MUNICIPALIDAD DISTRITAL DE CHORRILLOS
GERENCIA MUNICIPAL

"Año del Bicentenario del Perú: 200 años de Independencia"

RESOLUCIÓN DE GERENCIA MUNICIPAL Nº 136-2021-GM/MDCH

Chorrillos, 11 de noviembre de 2021

VISTO:

El Informe N° 099-2021-MDCH-GIT de fecha 04 de agosto de 2021, emitido por la Gerencia de Informática y Tecnología; el Informe Técnico N° 099-2021-MDCH/GPP/AFP de fecha 31 de agosto de 2021, emitido por el Área Funcional de Planeamiento Institucional; el Memorándum N° 498-2021-MDCH/GPP de fecha 01 de setiembre de 2021, emitido por la Gerencia de Planeamiento y Presupuesto; el Memorándum N° 314-2021-GAJ/MDCH de fecha 08 de setiembre de 2021, emitido por la Gerencia de Asesoría Jurídica; el Informe N° 114-2021-MDCH-GIT de fecha 27 de octubre de 2021, emitido por la Gerencia de Informática y Tecnología; y el Informe N° 259-2021-MDCH-GAJ de fecha 28 de octubre de 2021, emitido por la Gerencia de Asesoría Jurídica.

CONSIDERANDO:

Que, el artículo 194° de la Constitución Política del Perú, modificado por la Ley N° 27680, Ley de Reforma Constitucional, concordante con el articulo II del Título Preliminar de la Ley N° 27972, Ley Orgánica de Municipalidades, establece que "Los Gobiernos Locales gozan de autonomía política, económica y administrativa en los asuntos de su competencia". La autonomía radica en la facultad de ejercer actos de gobierno, administrativos y de administración, con sujeción al ordenamiento jurídico;

Que, el numeral 7.3 del artículo 73° del Texto único Ordenado de la Ley N° 27444 – Ley del Procedimiento Administrativo General, modificado por Decreto Supremo N° 004-2019-JUS, dispone que: Cada entidad es competente para realizar tareas materiales internas necesarias para el eficiente cumplimiento de su misión y objetivos;

Que, el artículo 4° de la Ley N° 27658, Ley Marco de la Modernización del Estado, señala que el proceso de modernización de la gestión del Estado tiene como finalidad fundamental la obtención de mayores niveles de eficiencia del aparato estatal de manera que se logre una mejor atención a la ciudadanía, priorizando y optimizando el uso de los recursos públicos;

Que, con Informe N°099-2021-MDCH-GIT de fecha 04 de agosto de 2021, de la Gerencia de Informática y Tecnología, presenta el proyecto de directiva denominada "Directiva para el Control de las Cuentas de Usuarios", para su aprobación, siendo ampliado mediante Informe N° 114-2021-MDCH-GIT de fecha 27 de octubre de 2021.

Que, mediante Informe Técnico 099-2021-AFPI-GPP-MDCH, inmerso en el Memorándum N° 498-2021-MDCH/GPP de la Gerencia de Planeamiento y Presupuesto, el Área Funcional de Planeamiento Institucional emite opinión técnica respecto al proyecto de Directiva denominada "**DIRECTIVA PARA EL CONTROL DE LAS CUENTAS DE USUARIOS**", de lo que se colige que, de acuerdo al ROF, es competencia la Gerencia de Informática y Tecnología velar por el cumplimiento de la misma, toda vez que será un instrumento que brindara lineamientos técnicos de carácter operativo; por lo que este despacho opina que está dentro de los criterios de modernización el Estado y se encuentra alineado a los objetivos estratégicos de la entidad resultando viable su aprobación;

Que, con el Informe N° 259-2021-GAJ/MDCH, de fecha 28 de octubre de 2021 de la Gerencia de Asesoría Jurídica, opina VIABLE la aprobación de la "**DIRECTIVA PARA EL CONTROL DE LAS CUENTAS DE USUARIOS**", formulada por la Gerencia de Informática y Tecnología, debiendo la Gerencia Municipal emitir el acto resolutivo para la aprobación de la mencionada Directiva;

Estando a lo expuesto y en uso de las facultades conferidas mediante Ley N° 27972, Ley Orgánica de Municipalidades y la Directiva N° 005-2020-MDCH/GM;

SE RESUELVE:

ARTÍCULO PRIMERO.- **APROBAR,** la Directiva N° 009-2021-GM/MDCH, denominada "**DIRECTIVA PARA EL CONTROL DE LAS CUENTAS DE USUARIOS**", la cual forma parte integrante de la presente resolución.

ARTÍCULO SEGUNDO.- **ENCARGAR** a la Gerencia de Informática y Tecnología y demás áreas competentes, el cumplimiento y seguimiento de las medidas establecidas en la presente Directiva.

ARTÍCULO TERCERO.- **ENCARGAR** a la Gerencia de Informática y Tecnología la publicación de la presente resolución en el portal Institucional (www.munichorrillos.gob.pe).

REGÍSTRESE, COMUNÍQUESE Y CÚMPLASE

MUNICIPALIDAD DE CHORRILLOS
GERENCIA DE ASESORIA JURIDICA
V°B°

MUNICIPALIDAD DE CHORRILLOS
V°B°
AREA FUNCIONAL DE PLANEAMIENTO, PROMOCION DE LA INVERSION

MUNICIPALIDAD DE CHORRILLOS
Mg. Luis A. Vega Marroquin
GERENTE MUNICIPAL

"Año del Bicentenario del Perú: 200 años de Independencia"

DIRECTIVA N° 09-2021-GM/MDCH

"DIRECTIVA QUE REGULA EL CONTROL DE LAS CUENTAS DE USUARIOS"

-2021-

ELABORADO POR:
Gerencia de Informática y Tecnología
REVISADO POR:

Gerencia de Planeamiento y Presupuesto	Gerencia de Asesoría Jurídica

APROBADO POR:
Gerencia Municipal

DIRECTIVA N° 009-2021-GM/MDCH

"DIRECTIVA QUE REGULA EL CONTROL DE LAS CUENTAS DE USUARIOS EN LA MUNICIPALIDAD DISTRITAL DE CHORRILLOS"

I. **Objetivo**:

Fortalecer el control y seguridad de las cuentas de usuarios, prevenir accesos no autorizados a los sistemas de Información de la entidad; asimismo, en el presente documento se establece los procedimientos, controles y accesos para resguardo de contraseñas de las Cuentas de Usuario y las Cuentas de los Administradores de Sistemas de Información.

II. **Finalidad**:

Establecer normas y controles, manteniendo un procedimiento uniforme para la creación, modificación y eliminación de las cuentas de los equipos informáticos y/o usuarios de los sistemas de información, pertenecientes a esta Entidad edil, las cuales están bajo la administración y control de la Gerencia de Informática y Tecnología de esta Municipalidad.

Para tal efecto, la Gerencia de Informática y Tecnología es la unidad orgánica responsable de dar soporte y administrar dichos accesos a los diferentes equipos informáticos y módulos de los sistemas de información, dependiendo de las funciones y responsabilidades asignadas y a ser ejecutadas, por cada uno de los usuarios.

III. **Base Legal**:

3.1 Ley N° 27972, Ley Orgánica de Municipalidades, y sus modificatorias.
3.2 Ley N° 28716, Ley de Control Interno de las Entidades del Estado, y sus modificatorias.
3.3 Decreto Supremo N° 004-2013-PCM, que aprueba la Política Nacional de Modernización de la Gestión Pública.
3.4 Decreto Supremo N° 081-2013-PCM, mediante el cual se aprueba la Política Nacional de Gobierno Electrónico 2013 - 2017.
Estratégicos para el Gobierno Electrónico en el Perú.
3.5. Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
3.6. Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412
3.7 Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC27001:2014, y sus modificatorias.
3.8. Resolución de Contraloría General N° 320-2006-CG, que aprueba las normas de Control Interno.
3.9 Ordenanza N° 413-2021-MDCH, que aprueba el Nuevo Reglamento de Organización y Funciones y la Estructura Orgánica de la Municipalidad Distrital de Chorrillos.
3.10 Norma Técnica Peruana NTP-ISO/IEC 17799:2004 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información - ONGEI.
3.11 Norma Técnica Peruana PNTP-ISO/IEC 27001:2008 EDI. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información.

IV. **Alcance**:

Las disposiciones contenidas en la presente Directiva, serán de aplicación obligatoria por todas las unidades orgánicas de la Municipalidad Distrital de Chorrillos, así como por todo el personal que labora o brinda servicios a esta Entidad edil, bajo cualquier régimen laboral o modalidad contractual.

V. **Responsabilidad:**

Todas las unidades orgánicas de la Municipalidad Distrital de Chorrillos, son responsables de la aplicación de la presente Directiva.

VI. **Definiciones:**

6.1 **Usuarios:** El usuario es la persona que labora o brinda servicios en esta Entidad edil, bajo cualquier régimen laboral o modalidad contractual que dispone de una cuenta de usuario de acceso a los equipos informáticos y/o cuenta de usuario de acceso a los sistemas de información, para hacer uso de los recursos de la red y demás sistemas de información

6.2 Cuentas de usuarios: En las cuentas de los usuarios, se establecen datos como el propietario de la misma, contraseña de acceso, localización de su directorio de inicio de sesión, grupo al que pertenece, etc.

6.3 Crear Cuenta: Asignar una identificación (usuario y una contraseña) para acceder a un equipo informático y/o sistema de información; por ejemplo, equipo, programas, entre otros.

6.4 Desactivar Cuenta: Aplica para casos como baja de personal, así como desplazamiento de éste, entre otras situaciones, en donde se desactiva la cuenta de usuario.

6.5 Bloqueo Cuenta: Suspender temporalmente los accesos a un equipo informático y /o sistema de información, por motivos de ausencia de personal, tales como: vacaciones, licencias, etc.

6.6 Desbloqueo Cuenta: Liberar los servicios de acceso a un equipo informático y/o sistema de información.

6.7 Clave o contraseña: Todo usuario de un equipo informático y/o sistema de informacion, debe contar con una clave o contraseña que lo identifique come tal. La contraseña o password o palabra clave, es de carácter privado, por lo que indistintamente de cual se use, se refiere al complemento del usuario, que es la parte secreta y sólo el dueño del usuario debe conocer.

6.8 Cambiar Clave: Se pueden cambiar las claves o contraseñas, tantas veces sea necesario, para así aumentar la seguridad y que nadie ajeno acceda a su equipo, aplicativo y/o sistema de información.

6.9 Perfil: Asignación de acceso a los usuarios de equipos informáticos y/o sistemas de información, de acuerdo al rol de las funciones a ser ejecutadas por los usuarios.

6.10 Dominio: Es un grupo lógico de equipos, que comparten cuentas de usuarios y seguridad de los recursos. Los usuarios de un mismo dominio, tendrán un inicio de sesión único en el servidor del dominio, para acceder a los recursos de cualquier parte de la red, asi como una cuenta única, para acceder a los equipos informáticos del dominio.

6.11 Administrador del sistema: Es la persona que tiene la responsabilidad de ejecutar y asegurar el correcto funcionamento de un sistema informático o algún aspecto de éste. El personal de la Gerencia de Informática y Tecnologia se encuentra organizado según su especialidad. En este caso, un Administrador del Sistema es aquel responsable del mantenimiento de un sistema informático existente.

6.12 Sistemas Web: Son aquellos sistemas que se encuentran alojados en el servidor web de esta Entidad edil. Los sistemas desarrollados en plataformas web, tienen marcadas diferencias con otros tipos de sistemas; que resulta beneficioso tanto para la Municipalidad, como para los usuarios que operan el sistema. Este tipo de diferencias se ven reflejada en los costos de la entidad, en la rapidez de obtención de la información, en la optimización de las tareas por parte de los usuarios y en alcanzar una gestión íntegramente informatizada dentro y fuera de la Municipalidad; dado que la información es accesible desde cualquier lugar, dentro de la organización e incluso desde el exterior.

6.13 Privilegio: Permiso para realizar una acción, asignable a un usuario o un rol.

6.14 Rol: Conjunto de privilegios, asignables a un usuario o un rol.

6.15 Usuario: Colección de objetos y privilegios identificado con un nombre y password.

6.16 Perfil: Conjunto de restricciones relativas al uso de recursos, y asignable a usuarios. Un usuario sólo puede tener un perfil.

6.17 Recurso: Uso susceptible de ser restringido, asignable a un perfil.

VII. **Disposiciones Generales:**

7.1 El usuario deberá suscribir el formulario denominado: "Acta de Confidencialidad" (Anexo N° 03);

comprometiéndose a seguir las instrucciones y/o recomendaciones impartidas par la Gerencia de Informática y Tecnologia, en cuestiones de seguridad, referidas al correcto uso y manejo de los equipos informáticos y/o sistemas de información.

7.2 Posteriormente, el usuario podrá ingresar a los equipos informáticos y/o sistemas de información; para tal efecto, se le asignará un nombre de usuario y una contraseña. El Gerente de Informática y Tecnologia será el único responsable de usar y/o asignar, mediante documento formal, el usuario de Administrador del Sistema.

7.3 En la primera pantalla de ingreso a la red; se consignará y requerirá la identificación del usuario. De esta manera, sólo ingresarán aquellos usuarios que se encuentren debidamente autentificados. Asimismo, la cuenta de usuario de red y la cuenta de usuario del Sistema, serán iguales para poder acceder a este último.

7.4 Cada operador tendrá un nivel de operatividad, el cual será asignado por la Gerencia de Informática y Tecnologia. También se definirán, de acuerdo a las niveles de operatividad, las tareas, que se permitan desarrollar en los mismos.

7.5 El uso de la cuenta de usuario será responsabilidad del personal al cual está asignada. La cuenta es de carácter privado, de uso personal e intransferible.

7.6 La contraseña asociada a la cuenta de usuario, deberá seguir los criterios para la Construcción de Contraseñas Seguras.

7.7 Las cuentas de usuarios (usuario y contraseña), serán sensibles a la redacción de mayúsculas y minúsculas; es decir, que éstas deberán ser tecleadas, según los caracteres que correspondan.

7.8 Por seguridad, no se deberá compartir la cuenta de usuario con otras personas: compañeros de trabajo, amigos, familiares, etc.

7.9 Si otra persona requiera hacer uso de la cuenta de usuario, se hará referencia a estas políticas. De ser necesaria la divulgación de la cuenta de usuario y su contraseña asociada, se deberá proceder a solicitarse, mediante documento formal, ante la Gerencia de Informática y Tecnología.

7.10 Si se detectara o se presumiera que las actividades de una cuenta de usuario, comprometen la integridad y seguridad de la información, el acceso a la precitada cuenta será suspendido temporalmente y será reactivada sólo después que la Gerencia de Informática y Tecnología, adopte las medidas que resulten necesarias.

VIII. Disposiciones Específicas:

8.1 De losTipos de cuentas de usuario:

Para efectos de la presente Directiva, se definen tres (03) tipos de cuentas de usuario:

8.1.1 Cuenta para Ingresar a la Red local.- Es la cuenta que conecta a una computadora con el servidor principal de la entidad, lo cual permitirá ingresar a los equipos informáticos y/o sistemas de información, para enviar y recibir información, gestionar mensajería instantánea, entre otros privilegios, propios de una red interna.

8.1.2 Cuenta de Usuario de Sistema de Información.- Todas aquellas cuentas que sean utilizadas por los usuarios para acceder a los diferentes sistemas de información. Estas cuentas permiten el acceso para consulta, modificación, actualización o eliminación de información, y se encuentran reguladas por los roles de usuario del Sistema.

8.1.3 Cuenta para la Administración de Sistema de Información.-
Corresponde a la cuenta de los Administradores del Sistema; quienes realizarán tareas específicas en relación a las cuentas de usuarios.

Se ha determinado, para un adecuado control el registro de los Administradores del Sistema, en el formulario denominado "Control de accesos a los sistemas de información".

Existen varios Administradores del Sistema, según se describen en siguiente la tabla:

Cuadro N° 01: Personal Informático encargado de las Administración de los SI.

N°	Administradores Responsables:	Control de Cuentas del:
1	Programador 1	- Control de Turnos y Otros sistemas de Información
		- Sistema de Observatorio Local de Seguridad y Convivencia
		- Sistema de Información Documentaria- SID
		- Módulo de Inventario
		- Módulo Registro de personal
2	Programador 2	- Sistema de Administración Tributario Municipal Basado en Experiencias - Satmun XP
3	Programador 3	- Sistema de Licencia de Funcionamiento y Publicidad de Exterior
		- Sistema de Licencia de Construcción y los Sistemas Web
4	Programador 4	- Sistema Integrado de Gestión Administrativa SIGA
5	Programador 5	- Módulo de Gestión
		- Servicios Digitales al Ciudadano
		- Módulo de Soporte Técnico
6	Soporte 01	- Instalación de SIAF
		- Creación de cuentas de usuario SIAF
		- Creación de cuenta de Correo
		- Otros sistemas de información
7	Soporte 02	- Instalación de SIAF
		- Creación de cuentas de usuario SIAF
		- Creación de cuenta de Correo
		- Creación de cuentas en los diversos sistemas
		- Otros sistemas de información

8.2 Derecho de acceso de los usuarios:

La revisión periódica de los derechos de acceso de los usuarios al Sistema, se realiza para un control efectivo del acceso a los datos y los sistemas de información, considerando las siguientes disposiciones y/o recomendaciones:

8.2.1 Cada seis (06) meses, y con motivo de haberse dispuesto el alta, la baja o el desplazamiento de personal en esta Entidad edil, la Gerencia de Informática y Tecnología revisará los derechos de acceso de los usuarios.

8.2.2 Los derechos de acceso de los usuarios deberán ser revisados y reasignados cuando el personal se desplaza de una unidad orgánica a otra, dentro de esta Municipalidad.

8.2.3 Cada tres (03) meses, se revisará las autorizaciones de derechos de acceso con privilegios especiales, para asegurar que no se han obtenido privilegios no autorizados.

8.2.4 Los cambios en las cuentas privilegiadas, deberán ser registradas para una revisión periódica.

8.2.5 Será responsabilidad del funcionario o servidor responsable de cada unidad orgánica, notificar a la Gerencia de Informática y Tecnología, la baja o el desplazamiento del personal, para su respectiva baja en los sistemas, así como para la auditoría de derecho a los accesos.

8.3 De la Responsabilidades del usuario:

Por ser responsabilidad del usuario, el uso y manejo de accesos a los equipos informáticos y/o sistemas de información, y con el objeto de evitar el acceso de usuarios no autorizados, así como el hurto de la información y de las instalaciones del procesamiento de información, a continuación, se detallan las siguientes disposiciones de estricto y cumplimiento obligatorio:

8.3.1 Las cuentas de los usuarios a los equipos informáticos y/o sistemas de información, son personales e intransferibles.

8.3.2 Es responsabilidad del usuario mantener en secreto su contraseña, así como modificarla periódicamente, debido a que las operaciones que realice dentro del Sistema, quedarán

registradas y lo sindicarán como responsable de los mismos, en los diferentes Sistemas que opere.

8.3.3 Los usuarios solicitarán el acceso a los equipos informáticos, según la disponibilidad física y especifica existente en cada oficina, y accederán a los sistemas de información, de acuerdo con las disposiciones y recomendaciones, emitidas por la Gerencia de Informática y Tecnologia.

8.3.4 Los usuarios tendrán cuidado, al momento de usar los equipos informáticos, así como al manipular toda la infraestructura complementaria.

8.3.5 Evitarán realizar cualquier acción, que de forma voluntaria o no pudiera perjudicar la integridad física de la instalación (destrozos, sustracción, traslado no autorizado, entre otros).

8.4 Para las contraseñas:

Se controlará la asignación de contraseñas, mediante un proceso de gestión formal, conforme se detalla a continuación:

8.4.1 Requerir que los usuarios suscriban el formulario denominado: "Acta de Confidencialidad " (Anexo N° 03), que consiste en un compromiso para mantener en secreto sus contraseñas, las que por recomendación, deberá cambiar imediatamente después de realizar su primer acceso.

8.4.2 La Gerencia de Informática y Tecnología verificará la identidad de un usuario, antes de generar y proveer una contraseña nueva.

8.4.3 Las contraseñas son únicas para cada individuo y no deberán ser obvias.

8.4.4 Las contraseñas nunca deberán ser almacenadas en equipos informáticos, y éstos deberán ser protegidos de un fácil acceso.

8.5 Políticas de uso de contraseñas:

Los usuarios, para la elección, el uso y la protección de sus contraseñas, deberán seguir las disposiciones emitidas por la Gerencia de informática y Tecnología, conforme se detalla a continuación:

8.5.1 Todas las contraseñas de nivel de usuario y de carácter administrativo, para acceso a los equipos informáticos y/o sistemas de información, deberán ser cambiadas al menos cada seis (06) meses.

8.5.2 Todas las contraseñas deberán ser tratadas con confidencialidad y con carácter reservado.

8.5.3 Las contraseñas, de ninguna manera, podrán ser transmitidas mediante servicios de mensajería instantánea, ni a través de aplicativos o equipos telefónicos móviles.

8.5.4 Si es necesario, el uso de mensajes de correo electrónico para la divulgación de contraseñas, éstas deberán transmitirse de forma segura.

8.5.5 Se evitará mencionar y en la medida de lo posible, teclear contraseñas en frente de terceros.

8.5.6 Se evitará el revelar contraseñas en cuestionarios, reportes u otros.

8.5.7 No se almacenarán las contraseñas en libretas, agendas, post-it, hojas sueltas, entre otros.

8.5.8 No se almacenarán las contraseñas sin encriptación, en sistemas electrónicos personales (asistentes electrónicos personales, memorias usb, equipos telefónicos móviles, agendas electrónicas, etc).

8.5.9 Si alguna contraseña es detectada y verificada como no segura, la Gerencia de Informática y Tecnología deberá dar aviso al(los) usuario(s), para efectuar un cambio inmediato en dicha contraseña.

8.5.10 No se revelarán las contraseñas a terceros, en forma verbal o a través de equipos telefónicos móviles.
8.5.11 No se revelarán las contraseñas o referencias de éstas, en un formulario en internet u otras similares.
8.5.12 No se utilizará el "Recordar Contraseña" en aplicaciones o correo electrónico o cualquier otro programa.
8.5.13 No se utilizarán siglas comunes como parte de las contraseñas.
8.5.14 No se utilizarán palabras comunes o el retroceso de la ortografía de las palabras, en una parte de las contraseñas.
8.5.15 No se utilizarán nombres de personas o lugares, como parte de las contraseñas.
8.5.16 No utilizar parte del nombre de usuario en su contraseña.
8.5.17 No utilizar partes de números que se pueda recordar fácilmente, como números de teléfono, números de seguridad social o direcciones de calles.
8.5.18 Tener cuidado con permitir que terceros, vean la contraseña al momento de redactarla.
8.5.19 Cualquier pérdida o ruptura de contraseña, será responsabilidad del usuario.

8.6 <u>Requisitos para la contraseña</u>:

Al respecto, teniendo en consideración que las contraseñas, deberán contener un considerable grado de dificultad, a efectos de que se pueda atenuarse o evitarse, eventuales ataques a la seguridad de los equipos informaticos y/o sistemas de información, la Gerencia de Informática y Tecnologia ha dispuesto los siguientes requisitos para la contraseña:

8.6.1 Longitud mínima: seis (06) caracteres, por recomendación o precaución.
8.6.2 Longitud máxima: catorce (14) caracteres.
8.6.3 Las contraseñas deberán utilizar tres tipos de caracteres:
  8.6.3.1 Minúsculas
  8.6.3.2 Mayúsculas
  8.6.3.3 Números
8.6.4 Las contraseñas deberán ser sensibles a mayúsculas y minúsculas. Los nombres de usuario o ID de inicio de sesión, no deberán ser sensibles a mayúsculas y minúsculas.
8.6.5 Edad máxima de la contraseña: ciento veinte (120) días.
8.6.6 Edad mínima de la contraseña: treinta (30) días.
8.6.7 Cuenta bloqueada temporalmente: a los seis (06) intentos de acceso fallido.
8.6.8 Restablecer la cuenta después del bloqueo temporal: el tiempo es tomado entre el acceso fallido, y es de treinta (30) minutos.
8.6.9 Los protectores de pantalla deberán tener contraseña y deberán estar activados. Estos se activarán dentro de cinco (05) minutos de inactividad del usuario. Los equipos informáticos no deberán ser descuidados por el usuario, cuando se encuentre conectado y haciendo uso de éstos. Para tal efecto, se recomienda a los usuarios, que por seguridad deberán asegurar o bloquear los equipos informáticos, cuando éstos se encuentren activos y sin uso, para lo cual pulsarán las teclas CTRL- ALT-DEL y seleccionar la opción: "Bloquear equipo".

8.7 <u>Elección de las contraseñas</u>:

Los usuarios generarán una contraseña, conforme a las siguientes recomendaciones:

8.7.1 Inserte una palabra o parte de una palabra dentro de otra.
8.7.2 Intercale dos o más palabras.
8.7.3 Utilice una frase personal y utilice el caracter de primer, segundo o tercer lugar, en cada palabra de cada frase. La frase puede ser una pregunta o frase de respuesta.
8.7.4 Use una representación numérica de las letras del alfabeto, como parte de la frase o una palabra en su frase. Por ejemplo, A es 1, B es 2, C es 3, etc.
8.7.5 Utilice letras mayúsculas y/o letras minúsculas.
8.7.6 Entremezclar números y caracteres, de una manera que pueda recordar.

8.8 Cuentas del "Active Directory" en el domínio:

8.8.1 La Gerencia de Informática y Tecnología establecerá el control de acceso a la red, a través de dominio lógico de red interna de esta Entidad edil, cada uno protegido por un perímetro definido de seguridad.

8.8.2 Los usuarios serán controlados en la red, a través del Dominio del "Active Directory", el mismo que es el Servidor de Controlador de Dominios.

Cada persona que tenga acceso a la red, requerirá una cuenta de usuario, lo cual permitirá:

8.8.2.1 Autentificar la identidad de la persona, que se conecta a la red.
8.8.2.2 Controlar el acceso a los recursos del dominio.
8.8.2.3 Auditar las acciones realizadas utilizando la cuenta.

8.9 Sobre el uso y asignación de privilégios:

8.9.1 El control de cuentas de usuarios, es definido por la Gerencia de Informática y Tecnologia, como un rol, el papel desempeñado por un individuo dentro de un conjunto de personas. En la base de datos, siempre existen un conjunto de personas que harán uso de ella, las acciones que pueden hacer son: visualización, modificación, agregación, eliminación de registros entre algunas otras, y la regla que lo permite, es conocido como privilegio.

8.9.2 En un grupo de usuarios existen privilegios globales e individuales, primero se consideran los globales y luego se consideran los individuales, agregándole o disminuyéndole privilegios basándose en los globales; es decir:

Grupo (UsuarioA, UsuarioB)
Grupo PUEDE ver
Usuario A PUEDE editar

8.9.2.1 En este caso el Usuario A puede "ver" (gracias a los privilegios globales) y puede "editar" (gracias a los privilegios individuales) y el Usuario B solo puede "ver".

8.9.2.2 El Uso y Asignación de privilegios están restringidos y controlados por la Gerencia de Informática y Tecnología, y obedecen a un proceso formal de autorización en los sistemas multiusuario que considera la identificación de los privilegios asociados a cada elemento del sistema. Los privilegios son asignados a los individuos, según los principios de "necesidad de su uso" y "caso por caso".

8.10 Registro de usuarios:

El registro de altas y bajas de usuarios, es para garantizar el acceso seguro a los equipos informáticos y/o sistemas de información de esta Municipalidad, conforme a las siguientes disposiciones:

8.10.1 Para obtener el identificador único para cada usuario, la correspondiente unidad orgânica deberá solicitarlo ante la Gerencia de Informática y Tecnología, mediante el formulario denominado: "Formulario Datos del Usuario" (Anexo N° 02), indicando el Sistema, en el que requiere, se cree o modifique el usuario y cuales son las opciones a las que va a tener acceso, de acuerdo a las funciones a realizar por parte del personal de la Entidad, de esta forma puede vincularse a los usuarios y a su responsabilidad por sus funciones.

8.10.2 La comprobación de la autorización del usuario, para utilizar el Sistema o el servicio de información, estará a cargo del funcionario o servidor responsable de la unidad orgánica, que tiene la condición de jefe inmediato. La entrega a los usuarios de una relación escrita de sus derechos de acceso; está comprendida en el formulario denominado: "Acta de

Confidencialidad" (Anexo Nº 03).

8.10.3 Los Administradores del Sistema, responsables de crear o modificar usuarios, deberán ingresar al sistema indicado en el formulario; crear el perfil de usuario y asignarle las opciones correspondientes. La clave de acceso será ingresada por el usuario, al momento que el administrador del sistema defina el nombre de usuario.

8.11 Modificación de accesos de cuentas de usuários:

8.11.1 En el caso de que ocurra un cambio en los roles o responsabilidades del personal, el funcionario o servidor responsable de la unidad orgánica, que tiene la condición de jefe inmediato o la Sub Gerencia de Recursos Humanos de esta Municipalidad, deberá solicitar la cancelación o modificación a todos los accesos del usuario, relacionados con las funciones y responsabilidades, que anteriormente le fueron asignadas.

8.11.2 Para tal efecto, en el formulario denominado: "Datos del Usuario" (Anexo N° 02), se deberá consignar la información y procedimiento pertinente, según lo detallado y requerido en el precitado formulario.

8.11.3 El funcionario o servidor responsable de la unidad orgánica, que tiene la condición de jefe inmediato del usuario, a efectos de cautelar la adecuada y oportuna ejecución de las funciones, a ser asignadas a este último, solicitará los accesos adicionales que el usuario necesite o requiera.

8.11.4 Este formulario de acceso a los sistemas o cuentas, se podrá descargar a través de la intranet de esta Municipalidad. Bastará consignar en el referido formulario, los sistemas que desea se le modifique.

8.11.5 Los formularios que se presenten, respecto de los cuales se verifique que el solicitante no tenga ninguna función o responsabilidad asignada, serán denegados por la Gerencia de Informática y Tecnología.

8.11.6 Los formularios deberán contar con la firma y/o el visto bueno del funcionario o servidor responsable de la unidad orgánica, que tiene la condición de jefe inmediato del usuario, así come del Gerente de Informática y Tecnología, el cual para el caso de formularios de solicitudes de modificación de permisos de acceso, para las cuentas de usuarios actuales, los derivará al Administrador del Sistema, de cada Sistema, para su correspondiente verificación y asignación de privilegios.

8.11.7 La Gerencia Informática y Tecnología verificará que los formularios presentados, se encuentren debidamente suscritos; posteriormente, procederá a evaluar la procedencia o no de la modificación de la cuenta, así como a generar los accesos correspondientes, según el resultado de la evaluación efectuada.

8.12 Cancelación de cuentas de usuários:

8.12.1 El usuario o el funcionario o servidor responsable de la unidad orgánica, que tiene la condición de jefe inmediato del usuario o el Gerente de Informática y Tecnología, podrá solicitar la cancelación de cuentas, con motivo de la baja o desplazamiento del personal de esta Municipalidad.

8.12.2 El usuario o el funcionario o servidor responsable de la unidad orgánica, que tiene la condición de jefe inmediato del usuario o la Sub Gerencia de Recursos Humanos, deberán comunicar o notificar oportunamente a la Gerencia de Informática y Tecnología, la baja del respectivo usuario y solicitar la cancelación de sus accesos a los equipos informáticos y/o sistemas de información.

8.12.3 Se cancelarán automaticamente las cuentas de los usuarios, que demuestren más de dos (02) meses de inactividad en el Sistema, que expiren el tiempo de acceso y aquellas que comunicadas por la Sub Gerencia de Recursos Humanos, según sea el caso. Para tal efecto, se les colocará en la fecha de expiración, la fecha de efectividad de la baja o desplazamiento del personal de esta Municipalidad, como acción de control y seguridad.

8.12.4 Si un usuario utiliza su cuenta de acceso, para realizar acciones no relacionadas a sus funciones y responsabilidades, su cuenta podrá ser inactivada por motivos de seguridad. En tanto se reporta y se realiza la investigación necesaria, de encontrarse acreditada la justificación, la Gerencia de Informática y Tecnología procederá a la cancelación inmediata

de la misma.

8.13 <u>Clasificación de la información por niveles</u>:

Siendo la información uno de los activos más importantes para la Municipalidad, éstos se han clasificados con el objetivo de asegurar un nivel de protección adecuado, así como también para indicar la necesidad, prioridades y grado de protección, en razón a que la información es sensible, crítica y privada, algunos elementos de información requieren un nivel adicional de protección o un uso especial. Por consiguiente, la Gerencia de Informática y Tecnología ha definido un conjunto de niveles de protección para los usuarios de esta Entidad edil, conforme a la siguiente descripción:

8.13.1 Nivel 1.- Es la cuenta de usuario con más bajo nivel, solo podrán realizar consultas y visualizar datos comunes. Acceso de "Solo Lectura", donde la autorización de lectura permite leer, pero no modificar la base de datos, conforme a la siguiente descripción:

Grupo y/o perfil:

a) **Caja-Consultas.-** Accesos de caja para la consulta de sub-módulos, acceso solo de lectura, con este nivel de protección no se puede realizar operaciones en caja.
b) **Recaudación-Consulta.-** Accesos de consulta al módulo de recaudación.
c) **Caja-Reportes.-** Accesos de caja para la emisión de sus reportes.
d) **Catastro.-** Accesos de consulta de catastro en el sistema de rentas-predios y PUs y DJs.
e) **Coactivo-Consulta.-** Accesos de consulta del módulo de Ejecutoría Coactiva.
f) **Estados de Cuenta.-** Accesos de rentas para visualizar estados de cuenta.
g) **Fiscalización-Consulta.-** Accesos de fiscalización para la consulta de los resultados del proceso de fiscalización.
h) **Fiscalización-Reporte.-** Accesos de fiscalización para la emisión de reportes.
i) **Gerencias-Decisiones.-** Accesos para la visualización de los reportes gerenciales.
j) **Multas Adminis-Repor.-** Accesos de multas administrativas para emitir reportes.
k) **Reportero.-** Accesos de consulta de reportes en general.

8.13.2 Nivel 2.- En este nivel los usuarios podrán ingresar, consultar y procesar la información en el sistema, en este nivel están todos los/las cajeros/as, conforme a la siguiente descripción:

Grupo y/o perfil:

a) **Caja-Cajeros.-** Accesos de caja para la realización de las operaciones de caja.
b) **Coactivo-Auxiliar.-** Accesos de coactivos necesarios para la función del Auxiliar Coactivo.
c) **Coactivo-Ejecutar.-** Accesos de coactivo necesarias para la función del Ejecutor Coactivo.
d) **Coactivo-Generador.-** Accesos de coactivo para la generación de expediente coactivos.
e) **Comercio-Ambulatorio.-** Acceso para la gestión de comercio ambulatorio.
f) **Fiscalización-Proceso.-** Accesos de fiscalización para la gestión del proceso de fiscalización.
g) **Multa-Administrativa-Descuento.-** Accesos de multas administrativas para la generación de descuentos.
h) **Multas Administrativa-Notificación.-** Accesos de multas administrativas

para el ingreso de papeletas de infracción administrativas.

i) **Multas Administrativas-Transferencia.-** Accesos de multas administrativas para transferencia de los mismos al módulo de coactivo.
j) **Proformas.-** Accesos del módulo de proformas para su gestión.
k) **Recaudación-Descargar y Otro.-** Accesos de recaudación necesarios para hacer operaciones de regularización de cuenta corriente y transferencias de pagos entre contribuyentes.
l) **Recaudación-Fracci-Transfe.-** Accesos de fraccionamiento para transferencia de los mismos al módulo de coactivo.
ll) **Recaudación-Fraccionamiento.-** Accesos de recaudación para la gestión de los fraccionamientos.
m) **Recaudación-Mantenimiento.-** Accesos de recaudación para el mantenimiento de las tablas de sus sub-módulos.
n) **Recaudación-Valores.-** Todos los accesos para la gestión de valores tributarios.
ñ) **Tributaria-Declaraciones.-** Accesos de operador de ventanilla de administración tributaria.

8.13.3 **Nivel 3.-** Este nivel permite ingresar, visualizar y autorizar, conforme a la siguiente descripción:

Grupo y/o perfil:

Caja-Supervisor.- Accesos de caja para la supervisión de los cajeros como cajero central.

8.13.4 **Nivel 4.-** En este nivel se pueden dar mantenimiento al Sistema, son para Administradores del Sistema, conforme a la siguiente descripción:

Grupo y/o perfil:

a) **Caja-Mantenimiento.-** Accesos de caja para el mantenimiento de sus tablas.
b) **Coactivo-Mantenimiento.-** Accesos de Ejecutoría Coactiva para el mantenimiento de tablas.
c) **Informática-Usuarios.-** Accesos de informática únicamente para la administración de usuarios.
d) **Multas Administrativa-Mantenimiento.-** Accesos para el mantenimiento de las tablas de multas administrativas.
e) **Recaudación-Mantenimiento.-** Accesos de recaudación para el mantenimiento de las tablas de sus sub-módulos.
f) **Tributaria-Mantenimiento.-** Accesos de administración tributaria para el mantenimiento de sus tablas.
g) **Informática-Sistema.-** Accesos de informática para la administración de opciones.

8.13.5 **Nivel 5.-** Máximo nivel, son para Administradores del Sistema, es el nivel de Auditoría General del Sistema. Permite el mantenimiento de la información incluyendo la restringida.

En este nivel de protección, el usuario accede a los registros de auditoría del Sistema Satmun XP. Registros de auditoría con incidencias importantes para la seguridad, que permiten futuras investigaciones y el seguimiento del control de los accesos, conforme a la siguiente descripción:

Grupo y/o perfil:

Gerente de Informática y Tecnología, Accesos para auditorías al Sistema.

- El identificador del usuario.
- Fecha y hora de conexión.
- Identificación del terminal (MAC del equipo).
- Registro de intentos aceptados y rechazados del acceso al Sistema y otros registros.

8.14 Definición de niveles de protección:

Los niveles de usuarios existentes, son escalonados en orden jerárquico, permitiendo que los niveles superiores puedan realizar las tareas de los inferiores. Los disponibles en el Sistema son: **Nivel del 1 al 5**.

IX. Disposiciones Finales:

9.1 Responsabilidad de los usuarios:

9.1.1 Los usuarios no deben acceder a los sistemas o cuentas, que no se relacionan con sus funciones y responsabilidades de trabajo.

9.1.2 La capacidad de tener acceso a un sistema o a una cuenta, no constituye la autorización de tal acceso. La autorización existe solamente para aquellos usuarios, a quienes se les ha concedido el acceso y tengan una responsabilidad, en relación a la función del trabajo que realizan.

9.1.3 El acceso desautorizado a los equipos informáticos y/o sistemas de información, puede dar lugar al inicio de acciones disciplinarias, que resulten necesarias, a cargo de la Secretaría Técnica de Procedimientos Administrativos de esta Municipalidad, sin perjuicio de la adopción de acciones legales que corresponda, para salvaguardar y cautelar los legítimos derechos e intereses de esta Entidad edil.

9.1.4. Los usuarios, bajo responsabilidad, se encuentra obligados, a no divulgar información alguna sobre los Sistemas de la Municipalidad Distrital de Chorrillos, asi como respecto de los datos que accede, mediante el uso de los mismos.

X. Anexos:

Anexo N° 01: Matriz de Aprobación.

Anexo N° 02: Datos del Usuario.

Anexo N° 03: Acta de Confidencialidad.

Anexo N° 01
MATRÍZ DE APROBACIÓN

Rol:	Unidad Orgánica	Sello y Visto
Elaborado por:	Gerencia de Informática y Tecnologia	
Revisado por:	Gerencia de Planeamiento y Presupuesto	
	Gerencia de Asesoría Jurídica	

Anexo N° 02
DATOS DEL USUARIO

1. DATOS DEL USUARIO		
APELLIDOS COMPLETOS	**NOMBRES COMPLETOS**	**D.N.I.**

2. DATOS DE LA CUENTA	
NOMBRE DE CUENTA DE USUARIO:	
FECHA DE INICIO:	
FECHA DE CADUCIDAD:	
PERFIL DE USUARIO:	
NOMBRE DEL MÓDULO	
CARGO O FUNCIÓN QUE DESEMPEÑA:	
OFICINA DONDE LABORA:	
N° DE FORMULARIO DE CUENTA DE USUARIO:	
DESCRIPCIÓN DEL PERFIL:	
IMPORTANTE:	

Siendo la información el activo principal de esta corporación edíl, hemos considerado necesario aplicar medidas de seguridad para protegerla adecuada - mente de amenazas y vulnerabilidades. Los Controles se han implementado de tal manera que los usuarios solo deberian tener acceso directo a los servidores para los que estén autorizados de una toma específica. Asimismo, se ha determinado que es responsabilidad del usuario mantener en secreto su pasword y modificarlo periódicamente, pues las operaciones que realice dentro del sistema quedaran registradas y lo sindicarán como responsable de los mismos, en los diferentes sistemas que opere. Por tanto la confidencialidad de los datos de la Cuenta de Usuario y contraseña del Usuariio son de exlcusiva responsabilidad del usuario. Asimismo, todas las actividades realizadas en el sistema de información, bajo su nombre de Usuario y contraseña son de su exclusiva responsabilidad, así como el uso que pueda hacerse de la información, imágenes y contenidos accesibles a través del mismo, estará supeditada a la ley aplicable, así como a los principios de buena fe y uso lícito por parte del Usuario, siendo este enteramente responsable de dicho acceso y correcto uso. El Usuario tiene prohibido realizar cualquier tipo de actividad en perjuicio de la Municipalidad Distrital de Chorrillos o de terceros. Se considera terminantemente prohibido el uso del Sistema de Información para fines ilegales, no autorizados. Finalmente, en señal de expresa conformidad y aceptación de los términos recogidos en el presente documento se rubrican las firmas en señal de fe y consentiiento de que las actividades sean susceptibles de ser auditadas en cualquier momento.

3. FIRMAS DE CONFORMIDAD			
AREA SOLICITANTE			**AUTORIZACIÓN**
USUARIO	**JEFE INMEDIATO**	**GERENTE**	**GERENTE DE INFORMÁTICA Y TECNOLOGÍA**

Anexo N° 03
ACTA DE CONFIDENCIALIDAD

ACTA DE CONFIDENCIALIDAD DE CUENTA DE USUARIO Y CONTRASEÑA		
FECHA DE APROBACIÓN	**NÚM. ACTA**	
1. DATOS DEL USUARIO		
APELLIDOS COMPLETOS	**NOMBRES COMPLETOS**	**D.N.I.**
2. DATOS DE LA CUENTA		
NOMBRE DE CUENTA DE USUARIO:		
FECHA DE INICIO:		
FECHA DE CADUCIDAD:		
PERFIL DE USUARIO:		
NOMBRE DEL SISTEMA		
NOMBRE DEL MÓDULO		
CARGO O FUNCIÓN QUE DESEMPEÑA:		
OFICINA DONDE LABORA:		
N° DE FORMULARIO DE CUENTA DE USUARIO:		
DESCRIPCIÓN DEL PERFIL:		
IMPORTANTE:		

Siendo la información el activo principal de esta corporación edíl, hemos considerado necesario aplicar medidas de seguridad para protegerla adecuada - mente de amenazas y vulnerabilidades. Los Controles se han implementado de tal manera que los usuarios solo deberian tener acceso directo a los servidores para los que estén autorizados de una forma específica. Asimismo, se ha determinado que es responsabilidad del usuario mantener en secreto su pasword y modificarlo periódicamente, pues las operaciones que realice dentro del sistema quedaran registradas y lo sindicarán como responsable de los mismos, en los diferentes sistemas que opere. Por tanto la confidencialidad de los datos de la Cuenta de Usuario y contraseña del Usuariio son de exlcusiva responsabilidad del usuario. Asimismo, todas las actividades realizadas en el sistema de información, bajo su nombre de Usuario y contraseña son de su exclusiva responsabilidad, así como el uso que pueda hacerse de la información, imágenes y contenidos accesibles a través del mismo, estará supeditada a la ley aplicable, así como a los principios de buena fe y uso lícito por parte del Usuario, siendo este enteramente responsable de dicho acceso y correcto uso. El Usuario tiene prohibido realizar cualquier tipo de actividad en perjuicio de la Municipalidad Distrital de Chorrillos o de terceros. Se considera terminantemente prohibido el uso del Sistema de Información para fines ilegales, no autorizados. Finalmente, en señal de expresa conformidad y aceptación de los términos recogidos en el presente documento se rubrican las firmas en señal de fe y consentiiento de que las actividades sean susceptibles de ser auditadas en cualquier momento.

3. FIRMAS DE CONFORMIDAD			
AREA SOLICITANTE			**AUTORIZACIÓN**
USUARIO	**JEFE INMEDIATO**	**GERENTE**	**GERENTE DE INFORMÁTICA Y TECNOLOGÍA**