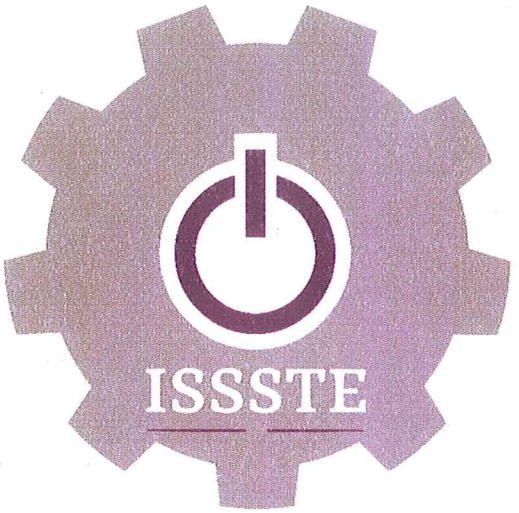

ADMINISTRACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ASI)

ASI FL – POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

CONTRASEÑAS

POL-SGSI-32

CONTENIDO

I. DESCRIPCIÓN GENERAL

El tratamiento diario de la información del Instituto requiere el acceso a distintos servicios, dispositivos y aplicaciones para los cuales utilizamos la pareja de credenciales: usuario y contraseña. Por la seguridad de los servicios y sistemas en los que existen cuentas de usuarios, se tiene que garantizar que las credenciales de autenticación se generan, actualizan y revocan de forma óptima y segura.

En el control de accesos el nombre de usuario nos identifica y la contraseña nos autentica (con ella se comprueba que somos quienes decimos ser).Todo sistema de autenticación de usuarios se basa en la utilización de uno, o varios, de los siguientes factores:

- Algo que sabes: contraseñas, preguntas personales, etc.
- Algo que eres: huellas digitales, iris o retina, voz, etc.
- Algo que tienes: tokens criptográficos, tarjeta de coordenadas, etc.

Como la contraseña es el más utilizado de estos factores, la gestión de las contraseñas es uno de los aspectos más importantes para asegurar los aplicativos y sistemas de información del Instituto. Las contraseñas deficientes o mal custodiadas pueden favorecer el acceso y el uso no autorizado de los datos, información y servicios del ISSSTE.

Dentro de la gestión de contraseñas se incluye el deber de difundir y hacer cumplir buenas prácticas: actualizarlas periódicamente, garantizar su fortaleza (dificultad para adivinarla o craquearla), no utilizar contraseñas por defecto o cómo custodiarlas.

La Subdirección de Tecnología de la Información es la Unidad Administrativa encargada de la operación y responsable del cumplimiento de las regulaciones de las presentes políticas, por lo cual tiene la facultad permitir o denegar acceso a recursos de índole informático con la finalidad de mantener la seguridad de la información del Instituto.

El uso adecuado proporciona garantía razonable de no exponer a riesgos adicionales a los activos de procesamiento y a la información misma.

II. PROPÓSITO

Establecer lineamientos para el correcto uso de cuentas usuario de dominio que proporciona el Instituto para poder ingresar a los equipos de cómputo, el correo electrónico y demás componentes tecnológicos, con el fin de evitar su utilización indebida o prohibida, propiciando un ambiente de seguridad del uso de la información.

Para garantizar que las contraseñas se generan y usan de forma robusta, se cuenta con la herramienta Active Directory (Directorio Activo).

III. ALCANCE

La política aplica a todos los servidores públicos y trabajadores del Instituto; Directores, Subdirectores, Jefes de Servicio, Jefes de Departamento, personal de base y confianza, que en función al desarrollo de sus actividades poseen o requieren una cuenta de dominio y/o de correo electrónico Institucional.

IV. POLÍTICA

1. Cuenta de usuario de dominio (directorio activo)

1. Las cuentas de usuarios de dominio y contraseñas de acceso son una herramienta de índole tecnológica que coadyuva al desempeño de las labores del personal del Instituto.
2. Las cuentas de usuario dominio tienen como objeto proporcionar acceso al usuario al equipo de cómputo, correo electrónico y a los recursos tecnológicos institucionales asignados para el desarrollo de sus funciones. La cuenta puede ser ligada al servicio de navegación a internet y algunos aplicativos institucionales en el caso de ser solicitados.
3. Las solicitudes de cuenta de usuario de dominio se tramitarán mediante el formato de Alta, Baja o Cambio (ABC), que será gestionado por los enlaces informáticos designados para tal efecto, con la autorización del subdirector inmediato superior del área administrativa a la que pertenezca el usuario.
4. Todos los usuarios deberán firmar la versión vigente de la responsiva de usuario (FR-001), mediante la cual se aceptan las políticas de uso antes de recibir el servicio.
5. Las cuentas serán personalizadas para el usuario final.
6. No se asignarán cuentas personalizadas a solicitud del usuario final.
7. Las cuentas de usuario de dominio no tendrán privilegios de administrador.
8. Los únicos usuarios con privilegios superiores estarán restringidos exclusivamente al personal autorizado de la Subdirección de Tecnología de la Información.
9. En caso de requerir cuentas especiales para la operación normal, ésta deberá solicitarse y justificarse plenamente, para lo cual deberá firmar la versión vigente del formato de usuario de Directorio Activo con privilegios (FUP-001), mismo que tendrá que renovarse cada seis meses; de lo contrario se revocarán los privilegios.

V. DE LAS CONTRASEÑAS

1. En el proceso de alta de usuario, la Subdirección de Tecnología de la Información asignará una contraseña de primer inicio de sesión.
2. La contraseña de ingreso al equipo de cómputo, accesorios y componentes tecnológicos, será la misma del correo electrónico institucional.
3. La contraseña (password) que se asignará al usuario deberá tener como mínimo una longitud de doce dígitos y contener al menos un carácter de cada uno de los siguientes cuatros grupos:
    a. *Mayúsculas (A-Z)*
    b. *Minúsculas (a-z)*
    c. *Caracteres Especiales (! " # $ % & ' ( ) * + - / = ? @ ` [\ ] ^ _ { | } ~ ¨)*
    d. *Números (0-9)*
4. Es responsabilidad del usuario el cambio de la contraseña de manera inmediata y cuidará de ella para que no sea difundida a terceros o le sea olvidada.
5. No se debe utilizar la misma contraseña para diferentes servicios. Tampoco se debe manejar las mismas contraseñas para uso profesional y personal. De esta forma se reducirá el riesgo en el caso de que alguna haya sido comprometida.
6. La contraseña tendrá una vigencia de noventa días. Antes de caducar el sistema enviará un mensaje solicitando su cambio. La nueva contraseña deberá ser diferente a la que acaba de vencer.
7. En caso de no llevar a cabo el cambio de contraseña, la cuenta pasará al estado de bloqueo.
8. Se contará con tres oportunidades de ingresar la contraseña para acceder a la red. En el caso de digitarla de manera inválida o incorrecta, se bloqueará el equipo automáticamente.
9. Para el desbloqueo de la cuenta, el usuario de dominio tendrá que generar un ticket en la Mesa Central de Servicios.
10. Todos los equipos de cómputo contarán con un usuario con privilegios de administrador local cuya contraseña será administrada únicamente por personal autorizado por la Subdirección de Tecnología de la Información.
11. Todas las contraseñas correspondientes a cuentas locales de administrador deberán ser resguardadas por cada uno de los enlaces informáticos, para su uso en caso de que se solicite una configuración particular, la solución de problemas e instalación de software especializado y por lo tanto no deberán ser compartidas por ningún motivo.

12. Las contraseñas correspondientes a cuentas especiales de administración de infraestructura en equipo de cómputo serán de uso y administración por el área de Atención a Usuarios en conjunto con el personal informático autorizado en cada una de las áreas del Instituto.
13. En el caso de que se requiera obtener información de algún equipo de escritorio o portátil, de un servidor público que se encuentre ausente de forma temporal o definitiva, únicamente podrá ser solicitado de manera oficial por el subdirector inmediato del área administrativa competente.

VI. DE LAS RESPONSABILIDADES

1. El usuario es responsable en su totalidad de su clave de acceso, por lo cual es personal e intransferible.
2. El usuario es responsable por las acciones que se lleven a cabo con su cuenta personal, en las bases de datos, archivos recibidos o enviados por correo electrónico y uso de recursos tecnológicos institucionales.
3. Es responsabilidad de cada usuario, notificar a su área administrativa y enlace informático la baja, suspensión temporal o cambio de adscripción al interior del Instituto.
4. Cada enlace informático será responsable de informar las bajas o cambio de adscripción a la Subdirección de Tecnología de la Información, para los trabajos de actualización del Directorio Activo.
5. Si las cuentas de dominio no registran actividad en dos meses y no se tiene notificación de baja, suspensión temporal o cambio de adscripción al interior del Instituto, serán deshabilitadas.
6. La Subdirección de Tecnología de la Información, se reserva la facultad de deshabilitar las cuentas de forma inmediata, cuando se detecte un mal uso de ellas.

VII. TÉRMINOS Y DEFINICIONES

Término	Descripción
Contraseña	Código secreto que se introduce en una máquina para poder accionar un mecanismo o para acceder a ciertas funciones informáticas.
Directorio Activo	Servicio de directorio que tiene una estructura de base de datos distribuida y jerárquica, comparte información de infraestructura para localizar, proteger, administrar y organizar los recursos del equipo y de la red, como archivos, usuarios, grupos y periféricos.
Riesgo	Potencial de que cierta amenaza pueda explotar las vulnerabilidades de un activo o grupo de activos y causar daño a la organización.
Usuario	El individuo que usa una computadora, sistema operativo, servicio u otro aplicativo; por lo general se identifica mediante nombre (ID) y contraseña.

VIII. BITÁCORA DE CAMBIOS

DESCRIPCIÓN DEL CAMBIO	IMPACTO	APROBÓ	FECHA DE APLICACIÓN
V 1. Primera versión del documento.	De observancia para todas las áreas del ISSSTE	GESI	Noviembre 2019