de alto riesgo.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE

MAXIMO PAVEZ CANTILLANO
Subsecretario General de la Presidencia

FGR/MCC/TGI/JRV/vvh
DISTRIBUCIÓN:
1. MINSEGPRES (Gabinete Subsecretario)
2. MINSEGPRES (División Jurídico-Legislativa:
   - Unidad de Asesoría Jurídica - Administrativa)
3. MINSEGPRES (División de Administración General:
   - Unidad de Tecnología de la Información)
4. MINSEGPRES (Oficina de Partes)