DIRECTIVA DE SEGURIDAD PARA LA CREACIÓN DE ACCESOS PARA LAS COMPUTADORAS Y SISTEMAS INFORMATICOS

1. FINALIDAD

Norma interna que establece un procedimiento de seguridad para la creación y asignación de accesos a las computadoras y a los sistemas informáticos de la entidad.

2. OBJETIVOS

a. Establecer una norma que le de legalidad a los accesos (Seguridad de la Información) que se otorgan a los usuarios para el uso de las computadoras y de los diversos sistemas informáticos que operan en la corporación municipal. La seguridad de la información, se entiende cómo aquellas técnicas preventivas que las organizaciones adquieren para resguardar y proteger sus activos de información, para mantener la confidencialidad, integridad y disponibilidad de los mismos.
b. Establecer las responsabilidades de cada usuario en el uso de los accesos que se les asigne.
c. Establecer una guía de buenas prácticas del uso de los accesos a los sistemas computacionales.
d. Implantar controles, procedimientos y políticas de seguridad para asegurar la disponibilidad, integridad y confidencialidad de la información; asegurando que el acceso a la información se realice por personal autorizado para su uso.

3. ALCANCE

La presente Directiva es de cumplimiento obligatorio para todos los usuarios finales de la Municipalidad Distrital de Cieneguilla, que soliciten acceso a los sistemas informáticos de la entidad, independientemente del régimen de contratación.

4. BASE LEGAL

a. Reglamento de Organización y Funciones (ROF) de la Municipalidad Distrital de Cieneguilla.
b. Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información Técnicas de Seguridad, Sistemas de Gestión de Seguridad de la Información, Requisitos, 2da. Edición".

5. DISPOSICIONES GENERALES

5.1. DE LA SOLICITUD DE LOS ACCESOS

Artículo 1.- La creación de usuarios para los accesos a los sistemas informáticos y la creación de usuarios en el dominio (usuarios para el uso de las computadoras), son solicitados a la Subgerencia de Tecnologías de la Información y Comunicación, que es la unidad orgánica competente para otorgarlos.

Artículo 2.- Los accesos señalados en el artículo 1, son solicitados mediante un documento por los Gerentes y/o Subgerentes del área usuaria; en el caso de las Subgerencias tiene que tener el visto bueno del Gerente

Artículo 3.- El Funcionario que solicita el acceso a las computadoras y sistemas informáticos debe indicar en el documento la siguiente información:

Uso de Computadoras

Nombre(s) del(los) usuario(s)

Sistemas Informáticos

Nombre(s) del(los) usuario(s)
Sistema(s) informático(s) a acceder
Niveles de acceso (mantenimiento y/o consultas)
Opciones del sistema(s) a acceder

Artículo 4.- Los accesos solo pueden ser solicitados para los sistemas que son competencia de la oficina.

Artículo 5.- En los casos que por necesidad de trabajo se requiera otorgar el acceso a un sistema que no es competencia de la oficina, la solicitud debe ir visada por el Gerente del Área y con el visto bueno del Gerente Municipal; así mismo debe de indicarse la información señalada en el Articulo 4.

Artículo 6.- Solo pueden solicitarse y otorgarse accesos a personas que laboran en la corporación edil sean funcionarios, personal estable, contratado permanente, CAS, asesores *y/o* cualquier otra modalidad de contrato.

5.2. DEL REGISTRO Y USO DE LOS ACCESOS

Artículo 7.- El nombre de usuario y la clave de acceso son de carácter personal e intransferible, queda terminantemente prohibido divulgar, ceder *y/o* prestar su clave de acceso. Las cuentas de los usuarios deben ser únicas, de manera que se puedan identificar las acciones que realizan las acciones de acuerdo a su perfil de acceso. La contraseña a generar debe tener las siguientes consideraciones:

a. Tener mínimo 5 caracteres y como máximo 10 caracteres
b. Tener en su contenido letras mayúsculas, minúsculas y números
c. No puede contener datos personales del usuario como su nombre, apellido, número de DNI, fecha de nacimiento, etc.

Artículo 8.- Cada usuario es responsable de la correcta actualización de la información de los sistemas para los que se les ha brindado los accesos. Por motivos de seguridad, la contraseña puede ser cambiada periódicamente por el usuario.

Artículo 9.- Queda prohibido dejar el acceso de la computadora cuando el usuario se retira de su puesto de trabajo, aunque sea por corto tiempo. Por seguridad tendrá que activar el protector de pantalla de la computadora.

5.3. DE LA BAJA DE USUARIO O DEL CAMBIO DE ACCESOS

Articulo 10.- Para ampliar o reducir los niveles de acceso de un usuario a los sistemas informáticos, el funcionario a cargo solicitará dicho cambio a través de un documento indicando la información señalada en el Articulo 4.

Artículo 11.- Cuando un usuario es trasladado a un área distinta de la que solicitó originalmente sus accesos, el funcionario responsable del área de origen, bajo responsabilidad funcional, informara a la Subgerencia de Tecnologías de la Información y Comunicación para que proceda a eliminar los accesos del usuario, los mismos que deberán ser solicitados por el funcionario responsable el área de destino del usuario (Ver Articulo 4)

Artículo 12.- Cuando un usuario se retira de la corporación edil, el funcionario del área, bajo responsabilidad funcional informara mediante un documento a la Subgerencia de Tecnologías de la Información y Comunicación para que se deshabiliten los accesos del usuario. El nombre del usuario debe de mantenerse en el sistema (sin accesos activos) hasta por dos años posteriores al retiro, cese y/o renuncia del trabajador a la corporación edil.

5.4. DEL MANTENIMIENTO DE LOS USUARIOS Y ACCESOS

Artículo 13.- La Subgerencia de Tecnologías de la Información y Comunicación como mínimo una vez al año debe realizar un mantenimiento general de los usuarios y accesos en el sistema, para tal fin emitirá previamente un memorándum circular solicitando a todas las áreas la relación de usuarios activos *y* sus respectivos accesos, otorgando siete (7) días calendario, vencido el plazo se procederá a deshabilitar a los usuarios cuyos accesos no se ha solicitado su renovación y/o actualización por los funcionarios respectivos.

Artículo 14.- La Subgerencia de Tecnologías de la Información y Comunicación puede realizar el mantenimiento descrito en el artículo precedente en cualquier momento, sin aviso previo y de considerarlo necesario, así como, por fuerza mayor y/o caso fortuito, para salvaguardar la información de la corporación edil.

6. DISPOSICIONES COMPLEMENTARIAS

Artículo 15.- El personal de la entidad que difunda por cualquier medio las contraseñas propias o de otros usuarios, cometerá una falta de grave y estará sujeto a las acciones de ley correspondientes.

Artículo 16.- El compartir información de usuarios y contraseñas es una falta al presente reglamento, y también conduce una falta grave, y estará sujeto a las acciones de ley correspondientes.

Artículo 17.- La Subgerencia de Tecnologías de la Información y Comunicación brindará el asesoramiento y apoyo técnico correspondiente.

Artículo 18.- Los casos no contemplados en la presente Directiva, serán resueltos por la Subgerencia de Tecnologías de la Información y Comunicación, en base a la Ley, su Reglamento y la presente Directiva.

Artículo 19.- Durante el tiempo en el que se reciban y resuelvan los pedidos de restricción o confidencialidad de acceso a algún módulo del sistema, cada funcionario será responsable del uso de la información para la cual solicitó el acceso

Artículo 20.- El incumplimiento de la presente Directiva por los funcionarios, personal nombrado, contratado permanente, CAS y/o bajo cualquier otra modalidad contractual son responsables de su ejecución, el mismo que dará lugar a las sanciones administrativas y/o contractuales a que hubiere lugar e inicio de las acciones judiciales de ser el caso.

7. DISPOSICION FINAL.-

La presente Directiva entrara en vigencia a partir del día siguiente de su aprobación.