MUNICIPALIDAD DISTRITAL DE MIRAFLORES

UNIDAD DE INFORMÁTICA Y PROCESAMIENTO DE DATOS

DIRECTIVA Nº 001– 2019-MDM/UIPD

DIRECTIVA ADMINISTRATIVA PARA EL CORRECTO USO DE LOS EQUIPOS Y SISTEMAS INFORMÁTICOS EN LA MUNICIPALIDAD DISTRITAL DE MIRAFLORES

MIRAFLORES 2019

INDICE

INTRODUCCIÓN

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 ciudadana, priorizando y optimizando el uso de los recursos públicos.

Conforme a la Oficina Nacional Electrónico e Informática (ONGEI) de la Presidencia del consejo de Ministros (PCM), la estrategia del Gobierno Electrónico es la siguiente:

- ESTADO ANTE EL CIUDADANO: integración de los procesos y trámites de las instituciones.
- PROMOVER UNA CULTURA DE SERVICIO DE CALIDAD: Promover la prestación de más y mejores servicios al ciudadano.
- TRANSPARENCIA Y DESCENTRALIZACION: Permitir un ágil acceso de los ciudadanos a la información del estado, favoreciendo la transparencia de la gestión pública y promoviendo la descentralización en la prestación de los servicios.
- ECONOMIA Y EFICACIA de los trámites internos de la administración Pública.

En el mundo globalizado, en el que actualmente se impone la tecnología de punta, se deben de utilizar los medios informáticos de comunicación instantánea que generan ahorro de horas/hombre en la transmisión de la información y simplificación el trabajo dentro de la organización o entre las organizaciones.

En los gobiernos locales, deben de participar en la mencionada estrategia, utilizando las herramientas informáticas que conforman los equipos y los sistemas informáticos que dispone la gestión, para que se puedan interrelacionar los sistemas administrativos básicos en toda entidad pública que se puede ejecutar los cuales son: sistema presupuestario , de planeamiento, contabilidad, logística, tesorería, personal y la ejecución de las actividades y proyectos a cargo de las diversas unidades orgánicas que conforman la estructura orgánica Municipal y ejecutan sus planes operativos de acuerdo a su competencia dicha interrelación va generar información final en cada uno de sus campos, lo cual conlleva a obtener registros administrativos los cuales deben de conservarse en fuentes de almacenamiento en forma física y digital, que servirá como seguridad para la consulta sobre la ejecución de la gestión en determinados ejercicios económicos.

Ante la situación mencionada, se hace necesario elaborar una Directiva que emita las normas internas para regular el uso eficaz de los equipos informáticos, sistemas informáticos y/o servicios de Internet puestos a disposición de los usuarios en sus diversos niveles jerárquicos y académicos conforme a las funciones que les corresponde desarrollar.

A su vez dicha Directiva sirva para crear conciencia colectiva en lo que corresponde a la prevención en el cuidado de la ejecución de los Backups de la información definitiva de las unidades orgánicas, en los medios digitales de mayor seguridad.

I. OBJETO

Contar con un documento normativo interno oficial que establezca las obligaciones y responsabilidades para el uso correcto de los equipos de cómputo, los servicios de red, y la Internet institucional en la Municipalidad Distrital de la Miraflores (MDM).

II. FINALIDAD.

La presente Directiva tiene por finalidad optimizar el uso de los equipos de cómputo, servicios de Red, Internet garantizando la integridad de la red y equipos de la MDM así como su uso eficiente.

III. ALCANCE.

El alcance de la presente Directiva, comprende a todo el personal que brinda servicios a la MDM, bajo toda modalidad laboral, incluyendo a los que realizan prácticas pre -profesionales, siendo en el caso de los locadores de servicios, la responsabilidad asumida por la supervisión de sus Jefes inmediatos.

IV. BASE LEGAL

- Decreto Legislativo N.º 604 -Ley de Organización y Funciones Técnicas del Instituto Nacional de Estadística e Informática.
- Decreto Supremo N.º 004-2019- JUS del Texto Único Ordenado de la Ley N.º 27444 Ley del Procedimiento Administrativo General.
- Resolución Jefatura N.º 347 - 2001- INEI, Aprueban Directiva sobre "Normas y Procedimientos Técnicos para garantizar la Seguridad de la Información publicadas por las entidades de la Administración Pública".
- Resolución Jefatura N.º 386 - 2002- INEI, Aprueban la Directiva N.º 016-2002-INEI/DTNP "Normas Técnicas para el Almacenamiento y Respaldo de la Información procesada por las Entidades de la Administración Pública".

DOCUMENTOS QUE SE NECESITA PARA LA DIRECTIVA

- Ordenanza Municipal Nº 234-2015-MDM que aprueba el Reglamento de Organización y Funciones (ROF), Manual de Organización y Funciones (MOF)
- Decreto de Alcaldía N° 02-2019-MDM/A, que aprueba la Modificación del Texto Único de Procedimientos Administrativos TUPA de la Municipalidad Distrital de Miraflores.

V. DISPOSICIONES GENERALES

1. Los equipos de cómputo y los servicios de red, Internet deben emplearse para las actividades directamente relacionadas con el cumplimento de las funciones en la institución. En cumplimiento de lo señalado en el párrafo precedente, ningún usuario podrá descargar música, videos, juegos o cualquier otro programa procedente de Internet ni instalarlos o copiarlos de cualquier fuente, ni acceder a lugares que incluyan material pornográfico o material en perjuicio de terceros.

   No está permitido el envío de mensajes a foros de discusión (listas de distribución y/o newsgroups), por ponerse en riego la información de la institución.

2. El usuario deberá utilizar la cuenta que le ha sido asignada para tener acceso a los servicios de red, Internet y correo electrónico. Es responsable de proteger y no olvidar su contraseña. En caso de olvido, el computador no permitirá su acceso, solicitará la atención de soporte técnico de la Unidad de Informática y Procesamiento de Datos.

3. Asimismo, el jefe de la respectiva Unidad u Oficina podrán solicitar a la Unidad de Informática y Procesamiento de Datos, el procedimiento de Backups de la información contenida en el equipo asignado al usuario, en forma física y digital, en medio magnética (CD, DVD) según sus necesidades.

4. La Información contenida en las computadoras no podrá reproducirse o utilizarse para fines ajenos a las funciones del usuario en la institución.

5. Los usuarios son responsables exclusivos de la información obtenida de Internet, del contenido de los mensajes enviados a través de Internet, para dichos efectos deberán extremar medidas de seguridad a fin de que otras personas no hagan uso o se adueñen de su usuario y/o password.

6. Los usuarios deben abstenerse de utilizar el acceso de otra persona, intentar apoderarse de las contraseñas de sus compañeros o intentar burlar los sistemas de seguridad.

7. A efectos de que se tomen las medidas correctivas y administrativas pertinentes, la Unidad de Informática y Procesamiento de Datos informará al Jefe Inmediato del usuario infractor, cualquier contravención a la presente Directiva que detecte.

VI. DISPOSICIONES ESPECÍFICAS

1. Acceso a los servicios de Red

1.1. El acceso a los servicios es solicitado por el titular de la unidad correspondiente.

1.2. Para la creación del Usuario (login) se utiliza la primera letra del nombre, segundo de un punto, y seguido el apellido paterno, se considera la letra inicial del segundo apellido materno y a su vez la segunda letra del apellido paterno, si fuese necesario.

1.3. La comunicación de las contraseñas se realizará de forma personal o vía teléfono, la misma que deberá ser cambiada inmediatamente por el usuario.

Para elegir una contraseña, se recomienda lo siguiente:

a. Difícil de adivinar: Elegida aleatoriamente de un conjunto suficientemente grande como evitar la identificación como consecuencia de una búsqueda exhaustiva.
b. Secreta: Conocida solo por su dueño.
c. Tener al menos seis caracteres.
d. Tener una mezcla de letras, dígitos y/o signos de puntuación.
e. No coincidir en: el número de cuenta o login, número de DNI, placa del automóvil o palabras escritas al revés.
f. Usar combinaciones de palabras cortas no relacionadas con uno o más signos de puntuación (rosa$vela, city%vidrio), palabras con dígitos insertados (avEN213ida, in80util), acrónimos, (EulDlmdCnnQa), errores ortográficos (¿holgazán),

consonantes y vocales alternados en forma pronunciable pero sin sentido (bedugale, tuponsiga) .

g. Evitar usar el mismo password para dos sistemas distintos.

1.4 El usuario deberá cambiar su contraseña de inicio de sesión al dominio informático, cada 90 días; previamente el usuario recibirá notificaciones o alertas para el cambio de contraseña con 15 días de anterioridad.

2. Uso del equipo de cómputo

2.1 Es de responsabilidad de la Gerencia de Administración y Finanzas (GAF) a través del personal encargado de realizar las actividades de Control Patrimonial y emitir la Papeleta de traslado, autorizando la entrada y salida de los equipos de cómputo.

2.2 Los usuarios deben brindar un uso adecuado a las computadoras que se les asigne, con el objeto de evitar su deterioro. El usuario es responsable del cuidado físico de los equipos que se le asigna.

2.3 En virtud de lo señalado en el numeral precedente, los usuarios se encuentran prohibidos de:

a. Pegar Sticker en las computadoras, así como colocar y/o manipular líquidos en su cercanía.
b. Rociar sobre las computadoras líquidos ambientadores.
c. Fumar cerca de las computadoras.
d. Colocar y/o apilar documentos u otros objetos sobre las computadoras y en las ubicaciones que obstruyan o impidan su adecuada ventilación y uso.
e. Ubicar el CPU en posición distinta a su diseño original (horizontal o vertical).
f. Dejar los equipos portátiles (laptop) y sus accesorios, en lugares inseguros.
g. Conectar artefactos eléctricos sobre la línea eléctrica estabilizada de uso exclusivo para las computadoras o sobre los estabilizadores de corriente.
h. Modificar los parámetros o configuración de las computadoras, así como el (los) software(s) y/o sistemas informáticos instalados.
i. Manipular y abrir las computadoras, así como extraer o cambiar componentes.
j. Cualquier otro uso no autorizado y que ponga en riesgo la integridad y/o funcionalidad de los equipos.

2.4. La instalación, reubicación, reasignación y cualquier movimiento de cómputo en la entidad deberá ser realizado en coordinación con la Unidad de Informática y Procesamiento de Datos.

2.5. Es de responsabilidad de la Gerencia de Administración y Finanzas (GAF) a través del personal encargado de realizar las actividades de Control Patrimonial, realizar el inventario de los equipos informáticos y dar la baja de los equipos de la MDM.

2.6. Es de responsabilidad de la Gerencia de Administración y Finanzas (GAF) a través de la Unidad de Logística y Bienes Patrimoniales, la adquisición de los componentes, accesorios y servicios necesarios para reparar los equipos de cómputo.

3. Uso de los Sistemas de Información

3.1. Asignación de permisos (permisos de lectura, escritura, ejecución, etc.) a las cuentas de los usuarios que trabajan con los sistemas. (SIAF, RENTAS SIAM, SISGUB, etc.).

3.2. A través del Servidor de Archivos todos los usuarios de la MDM podrán acceder a través de una unidad de red identificada en el explorador de Windows por una Letra "Z", la cual está estructurada por carpetas con los nombres de las Oficinas y/o Gerencias de la Municipalidad; con la finalidad de que el usuario pueda almacenar, leer y modifica información única y exclusivamente en la carpeta que identifica su respectiva Unidad Orgánica con la frecuencia de tiempo que considere el usuario. A esta unidad de red, se le llama "CARPETA COMUN", a la cual acceden TODOS los usuarios de la MDM con el fin de compartir información con otros usuarios de las diferente Oficinas y/o Gerencias de la MDM, el almacenamiento en esta carpeta es de uso temporal, cada usuario debe almacenar la información definitiva en la carpeta asignada a su unidad orgánica.

3.3. través del servicio del correo electrónico Institucional existe fluidez de información entre los usuarios de la MDM y usuarios externos a la institución.

3.4. Los usuarios de las diversas Unidades Orgánicas de la MDM deben de realizar la copia de seguridad de sus archivos informáticos almacenado en su PC previa coordinación con la Unidad de Informática y Procesamiento de Datos y remitirlas a la Unidad de Informática y Procesamiento de Datos en medios digitales (CDs, DVDs) previa limpieza de virus, con una frecuencia 01 semestral minima.

4. Uso del servicio de Internet

4.1. Es obligatorio para los usuarios tener como página Web de inicio predeterminada la página Oficial de la Municipalidad Distrital de la Miraflores cuya dirección es www.munimiraflores.gob.pe

La Gerencia Municipal por intermedio de la Unidad de Informática y Procesamiento de Datos, administra los permisos de acceso a los servicios de Internet para todos los usuarios de la MDM. Se estableció Niveles de Acceso a los Servicios de Internet según el cargo y función que realice el usuario: VER ANEXO Nº 1.

4.2. El usuario solo debe acceder a los servicios de Internet únicamente a sitios relacionados con sus funciones laborales.

4.3. Todo archivo adjunto descargado desde las páginas Web es examinado por el antivirus (debiendo estar actualizado) que los usuarios tienen instalados en su equipo de Cómputo.

a. El no realizar esta acción puede poner en riesgo la información de la MDM ya que pueden provocar que ingrese a la red informática archivos con virus o con código malicioso los cuales pueden borrar o alterar información de archivos, consumir recursos del equipo, acceso no autorizado a archivos.
b. El virus se puede extender por los equipos informáticos de la MDM y producir cortes o instantes prolongados de inactividad y pérdidas de datos muy graves.

4.4. Borrar las cookies, los ficheros temporales y el historial cuando un usuario acceda a los servicios de Internet, para no dejar rastro de su navegación.

4.5. El usuario es responsable por cualquier información obtenida desde Internet.

4.6. Mantener siempre deshabilitada la opción de los navegadores Web que ofrecen recordar su password para su próxima visita a una página.

VII. PROHIBICIONES PARA EL USUARIO

1. Instalación de programas adicionales (propios u obtenidos desde Internet) a los que se configuró en su perfil, salvo situaciones en las que requiera instalar programas remitidos por los organismos externos, relacionados al campo especializado de cada Unidad Orgánica, para lo cual la misma deberá de ejecutar las coordinaciones pertinentes con la Unidad de Informática y Procesamiento de Datos.
2. Almacenar información personal como: música, videos, imágenes, etc.
3. Inicio de sesión, con su cuenta asignada, a un equipo de cómputo diferente al que le fue asignado.
4. Usar los servicios de Internet para actividades lucrativas o comerciales de carácter individual.
5. Suplantar la cuenta de otro usuario.
6. Usar irracional, ineficiente y desconsideradamente los recursos informáticos disponibles, por ejemplo: Espacio en el Disco Duro, guardar documentos no relacionados a la Municipalidad Distrital de la Miraflores (Fotos, música, videos, etc.).
7. Utilizar los recursos informáticos para obtener acceso no autorizado a otros equipos y Servidores.
8. Utilizar los servicios de Internet para ejecutar juegos, emisoras radiales, TV en línea, videos en línea, salvo los casos relacionados a capacitaciones, conferencias en línea o videos descriptivos sobre las competencias que deben ejecutar los gobiernos locales.
9. Acceder a cualquier tipo de servicios de mensajería instantánea, como Messenger, Skype, etc.
10. El acceso a sitios obscenos, que distribuyen libremente material pornográfico, material subversivo, ofensivo, en prejuicio de terceros y que riñan contra la moral y las buenas costumbres y así como la redistribución de dicho material a través de correo electrónico o medio similar.
11. Utilizar los servicios Internet, incluyendo el correo electrónico o cualquier otro recurso, para intimidar, insultar o acosar a otras personas interfiriendo con el trabajo de los demás provocando un ambiente de trabajo no deseable.
12. Guardar información en la red que infrinja los derechos de los demás.
13. Violar o intentar violar los sistemas de seguridad de los equipos de cómputo a las cuales se tenga acceso, tanto a nivel local como remoto.
14. Modificar el estado de la configuración de Red de las computadoras o servidores, cambiando el numero IP (Internet Protocol) configurado por la Unidad de Informática y Procesamiento de Datos.
15. Decodificar el tráfico de la red o cualquier intento de obtención de información de correo electrónico confidencial que se trasmita a través de la misma.
16. Acceder mediante los servicios de Internet a contenidos que pueden estar relacionados con servidores generadores de SPAM o VIRUS, o que puedan contener programas que permitan romper las claves de acceso, u otros que puedan entenderse como contenidos que puedan utilizarse con fines no lícitos o no autorizados para la MDM.
17. Compartir archivos y/o carpetas entre las PC's (No usan el servidor Fileserver).

18. No apagar y/o reiniciar el equipo informático debidamente sino desconectarlo bruscamente de la energía eléctrica.
19. Al final de las labores diarias deberán apagar la Pc's y el estabilizador, se realizara inspecciones para verificar el cumplimiento.
20. Otros que no estén relacionados estrictamente con las tareas asignadas.

VIII. DISPOSICIONES COMPLEMENTARIAS

RESPONSABILIDAD DE LA UNIDAD DE TECNOLOGIA DE LA INFORMACION

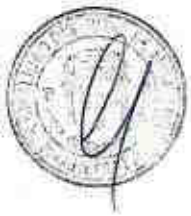
1. La Unidad de Informática y Procesamiento de Datos, conforme a sus competencias funcionales, adopta, propone y/o coordina las medidas pertinentes, a fin de garantizar la integridad y el correcto funcionamiento de los equipos de cómputo y los servicios de red, Internet de la MDM. Dichas medidas corresponden, pero no se limitan a:

1.1. Efectuar el mantenimiento preventivo y correctivo de los equipos de cómputo, la conservación de su instalación, la verificación de la seguridad física, así como su acondicionamiento.

El Mantenimiento Correctivo de los equipos de cómputo (reparación o repotenciación) seguirá el siguiente procedimiento:

a. El área usuaria efectuará el requerimiento de servicio a la Unidad de Informática y Procesamiento de Datos.
b. La Unidad de Informática y Procesamiento de Datos elaborará un Informe Técnico de servicio (Ficha de Soporte Técnico), detallando el servicio, los componentes que han sido reemplazados y la condición del equipo luego de la revisión.
c. En caso que dicho equipo de cómputo se encuentre dentro del periodo de garantía de uso, se comunicará a la empresa proveedora para que proceda a la reparación correspondiente.

1.2. Realizar la actualización de los equipos de cómputo, a fin de conservar e incrementar la calidad del servicio que se prestan.
1.3. Proveer de la infraestructura de seguridad adecuada en atención a los requerimientos específicos de cada área.
1.4. Establecer las disposiciones pertinentes para el acceso a áreas críticas (centros de cómputo) y uso de equipos cuya misión es crítica (información clasificada), así como para el registro del tráfico de personal en dichas áreas, teniendo en cuenta las situaciones de emergencia o de urgencia manifiesta.



1.5. Proporcionar el servicio de acceso remoto (fuera del centro laboral) a personal autorizado y establecer las disposiciones complementarias pertinentes para salvaguardar la integridad de la red.
1.6. Efectuar el monitoreo constante de las tecnologías de Internet, así como de los sistemas considerados críticos.

1.7. Controlar el acceso a la red e Internet, restringiendo el acceso al usuario que contravenga las normas contenidas en la presente Directiva.
1.8. Implementar herramientas que filtren y limiten aquellos contenidos y servicios que se ofrecen en Internet, que puedan atentar contra el buen desempeño de los usuarios, la moral, entre otros.
1.9. Mantener instalados softwares antivirus licenciados en todos los equipos de cómputo.

1.10. Coordinar, evaluar y proponer las medidas pertinentes para solucionar los problemas informáticos correspondientes.

1.11. La Unidad de Informática y Tecnología de la Información debe evitar que a través del correo electrónico institucional se reciba publicidad privada que no tenga ninguna relación con las competencias municipales.

2. El personal técnico responsable de la Unidad de Informática y Procesamiento de Datos coordinará permanentemente e informarán sobre el estado general de los servicios de red, a la Jefatura de UIPD.
3. A través de la implementación del Servidor WSUS, se actualizará el sistema operativo Windows y demás aplicaciones, a todos los equipos de cómputo con las últimas actualizaciones críticas y de seguridad.
4. Implementó políticas de Dominio que se ejecutan en los equipos de cómputo a nivel de usuario y equipo.
5. Las políticas de seguridad de usuario se implementarán de acuerdo a las funciones que cumplan. VER ANEXO Nº 2.
6. Configurar el perfil del usuario con permisos de "Usuario Avanzado" en el equipo local con fines de seguridad. (evitar los ataques de virus, daños en el sistema operativo, instalación de programas ajenos a las funciones del usuario, etc.).
7. Realizar el Inventario de Hardware y Software de los equipos de cómputo (PC's e impresoras) cada fin de año y cuando disponga la Gerencia Municipal.
8. Establecer Políticas en la consola de Administración del Antivirus Corporativo como:
   a. Realizar el análisis de un medio extraíble, USB, de manera automática cuando el usuario inserte a su PC.
   b. Definir contraseña para la no desactivación del Antivirus instalados en los equipos de cómputo.
   c. Programar y realizar el escaneo de la red de la Municipalidad con el Antivirus corporativo adquirido, este escaneo se realizará semanalmente cada lunes a las 7:00 PM, previamente la UIPD coordinara con las unidades orgánicas con la finalidad de que los usuarios dejen encendidas sus PC's para su escaneo, terminado el análisis el equipo de cómputo se apagará automáticamente.
9. Revisar trimestral o semestralmente el tipo de Información que el usuario almacena en su PC con la finalidad de evitar que el usuario almacene contenido no permitido como: música, fotos y videos; salvo sea necesario para la ejecución de sus funciones.

IX. DISPOSICIONES FINALES

1. En ningún caso, la Municipalidad Distrital de la Miraflores se hace responsable por documentos emitidos a través de la red o por el uso mal intencionado o ilegal de la misma por el usuario, o el daño causado a terceros por el uso no apropiado de los servicios habilitados a los usuarios
2. La Gerencia de Administración y Finanzas (GAF) a través de la Unidad de Informática y Procesamiento de Datos, se encargará de la actualización y/o cumplimiento de lo dispuesto en la presente Directiva.

X. GLOSARIO DE TERMINOS

Para efectos de la presente Directiva, se enmendará por:

a. **INTERNET**: Es una gran comunidad de computadoras conectadas entre sí por medio de líneas de comunicaciones especiales.
b. **INTERFACE**: Medio con el cual se puede interactuar con unas computadoras.
c. **NAVEGADOR**: Es un programa que provee una interfase para acceder y ver archivos.
d. **CORREO ELECTRÓNICO**: El correo electrónico, es el medio por el cual se pueden recibir y enviar información a través de un dispositivo electrónico.
e. **SERVIDOR**: En una red, se denomina servidor a una computadora compartida por múltiples usuarios. Existen servidores de archivos, servidores de impresión, etc. Los Servidores son computadoras de gran potencia que se encuentran a disposición de los usuarios. Cuando los usuarios se intercomunican, en realidad, lo hacen a través de servidores.
f. **SOFTWARE**: Conjunto de programas, documentos, procesamientos y rutinas asociadas con la operación de un sistema de computadoras, es decir la parte intangible o lógica de una computadora.
g. **USUARIO**: Personal de la Municipalidad de la Miraflores que se encuentra autorizado a utilizar los equipos y sistemas informáticos pertenecientes a la Municipalidad.

ANEXO N° 1

POLITICAS DE SEGURIDAD A NIVEL DE DOMINIO

NIVELES DE PERMISO	CATEGORIA DEL ACCESO O PERMISO
A	ACCESO ALTO Tienen acceso total a la Internet, limitadas descargas excepto a Páginas de contenido Pornográfico y aquellas que pongan en riesgo la seguridad implementada en la Municipalidad. **GERENTE GENERALES.**
B	ACCESO MEDIO Tienen acceso para la navegación a las redes sociales y limitadas descargas. Excepto mensajería, ftp, radio. **GERENTES Y PERSONAL AUTORIZADO**
C	ACCESO BAJO Tienen acceso para la navegación institucional, pero no tiene acceso a mensajería, ni comunicación en línea (radios, videos, etc.) ni a redes sociales (facebook, youtube, whatsApp etc.) **USUARIOS**
D	SIN ACCESO Se le restringe la salida a Internet, solo puede trabajar con los servicios internos como página web corporativa, correo corporativo y aplicaciones de la municipalidad (SIAF, SEACE, SISTEMA RENTAS, LOGISTICA)

- **Descargas Limitadas:** Puede bajar archivos adjuntos (archivos para uso de Oficina) Tipo Word, Excel, Pdf, Zip, Rar, etc.
- **Para todos los casos los usuarios de todos los grupos tienen acceso al correo MUNIMIRAFLORES.GOB .PE.**
- **Para todos los casos los usuarios están impedidos de acceder a las páginas de adultos.**

ANEXO Nº 2

POLITICAS DE SEGURIDAD A NIVEL DE DOMINO

A. POLITICA A NIVEL DE USUARIO

a. Internet Explorer, Mozilla Firefox, Opera, Chrome

-Título de la barra de Texto: Municipalidad de la Miraflores.

-Configurar como página de inicio de Internet Explorer a: www.munimiraflores.gob.pe.

B. Panel de control

-Prohibir el acceso al Panel de Control.

C. Panel de control /Agregar y quitar Programas

-Ocultar la opción agregar y quitar programas desde la red.

-Ocultar la opción agregar y quitar programas desde Microsoft.

-Ocultar la opción agregar y quitar programas desde un CD-ROM o Disquete.

-Ocultar la página agregar nuevos programas.

-Ocultar la página agregar o quitar componentes de Windows.

-Ocultar la página agregar y quitar programas.

-Ocultar la página configurar acceso y programas predeterminados.

-Quitar agregar o quitar programas.

-Quitar la información de Soporte Técnico.

D. Panel de control /Pantalla

-Impedir cambios en el papel Tapiz.

-Ocultar la ficha apariencia y temas.

-Ocultar la ficha configuración.

E. Sistema Desactivar reproducción automática

-(Desactivar reproducción automática en: Todas las Unidades.)

-No mostrar la Pantalla de bienvenida de introducción al iniciar sesión.

F. Escritorio

-No agregar recursos compartidos de documentos abiertos recientemente a mis sitios de red.

-Ocultar el icono de mis sitios de red del escritorio. Prohibir al usuario cambiar la ruta de mis documentos.

-Prohibir el ajuste de las barras de herramientas del escritorio.

-Quitar el elemento propiedades del menú contextual de mis documentos.

G. Escritorio /Active Desktop

-Configurar el papel tapiz del escritorio una imagen de la Municipalidad de la Miraflores.

H. Menú Inicio y barra de tareas.

-Bloquear la barra de tareas.

-Borrar el historial de documentos abiertos recientemente al salir.

-Forzar menú inicio clásico.

-Impedir cambios en la configuración de la barra de tareas y del menú inicio.

-No guardar el historial de documentos abiertos recientemente.

-No mostrar ninguna barra de herramientas personalizada en la barra de Tareas.

-Quitar conexiones de red del menú inicio.

-Quitar el icono mi música del menú inicio.

-Quitar el icono mis documentos del menú inicio.

-Quitar el icono de mis imágenes del menú inicio.

-Quitar el icono mis sitios de red del menú inicio.

-Quitar el menú mis documentos del menú inicio.

-Quitar el menú favorito del menú inicio.

-Quitar las carpetas de usuario del menú inicio.

-Quitar programas del menú configuración.

-Quitar vínculos y accesos a Windows update.

I. POLITICA A NIVEL DE EQUIPO

a. Sistema

- Impedir el acceso a herramientas de edición de registro.

b. Red /Conexiones de Red

- Impedir el cambio de nombre en la conexión LAN.
- No mostrar la conexión LAN en la barra de tareas.
- Prohibir la configuración TCP/IP avanzada.