Servicio de Salud Metropolitano Sur Oriente
Región Metropolitana
Ministerio de Salud

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

4801 *11.12.2018

APRUEBA POLITICA DE CONTROL DE ACCESO LÓGICO

DE LA DIRECCIÓN DEL SERVICIO DE SALUD METROPOLITANO SUR ORIENTE

RESOLUCION EXENTA N° _____/

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 Control de acceso lógico en esta institución, dictando lo siguiente:

RESOLUCIÓN

ARTICULO N°1- APRUEBASE la Política de Control de Acceso Lógico 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
- 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 CONTROL DE ACCESO LÓGICO

DE LA DIRECCIÓN DEL SERVICIO DE SALUD

METROPOLITANO SUR ORIENTE

AÑO 2018

INDICE

1. OBJETIVO DEL DOCUMENTO 3
2. ALCANCE 3
3. DOCUMENTOS DE REFERENCIA 4
4. DEFINICIONES 4
5. ROLES Y RESPONSABILIDADES 6
   5.1 Encargado de Seguridad de la Información SSMSO (ESI): 6
   5.2 Comité Técnico de Seguridad de la Información SSMSO (CTSI): 6
   5.3 Coordinador de Redes y Comunicaciones DSS / Unidad de Redes y Comunicaciones DSS: 6
   5.4 Funcionarios del SSMSO: 6
6. NOTA DE CONFIDENCIALIDAD DE ACUERDO A CLASIFICACIÓN 7
7. DECLARACIÓN INSTITUCIONAL 7
8. DEFINICIÓN DE LA POLÍTICA 8
   8.1 CONSIDERACIONES GENERALES 8
   8.2 POLITICA CONTROL DE ACCESO 8
9. CUMPLIMIENTO 10
10. CONTROL DE CAMBIOS 10

1. OBJETIVO DEL DOCUMENTO

La presente política tiene como objetivo, proporcionar niveles control con respecto a la integridad y seguridad de los sistemas y recursos de información, a través de un adecuado manejo y mantenimiento de las cuentas del usuario y los derechos y privilegios asociados al acceso a los servicios de comunicación y a las instalaciones de procesamiento de la información.

2. ALCANCE

Esta política aplica a todos los sistemas que se encuentran en la Dirección del Servicio de Salud Metropolitano Sur Oriente, incluyendo sin limitar a las aplicaciones comerciales, bases de datos, aplicaciones desarrolladas internamente, equipos, instalaciones, y redes que la organización posea en la actualidad o en el futuro, de manera que la no inclusión explícita en el presente documento, no constituye argumento para no proteger los activos de información que se encuentren en otras formas.

Abarca además todos los activos de información que la Dirección del Servicio de Salud Metropolitano Sur Oriente, posee en la actualidad o en el futuro, de manera que la no inclusión explícita en el presente documento no constituye argumento para no proteger activos de información que se encuentren en otras formas.
La política cubre toda la información impresa o escrita en papel, almacenada electrónicamente, trasmitida por correo o usando medios electrónicos, mostrada en películas o hablada en una conversación. Se ha definido según las buenas prácticas del estándar NCh-ISO 27001.Of2013, además de los requisitos legales, normativos y contractuales relativos a seguridad de la información que sean aplicables a la organización, como el Decreto Supremo Nº83 del Ministerio Secretaría General de la Presidencia.

3. DOCUMENTOS DE REFERENCIA

- 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"
- Política General de Seguridad de la Información de la Dirección del Servicio de Salud Metropolitano Sur Oriente
- NCh-Iso 27001 – Técnicas de Seguridad – Sistemas de Seguridad de la Información

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 de Desarrollo:** Grupo de trabajo cuyo enfoque principal es la generación, administración, mantención y soporte de aplicativos, programas y soluciones utilizadas tanto en DSS como aquellas disponibles para la red SSMSO.

✓ **Unidad de Redes y Comunicaciones:** Grupo de trabajo cuyo enfoque principal es la administración, gestión, mantención y soporte de todo equipamiento y canales de comunicación digitales y físicos que posee tanto la DSS como aquellos disponibles para la red SSMSO.

- ✓ **Soporte de Infraestructura:** Labor desarrollada por la Unidad de Soporte y Mesa de ayuda en conjunto con la Unidad de Redes y Comunicaciones, cuyo enfoque principal es la administración y mantención de todo equipamiento que compone la arquitectura base necesaria para el correcto funcionamiento de servidores.

- ✓ **Activo:** Es todo aquel que tenga valor para la organización. Una organización incluye diferentes tipos de activos: aquellos relacionados con el entorno (edificios, instalaciones, equipamiento) y personal, activos relacionados con los sistemas de tecnologías de información (equipos, software, comunicaciones), activos relacionados con la información (datos, soporte), activos relacionados con las funcionalidades de la organización (productos, servicios) y activos intangibles (credibilidad, conocimiento acumulado).

- ✓ **Custodio de la información:** Es cualquier persona que mantiene bajo su responsabilidad información de la cual no es el Propietario. Es responsable de aplicar las medidas de seguridad que se definan de acuerdo al valor de los activos.

- ✓ **Incidente de seguridad**: Situación adversa que amenaza o pone en riesgo un sistema.

- ✓ **Información:** Contenido o grupo de datos de interés. Se clasifican en:
  - **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 N°20.285.
  - **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.

- ✓ **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 tanto en la definición del valor de la información como en la definición de permisos de acceso, de manera que se puedan establecer los controles apropiados para protegerla.

- ✓ **Riesgo:** Probabilidad de ocurrencia de un evento indeseado con consecuencias negativas.

5. ROLES Y RESPONSABILIDADES

5.1 Encargado de Seguridad de la Información SSMSO (ESI):

- Revisión de las Políticas de Seguridad de la Información generadas y establecidas por el CGSI.
- Informar al CGSI sobre las situaciones anómalas acontecidas

5.2 Comité Técnico de Seguridad de la Información SSMSO (CTSI):

- Elaboración e implementación de las Políticas de Seguridad de la Información definidas por el CGSI
- Planificación de lineamientos generales para Políticas asociadas a la Seguridad de la Información
- Definir los mecanismos de control para los dominios de seguridad establecidos

5.3 Coordinador de Redes y Comunicaciones DSS / Unidad de Redes y Comunicaciones DSS:

- Aplicación de las Políticas de Seguridad de la Información definidas por CGSI
- Aprobar medidas de control para las excepciones que permitan accesos directos desde orígenes "no confiables"[1] hacia servidores, servicios y sistemas pertenecientes a la DSS, con especial enfoque en aquellos en producción.
- Informar al CTSI y al ESI sobre las situaciones anómalas acontecidas
- Enviar avisos por violación a las normas, políticas, procedimientos y estándares

5.4 Funcionarios del SSMSO:

- Todo funcionario de la Dirección del Servicio de Salud Metropolitano Sur Oriente tiene la obligación de informar a sus Jefaturas Directas de cualquier actividad que contravenga lo aquí estipulado o que simplemente le resulte sospechosa.
- Ser responsable del acceso permitido a las redes de comunicación de la Dirección del Servicio de Salud Metropolitano Sur Oriente
- Utilizar los recursos disponibles indicados en esta Política de una manera acorde al uso responsable de los recursos del Estado

[1] Ver ítem 4: "Definiciones"

6. NOTA DE CONFIDENCIALIDAD DE ACUERDO A CLASIFICACIÓN

Este documento es de propiedad exclusiva de la Dirección del Servicio de Salud Metropolitano Sur Oriente y su uso debe ceñirse a la clasificación del mismo, quedando prohibida la divulgación y/o reproducción total o parcial de su contenido sin la debida autorización por parte del CGSI. Su uso y distribución están restringidos al interior del SSMSO y por parte del personal debidamente habilitado para tal efecto.

7. DECLARACIÓN INSTITUCIONAL

A través de esta Política, la Dirección del Servicio de Salud Metropolitano Sur Oriente establece las normas de gestión y control que permitan proteger la información en los diversos sistemas, aplicaciones, equipamientos o similares que posean algún servicio utilizado a través de la red de comunicaciones, tanto local como metropolitano.

8. DEFINICIÓN DE LA POLÍTICA

8.1 CONSIDERACIONES GENERALES

Referente a servidores y sistemas, dentro de las labores de soporte de Infraestructura se debe limitar la cantidad de intentos continuos errados de conexión hacia los equipamientos, además de llevar un registro de dichos eventos.

Referente a la administración y operatividad de las redes de comunicaciones, la Unidad de Redes y Comunicaciones debe asegurar el límite de duración de las conexiones activas en la red además de sus destinos, junto con mantener un registro de dichos eventos.

Todos los usuarios que accedan y utilicen la red, deben contar con una identificación única que se homologue al menos a alguno de los tres métodos de autenticación recomendados por las normas nacionales e internacionales de Seguridad de la Información (contraseña, token y/o biometría), siguiendo además los lineamientos de la Política de Identificación y Autenticación de Usuarios.

8.2 POLITICA CONTROL DE ACCESO

- ✓ Los funcionarios sólo pueden acceder a visualizar y/o trabajar aquella información para la que están expresamente autorizados por el dueño del activo o el proceso.

- ✓ Ningún usuario debe descargar programas utilitarios sin el visto bueno de Departamento de Informática DSS.

- ✓ Todos los requerimientos de información de la organización que incluyan, sin limitar, comunicados públicos, declaraciones, cuestionarios, encuestas o entrevistas periodísticas, deben ser referidos a la Unidad de Comunicaciones y Relaciones Públicas de la DSS.

- ✓ Se deben establecer procedimientos formales para el registro y eliminación de usuarios, de modo de garantizar que se otorguen y quiten accesos a los sistemas y servicios de información, en consistencia con los niveles de autorización de los usuarios.

- ✓ Se deben revisar los derechos de acceso otorgados a los usuarios regularmente a través de procedimientos formales.

- ✓ Cuando un funcionario deja algún puesto en la organización, los archivos residentes en los computadores y los archivos impresos, deben ser revisados por

su supervisor o jefatura directa, para una inmediata reasignación formal de obligaciones y responsabilidades.

- ✓ Los funcionarios de la organización no deben utilizar herramientas para obtener información de la red, como detección de puertos, servicios y archivos en general en los sistemas de información de la organización.

- ✓ El acceso lógico a la configuración de puertos de manera remota debe ser controlado por el Departamento de Informática de la dirección del Servicio de Salud Metropolitano sur Oriente. Se deben establecer métodos apropiados de autenticación para los usuarios que utilicen accesos remotos. Por ejemplo: Utilización de protocolos de autenticación y autorización como PAP, CHAP o EAP, integración con repositorios de usuarios del IPS (por ejemplo: LDAP o bases de datos de usuarios) y accesos seguros a través de VPN IPSEC o SSL VPN para accesos fuera del perímetro de la red SSMSO.

- ✓ Para los accesos a sistemas, se deben establecer procedimientos de autenticación seguros de modo de minimizar la oportunidad de accesos no autorizados.

- ✓ No se deben utilizar cuentas genéricas para acceder a los sistemas y aplicaciones de la Organización. Cualquier excepción a esta regla, debe ser revisada, formalizada, visada y documentada por la Jefatura del Departamento de Informática de la DSS.

- ✓ Los funcionarios y funcionarias de áreas técnicas, de informática o que tengan algún control administrativo de sistemas, no deben utilizar ninguna estructura de contraseña que resulte predecible o fácil de adivinar. Esto incluye, sin limitar, a contraseñas en blanco, palabras que aparezcan en diccionarios, secuencias comunes de caracteres y datos personales.

- ✓ Las contraseñas fijas no deben ser almacenadas en archivos de ejecución por lotes, scripts automáticos, macros de software, computadoras de control de acceso o en otros medios donde personas no autorizadas pueden conocerlas.

- ✓ Las contraseñas no deben ser escritas o almacenadas en lugares visibles o cerca de los sistemas a los cuales permiten el acceso.

- ✓ Todos los funcionarios de la organización deben dejar siempre sus equipos bloqueados en caso de no estar en su lugar de trabajo.

- ✓ Todos los Equipos de trabajo del personal de la DSS deben estar configurados con protector de pantalla con contraseña.

- ✓ Las sesiones que se encuentren inactivas serán desconectadas después de un periodo de inactividad.
- ✓ El acceso a información, puede ser otorgado de manera individual o ser otorgado a grupos de funcionarios.
- ✓ Las actividades que afectan información sensible de sistemas en producción, deben ser reconstruibles a partir de registros de transacciones.
- ✓ Los mensajes enviados por el sistema electrónico de correos de la organización sólo pueden ser leídos bajo los requerimientos establecidos en la normativa legal, en caso de persecución criminal o administrativa.
- ✓ Todos los dispositivos móviles (como notebooks y smartphones, entre otros) que contienen información sensible de la Organización, deben considerar protección o encriptación de disco duro y archivos.
- ✓ Antes de otorgar los permisos de trabajo remoto a funcionarios de la organización, se debe establecer un Acuerdo de Confidencialidad que proteja la información sensible de la Organización.
- ✓ Los accesos a las salas de equipos de laboratorios de capacitación y de análisis que requieran restricción de ingreso, serán de responsabilidad del encargado del área, ya sea en la definición de quienes puedan ingresar y el control de acceso utilizado para ello.
- ✓ Los accesos físicos y remotos de externos (proveedores, visitas u otros) deben ser controlados.

9. CUMPLIMIENTO

El cumplimiento de las políticas de seguridad, sus normas, procedimientos y estándares, deberá ser una tarea cotidiana y de estricta aplicación por parte de todos los funcionarios, desde el más alto nivel, hasta el último funcionario del escalafón. El incumplimiento de la presente política expone a quien la vulnere a las sanciones pertinentes según la resolución de las investigaciones regidas por vía legal o por un sumario según sea el caso.

10. CONTROL DE CAMBIOS

Fecha	Versión	Página	Numeración del contenido	Cambio Efectuado / Nombre del responsable

Elaborado por:	Revisado por:	Aprobado por:
Nelson Grez Vivanco Jefe de Unidad de Redes y Comunicaciones de la Dirección de la Dirección del Servicio de Salud Metropolitano Sur Oriente	**Cinthia León Fuentealba** Encargada de Control Interno de la Dirección del Servicio de Salud Metropolitano Sur Oriente **Comité Técnico de Seguridad de la Información de la Dirección del Servicio de Salud Metropolitano Sur Oriente.** **Comité de Seguridad de la Información de la Dirección del Servicio de Salud**	**Fernando Betanzo Vallejos** Director de la Dirección Servicio de Salud Metropolitano Sur Oriente