REPÚBLICA DE CHILE

PROVINCIA DE CURICÓ

MUNICIPALIDAD DE ROMERAL

ALCALDÍA.

DECRETO ALCALDICIO N° 0000953 /

REF.: APRUEBA POLITICA DE CONTROL DE ACCESO LOGICO PARA LA ILUSTRE MUNICIPALIDAD DE ROMERAL.

Romeral, 08 ABR 2024

VISTOS

1. La ley N° 19.880 que Establece las Bases de los Procedimientos Administrativos que rigen los actos de los Órganos de la Administración del Estado.
2. La Ley N° 18.883, sobre Estatuto Administrativo para Funcionarios Municipales.
3. El Decreto Exento N° 1652, que Aprueba el Reglamento de la Organización Interna Municipal de fecha 02 de Diciembre de 2019.
4. El Decreto Supremo No 83, que Aprueba la Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos, MINSEGPRES, promulgado con fecha 03 de Junio de 2004.
5. Las facultades que me confiere la ley Nº 18.695 Orgánica Constitucional de Municipalidades, y sus modificaciones.

CONSIDERANDO:

1. La necesidad de la I. lustre Municipalidad de Romeral de contar con una Política de Control de Acceso Lógico del Sistema de Seguridad de la Información.

2. Que, el Decreto Supremo N° 83, que Aprueba la Norma Técnica para los órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los documentos electrónicos, establece en su Artículo 9° que: *"Durante la primera etapa de aplicación de esta norma, los órganos de la Administración del Estado desarrollarán las políticas, procedimientos, acciones y medidas tendientes a obtención del Nivel Básico de Seguridad de los documentos electrónicos que se establecen en este Título".*

DECRETO:

MATERIAS QUE ABORDA La presente política aborda lineamientos de Control de Acceso Lógico del Sistema de Seguridad de la Información, en tópicos de:

- Lineamientos generales de control del acceso
- Accesos a las redes y a los servicios de la red
- Registro y cancelación de registro de usuario
- Gestión de asignación de acceso de usuarios
- Gestión de derechos de acceso privilegiados
- Gestión de información secreta de autenticación de usuarios

- Revisión de los derechos de acceso de usuario
- Eliminación o ajuste de los derechos de acceso
- Uso de información de autenticación secreta
- Restricción de acceso a la información
- Procedimiento de inicio de sesión seguro
- Sistema de gestión de contraseñas
- Uso de programas utilitarios privilegiados
- Control de acceso al código fuente de los programas

Lineamientos generales de control del acceso

- Las reglas de acceso a la red estarán basadas en el principio de Negación por Omisión: "todo está restringido, a menos que esté expresamente permitido".
- Las reglas específicas para el control de acceso, estarán documentadas a través de los diferentes procedimientos de control de acceso a los recursos tecnológicos correspondientes.
- Se establecerá, documentará y revisará los lineamientos de control de accesos en base a las necesidades de seguridad y de servicio de la institución.

Accesos a las redes y a los servicios de la red

- El acceso a redes desde y hacia afuera de la Institución cumplirá con los lineamientos de "Responsabilidad de los Usuarios" y adicionalmente se utilizarán métodos como autenticación de protocolo de enrutamiento, rutas estáticas, traducción de direcciones y listas de control de acceso.
- Se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán, al menos:
- Controlar el acceso a los servicios de red tanto internos como externos.
- Identificar las redes y servicios de red a los cuales se permite el acceso.
- Establecer normas, controles y procedimientos de administración para proteger el acceso a la red de datos de la institución.

Registro y cancelación de registro de usuario

- Se mantendrán protocolos de registro (alta) y cancelación (baja) de usuarios con objeto de habilitar la asignación de derechos de acceso.
-

Gestión de asignación de acceso de usuarios •

- Se deben establecer procedimientos que controlen la asignación y revocación de derechos de acceso o privilegios de acceso a los servicios y sistemas de la I. Municipalidad de Romeral y sus Programas.
- Se establecerán los procedimientos de registro, modificación y borrado de usuario.

Gestión de derechos de acceso privilegiados

- La asignación y uso de derechos de acceso con privilegios especiales o de administrador, debe ser restringido y controlado, dado su alto riesgo en la continuidad operacional de las plataformas tecnológicas.

-

Gestión de información secreta de autenticación de usuarios

- La asignación de información confidencial, como parte de la autenticación del usuario, debe ser controlada mediante un proceso de gestión seguro y auditable.

Revisión de los derechos de acceso de usuario

- Los propietarios de los activos deben poder revisar los derechos de acceso asignados o en curso, de todos los usuarios de los sistemas o plataformas a su cargo.

Eliminación o ajuste de los derechos de acceso

- Se deben retirar los derechos de acceso a la información y a las instalaciones del procesamiento de información para todos los funcionarios, proveedores o usuarios de terceros, a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio.
- Al momento del cese de labores de un funcionario del área Tecnologías de Información se deberá modificar contraseñas de los equipos de producción y accesos remotos.

Uso contraseñas y de cualquier información de autenticación secreta

- Se exige a los usuarios el uso de las mejores prácticas de seguridad en el uso y protección de información confidencial de sus contraseñas e información adicional usada para la autenticación.

Restricción de acceso a la información

- Se debe controlar el acceso de los usuarios y personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, según rol y perfil de cada uno.
-

Procedimiento de inicio de sesión seguro

- Cuando sea requerido por la política de control de accesos se debe controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-on.

Sistema de gestión de contraseñas

- Emplear un identificador formal de autenticación único, con una estructura definida y contraseñas configuradas con mayúsculas y minúsculas, con dígitos, y con al menos 8 caracteres.
- La contraseña asignada a una nueva cuenta de usuario, debe crearse expirada, de modo de obligar a ser cambiada por éste durante su primera conexión.
- Las contraseñas son confidenciales, personales e intransferibles y no deben ser enviadas por email, ni por ningún otro tipo de formulario electrónico.
- Las contraseñas de equipamiento y sistemas en producción se deben modificar cada tres meses.
- Las contraseñas de usuarios de la red corporativa caducan cada tres meses.
- Las contraseñas de Equipos y Sistemas en producción se deben almacenar en sobres cerrados, en un área segura, y se debe informar y copiar a la Jefatura respectiva.

Uso de programas utilitarios privilegiados

Se debe restringir y controlar estrechamente el uso de los Software Utilitarios que poseen la capacidad de sobrepasar (anular o evitar) los controles de acceso a los sistemas y aplicaciones. Debe existir un procedimiento de identificación, autorización y autenticación para este tipo de Software, además, se debe asegurar que:

- Exista una segregación entre los Sistemas en Producción y los softwares utilitarios
- Existe un límite en el uso de softwares utilitarios a un número mínimo y práctico de funcionarios autorizados expresamente por el Encargado de la Unidad de TIC.
- Debe existir una lista de los softwares de estas características permitidos en la Municipalidad de Romeral, a la que sólo el Encargado de Operaciones y Superiores pueden tener acceso.

Control de acceso al código fuente de los programas.

- Se debe restringir el acceso al código fuente de las aplicaciones software.

PERIODO DE REVISIÓN

- La Municipalidad debe establecer una revisión independiente la cual asegure la idoneidad, adecuación y efectividad continua del enfoque para administrar la seguridad de la información. Dicha revisión la deberían realizar personas independientes del área bajo revisión o una organización externa que se especialice. Los resultados de la revisión independiente se deberían registrar e informar a la dirección que inició esta revisión y mantener estos registros.
- Esta política de Seguridad debe ser revisadas cada 3 años como máximo, para mantener al día su vigencia.

EVALUACIÓN DE CUMPLIMIENTO

- La revisión del cumplimiento de esta Política se efectuará anualmente por el Encargado de Seguridad de la Información. Adicionalmente, según lo requiera un caso particular, podría requerirse una revisión de cumplimiento por Auditoría Municipal, auditoría interna, jefaturas de cada Unidad o el Comité de Seguridad de la Información, atendiendo necesidades de cambios, para garantizar su idoneidad, adecuación y efectividad.

EXCEPCIONES AL CUMPLIMIENTO DE ESTA POLÍTICA

- Frente a casos especiales, el Comité de Seguridad de la Información podrá establecer condiciones puntuales de excepción en el cumplimiento de las directrices de esta Política de Seguridad de la Información, siempre que no infrinja la legislación vigente ni afecte directrices de otras Políticas. Toda excepción debe ser documentada y se le debe efectuar seguimiento, generando un proceso de revisión de la misma, para determinar si amerita una nueva directriz particular o un cambio en otra ya existente.

0007953

0 8 ABR 2024

COMUNÍQUESE el presente Decreto a las Direcciones, Departamentos y Oficinas Municipales, y publíquese en la pagina web de transparencia activa de la Ilustre Municipalidad de Romeral.

ANÓTESE, COMUNIQUESE, Y ARCHIVESE

GUILLERMO MONTERO RAMÍREZ
SECRETARIO MUNICIPAL

CARLOS VERGARA ZEREGA
ALCALDE

CVZ/GMR/JGR/fpm
DISTRIBUCIÓN:

- Informática
- Oficina de Partes
- Departamento RRHH