SUBDIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN

Secretaría de Salud del Estado de Chihuahua

STI-POL-002 POLÍTICA DE CONTROL DE ACCESO

Vigencia al 01 de octubre del 2024

Índice

1. Objetivo.

Garantizar que la información, las áreas de procesamiento de información, las redes de datos, los recursos de la plataforma tecnológica y los sistemas de información de Secretaría de Salud y sus Órganos Descentralizados estén debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico y físico.

2. Alcance.

Esta política aplica a toda la información contenida en cualquier medio (digital o físico), en áreas de procesamiento de información, redes de datos, recursos de la plataforma tecnológica y sistemas de información de los Secretaría de Salud y sus Órganos Descentralizados, además para todo el personal y personas que tengan acceso a las instalaciones y sistemas de información.

3. Vigencia.

Esta política está vigente hasta el 01 de octubre del 2024.

4. Generalidades.

Para la Institución, es prioritario definir el personal que tenga acceso a información sensible, por lo cual, limita el acceso de usuarios de aplicaciones computarizadas únicamente, a los funcionarios y demás personal tanto interno como externo, que tengan que ver directamente con sus responsabilidades y funciones a cargo, debido a que la información puede ser sensible o tener un carácter confidencial. Así mismo, es necesario restringir el acceso a las instalaciones donde dicha información se encuentra guardada, garantizando así la confidencialidad e integridad de la misma.

4.1. Directrices de seguridad para todo el personal.

Para dar cumplimiento al control de acceso a la información, todos los involucrados en el alcance deberán acatar lo siguiente:

- Se deberá asignar un nombre de usuario para conceder el acceso a los sistemas de información de los Secretaría de Salud y sus Órganos Descentralizados.
- Para generar acceso tanto físico como lógico a proveedores como contratistas, el supervisor del contrato se deberá realizar la solicitud al área respectiva.
- Una vez que el contrato del contratista o proveedor haya finalizado, el supervisor del contrato tiene la responsabilidad de solicitar la cancelación de los derechos de acceso a el(los) usuario(s) vinculado(s) con ese contrato.
- Se deberá deshabilitar los usuarios y nombres de usuario correspondientes al personal que ya no tenga relación con los Secretaría de Salud y sus Órganos Descentralizados.
- De manera automatizada el sistema deshabilitara los usuarios que no tengan actividad por más de 30 días.

- Cada miembro del personal de los Secretaría de Salud y sus Órganos Descentralizados deberán hacerse responsable de los usuarios y contraseñas asignados para el acceso a los servicios de red, los recursos de la plataforma tecnológica y los sistemas de información.
- El personal no deberá compartir sus cuentas de usuario y contraseñas con otros usuarios, con personal externo o con personal provisto por terceras partes.

4.2. Normas de seguridad para el control de acceso lógico.

- El jefe de área o líder de proceso deberá ser el único autorizado para solicitar el acceso a los servicios de red, a los recursos de la plataforma tecnológica y a los sistemas de información; así mismo deberá especificar los privilegios de acceso al cual está vinculado el usuario, a través de las diferentes categorías.
- La administración de los perfiles de usuario es responsabilidad del encargado de Tecnologías de Información en cada Región Sanitaria; del personal de Soporte de Aplicaciones en Oficinas Centrales y de las áreas responsables de dicho activo.
- El jefe de área o Líder de proceso deberá establecer los permisos que corresponde a cada perfil que puede acceder a los recursos de la plataforma tecnológica, servicios de red y los sistemas de información.
- La Subdirección de Tecnologías de Información deberá crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información cuando esto sea solicitado por el jefe de área o líder de proceso.
- Se deberá establecer controles de acceso a los sistemas de información y garantizar que solo el personal autorizado tenga los privilegios adecuados, para garantizar el acceso a la información. Los privilegios están establecidos, por el nivel de usuarios descritos en el punto *6.1 Tabla de accesos por perfil de usuarios.*

4.3. Normas de seguridad para el control de acceso físico.

- La puerta con cerradura biométrica del centro de datos deberá permanecer siempre cerrada y solo podrá acceder el personal autorizado con acceso biométrico.
- Se deberá aprobar de manera previa las solicitudes de acceso de terceros al centro de cómputo, administración de infraestructura, unidad de diagramación o a los centros de cableado, además se deberá acompañar permanentemente a los visitantes durante su estancia en las áreas mencionadas.
- Se deberá monitorear los ingresos al centro de cómputo permanentemente para identificar accesos no autorizados y para confirmar que los controles de acceso son efectivos.
- Se deberá bloquear de manera inmediata, los privilegios de acceso físico a las instalaciones de la Subdirección de Tecnologías de Información, tan pronto el personal termine su vinculación.
- Se deberá implementar controles de acceso físico al centro de cómputo, para evitar la manipulación no autorizada del cableado.

5. Creación de usuarios.

Para la creación de los usuarios, después de la previa autorización de la Subdirección de Tecnologías de la Información; se toman en cuenta el nombre del usuario para sentar la base de la generación de la contraseña.

Dentro del configurador de cada sistema se gestionan los usuarios; para la creación de la contraseña requiere ciertos lineamientos específicos para ser válida.

Los cuales son:

- Debe ser mayor a 8 caracteres.
- Una letra mayúscula y una minúscula.
- Al menos 1 carácter especial.
- Sin incluir patrón 111.

6. Lineamientos para accesos a sistemas de la Subdirección de Tecnologías de Información.

Para conceder accesos a sistemas como GEHOS, MCE, ECI, LOGOS, todos los usuarios deberán presentar el ***FR-POL-003 Formato de solicitud de cuentas de usuario*** que se encuentra disponible con los responsables de sistemas de cada unidad o en Subdirección de Tecnologías de Información.

Después, pasará por un proceso de autorización, el cual el Subdirector de TI o el responsable de TI de cada unidad aprobará o rechazará la solicitud.

6.1. Tabla de accesos por perfil de usuarios.

Dependiendo del perfil del solicitante, se dará acceso a los sistemas.

La siguiente tabla muestra dependiendo del perfil que acceso se permitirá:

SISTEMA	PERFIL DE USUARIO	ACCESOS
GEHOS	SUPERVISOR MÉDICO	Análisis de consulta.
	SUPERVISOR DE ABASTO	Abasto CPMS, abasto SSCH, abasto ICHISAL.
	DIRECTOR DE UNIDAD	Análisis de consulta, abasto CPMS, abasto SSCH, abasto ICHISAL.
	ADMINISTRADOR DE UNIDAD	Abasto CPMS, abasto SSCH, abasto ICHISAL.
	DIRECTOR DE REGIÓN	Análisis de consulta, abasto CPMS, abasto SSCH, abasto ICHISAL.
	SUPERVISIÓN COVID	Salud digital COVID.
MCE	ESTADÍSTICAS	Impresión de hojas diarias, detalle de la atención, reporteador.
	SUPERVISOR DE UNIDAD	Detalle de la atención, reporteador.

	PERSONAL DE SISTEMAS	Catálogo de médicos, usuarios de consulta externa, disponibilidad, consulta externa offline, impresión de hojas diarias, detalle de la atención, reporteador.
ECI	PERSONAL MÉDICO OPERATIVO	Acceso al expediente clínico integral ECI, modalidad consulta externa, hospitalario según configuración de la unidad médica.
	PERSONAL DE ENFERMERÍA	Acceso al expediente clínico integral ECI, modalidad consulta externa, hospitalario según configuración de la unidad médica.
	SUPERVISOR DE UNIDADES	Acceso al expediente clínico integral ECI, modalidad consulta externa, hospitalario según configuración de la unidad médica.
CITAS	ADMINISTRADOR	Acceso a sistema de citas médicas
	SUPERVISOR DE UNIDADES	Acceso a sistema de citas médicas
	PERSONAL DE CITAS	Acceso a sistema de citas médicas
	REPORTES	Acceso a sistema de citas médicas
LOGOS	PERSONAL OPERATIVO	Acceso a enviar logos al flujo de tecnología.

7. Acuerdos de confidencialidad.

Los acuerdos de confidencialidad, afectan a la información propia de Secretaría de Salud y sus Órganos Descentralizados por lo que se consideran acuerdos de confidencialidad para el personal que cuente con usuario a los sistemas.

Independientemente del acceso otorgado a cada usuario, es de suma importancia cumplir con todos los puntos descritos dentro del acuerdo de confidencialidad ***FR-POL-001 Responsiva de entrega de claves de usuario*** garantizando en todo momento, la confidencialidad y seguridad de la información contenida en los sistemas.

Los acuerdos de confidencialidad se deberán tener firmados por escrito al entregar el acceso al usuario final.

Se manejará con discreción y confidencialidad, la información de Secretaría de Salud y sus Órganos Descentralizados, por lo cual el personal de la Subdirección de Tecnologías de información deberá cumplir y firmar el ***FR-POL-002 Acuerdo Confidencialidad*** para uso de los sistemas informáticos de Secretaría Salud y sus Órganos Descentralizados.