Servicio de Salud Metropolitano Sur Oriente
Región Metropolitana
Ministerio de Salud

UNIDAD DE CONTROL INTERNO
DR.FBV. /JTF. /HPR. /clf.

APRUEBA POLITICA DE DESARROLLO SEGURO DE LA DIRECCIÓN DEL SERVICIO DE SALUD METROPOLITANO SUR ORIENTE

RESOLUCION EXENTA N° 5226 31.12.2018 /

PUENTE ALTO,

VISTOS:

Lo dispuesto en la ley N° 19.880 que establece bases de los procedimientos administrativos; en la ley N° 19.799 sobre documentos electrónicos, forma electrónica y servicios de certificación de dicha firma; en el Decreto Supremo N° 83, de 2005, del Ministerio Secretaria general de la presidencia, que aprueba norma técnica para órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos , en la ley N° 19.233 del 7 de junio de 1993 del Ministerio de Justifica sobre tipificación de figuras penales relativas a la informática; Resolución N° 1.161 de 4 de octubre de 2016 Subsecretaría de redes y Subsecretaría de Salud, que aprueba el Sistema de Seguridad de la información, en la Norma Chilena NCh-ISO 27002 Of. 2013. Que, de acuerdo a lo dispuesto en el Decreto con fuerza de ley N°1 de 2005 de salud, que fija el texto refundido, coordinado y sistematizado del Decreto de Ley N° 2.763/79 y de las leyes N° 18.933 y N° 18.469; Resolución N° 1600 de 2008, de la Contraloría General de la República y las facultades que me confiere el Decreto Afecto N° 53 de 12 de julio de 2018, de Salud.

CONSIDERANDO:

1.Que, las nuevas tecnologías de la información y de las comunicaciones (TIC) al ser progresivamente incorporadas a los procesos institucionales y al quehacer personal de los funcionarios en el ejercicio de sus funciones, presentan una serie de beneficios, ventajas de diversa índole. Sin embargo, también conlleva riesgos que pueden afectar a los activos de información institucional.

2. Que, gestionar la seguridad de la información es un imperativo que se debe cumplir en el marco de la normativa gubernamental existente y que consiste básicamente en la realización de todas aquellas actividades y tareas que sean necesarias para establecer los niveles de seguridad que la propia institución determine, basándose para ello en metodologías y técnicas estándares en estas materias. Todo, con el firme propósito de lograr introducir un ciclo de mejoramiento continuo y sostenible en el tiempo que permita alcanzar niveles de integridad, confidencialidad y disponibilidad, con todos los activos de información relevantes para la institución, como un principio clave en la gestión de procesos.

3. Que, siendo la seguridad de la información un tema de suma relevancia en el Servicio de Salud metropolitano sur oriente, por el alto volumen de información sensible con la cual se trabaja, existe la necesidad de contar con una estructura que considere la definición de lineamientos y prácticas de seguridad de la información a ser aplicadas a todos los organismos relacionados. En este sentido, es una prioridad para la Dirección del Servicio de Salud implementar, mantener y mejorar continuamente la gestión de la seguridad de la información, basada en los principios de confidencialidad, integridad y disponibilidad de la información.

4. Que, a la fecha, existen una serie de normas en materias de seguridad de la información entre las que se encuentra 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 las Normas Chilenas NCh- ISO 27001 Of. 2013 y NCh-ISO 27002 Of. 2013 que proporcionan un marco de gestión de Seguridad de la información utilizable por cualquier tipo de organización, pública o privada.

5.Que, conforme a los principios de eficiencia, eficacia y coordinación reconocidos en el artículo N°3 de la ley N° 18.575, orgánica constitucional de bases generales de la administración del Estado, se justifica que la Dirección del Servicio de Salud Metropolitano Sur Oriente, adopte las medidas que estime pertinente para resguardar la seguridad de la información.

6. Que, la Dirección del Servicio de Salud Metropolitano Sur Oriente comprende la importancia de un Sistema de Seguridad de la Información estándar y replicado en los Establecimientos Hospitalarios de la red Sur Oriente, con el objetivo de gestionar la seguridad de la información de forma homogénea en la Dirección del Servicio y red de salud.

7. En este contexto, y por todas las consideraciones expuestas, la Dirección del Servicio de Salud Metropolitano Sur Oriente, define y formaliza la Política de Desarrollo Seguro de la Dirección del Servicio de Salud Metropolitano Sur Oriente, dictando lo siguiente:

RESOLUCIÓN

ARTICULO N°1- APRUEBASE Política de Desarrollo Seguro de la Dirección del Servicio de Salud Metropolitano Sur Oriente, que se encuentra descrita en el documento adjunto, como anexo, es parte integrante de la presente Resolución.

ARTÍCULO 2. La presente Resolución surtirá sus efectos a contar de esta fecha

ANOTESE, COMUNIQUESE Y ARCHIVESE

SERVICIO SALUD SUR ORIENTE
DIRECTOR

DR. FERNANDO BETANZO VALLEJOS

DIRECTOR

SERVICIO DE SALUD

METROPOLITANO SUR ORIENTE

DISTRIBUCION:

- Dirección S.S.M.S.O.
- Subdirección Administrativa del S.S.M.S.O
- Subdirección de Gestión Asistencial S.S.M.S.O
- Subdirección de Gestión y Desarrollo de las Personas S.S.M.S.O
- Establecimientos Hospitalarios de la Red Sur Oriente
- Unidad de Control Interno S.S.M.S.O
- Asesoría Jurídica S.S.M.S.O
- Departamento de Auditoría Interna S.S.M.S.O
- Oficina de Partes S.S.M.S.O

SERVICIO SALUD METROP. SUR ORIENTE
MINISTRO DE FE

TRANSCRITA FIELMENTE

MINISTRO DE FE

POLÍTICA DE DESARROLLO SEGURO

DE LA DIRECCIÓN DEL SERVICIO DE

SALUD METROPOLITANO SUR ORIENTE

AÑO 2018

INDICE

1. OBJETIVO GENERAL 3
2. ALCANCE 3
3. DOCUMENTOS DE REFERENCIA 3
4. DEFINICIONES 4
5. ROLES Y RESPONSABILIDADES 5
6. DE LA POLÍTICA 6
   6.1 Consideraciones Generales 6
   6.2 Desarrollo por terceros 6
   6.3 Gestión de Vulnerabilidades 7
   6.4 Documentación 7
   6.5 Evaluación o Casos de Negocio 7
   6.6 Especificación detallada de requerimientos 7
   6.7 Diseño del Sistema 8
   6.8 Codificación y Pruebas 8
   6.9 Implementación 8
   6.10 Post Implementación 8
   6.11 Controles a implementar 9
7. MECANISMOS DE DIFUCIÓN Y DISTRIBUCIÓN 9
8. PERIODO DE REVISIÓN DEL DOCUMENTO 10
9. CONTROL DE CAMBIOS 10

1. OBJETIVO GENERAL

La presente política tiene como objetivo poder definir reglas y criterios transversales y controles de seguridad y confidencialidad para un Desarrollo Seguro, ya sea para desarrollo interno o desarrollo de terceros para la Dirección del Servicio de Salud Metropolitano Sur Oriente.

2. ALCANCE

La presente Política de Desarrollo Seguro se aplica a todos los sistemas de información desarrollados y/o actualizados en la Dirección del Servicio de Salud Metropolitano Sur Oriente, ya sea en forma interna como por empresas o profesionales externos contratados para tales efectos.

Esta Política se aplica a todos los usuarios de la Dirección del SSMSO, ya sean funcionarios de planta, contrata, honorarios, asesores, consultores, practicantes, y otros trabajadores, incluyendo las empresas que presten servicios en la Dirección del SSMSO, a todos a quienes se les otorgue una casilla de correo electrónico institucional.

3. DOCUMENTOS DE REFERENCIA

- Resolución Exenta N° 4.636, de 2018 que Aprueba Sistema de Seguridad de la Información de la Dirección del Servicio de Salud Metropolitano Sur Oriente.
- Resolución Exenta N°4.778, de 2018, que Aprueba la Política de Seguridad de la Información de la Dirección del Servicio de Salud Metropolitano Sur Oriente.
- NCh-ISO27001.Of2013 Tecnologías de la Información – Técnicas de Seguridad – Sistemas de Gestión de la seguridad de la Información.
- NCh-ISO27002.Of2013 Tecnologías de la Información – Códigos de Prácticas para la gestión de la Seguridad de la Información.
- -Decreto Supremo Nº83 del 03/06/2004 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"
- Resolución Exenta N° 1592, de 2017, de la Subsecretaría de salud Pública, que aprueba Política Especial de seguridad para la adquisición, desarrollo y mantenimiento de sistemas de información para las Subsecretarías de Salud Pública y Redes Asistenciales.
- Resolución Exenta N° 778, de 2014, del Ministerio de Salud, que Aprueba Política de Desarrollo de Sistemas.
- Decreto N° 41, de 2012, del Ministerio de Salud, que aprueba reglamento sobre fichas clínicas:
    - Regula el contenido, almacenamiento, administración, protección y eliminación de fichas clínicas de manera de resguardar el correcto empleo, disponibilidad y confidencialidad de los mismos.

4. DEFINICIONES

- ✓ **Servicio de Salud Metropolitano Sur Oriente (SSMSO)**: Corresponde a la separación sectorial realizada por el Ministerio de Salud para la administración de la atención de salud pública bajo una entidad gubernamental y una red de prestadores médicos, la cual se enmarca en la zona Sur Oriente de la capital del país, y abarca las comunas de Puente Alto, La Florida, San Ramón, La Granja, La Pintana, San José de Maipo y Pirque.

- ✓ **Dirección del Servicio de Salud Metropolitano Sur Oriente (DSS):** Corresponde a la entidad administrativa definida por el Ministerio de Salud como encargada de la red del SSMSO, cuya misión es la generación, implementación y evaluación de políticas, planes y programas para todo aquel territorio bajo su jurisdicción.

- ✓ **Encargado de Seguridad de la Información (ESI)**: Cargo definido como responsable de los procesos y procedimientos asociados a los protocolos y políticas que aseguran los recursos de información del SSMSO.

- ✓ **Comité Técnico de Seguridad de la Información (CTSI)**: Corresponde a la comisión encargada de la planificación y elaboración de políticas de seguridad de la información y sus mecanismos de control.

- ✓ **Unidad Investigación y Desarrollo TIC**: Grupo de trabajo cuyo enfoque principal es la generación, administración, mantención y soporte de aplicativos, programas, integraciones y soluciones utilizadas tanto en DSS como aquellas disponibles para la red SSMSO.
- ✓ **Proveedor**: Personas naturales o jurídicas que tienen una relación contractual directa o indirecta con la red SSMSO.
- ✓ **Riesgo:** Probabilidad de ocurrencia de un evento indeseado con consecuencias negativas.
- ✓ **Propietario de la información**: Es el responsable de la información y de los procesos que la manipulan, sean estos manuales, mecánicos o electrónicos. Debe participar activamente en la definición del valor de la información para el negocio, de manera que se puedan definir los controles apropiados para protegerla.

- ✓ **Información:** Contenido de un documento. Ejemplos de tipos de información:

  - **Pública:** Aquella información cuyo conocimiento no está circunscrito, se presume pública toda la información que obre en poder de la Administración

del Estado, salvo en los casos de excepción contemplados en el artículo 21 de la Ley Nº20.285.

- **Reservada:** Calidad de un acto, resolución, fundamento, procedimiento o documento que le permite ser conocido únicamente en el ámbito de la unidad del órgano a que sean remitidos, tales como división, departamento, sección u oficina.

- **Secreta:** Calidad de un acto, resolución, fundamento, procedimiento o documento que le permite ser conocido sólo por las autoridades o personas a las que vayan dirigidos y por quienes deban intervenir en su estudio o resolución.

5. ROLES Y RESPONSABILIDADES

- **Encargado de Seguridad de la Información**
  - Coordinar revisiones periódicas de seguridad en los sistemas de producción.
  - Proponer nuevas prácticas de seguridad para el desarrollo seguro de sistemas.

- **Unidad de Soporte**

  - Recibir, canalizar y gestionar cualquier aviso de problema o incidente en la operación de los sistemas de información.

- **Unidad de Desarrollo**

  - Cumplir con las disposiciones definidas en esta Política
  - Documentar el Sistema y/o sus modificaciones

- **Unidad de Infraestructura**

  - Disponer de medidas de protección adecuadas para el desarrollo y mantenimiento correcto y seguro de los sistemas de información.

6. DE LA POLÍTICA

6.1 Consideraciones Generales

La Unidad Investigación y Desarrollo TIC, es la responsable de planificar y ejecutar el mantenimiento de los sistemas de la institución. Además, debe planificar y coordinar la ejecución de pruebas de funcionamiento de los sistemas nuevos o modificados antes de ejecutar la instalación en los servidores de producción.

Se debe estandarizar el ciclo de desarrollo de sistemas, tal como lo establece la metodología de desarrollo y mantención de sistemas definida en el Ministerio de Salud.

Se debe establecer estándares de criterios de seguridad y de calidad en el desarrollo de sistemas.

Toda modificación de software crítico, por parches o módulos adicionales debe ser analizada previamente en los ambientes de desarrollo y prueba.

Se debe planificar detalladamente las etapas de paso a producción, incluyendo respaldos, recursos, conjunto de pruebas pre y post-instalación, criterios de aceptación del cambio y un plan de vuelta atrás.

Los programadores y personal de terceros no deben tener acceso a información de producción que contenga datos sensibles.

Para propósitos de desarrollo y pruebas, los responsables deben generar sus propios datos, debiendo ser distintos a los que se encuentran en ambiente de producción.

Un sistema desarrollado o modificado por terceras partes debe cumplir con lo establecido en esta política, incluyendo los criterios de seguridad.

6.2 Desarrollo por terceros

Se debe establecer un acuerdo previo con los terceros, que resguarde la propiedad intelectual y asegure los niveles de confidencialidad de la información manejada en el proyecto.

Se debe diferenciar entre el encargado de establecer y autorizar los acuerdos con terceros, de los que deban auditar su cumplimiento.

6.3 Gestión de Vulnerabilidades

Se debe establecer una gestión de vulnerabilidades técnicas orientada a analizar los problemas de seguridad (vulnerabilidades) que surgen en los productos de software, que son publicadas en internet por lo proveedores de tecnología asociada y proponer las medidas de mitigación al riesgo definido.
Se debe efectuar validaciones y evaluaciones periódicas de seguridad durante el ciclo de vida del proyecto.
A lo menos una vez cada tres meses, se debe realizar un escaneo de las aplicaciones en busca de vulnerabilidades, manteniendo un registro de los resultados y las acciones correctivas tomadas.

6.4 Documentación

El diccionario de datos, o repositorio de metadatos, debe mantener una descripción actualizada de las definiciones de datos.
Si el programador incluye comentarios en el programa fuente, éstos deben ser útiles para un tercero y no divulgar información de configuración innecesaria.
Respecto a la documentación, ésta se debe:

- Generar durante el ciclo de desarrollo y no postergarla hasta el final.
- Revisar por los usuarios finales del sistema.
- Actualizar si el programa cambia alguna de sus funcionalidades.
- Almacenar en un sitio centralizado (Servidor) administrado por del Departamento de Gestión Sectorial TIC.

6.5 Evaluación o Casos de Negocio

Como parte de las actividades a realizar en esta fase de un proyecto de desarrollo de un sistema de información, se debe clarificar la problemática actual referida a la seguridad de la información, que debe ser cubierta por el nuevo sistema.
En el estudio de factibilidad o anteproyecto, se debe considerar el aspecto de seguridad, en cuanto al nivel de criticidad del sistema y de los controles que se debieran predefinir.

6.6 Especificación detallada de requerimientos

En el análisis de factibilidad de los requerimientos, se debe considerar el nivel de criticidad del sistema, además del nivel de protección de seguridad que requerirán los datos y las aplicaciones que lo compongan.

Los requerimientos de seguridad deben ser compatibles con lo que se establece en las otras Políticas de Seguridad.

6.7 Diseño del Sistema

El nivel de sensibilidad debe ser definido para cada elemento de datos, archivo, programa y sistema.
Si se define utilizar cifrado de datos, debe estar definido en el estándar de cifrados.
Si se utiliza un administrador de bases de datos, se debe emplear las herramientas de seguridad que el producto provee.
Todos los programas críticos deben incluir la generación de registros de auditoria, considerando como mínimo, la identidad del usuario que lee o escribe y la fecha y hora del evento. Estos registros deben ser protegidos contra la manipulación no autorizada.
En la etapa de diseño se debe proyectar el rendimiento esperado de un sistema informático, con el objetivo de no sobre dimensionar los recursos necesarios para el funcionamiento del Sistema (ancho de banda, RAM, recursos del servidor, etc.).

6.8 Codificación y Pruebas

No está permitido modificar programas sin que quede registrado o documentado el cambio.
Se debe usar técnicas de programación modular, usando lenguajes de alto nivel.
No está permitido escribir o modificar código auto-copiante o cualquier otro tipo de código malicioso (virus y gusanos), así como funciones u operaciones no documentadas o no autorizadas en los programas.
En lo posible, las pruebas del sistema deberían incluir: instalación, volumen, stress, rendimiento, almacenamiento, configuración, funcionalidad, seguridad, recuperación ante errores.
En lo posible, las pruebas deben ser realizadas en forma automática, almacenando criterios y datos de pruebas en archivos, de modo de permitir la verificación rápida y repetitiva.

6.9 Implementación

Se debe velar por la implementación de los controles de seguridad al mismo tiempo que la implementación de los componentes, funciones o módulos a los cuales controla.
Se debe efectuar sintonía o ajuste (tuning) de los controles establecidos en la fase de diseño.

6.10 Post Implementación

Se debe revisar y auditar la existencia de los controles de seguridad definidos en la etapa de diseño.

6.11 Controles a implementar

Se debe considerar e implementar, al menos, los siguientes controles:

a. Validación de datos de entrada y de salida
b. Controles de procesamiento interno.
c. Controles criptográficos
d. Protección de los datos de prueba.
e. Segregación de acceso a datos.

7. MECANISMOS DE DIFUSIÓN Y DISTRIBUCIÓN

Esta política, en su versión N°1 se encontrará vigente en página web de la Dirección del Servicio de Salud Metropolitano Sur Oriente, en un banner, cuyo nombre será: Sistema de Seguridad de la Información; en la Intranet de la Dirección del SSMSO, en las mismas condiciones de la página web de esta Institución.
En encargado de seguridad de la información de la Dirección del SSMSO, velará por maximizar la cobertura de su difusión, a lo menos, a través de:

- Publicación en la intranet de la DSS y página web de la Dirección del SSMSO
- Correo informativo
- Manual de la dirección del Servicio
- Entrega de documentos directamente a cada funcionario de la Dirección del SSMSO.

Los establecimientos hospitalarios de la Red Sur Oriente deberán establecer canales accesibles para la comunicación interna permanente de esta Política y todas sus Políticas, procedimientos y otros documentos generados en el marco del Sistema de Seguridad de la Información de cada establecimiento hospitalario.

8. PERIODO DE REVISIÓN DEL DOCUMENTO

La revisión del contenido de esta Política se efectuará, al menos, una vez al año, o atendiendo necesidades de cambios para garantizar su actualización, idoneidad, adecuación y efectividad en su ámbito de control.

Elaborador por:	Revisado por:	Aprobado por:
José Balmaceda Gallardo Jefe (S) Unidad de Desarrollo, Departamento Informática	Cinthia León Fuentealba Encargada de Control Interno SSMSO	Fernando Betanzo Vallejos Director de la Dirección del Servicio de Salud Metropolitano Sur Oriente