REF.: APRUEBA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL SERVICIO NACIONAL DEL PATRIMONIO CULTURAL Y DEJA SIN EFECTO RESOLUCIÓN EXENTA N° 1445 DE FECHA 17 DE SEPTIEMBRE DEL AÑO 2019.-

RESOLUCIÓN EXENTA N° 841

SANTIAGO, 19 DE MAYO DE 2025

VISTOS:

La Ley N°21.045 que crea el Ministerio de las Culturas, las Artes y el Patrimonio: el Decreto con Fuerza de Ley N°35, del año 2017; el D.F.L N°1, que fija el texto refundido, coordinado y sistematizado de la Ley N°15.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; Ley N°19.880 que establece las Bases de los Procedimientos Administrativos que rigen los Actos de los órganos de la Administración del Estado; Ley N°19.799, sobre documentos electrónicos, firma electrónica y la certificación de dicha firma; Ley N°19.553, concede asignación de modernización y otros beneficios; D.S. N°83. de 2004, y D.S. N°93, de 2006, ambos del Ministerio Secretaría General de la Presidencia, Decreto N°273 del 2022 del ministerio del interior y seguridad pública, sobre la obligación de reportar incidentes de ciberseguridad; Decreto N°7, de 2023, del Ministerios Secretaría General de la Presidencia, que establece norma técnica de seguridad de la información y ciberseguridad conforme a la ley°21.180; Ley N°21.459, de 2022, que Establece normas sobre delitos informáticos, Ley N°21.663, de 2024, que tiene por objeto regular la normativa general aplicable a las acciones de ciberseguridad de los organismos del Estado, Ley N°21.719, de 2024Decreto N°164, de 2023, del Ministerio del Interior y Seguridad Publica que aprueba Política Nacional de Ciberseguridad, la Ley N°19.628 sobre protección de la vida Privada, la Resolución N°1600 de 2008, de la Contraloría General de la República, que fija Normas sobre exención del trámite de toma de razón; La resolución exenta N°1686, de 2019, del Servicio Nacional del patrimonio Cultural, que aprueba la "Política General de Seguridad de la Información, versión N°11"; y

CONSIDERANDO:

1.- Que, con el objetivo de mitigar los riesgos de los activos de información y cumplir con los controles establecidos en esta materia, se han dictado una serie de normas entre las que se encuentran el Decreto Supremo N°83, de 2005, 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 y la Norma Chilena NCh-ISO 27001 que proporciona un marco de gestión de Seguridad de la Información utilizable por cualquier tipo de organización, pública o privada.

2.- Que, mediante la Resolución N°1686 del 17 de septiembre de 2019 del Servicio Nacional del Patrimonio Cultural, fue aprobada y actualizada la Política General de Seguridad de la Información en su versión N°10.

3.- Que, la política mencionada en el considerando anterior tiene como principal objetivo mitigar los riesgos en la gestión de activos de información, instaurar un marco normativo interno y entregar las directrices y recomendaciones sobre el uso de activos de información institucional, presentado en este sentido una herramienta organizacional para instruir a cada uno de los miembros de este Servicio y la importancia y sensibilidad de la información que este maneja y la información que se genera. Dicha política se entiende como un proceso continuo en el tiempo, que esta política general y especificas están basados en la norma NCH-ISO 27001, que son los requisitos fundamentales para el Sistema de Gestión de la Información, que se sustentan de acuerdo con el decreto N°83 del año 2004 del Ministerio General de la presidencia y otras normativas aplicables.

4.- Que, de acuerdo con la Política Nacional de Ciberseguridad y ley Marco de Ciberseguridad, donde determina que los servicios públicos son clasificados como esenciales, el decreto 273 del 2024 del ministerio de seguridad pública sobre la respuesta a incidentes de Ciberseguridad y la necesidad de reportar estos en plazos definidos a la Agencia Nacional de Ciberseguridad (ANCI), entregando nuevos lineamientos en esta materia.

5.- Que, de acuerdo con lo expuesto en los considerandos anteriores, por el presente acto se aprueba la actualización de la Política General de Seguridad de la Información del Servicio Nacional del Patrimonio Cultural en su versión N°11, tal como se indica en la parte resolutiva del presente acto administrativo.-

RESUELVO:

1.- APRUÉBASE, el presente documento denominado "Política General de Seguridad de la Información del servicio Nacional del Patrimonio Cultural, versión 11", de fecha 06 de mayo del 2025, cuyo texto se entiende íntegramente reproducido en este acto, formando parte integrante de esta resolución, y reemplazando íntegramente a la versión N°10 aprobada mediante resolución Exenta N°1686 del año 2019, el cual deberá comenzar a regir a partir de la total tramitación de este acto.

POLÍTICA GENERAL DE SEGURIDAD

DE LA INFORMACIÓN

DEL

SERVICIO NACIONAL DEL PATRIMONIO CULTURAL

1. INTRODUCCIÓN

El Servicio Nacional del Patrimonio Cultural, es un servicio público descentralizado, con personalidad jurídica y patrimonio propio, que está sometido a la supervigilancia del Presidente de la República a través del Ministerio de las Culturas, las Artes y el Patrimonio. Conforme a lo establecido en la ley N°21045 publicada con fecha 3 de noviembre de 2017, que crea el Ministerio. El Servicio Nacional del Patrimonio Cultural, es el encargado de implementar políticas y planes, y diseñar y ejecutar programas destinados a dar cumplimiento a las funciones del Ministerio, en materias relativas al folclor, culturas tradicionales, culturas y patrimonio indígena, patrimonio cultural material e inmaterial; e infraestructura patrimonial como, asimismo, a la participación ciudadana en los procesos de memoria colectiva y definición patrimonial. Su misión es: "Gestionar el reconocimiento, el resguardo y el acceso al patrimonio y la memoria, de forma participativa y en su diversidad, para generar conocimiento y contribuir a mejorar la calidad de vida de las personas" y para cumplir la misión cuenta con objetivos estratégicos que, si bien son variados, en su conjunto buscan entregar un servicio a la comunidad, el acceso a la información de artes, cultura y patrimonio del país. Para lo cual el servicio recopila y está encargado de resguardar una gran cantidad de información de las artes, cultura del país la cual expone en sus museos, bibliotecas a nivel nacional, como también el archivo nacional donde se reúne y conserva la historia de Chile en cuanto a los archivos de departamento de estado y todos los documentos y manuscritos en sus distintos formatos para ser usados en los procesos internos del servicio y ser puesta a disposición de la sociedad contribuyendo al desarrollo del país conservando su historia a través del tiempo.

El Servicio Nacional del Patrimonio Cultural debe llevar a cabo procesos, tareas y desarrollar funciones a lo largo del país y cumplir con sus objetivos estratégicos, que corresponden a los siguientes:

1. Mejorar y ampliar los servicios y espacios patrimoniales a lo largo del país, mediante el fortalecimiento institucional y el fomento de la participación de comunidades y personas, para contribuir a la sustentabilidad de sus identidades, memorias y territorios.

2. Fomentar el reconocimiento, resguardo y salvaguardia del patrimonio material e inmaterial del país, fortaleciendo e incrementando su investigación, registro, inventario, documentación, conservación y restauración, con la finalidad de ponerlo al servicio de las personas.

3. Contribuir a los procesos de transparencia del Estado, catalogando y archivando la documentación que éste genera, para que sea entregada en forma oportuna y completa a las personas que la requieran.

4. Mejorar el acceso a los servicios patrimoniales que genera y gestiona la institución, mediante iniciativas de difusión, transferencia de conocimientos y mediaciones patrimoniales, que incorporen el desarrollo de nuevas tecnologías y condiciones de seguridad pertinentes.

5. Fomentar el reconocimiento, resguardo y salvaguardia del patrimonio y cultura de los pueblos indígenas, rescatando y promoviendo iniciativas vinculadas a las diversas prácticas y tradiciones.

6. Fortalecer los procesos de reconocimiento patrimonial y de construcción de memorias, por medio del desarrollo de modelos de participación pertinentes a los contextos socioculturales, con la finalidad de visibilizar y resguardar la diversidad cultural del país.

7. Potenciar las capacidades en regiones, mediante la delegación de funciones y atribuciones a las Direcciones Regionales, el fortalecimiento de la gestión y el desarrollo del capital humano, en función de los contextos específicos de cada región.

2. DECLARACIÓN INSTITUCIONAL

El Servicio Nacional del Patrimonio Cultural (en adelante SERPAT) reconoce la información como un activo esencial para desarrollar sus procesos y para poder alcanzar los objetivos institucionales, y junto con esto entiende que se debe contar con tecnología de información así como infraestructura que soporten tales tecnologías, por lo tanto, el SERPAT se compromete a gestionar la seguridad de la información y el buen uso de los activos de información donde está contenida, para lograr niveles adecuados de protección ante la pérdida de confidencialidad, integridad y disponibilidad.

En consideración de lo anterior, el Servicio asume la responsabilidad de implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información basado en la norma Nch ISO 27001:2023, y en cumplimiento con lo establecido en el Decreto Supremo Nro. 83 del Ministerio Secretaria General de la Presidencia, para lo cual define una política de seguridad de la información, que permita alcanzar niveles adecuados de seguridad en todos los activos de información institucional, de tal manera de garantizar que los riesgos de seguridad de la información sean conocidos, asumidos, gestionados y minimizados por el Servicio de una forma documentada, sistemática, estructurada y eficiente pudiéndose adaptar a los cambios que se produzcan en los riesgos, en el entorno y la tecnología.

El Servicio entiende que la única forma de conservar y preservar la información es protegiéndola para eso es necesario su clasificación y evaluación de riesgos, determinar controles necesarios que permitan que los recursos bibliográficos, información de nuestros orígenes, documentos históricos y en resguardo, recursos con derechos de propiedad intelectual, material museológico e información de los usuarios y personal puedan ser protegidos ante pérdida y acceso indebido, de esta manera no afectar la imagen de la institución por interrupciones parciales o totales de los procesos y/o enfrentarse a

consecuencias legales derivadas por el no cumplimento de la leyes o requisitos aplicables relacionados con la protección de la privacidad, seguridad de la información y Ciberseguridad.

3. OBJETIVO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Establecer los principios y marco general de trabajo para administrar, mantener, sensibilizar, monitorear y revisar el Sistema de Gestión de Seguridad de la Información (SGSI) acorde a las Definiciones Estratégicas, la misión/visión y objetivos estratégicos del SERPAT, asegurando la confidencialidad, integridad y disponibilidad de los activos de la información a través de su adecuada implementación, asignación de roles, funciones y responsabilidades.

En términos generales, el SERPAT destaca, los objetivos de gestión de seguridad de la información que se desprenden de esta política, en tres áreas, las que permiten definir las tareas requeridas:

3.1 Gestión de activos

Garantizar que los activos de información (que correspondan) y la tecnología utilizada para su procesamiento, reciban un apropiado nivel de protección, sean clasificados para señalar su sensibilidad y criticidad. Definiendo directrices para su buen uso, con el fin de asegurar los correctos niveles de confidencialidad, integridad y disponibilidad.

3.2 Análisis de Riesgos

Garantizar la identificación de los riesgos y su posterior mitigación, que afectan a la Seguridad de la Información, conforme a las metodologías establecidas como el proceso de gestión de riesgos del SERPAT, en cuanto a los activos de información, inventario y valoración de estos. Este proceso se implementa, sobre la base de las exigencias del Oficio de Objetivos Gubernamentales de Auditoría emitido por Gabinete Presidencial y del Documento Técnico emitido por el Consejo de Auditoría Interna General de Gobierno (CAIGG) y la resolución vigente que aprueba la Política de Gestión de Riesgos y la definición de roles y responsabilidades en la Gestión de Riesgos del Servicio Nacional del Patrimonio Cultural.

3.3 Recursos Humanos y Seguridad

Promover, capacitar e informar al personal desde su ingreso y en forma permanente, cualquiera sea su calidad jurídica de contratación, acerca de las políticas y procedimientos de seguridad de la información que afectan al desarrollo de sus funciones y de mantener actualizados los conocimientos frente a los objetivos en materia de Seguridad de la Información y asuntos de confidencialidad.

4. OBJETIVOS ESPECIFICOS

1) Definir una metodología para identificar, analizar y controlar los riesgos que afecten a los activos de información de forma de ser clasificados de acuerdo con el cumplimiento de los objetivos institucionales esta debe ser complemento de la matriz de riesgo institucional definida en el sistema de gestión de riesgos.
2) Determinar y monitorear la implementación de controles de seguridad, buenas prácticas de acuerdo con la norma vigente y los mandatos que requiera el gobierno que se deban adoptar para protegerlos de las amenazas que puedan afectar a la confidencialidad, integridad y disponibilidad de la información.
3) Definir y dar cumplimiento a un proceso de respuesta ante eventos e incidentes de Seguridad del a Información apoyando de esta manera a la continuidad operacional de la institución.
4) Definir el ámbito de trabajo y responsabilidades de la institución e individuales respecto al uso de los recursos tecnológicos que provee la empresa y al manejo de la información.
5) Contar con una visión global sobre el estado de los activos de información, las medidas de seguridad que se están aplicando y los resultados que se están obteniendo de dicha aplicación evaluar mejoras en cuanto a tecnologías.

6) Establecer un marco de Gestión de Riesgo Cibernético para cada sistema, proceso, actividad crítica, que permita alcanzar los objetivos estratégicos.

5. ALCANCE

La Política, debe ser aplicada a todo el ámbito de la Institución así como a todo el personal cualquiera sea su situación contractual Planta, contrata, Código del trabajo, Honorario, estudiantes en práctica, personal tercerizado como también proveedores de servicios externos, contratistas u otro tipo de personal relacionado con empresas que presten servicios al SERPAT, que involucren a los activos de información y a la totalidad de los procesos, internos y externos, vinculados a la entidad a través de todo tipo de contratos o acuerdos con terceros.

6. REFERENCIA NORMATIVA.

Se integrarán al Sistema de Seguridad de la Información, las siguientes metodologías de gestión que operan en el Servicio Nacional del Patrimonio Cultural:

- "Sistema de Gestión de Calidad Institucional",
- "Sistema de Gestión de Riesgos Institucional".
- Sistema de Prevención de Lavados de Activos, Financiamiento del Terrorismo y Delitos funcionarios (LA/FT/DF),
- Sistema de Integridad.

Además, se apoya y responde a las siguientes normativas vigentes:

- Ley 21.663, de 2024: Ley Marco de Ciberseguridad
- Decreto N°164, de 2023, del Ministerios del Interior y Seguridad Pública: Aprueba Política Nacional de Ciberseguridad 2023-2028.
- Decreto N°7, de 2023, del Ministerios secretaria general de la Presidencia: Establece Norma Técnica de Seguridad de la información y Ciberseguridad a la ley N°21.180
- Ley 21.459, de 2022: Establece normas sobre delitos informáticos, deroga la Ley N°19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest. Esta ley establece los delitos informáticos reconocidos en Chile; su conocimiento es esencial para un encargado de ciberseguridad.
- Ley N°21.459 de 2022: Establece normas sobre delitos informáticos, deroga la Ley N°19.223.
- Decreto N°273, de 2022, El que establece obligación de reportar incidentes de ciberseguridad.
- Ley N°21.180, de 2022: Transformación digital del Estado.
- **I**nstructivo presidencial N°8 de 2018**:** Imparte instrucciones urgentes en materia de ciberseguridad a los órganos de la administración del Estado – Presidencia de la República.
- Instructivo presidencial N°1 de 2018**:** Imparte instrucciones sobre uso de servicios en la nube a los órganos de la Administración del Estado – Presidencia de la República
- Decreto N°83, de 2017: Convenio sobre la ciberdelincuencia.
- Ley N°20.435, de 2010: Modifica Ley sobre propiedad Intelectual
- Ley N°20.285, de 2008: Principio de Transparencia de la función pública y el derecho de acceso a la información.
- DS N°83, de 2005: Norma técnica para los Órganos del Estado sobre la seguridad y confidencialidad de documentos electrónicos.
- Ley N°18.834, de 2005: Ley sobre Estatuto Administrativo.
- Ley N°19.880, de 2003: Sobre Bases de los Procedimientos Administrativos que rigen los actos de los órganos de la Administración del Estado.
- Ley N°19.799, de 2002: Sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
- Ley N°19.628, de 1999: Sobre Protección de la vida privada.

- Ley N°17.336, de 1970: Ley sobre propiedad Intelectual y derecho de autor.
- ISO 27001: Sistema de Gestión de la Seguridad de Información.
- ISO 27002: Prácticas para la gestión de la seguridad de la información.

7. DEFINICIÓNES

Seguridad de la Información
La Seguridad de la Información es conjunto de medidas técnicas, organizativas y legales que permiten alcanzar a la Institución niveles adecuados de Integridad, Confidencialidad y Disponibilidad en los diferentes sistemas de información, con el objeto de asegurar la continuidad operacional de los procesos y servicios proporcionados por el Servicio Nacional del Patrimonio Cultural.

La seguridad de la información debe garantizar que los activos de información cumplan con estas tres condiciones:

- **Confidencialidad**: Necesidad de permitir el acceso al activo solo a las personas debidamente autorizadas de acuerdo con lo definido por la institución. El acceso no autorizado tiene impacto para la institución o terceros.

- **Integridad**: Necesidad de preservar la configuración y contenido de un activo de Información. Su modificación no deseada tiene consecuencias que generan distintos niveles de impacto para la institución o terceros. El Valor de este atributo está directamente relacionado con la magnitud de dicho impacto.

- **Disponibilidad**: Necesidad de preservar el tiempo de acceso al activo bajo un umbral predefinido por la institución. Sobrepasar dicho umbral implica el no acceso al activo, que genera distintos niveles de impacto para la institución o terceros. El Valor de este atributo está directamente relacionado con la magnitud de dicho impacto.

Información
Es un conjunto de datos que tienen relación y sentido que entrega conocimiento sobre un tema determinado, esto pude ser de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, que se transmite por enlaces de comunicación, en medios audiovisuales e incluso hablados.

Activo de información
Corresponden a todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de la información de valor para el Servicio Nacional del Patrimonio Cultural.
Se pueden distinguir tres (3) tipos o niveles básicos de activos de información:

- La información propiamente tal, en sus múltiples formatos (papel, digital, texto, imágenes, audio, video, etc.)
- Los equipos y sistemas como también la infraestructura que soportan esta información.
- Las personas que utilizan la información y que tienen el conocimiento de los procesos y procedimientos institucionales.

Sistema de información
Se refiera al conjunto de información referida a un tema en particular y que puede o no relacionarse con otros sistemas, en estos se recopilan procesa, almacena y difunde la información. En el proceso la finalidad es usarla para la coordinación, control y análisis que en su conjunto permite la toma de decisiones del servicio. Los componentes de los sistemas de información son las personas, hardware, software, datos y las redes.

Tecnologías de información
Se refiere al hardware, software (herramientas de aplicación y sistemas) y redes de comunicación utilizada por personal del SERPAT o por un tercero que procese información en su nombre, donde se busca, procesa y trasmite información.

Autenticidad
Corresponde a la validez de la información en tiempo, forma y distribución, además de garantizar el origen de esta, validando el emisor para evitar suplantación de identidades.

Incidente de Seguridad
Corresponde a un evento adverso que afecta a un sistema de información, a un computador o a una red de computadores, que compromete la confidencialidad, la integridad y/o la disponibilidad de uno o más activos de información. Puede ser causado mediante la explotación de alguna vulnerabilidad o a un intento de romper los mecanismos de seguridad existentes, es decir, puede tener un origen externo o interno.

Ciberseguridad y Seguridad de la Información
Conjunto de acciones, políticas, medidas preventivas y reactivas destinadas a la prevención, mitigación, manejo, respuesta y estudio de las amenazas y riesgos de incidentes de seguridad, a la reducción de sus efectos y el daño causado; antes, durante y después de su ocurrencia; respecto de los activos y activos de información y la continuidad de servicios, con el fin de proteger, preservar y restablecer la confidencialidad, integridad y disponibilidad de aquellos y de las plataformas electrónicas de los órganos de la Administración del Estado, aumentando su resiliencia en el tiempo.

Plataforma electrónica (en adelante también "plataforma")
Software o conjunto de software, datos e infraestructura tecnológica que sustenta procesos o procedimientos.

Riesgo
Efecto de la incertidumbre sobre los activos de información y los objetivos de una entidad, habitualmente expresado en relación con las consecuencias de un evento o incidente de seguridad y su probabilidad de ocurrencia.

Servidor
Equipo virtual o físico dedicado a entregar servicios de red, servicios de bases de datos, sitios web, sistemas informáticos, carpetas compartidas y, en general, brindar los recursos necesarios para responder las peticiones de usuarios

8. ROLES Y RESPONSABILIDADES

8.1 Comité de Seguridad de la Información (CSI)

El SERPAT contará con un Comité de Seguridad de la Información cuyos miembros serán designados por resolución exenta del/de la Director(a) Nacional del SERPAT, y tendrá entre sus funciones la implementación de las políticas, procedimientos, normas y estándares institucionales en materias de seguridad de la información, así como también realizar reuniones y revisar la implementación de las normativas vigentes. Además, tendrá la responsabilidad de asegurar el cumplimiento de esta política y de establecer los mecanismos de difusión en la Institución. Esta resolución debe contener el detalle de sus funciones y deberá ser publicada en el sitio colaborativo institucional en la sección de Seguridad de la Información.

8.2 Encargado/a de Seguridad

El SERPAT contará con un Encargado/a de Seguridad de la Información designado mediante resolución exenta del/de la Director(a) Nacional del SERPAT, y tendrá entre sus responsabilidades la difusión de la política, la vigilancia de su cumplimiento, la aplicación de sus procedimientos y la coordinación de inducciones si fuese necesario. Esta resolución debe contener el detalle de sus funciones y deberá ser publicada en el sitio colaborativo institucional, en la sección de Seguridad de la Información.

8.3 La Dotación del Servicio

La Dotación, entendida como las personas que desempeñan funciones en el SERPAT (funcionarios(as) de planta, funcionarios(as) a contrata, personal contratado por código del trabajo, personal a honorarios o alumnos/as en práctica que preste servicios permanentes o temporales) deberán hacerlo en estricto cumplimiento con las políticas de seguridad, de acuerdo con los procedimientos existentes en la organización. Cabe mencionar, que las responsabilidades básicas en materias de seguridad de la información, en los casos que corresponda, quedarán descritas en los contratos y/o en los perfiles de cargo, en alguna acta o resolución específica y en las políticas de seguridad de la información.

La formalización de las tareas, funciones y responsabilidades sobre los procesos de tratamiento y gestión de la información, son establecidos en la primera Política Específica, denominada ***Política de Organización de Seguridad de la Información.***

9. REVISIÓN Y APROBACIÓN

Se establece que la Política de Seguridad de la Información y las Políticas Específicas, serán revisada por persona Encargada(o) de Seguridad de la Información en intervalos de tiempo de dos años o cuando se produzcan cambios significativos, proponiendo caso que corresponda las modificaciones al Comité de Seguridad de la Información (CSI) y presentada al/la Director(a) Nacional del Servicio para su aprobación. La aprobación y/o modificación de normas, procedimientos o controles, serán aprobados directamente por el Comité de Seguridad de la Información.

Estos cambios podrán ser frente a eventos que afecten o tengan impacto en los riesgos previamente identificados en la Institución, por ejemplo: cambios normativos o legales relacionados con esta materia de seguridad de la información o ciberseguridad, de autoridades, surgimiento de nuevas tecnologías, cambios en el entorno ambiental, etc. Los cambios deberán ser registrados con control documental y actas del Comité de Seguridad de la Información.

10. DIFUSIÓN

Esta Política será difundida a todos los funcionarios(as) del Servicio Nacional del Patrimonio Cultural, independiente de su calidad jurídica de nombramiento o estamento, será difundida utilizando para ello la intranet institucional y correo electrónico con comunicados masivos, para asegurar el permanente entendimiento y compromiso en todos los niveles de la organización. La difusión deberá ir acompañada, en la medida de lo posible, de capacitaciones en el tiempo.

11. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La presente **Política General de Seguridad de la Información**, recoge los lineamientos generales que el SERPAT dicta en el cumplimiento de las disposiciones legales vigentes y la norma Nch-ISO 27001 que proporciona la dirección en este tema, con el objeto de gestionar adecuadamente la Seguridad de la Información.

El/La Director(a) Nacional del Servicio reconoce la necesidad de proteger los activos de información en todos sus medios utilizados para su procesamiento, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información, implementando políticas específicas, procedimiento y buenas prácticas en los procesos, realizando acciones que estén al alcance para garantizar la seguridad de la información y la continuidad operativa del servicio.

El/La Directora(a) Nacional del Servicio se compromete a través del SGSI establecer las acciones necesarias para proteger los sistemas de información críticos asegurando el resguardo de la información contenida en su completitud y a crear una cultura de protección hacia la información, involucrando a los funcionarios y funcionarias en su día a día, mediante capacitación y charlas, desarrollando sus competencias en este ámbito para que lo apliquen en tanto en el Servicio como en su vida, entendiendo que este activo es fundamental para llevar a cabo los objetivos de la presente política.

El/La Directora(a) Nacional del Servicio se compromete a cumplir con los requisitos aplicables de acuerdo con la naturaleza del Servicio y las leyes, buenas prácticas y normativa vigente, apoyando y entregando recursos para la solución de riesgos detectados que podrían afectar a la continuidad operacional, que define o detecta el SGSI o de los diferentes sistemas de gestión a los cuales se integra y entrega recursos para mantener su mejora continua.

11.1 Organización de la Seguridad de la Información

Se debe mantener una organización que permita prevenir, detectar y responder apropiadamente a eventos e incidentes de seguridad. Para lo cual el/la Director(a) Nacional del Servicio apoyara en forma activa, otorgando los recursos necesarios para la mejora continua del SGSI, cumpliendo los compromisos acordados y aprobando la presente política y resoluciones de nombramiento del Comité y la persona encargada de Seguridad de la Información con sus roles y responsabilidades.
Las directrices respecto a cómo opera el SGSI se defines en el documento ***Política de Organización de Seguridad de la Información.***

11.2 Seguridad ligada a Recursos Humanos

Se debe asegurar un proceso formal que permita la revisión y validación de los antecedentes o documentos necesarios antes de la contratación de todo personal y colaborador que se integren a la Institución, que comprendan la responsabilidad con la seguridad de la información según los roles y accesos a los sistemas de acuerdo con sus funciones. En cuanto a proveedores, la necesidad de firmar acuerdos de confidencialidad, comprometiéndose a cumplir con las políticas, procedimientos e instructivos de seguridad de la información, informándoles que él no cumplimiento de estos podrían derivar en sanciones.
Se debe asegurar también el proceso formal para informar la contratación y cese de funciones en forma oportuna, con el fin asegurar el resguardo de los activos asociados, así como la administración de accesos a la red del Servicio. Todo esto, para mitigar riesgos asociados a hurto, fraude o mal uso de los activos de información.
Las directrices respecto a este punto se definen en el documento ***Política de Seguridad de la Información en el Recurso Humano.***

11.3 Gestión de activos

Se debe asegurar un proceso formal para mantener una apropiada protección de los activos institucionales, permitiendo la identificación, clasificación, definición de propietario y evaluación de criticidad de estos según, logrando la protección de confidencialidad, integridad y disponibilidad, evaluando los riesgos asociados y generando un plan de tratamiento. La actualización y evaluación de su criticidad y riesgo en el tiempo deberá ser responsabilidad de cada unidad y/o departamento quien deberá resguardar y mantener el inventario de activos que el Servicio les ha encomendado.
Las directrices respecto a este punto se definen en el documento ***Política de Clasificación y Gestión de Activos de Información.***

11.4 Control de acceso

Se debe asegurar el correcto acceso de los funcionarios o funcionarias debidamente autorizados a los sistemas de información, para lo cual se debe definir un proceso para controlar las asignaciones, desde su ingreso hasta su egreso, incluidos los cambios de funciones. Se debe llevar un control especial a los accesos de funcionarios(as) definidos como administradores, con controles de seguridad especiales. Se deben definir roles y responsabilidades, manteniendo una matriz de control de acceso para proteger el acceso a datos críticos y confidenciales.
Se deberán implementar controles de manera de evitar el acceso no autorizado a los servicios de red tanto para personal interno como externo.
Se debe monitorear y revisar en forma periódica los accesos de acuerdo con lo definido, para evitar un mal uso de los accesos, pérdida de confidencialidad e integridad de la información.
Las directrices respecto a este punto se definen en el documento ***Política de Control de acceso.***

11.5 Controles Criptográficos y gestión de claves

Se deberá definir un proceso formal y responsables para cuando de acuerdo con la clasificación de la información y evaluación de riesgo, la información deba ser protegida ante a acceso físico no autorizado, la protección para este control puede ser para distintos objetivos de seguridad de la información, tales como:
Confidencialidad: Uso cifrado de la información sensible crítica ya sea almacenada o transmitida.
Integridad/autenticidad: Uso de firmas digitales o códigos de autentificación de mensajes para verificar la autenticidad o integridad de la información crítica almacenada o transmitida.
No repudio: uso de técnicas criptográficas para brindar evidencia de la ocurrencia y no ocurrencia de un evento o acción.
Se deberán implementar políticas sobre el uso, protección y vida útil de las claves criptográficas durante el ciclo de vida.

11.6 Seguridad física y medioambiental

Para evitar el acceso físico no autorizado que pueda generar daño y/o interferencia en las operaciones del Servicio afectando a los activos de información. Se debe implementar medidas para el control de accesos a lugares definidos como críticos y/o sensible, es el caso del lugar donde se procesan datos, se deben mantener en áreas seguras, protegidas de un perímetro, controles de ingreso, tanto para el personal como para proveedores y visitas, para prevenir pérdida, hurtos y daños de activos.
El personal (interno o externo) debe conocer la responsabilidad de proteger los activos y prevenir accesos no autorizados.
Las directrices respecto a este punto se definen en el documento ***Política de seguridad física y medioambiental, y Política de escritorio y pantalla despejados.***

11.7 Seguridad de las operaciones

Se deben definir procedimientos operacionales, donde se especifique la forma correcta de operación de sistemas y software para que queden a disposición de quienes los operan, debe haber responsables de la actualización y mantención de estos documentos, que permitirán la correcta operación del servicio. En la operación se deben controlar los cambios a los sistemas, control del posible código malicioso, respaldo de información en forma correcta, registrar, mantener y revisar eventos de actividades de usuarios(as) en la red y/o sistemas, proteger los registros de las aplicaciones contra alteraciones, mantener y proteger la información que generen los software y sistemas ante modificaciones o eliminación, con la documentación adecuada, para que ante un evento poder determinar la causas, soluciones y reestablecer la operación en casos complejos.
Las directrices respecto a este punto se definen en el documento ***Política de seguridad de las operaciones.***

11.8 Seguridad de las comunicaciones

Se deberá implementar controles sobre las redes de datos o comunicaciones, a fin de proteger la información en los sistemas y aplicaciones que viajan en la red. El Servicio deberá definir los mecanismos de seguridad sobre la gestión de todos los servicios de redes prestados por el Servicio o por terceros, se deberán definir segregación de redes por servicios o sistemas de información dependiendo de la criticidad de la información. Además, se deberá monitorear el acceso a la red y el uso redistribuyendo el ancho de banda de la red de acuerdo con la necesidad del servicio, restringiendo el acceso a sitios web o dominios que se consideren inseguros, definiendo procedimientos de transferencia de información. Las directrices respecto a este punto se definen en el documento ***Política de Seguridad de las Comunicaciones*.**

11.9 Adquisición, desarrollo y mantenimiento de sistemas

Se debe definir un proceso formal y cumplir con requisitos específicos tanto para el desarrollo de software interno o externo, se debe garantizar que la seguridad será parte integral de los sistemas de información, que se incluya la seguridad de la información en todas las etapas del ciclo incluyendo para esto la infraestructura, aplicaciones y servicios, protegiendo la información antes acceso no autorizado, manipulación indebida y confidencialidad.
Las directrices respecto a este punto se definen en el documento ***Política de Seguridad, Adquisición, Desarrollo y Mantenimiento de Sistemas.***

11.10 Relaciones con el proveedor

Se debe definir un proceso formal y determinar seguridades para cuando el proveedor acceda a los datos del Servicio, se deben firmar cláusulas de confidencialidad, de protección de datos y todos los requisitos de seguridad de la información pertinente, estas deben ser definidas y acordadas con el proveedor. El Servicio debe definir mecanismos de control y supervisión, delimitar las responsabilidades, solo permitir acceder a lo que por acuerdo está establecido y auditar los servicios entregados. En cuanto a los activos de propiedad del proveedor que operen en la red del Servicio, deberán cumplir con lo exigido en la presente Política, todo esto para proteger la información de uso indebido, pérdida y confidencialidad.

11.11 Gestión de incidentes de seguridad de la información

Se debe definir un proceso formal que asegure que las debilidades de la seguridad de la información sean denunciadas, se deben definir las correctas acciones a tomar desde los mecanismos de detección por parte los usuarios(as) o del monitoreo continuo en la red, los eventos deben se clasificados, reportarlos para su tratamiento, y deben documentarse para poder aprender de los incidentes y soluciones, esto con el fin de proteger los activos ante eventos de seguridad (cambio en las operaciones diarias en la red o servicio tecnológico). Se deben definir responsables y responsabilidades en las etapas

del ciclo de vida de un incidente. Las directrices respecto a este punto se definen en el documento ***Política de Gestión de Incidentes de Seguridad de la Información*.**

11.12 Gestión de la continuidad del negocio

Se debe asegurar la continuidad operacional del Servicio ante un incidente de seguridad que comprometa a los activos de información, respondiendo frente a interrupciones dando continuidad operativa, protegiendo los procesos críticos. Se debe definir un proceso de gestión de la continuidad del negocio con el fin de responder de la mejor manera ante un incidente de determinadas naturalezas, para lo cual se deben definir planes de continuidad, las elecciones de los incidentes se definirán de acuerdo con los riesgos institucionales, así como también los planes. Las directrices respecto a este punto se definen en el documento ***Política de Continuidad de Seguridad de la Información.***

11.13 Cumplimiento

Se debe evaluar cada ley y normativa que afecte al Sistema de Gestión de Seguridad de la Información, en cuanto a modificaciones o creaciones de nuevas leyes, el desconocimiento de esto podría generar problemas y no garantizar el correcto cumplimiento en esta materia. Para lo cual se debe definir un proceso formal donde el sistema se asegura el recibimiento oportuno y en completitud de la información que lo afecte. Las directrices respecto a este punto se definen en el documento ***Política de Cumplimiento.***

12. AUDITORIAS

El Servicio a través de los sistemas de gestión de riesgos y calidad implementados en la institución o del propio sistema de seguridad podrán solicitar a una Unidad interna u organismo auditor externo, la realización de auditorías o revisiones independientes sobre el cumplimiento de la Política de Seguridad de la Información, las Políticas específicas, los Procedimientos establecidos a partir de las políticas.
Las auditorías deberán ser realizadas por personal independiente de quien maneja el Sistema de Seguridad de la Información.

13. EXENCIONES Y EXCEPCIONES

Podrán existir casos particulares en el cual no se pueda cumplir con algún punto de la presente Política o sus Políticas específicas, de ser el caso, esto debe ser debidamente justificado de exclusión total o parcial, lo cual deberá ser calificado y autorizado por escrito por el Comité de Seguridad de la Información, quien deberá considerar todos los riesgos y activos involucrados para tener en consideración, la excepción deberá ser informada al/la Director(a) Nacional del Servicio, con toda su documentación.

En el caso de tratarse de una exención, esta se otorga por un tiempo determinado, no mayor a un año, y se aprueba un procedimiento alternativo que mantiene los mismos niveles de seguridad.

En el caso de tratarse de una excepción, se trataría de una autorización a largo plazo que libera de la obligación legal.

14. INCUMPLIMIENTO Y SANCIONES

El no cumplimiento de la Política de Seguridad de la Información y Política de Control de Accesos será sancionado en conformidad a las disposiciones administrativas internas según el Estatuto Administrativo y/o Código del trabajo. Lo anterior, sin perjuicio de la responsabilidad civil o penal que corresponda de acuerdo con la Ley N°21.459 de 2022: que establece normas sobre delitos informáticos.

15. CONTROL DE INFORMACIÓN DOCUMENTADA

CONTROL DE DOCUMENTOS Y REGISTROS									
			ALMACENAMIENTO				NIVEL DE CRITICIDAD		
N°	IDENTIFICACIÓN	RESPONSABLE EMISIÓN	TIEMPO DE RETENCIÓN / RECUPERACIÓN	MEDIO DE SOPORTE	LUGAR / RESPONSABLE	DISPOSICIÓN	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
1.	Política General de Seguridad de la Información	Encargado(a) de Seguridad de la Información SERPAT	5 años /año	Digital	Intranet Institucional de Seguridad de la Información /Archivador/ Encargado(a) de Seguridad de la Información SERPAT	Respaldo Digital / Físico	Uso interno	Alto	Medio

2.- DÉJASE, sin efecto la resolución Exenta N° 1686 de fecha 17 de septiembre del año 2019, del Servicio Nacional del Patrimonio Cultural, que aprobó las Políticas de Seguridad de la Información del Servicio Nacional del Patrimo0nio Cultural.-

3.- PUBLÍQUESE, la presente resolución, en la Intranet del Servicio Nacional del Patrimonio Cultural, en el apartado Seguridad de la información y Ciberseguridad.

ANÓTESE, COMUNÍQUESE Y PUBLÍQUESE

Diego Sergio Montecinos Fernández
2025.05.19 15:35:11 -04'00'

DIEGO MONTECINOS FERNÁNDEZ
DIRECTOR NACIONAL (S)
SERVICIO NACIONAL DEL PATRIMONIO CULTURAL

JCV/POS/AGL/OEC/LZ

DISTRIBUCIÓN:
Dirección Nacional, SERPAT.
Biblioteca Nacional
Sistema Nacional de Bibliotecas Públicas
Subdirección Nacional de Museos, SERPAT.
Subdirección de Archivos, SERPAT.
Subdirección Nacional de Gestión Patrimonial, SERPAT.
Subdirección Nacional de Investigación, SERPAT.
Departamento de Administración y Finanzas, SERPAT.
División de Planificación y Presupuesto, SERPAT.
Museo Nacional de Bellas Artes
Museo Nacional de Historia Natural
Museo Histórico Nacional
División Jurídica, SERPAT.
Departamento de Gestión y Desarrollo de Personas, SERPAT.
Consejo de Monumentos Nacionales
Subdirección de Pueblos Originarios, SERPAT.
Subdirección de Patrimonio Cultural Inmaterial, SERPAT.
Direcciones Regionales, SERPAT.
Coordinación de Política Digital, SERPAT.
Programa Biblioredes, SERPAT.
Auditoría Interna, SERPAT.
Encargado de Seguridad de la Información
Secretaría General y Oficina de Partes, SERPAT.