1.0 OBJETIVO

Establecer las actividades necesarias para la gestión de derechos de accesos a los sistemas de información del organismo

2.0 ALCANCE Y CAMPO DE APLICACIÓN

Este procedimiento es aplicable a toda la información que se encuentra en las carpetas compartidas, bases de datos, sistemas computacionales, servidores, etc., del organismo. Es aplicable a todos los empleados y terceros que presten sus servicios al Organismo de Agua Potable, Alcantarillado y Saneamiento de Naucalpan.

3.0 REFERENCIAS

Manual de Gestión, sección 7.1.3 Infraestructura
DF-14-03 Soporte a Sistemas y BD
MG-15 Declaración de Aplicabilidad (SoA)

- A.6.2.2 Teletrabajo
- A.9.1.2 El acceso a las redes y servicios de red.
- A.9.2.1 Registro y cancelación de usuario
- A.9.2.2 Provisión de acceso de los usuarios
- A.9.2.3 Gestión de derechos de acceso privilegiado
- A.9.2.4 Gestión de la información secreta de autenticación de los usuarios
- A.9.2.5 Revisión de los derechos de acceso de usuario
- A.9.2.6 Retirada o ajuste de los derechos de acceso
- A.9.3.1 Uso de la información de autenticación secreta
- A.9.4.1 Restricción del acceso a la información
- A.9.4.3 Sistema de gestión de contraseñas
- A.9.4.4 Uso de las utilidades privilegiadas de los programas

4.0 RESPONSABILIDADES

Subgerencia de Informantica: Define los accesos a los datos por parte de los usuarios del organismo y terceros, cuidando tener una adecuada segregación de funciones, así como gestionar los accesos definidos.

Unidad de Soporte a Redes: Dispone de los controles y políticas de controles de acceso. Así como gestionar los derechos de acceso a los medios de procesamiento de información según lo descrito en las Políticas de Seguridad de la Información (MG-16).

5.0 GENERALIDADES

A.6.2.2 Teletrabajo

Todo acceso desde redes externas a la red del OAPAS, será autorizado por la Subgerencia de informática. Para el acceso al teletrabajo se deben tener en cuenta las necesidades técnicas y tecnológicas que garanticen que los usuarios cuentan con las herramientas necesarias como: lugar donde se realizaran las actividades, horario en el que se realizan las actividades y requisitos técnicos para la realización de las actividades que solicite el usuario del proceso manteniendo en todo momento los principios de eficiencia, eficacia y uso racional de los recursos.

Los servicios de teletrabajo deben garantizar en todo momento la seguridad de la información, las condiciones mínimas que se deben implementar incluyen:

- Comprobar y certificar la identidad de los usuarios que utilizan la conexión para el teletrabajo.
- Autorizar el acceso únicamente a la información, servicios y sistemas de información necesarios.
- Separar los accesos de comunicación entre los diferentes usuarios de teletrabajo, para impedir acceso no autorizado a información o servicios, garantizar la integridad de la información y acceso a los sistemas de información cuando se usan los servicios de teletrabajo.
- Las conexiones a servicio de teletrabajo deben permanecer cifradas y utilizando conexiones seguras o redes privadas.

Por lo tanto, cualquier petición de acceso se debe de realizar por medio de un correo electrónico dirigido a la Unidad de Soporte a Redes.

A.9.1.2 El acceso a las redes y servicios de red .

Los servicios de red con los cuales cuenta el organismo se clasifican de la siguiente manera:

- Administración/configuración: Facilita la administración y configuración de las configuraciones de los distintos equipos de la red (DHCP/DNS).
- Acceso: El usuario debe identificarse conectándose con un servidor en el cual se autentifica por medio de un nombre de usuario y una clave de acceso.
- Impresión: Permite compartir impresoras entre varios equipos de la red
- Información: Los servidores de información pueden almacenar bases de datos para su consulta por los usuarios de la red.

- Comunicación: Permiten la comunicación entre los usuarios a través de mensajes escritos (correo electrónico).

Los servicios antes mencionados son solicitados por medio de **Orden de Trabajo** (registro **ON-SIN-01**) en el sistema RAS u oficio si tienen que ser autorizados por la Subgerencia de informática.

A.9.2.1Registro y cancelación de usuario.

La Subgerencia de Informática, mantiene los registros donde cada uno de los responsables de los procesos haya autorizado a usuarios o terceros el acceso a los diferentes sistemas de información del organismo como lo establece el procedimiento DF-14-03 Soporte a Sistemas y BD. Cuando se retire o cambie de contrato cualquier usuario o tercero, se debe de notificar a la Subgerencia de informática mediante un oficio para que elimine o cambie de privilegios en los sistemas de información a los que el usuario está autorizado o se dé totalmente dado de baja.

A.9.2.2 Provisión de acceso de los usuarios

Para administrar los accesos a los sistemas de información se definen perfiles de cada usuario y se utilizan IDs únicos que permitan relacionar a los usuarios con sus responsabilidades como lo establece el procedimiento DF-14-03 Soporte a Sistemas y BD. La Subgerencia de Recursos Humanos en conjunto con la Subgerencia de Control Patrimonial elabora el **Constancia de no adeudo de bienes muebles** (registro **ON-SHR-09**) del personal que deja de laborar en el organismo para que el personal no tenga acceso al equipo de cómputo como a los sistemas de información.

A.9.2.3 Gestión de derechos de acceso privilegiado.

Se deben realizar revisiones de privilegios de acceso a los diferentes sistemas de información por parte de usuarios y terceros, manteniendo los registros de las revisiones y hallazgos.
La asignación de los accesos privilegiados se hace a través del Active Directory de la siguiente manera:

- La solicitud de usuarios con derechos de acceso privilegiado de otras áreas distintas a la Subgerencia de Informática se hace mediante correo electrónico y/u oficio.
- Los sistemas de información deben garantizar la administración de usuarios con perfiles especiales de consulta para auditoría de los sistemas de información.

A.9.2.4Gestión de la información secreta de autenticación de los usuarios

Todos los usuarios (incluido el personal de la Subgerencia de informática, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de Usuario) solamente para su uso personal exclusivo, de manera que las actividades tengan trazabilidad.

A.9.2.5 Revisión de los derechos de acceso de usuario

La Subgerencia de informática es la responsable de los accesos de los administradores de

aplicaciones, de forma que se establezca un control efectivo desde el registro inicial de la cuenta hasta el momento en que se requiera ser modificada, revocada o eliminada. Todo aquello que no puede ser realizado por la aplicación es considerado como mantenimiento de la base de datos y es solicitado mediante oficio, memorándum u **Orden de Trabajo** (registro **ON-SIN-01**) por medio del Sistema RAS.

A.9.2.6 Retirada o ajuste de los derechos de acceso.
La Subgerencia de Recursos humanos o jefe de área debe revisar en forma periódica los perfiles de usuario del personal vigente, y solicitar a la Subdirección de Informática la actualización de estos como lo establece el procedimiento DF-14-03 Soporte a Sistemas y BD

A.9.3.1 Uso de la información de autenticación secreta
Todos los usuarios deben cumplir con las directrices establecidas en el MG-16 Políticas de Seguridad de la información, así como mantener la información de autenticación secreta, como sensible, asegurándose de que no se divulguen, incluidas las personas con autoridad.

A.9.4.1 Restricción del acceso a la información
El nivel de privilegios de una cuenta de usuario estándar es definido de acuerdo al procedimiento DF-14-02 Mantenimiento correctivo y procedimiento DF-14-03 Sistema de Base de Datos cualquier requerimiento adicional de acceso debe ser se hace mediante correo electrónico y/u oficio.

A.9.4.3 Sistema de gestión de contraseñas
Cada usuario debe apegarse a la Política de Control de Acceso, establecida en el MG-16 Políticas de Seguridad de la información. El sistema de administración de contraseñas:

a) Obliga el uso de User ID´s y contraseñas individuales para determinar responsabilidades.
b) Permite que los usuarios seleccionen y cambien sus propias contraseñas luego de cumplido el plazo mínimo de mantenimiento de las mismas o cuando consideren que la misma ha sido comprometida e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
c) Obliga a los usuarios a cambiar las contraseñas provisionales o que han sido asignadas por el administrador del sistema de información.
d) No permite mostrar las contraseñas en texto claro cuando son ingresadas.
e) Almacenar las contraseñas en forma cifrada.

A.9.4.4 Uso de las utilidades privilegiadas de los programas
Se establece un conjunto de programas utilitarios instalados por defecto en cada equipo de cómputo, para el uso de cualquier software adicional el Jefe de Área debe hacer la solicitud

a través de oficio a la Subgerencia de Informática para su evaluación y aprobación en caso de ser viable. En el Active Directoy son realizadas por medio de la consola de administración de directivas de grupo en la cual se configura los privilegios de los usuarios que se encuentran en la red.

6.0 DIFUSIÓN

• MG-02 ESTRUCTURA ORGANIZACIONAL			
• Dirección General	• Secretaría Particular	• Secretaría Técnica	• Subgerencia de Calidad
• Subgerencia de Planeación y Evaluación	• Subgerencia de Transparencia y Oficialía de Partes	• Subgerencia de Relaciones Publicas	• Contraloría Interna
• Subgerencia de Responsabilidades	• Subgerencia de Control de Obras	• Subgerencia de Auditoria Administrativa Financiera y Administrativa	• Dirección de Administración y Finanzas
• Gerencia de Administración	• Gerencia de Finanzas	• Subgerencia de Recursos Humanos	• Subgerencia de Informática
• Subgerencia de Recursos Materiales	• Subgerencia de Patrimonio	• Subgerencia de Tesorería	• Subgerencia de Contabilidad
• Dirección Jurídica	• Subgerencia de Ejecución Fiscal	• Subgerencia de Penal, Civil, Laboral.	• Subgerencia de lo Contencioso y Procedimientos Administrativos
• Dirección de Comercialización	• Gerencia de Atención a Usuarios	• Gerencia de Inspecciones y Restricciones	• Subgerencia de Altas Padrón y Censo
• Sugerencia de Medidores	• Subgerencia Central	• Subgerencia San Esteban	• Subgerencia San Esteban
• Subgerencia Tecamachalco	• Subgerencia Satélite	• Subgerencia Lomas Verdes	• Subgerencia Echegaray
• Subgerencia San Mateo	• Dirección de Construcción y Operación Hidráulica	• Gerencia de Operación Hidráulica	• Gerencia Técnica
• Subgerencia de Drenaje y Alcantarillado	• Subgerencia de Electromecánica	• Subgerencia de Efluentes y Calidad del Agua	• Subgerencia de Agua Potable
• Subgerencia de Planeación e	• Subgerencia de Construcción	• Subgerencia de Estudios y	• Subgerencia de Bacheo

Integración de Obra		Proyectos y Sectorización	
• Subgerencia de Factibilidades			

8.0 REGISTROS DE CALIDAD

1. ON-SHR-09 **“Constancia de no adeudo de bienes muebles**”
2. ON-SIN-01 **“Orden de Trabajo”**

9.0 TABLA DE REVISIONES

TABLA DE REVISIONES	
TÍTULO:	Control de Acceso
CÓDIGO:	PC-14-03
REVISIÓN:	07
CAMBIO / DESCRIPCIÓN:	Se realiza corrección en el nombre de la persona que elaboro.
FECHA DE ELABORACIÓN:	10 de Octubre del 2017
FECHA DE REVISIÓN:	07 de Julio del 2021

10.0 AUTORIZACIÓN

ELABORÓ	REVISÓ	AUTORIZÓ
José Frías Godínez **Unidad de Soporte a Redes**	José Antonio Arias Montes **Subgerencia de Informática**	Armando Rodríguez García **Dirección de Administración y Finanzas**
NOMBRE Y CARGO		