MUNICIPALIDAD PROVINCIAL DE
CHACHAPOYAS

RESOLUCIÓN DE ALCALDÍA Nº 127 -2021-MPCH

San Juan de la Frontera de los Chachapoyas, 23 ABR. 2021

VISTO:

El Oficio Nº 000022-2021-MPCH/GPP-SGTI con registro Nº 212207.002 de fecha 17 de febrero del 2021, Informe Nº 000074-2021-MPCH/SG con registro Nº 212207.003 de fecha 05 de marzo del 2021, Informe Nº 000034-2021-MPCH/GPP-SGM con registro Nº 212207.004 de fecha 13 de abril del 2021, Informe Nº 000085-2021-MPCH/GPP-SGTI con registro Nº 2110423.001 de fecha 13 de abril del 2021, Informe Nº 000108-2021-MPCH/GPP con registro Nº 2110423.002 de fecha 14 de abril del 201, y proveído de Gerencia de Administración y Finanzas de fecha 15 de abril del 2021, y;

CONSIDERANDO:

Que, la Municipalidad Provincial de Chachapoyas es un órgano de Gobierno Local con autonomía política, económica y administrativa en asuntos de su competencia, conforme lo dispone el Artículo 194° de la Constitución Política del Perú, modificada por la Ley Nº 30305, concordante con el Artículo II del Título Preliminar de la Ley Orgánica de Municipalidades N° 27972, adoptando para su administración una estructura gerencial, sustentándose en principios de programación, dirección, ejecución, supervisión y control concurrente;

Que, mediante Oficio Nº 000022-2021-MPCH/GPP-SGTI con registro Nº 212207.002 de fecha 17 de febrero del 2021, el Sub Gerente de Tecnologías de la Información remite al Gerente de Planeamiento y Presupuesto las políticas a implementar en la institución, como parte de las políticas de tecnologías de la información; cuyo propósito es establecer un estándar de uso de contraseñas seguras, la protección de las contraseñas y su frecuencia de cambios; asimismo, solicita comunicar a la Secretaria General para su socialización y posterior aprobación e implementación en la institución;

Que, con Informe Nº 000074-2021-MPCH/SG con registro Nº 212207.003 de fecha 05 de marzo del 2021, el Secretario General informa al Gerente de Planeamiento y Presupuesto que revisado el proyecto de Políticas de Cuentas de Usuario realizado por la Sub Gerencia de Tecnologías de la Información y se encuentra conforme, y solicita que su revisión por la Sub Gerencia de Modernización y se derive a la Oficina de Asesoría Jurídica para la proyección del acto administrativo de aprobación; asimismo, precisa que en los últimos años la entidad ha tenido serios problemas de seguridad y malas prácticas de usurarios y contraseñas en el sistema informático, siendo de suma importancia y urgencia aprobar las políticas adjuntas para conocimiento y aplicación de todos los servidores de la municipalidad;

Que, mediante Informe Nº 000034-2021-MPCH/GPP-SGM con registro Nº 212207.004 de fecha 13 de abril del 2021, la Sub Gerente (e) de Modernización informa al Gerente de Planeamiento y Presupuesto, que procedió a revisar el proyecto de Políticas de Cuentas de Usuario, cuyo instrumento no presenta observaciones en su contenido; por lo que remite con la finalidad de continuar con su trámite de aprobación para su implementación;

Que, con proveído de fecha 13 de abril del 2021 el Gerente de Administración y Finanzas remite el Informe Nº 000034-2021-MPCH/GPP-SGM a la Oficina de Asesoría Jurídica, solicitando la proyección de acto resolutivo;

En uso de las atribuciones que le otorga la Constitución Política del Perú, el numeral 6) del Artículo 20º de la Ley Orgánica de Municipalidades Nº 27972, y con la visación correspondiente;

SE RESUELVE:

ARTÍCULO PRIMERO.- APROBAR las Políticas de Seguridad – Política de Contraseñas de la Municipalidad Provincial de Chachapoyas, por los considerandos expuestos, contenido por:

1. Introducción
2. Propósito
3. Ámbito de aplicación
4. Vigencia
5. Revisión y evaluación
6. Referencias
7. Desarrollo de la política
8. Administración día a día de cuentas de acceso a recursos

RESOLUCIÓN DE ALCALDÍA Nº 127 -2021-MPCH

9. Responsabilidades
10. Cumplimiento de la Política
11. Criterios en la construcción de contraseñas seguras
12. Historial de Revisiones

Anexo: Acrónimos y glosario de términos.

ARTÍCULO SEGUNDO.- **DISPONER** la implementación de las Políticas de Seguridad – Política de Contraseñas de la Municipalidad Provincial de Chachapoyas, por la Sub Gerencia de Tecnologías de la Información, Gerencia de Planeamiento y Presupuesto, y demás áreas de la Municipalidad Provincial de Chachapoyas.

ARTÍCULO TERCERO.- **NOTIFICAR** la presente a las instancias administrativas correspondientes de la Municipalidad Provincial de Chachapoyas, y a los servidores públicos indicados, para los fines de Ley.

REGÍSTRESE, COMUNÍQUESE, CÚMPLASE

MUNICIPALIDAD PROVINCIAL DE CHACHAPOYAS
VICTOR RAÚL CULQUI PUERTA
Alcalde

MUNICIPALIDAD PROVINCIAL V°B° GERENCIA MUNICIPAL CHACHAPOYAS

MUNICIPALIDAD PROVINCIAL V°B° GERENCIA DE PLANEAMIENTO Y PRESUPUESTO CHACHAPOYAS

MUNICIPALIDAD PROVINCIAL V°B° GERENCIA DE ADMINISTRACION Y FINANZAS CHACHAPOYAS

MUNICIPALIDAD PROVINCIAL V°B° OFICINA DE ASESORIA JURIDICA CHACHAPOYAS

151

MUNICIPALIDAD PROVINCIAL
DE CHACHAPOYAS
GERENCIA DE PLANEAMIENTO Y
PRESUP...

26 ABR. 2021

RECIBIDO

HORA: 8:45 FOLIOS: 02 FIRMA:

MUNICIPALIDAD PROVINCIAL
VB°
SUB GERENCIA DE
TECNOLOGIAS DE
LA INFORMACIÓN
CHACHAPOYAS

MUNICIPALIDAD PROVINCIAL DE
CHACHAPOYAS

Políticas de Seguridad

Política de contraseñas de la Municipalidad Provincial de Chachapoyas

Contenido

1. Introducción

La Municipalidad Provincial de Chachapoyas (en adelante, MPCH) establece una Política de Contraseñas acorde a los requisitos legales vigentes que debe ser aplicada a cualquier mecanismo de autentificación que utilicen los miembros de la institución para acceder a los Servicios de Tecnologías de la Información y las Comunicaciones (en adelante, TIC) de la MPCH.

Concretamente se aplica al Usuario Virtual de la Municipalidad Provincial de Chachapoyas (en adelante, UVMPCH), que es el mecanismo de acceso a los servicios más extendidos, así como a los usuarios locales de las aplicaciones informáticas que no utilizan el UVMPCH como medio de autenticación y a los usuarios externos que acceden a la Red Informática de la Municipalidad Provincial de Chachapoyas (RIMPCH) a través de Escritorio Remoto o Redes Privadas Virtuales (VPN).

2. Propósito

El propósito de esta política es establecer un estándar de uso de contraseñas seguras, la protección de esas contraseñas y su frecuencia de cambios.

3. Ámbito de aplicación

El alcance de esta política es de aplicación y de obligado cumplimiento para todo el personal que tiene o es responsable de una cuenta (o cualquier forma de acceso que requiera una contraseña) en cualquier sistema que resida en las instalaciones de la municipalidad, tenga acceso a la red de la municipalidad, puntos de venta o de cualquier información privada de la municipalidad.

Su usuario y contraseña le permite el acceso a los siguientes servicios y aplicaciones de la Municipalidad Provincial de Chachapoyas:

Autenticación local para acceso a su puesto de trabajo (equipos conectados a dominio)

- SISADMIN
- SIAM Soft
- SIGA
- SRTM
- Correo Electrónico
- Red Privada Virtual (VPN)
- Acceso a la red inalámbrica
- Usuarios de Escritorio remoto
- Servicios de Intranet

4. Vigencia

Esta política ha sido aprobada por la Comisión de Seguridad de la MPCH con fecha 03 de febrero de 2021, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la MPCH pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en ella.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de la MPCH. Las versiones anteriores quedan anuladas por la última versión de esta política

5. Revisión y evaluación

La gestión de esta política corresponde a la Sub Gerencia de Tecnologías de la Información (en adelante, SGTI) de la MPCH, que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.
- Proceder a su revisión, cuando sea necesario, para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
- Verificar su efectividad.

Cuando las circunstancias así lo aconsejen se revisará la presente política, que se someterá, de haber modificaciones, a la aprobación de la Comisión de Seguridad de la MPCH.

La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica y organización general o cualquier otra cuestión que pueda provocarla.

Será el responsable de la Sub Gerencia de Tecnologías de la Información la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

6. Referencias

La presente política se fundamenta en la legislación vigente en materia de seguridad de las Tecnologías de la Información y las Comunicaciones de ámbito internacional, estatal y autonómico, así como en las normas y procedimientos internos que resulten de aplicación a la Municipalidad en el marco de la Política de Seguridad de la Información.

7. Desarrollo de la política

7.1. Política General

- El uso de la cuenta de usuario es responsabilidad de la persona a la que está asignada. La cuenta es para uso personal e intransferible.
- La cuenta de usuario se protegerá mediante una contraseña. La contraseña asociada a la cuenta de usuario, deberá seguir los Criterios para la Construcción de Contraseñas Seguras descrito más abajo.
- Las cuentas de usuario (usuario y contraseña) son sensibles a mayúsculas y minúsculas, es decir que estas deben ser tecleadas como están.
- No compartir la cuenta de usuario con otras personas: compañeros de trabajo, amigos, familiares, etc.
- Si otra persona demanda hacer uso de la cuenta de usuario hacer referencia a estas políticas. De ser necesaria la divulgación de la cuenta de usuario y su contraseña asociada, deberá solicitarlo por escrito y dirigido al Administrador del Sistema.
- Si se detecta o sospecha que las actividades de una cuenta de usuario pueden comprometer la integridad y seguridad de la información, el acceso a dicha cuenta será suspendido temporalmente y será reactivada sólo después de haber tomado las medidas necesarias a consideración del Administrador del Sistema.

7.2. Tipos de Cuentas de Usuario

Para efectos de las presentes políticas, se definen dos tipos de cuentas de usuario:

1. 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.
2. Cuenta de Administración de Sistema de Información: corresponde a la cuenta de usuario que permite al administrador del Sistema realizar tareas específicas de usuario a nivel directivo como, por ejemplo: agregar/modificar/eliminar cuentas de usuario del sistema.

7.3. Protección de Contraseñas

- Las contraseñas no deben de compartirse con nadie. Todas las contraseñas deben ser tratadas como sensibles, como Información confidencial de la municipalidad.
- Las contraseñas no se deben adjuntar en mensajes de correo electrónico u otras formas de comunicación electrónica.
- Las contraseñas no deben ser reveladas por teléfono a nadie.
- No debe de revelar contraseñas en cuestionarios o formularios de seguridad o de ningún tipo.
- No deje pistas del formato de una contraseña (por ejemplo, "nombre de mi familia").
- No comparta contraseñas de la municipalidad con nadie, incluyendo asistentes, administrativos, secretarias, directivos, dueños, socios, compañeros de trabajo durante las vacaciones, amigos o miembros de la familia.
- No escriba ni guarde contraseñas en post-its o papel en cualquier lugar de su oficina. No guarde las contraseñas en archivos en su computadora o dispositivos móviles (teléfonos, tablets) sin cifrado.
- No utilice la función "Recordar Contraseña" de aplicaciones (por ejemplo, navegadores web).
- Cualquier usuario que sospeche que su contraseña puede haber sido comprometida debe reportar el incidente inmediatamente y cambiar todas sus contraseñas a la brevedad.

Se aplica a todos los usuarios de los Servicios TIC de la Municipalidad Provincial de Chachapoyas la siguiente política de contraseñas:

- La longitud de la contraseña debe ser como mínimo de 8 caracteres, si bien se recomienda usar contraseñas más largas.
- La contraseña debe contener al menos 4 caracteres alfabéticos de los cuales serán, al menos, dos letras mayúsculas y dos minúsculas.
- La contraseña debe contener al menos 2 caracteres numéricos.
- El número máximo de repeticiones de caracteres adyacentes de la contraseña será 4.
- El número máximo de caracteres numéricos en secuencia de la contraseña será 4.
- La contraseña no podrá contener el nombre o apellido del usuario, ni el documento de identidad del mismo o su UVMPCH.
- No compartir la contraseña bajo ningún concepto con otras personas, aunque sean de su mismo entorno.
- Guardar la información de contraseñas en un lugar seguro.
- Cambiar la contraseña al menos una vez al año.
- No utilizar para generar la contraseña palabras o nombres comunes que puedan figurar en diccionarios.
- No se podrán utilizar las tres últimas contraseñas empleadas.

7.4. Cambios en las contraseñas

- Todas las contraseñas para acceso al Sistema Web con carácter administrativo deberán

ser cambiadas al menos cada 6 meses.

- Todas las contraseñas para acceso al Sistema Web de nivel usuario deberán ser cambiadas al menos cada 12 meses.
- Todas las contraseñas deberán ser tratadas con carácter confidencial.
- Las contraseñas de ninguna manera podrán ser transmitidas mediante servicios de mensajería electrónica instantánea ni vía telefónica.
- Si es necesario el uso de mensajes de correo electrónico para la divulgación de contraseñas, estas deberán transmitirse de forma cifrada.
- Se evitará mencionar y en la medida de lo posible, teclear contraseñas en frente de otros.
- Se evitará el revelar contraseñas en cuestionarios, reportes o formas.
- Se evitará el utilizar la misma contraseña para acceso a los sistemas operativos y/o a las bases de datos u otras aplicaciones.
- Se evitará el activar o hacer uso de la utilidad de ¿Recordar Contraseña? o ¿Recordar Password? de las aplicaciones.
- No se almacenarán las contraseñas en libretas, agendas, post-it, hojas sueltas, etc. Si se requiere el respaldo de las contraseñas en medio impreso, el documento generado deberá ser único y bajo resguardo.
- No se almacenarán las contraseñas sin encriptación, en sistemas electrónicos personales (asistentes electrónicos personales, memorias USB, teléfonos celulares, agendas electrónicas, etc.).
- Si alguna contraseña es detectada y catalogada como no segura, deberá darse aviso al(los) usuario(s) para efectuar un cambio inmediato en dicha contraseña.

7.5. Desarrollo de Aplicaciones

Los desarrolladores de aplicaciones deben garantizar que sus programas contienen las siguientes medidas de seguridad:

- Las Aplicaciones deben admitir autenticación de usuarios individuales no de grupos.
- Las aplicaciones no deben almacenar las contraseñas en texto claro o ni en algún formato fácilmente reversible.
- Las aplicaciones no deben transmitir contraseñas en texto claro por la red.
- Las Aplicaciones deben proveer de algún tipo de gestión por roles, de tal manera que un usuario pueda hacerse cargo de las funciones de otro sin necesidad de conocer la contraseña del otro.

7.6. Uso de Contraseñas y Passphrases.

- Las Passphrases (Frases de Contraseña) se utilizan generalmente para la autenticación de llave pública/privada. Un sistema de llave pública/privada define una relación matemática entre la llave pública que es conocida por todos y la llave privada, que es conocido sólo por el usuario. Sin la Passphrase para "desbloquear" la clave privada, el usuario no puede acceder.
- Las Passphrases no son lo mismo que las contraseñas. Una Passphrase son una versión más larga de una contraseña y es por lo tanto más segura. Una Passphrase se compone típicamente de varias palabras. Debido a esto es más segura contra "ataques de diccionario".
- Una buena Passphrase es relativamente larga y contiene una combinación de letras mayúsculas, minúsculas, caracteres numéricos y de puntuación. Un ejemplo de una buena Passphrase:
- "El*TraficoEnLa101Estava&EstaMañana"
- Todas las reglas anteriores que aplican a las contraseñas aplican a las Passphrases.

8. Administración día a día de cuentas y acceso a recursos

En toda institución hay cambios constantes de personal, por lo que es necesario contar con una política respecto al manejo de las cuentas de usuario de dicho personal, a continuación, se detallan los procedimientos a realizar en cada uno de los casos:

8.1. Nuevos empleados

Cuando una nueva persona entra a la organización, normalmente se les da acceso a varios recursos (dependiendo de sus responsabilidades). Por lo tanto también se le deben crear su usuario y contraseña para el acceso a los diferentes sistemas de la institución.

Para ello se debe tener en cuenta lo siguiente:

- La Sub Gerenciad de Recursos Humanos debe notificar sobre la llegada de una nueva persona a la institución.
- Además, debe llenar una forma solicitando los accesos correspondientes para la nueva persona, la cual será facilitada por la SGTI en una plataforma digital.

8.2. Terminaciones

Se debe enviar un informe de la terminación de relaciones laborales con un usuario para que la SGTI tome las medidas correspondientes.

Como mínimo, las acciones apropiadas a realizar deben incluir:

- Inhabilitar el acceso del usuario a todos los sistemas y recursos relacionados (usualmente mediante el cambio o bloqueo de la contraseña)
- Hacer una copia de seguridad de los archivos del usuario, en caso de que contengan algo que se pueda necesitar en un futuro.
- Coordinar el acceso a los archivos del usuario para el supervisor

La principal prioridad es asegurar los sistemas contra un usuario que ha dejado de trabajar con la organización recientemente, por lo que se procede a desactivar rápidamente el acceso a una persona que ya no pertenece a la compañía.

Esto indica la necesidad de que recursos humanos comunique sobre las terminaciones - preferiblemente antes de que estas sean efectivas.

Una vez desactivado el acceso, se debe hacer una copia de seguridad de los archivos de esta persona. Este respaldo puede ser parte de los respaldos estándares de la institución, o puede ser un procedimiento dedicado a hacer copias de seguridad de viejas cuentas de usuario. Aspectos tales como regulaciones sobre la retención de datos, guardar evidencia en casos de demandas por liquidaciones erróneas y otras parecidas, todas forman parte en determinar la forma más apropiada de manejar las copias de seguridad.

En cualquier caso, se hará un respaldo, pues el próximo paso (cuando el supervisor accede a los datos de la persona liquidada) puede resultar en la eliminación accidental de los archivos. En tales circunstancias, el tener una copia de seguridad reciente hace posible recuperarse fácilmente de este tipo de accidentes, haciendo el proceso más fácil tanto para el supervisor como para la SGTI.

En este punto, se debe determinar qué tipo de acceso requiere el supervisor de la persona recientemente terminada a los archivos de esta. En la institución se le otorgará acceso total a los archivos para los fines correspondientes.

Si la persona utilizó los sistemas para cosas más allá que simplemente correo electrónico, es posible que el supervisor tenga que revisar y colar un poco los archivos, determinar lo que se debería mantener y qué se puede desechar. Al concluir este proceso, al menos algunos de estos archivos serán entregados a la persona que tomará las responsabilidades de la persona liquidada, a cargo del supervisor y si éste lo solicitara acompañado de la SGTI.

8.3. Cambios de trabajo

La situación no es tan clara cuando la persona cambia de responsabilidades dentro de la institución. Algunas veces la persona puede requerir cambios a su cuenta y algunas veces no. Para ello se tendrá al menos tres personas relacionadas en asegurarse de que la cuenta del usuario sea configurada adecuadamente para coincidir con las nuevas responsabilidades:

- Sub Gerencia de Tecnologías de la Información
- El supervisor original del usuario
- El nuevo supervisor del usuario

Entre los tres se determina qué se debe hacer para cerrar limpiamente las responsabilidades anteriores del empleado y qué se debe hacer para preparar la cuenta para sus nuevas responsabilidades. Dependiendo del caso y del sistema, se debe proceder a cerrar la cuenta existente y crear una nueva cuenta para el usuario. Pero en caso no se pueda realizar este procedimiento se debe modificar la cuenta de usuario para las nuevas responsabilidades. La SGTI en coordinación con los supervisores del usuario debe revisar cuidadosamente la cuenta para asegurarse de que no se están dejando recursos o privilegios de acceso en la cuenta y que esta tiene solamente los recursos y privilegios adecuados para las nuevas responsabilidades de la persona.

Si se necesitase que el usuario esté en un período de transición donde la persona realiza tareas relacionadas a ambos grupos de responsabilidades, es aquí donde los supervisores original y nuevo, deben ayudar a la SGTI brindando una ventana de tiempo para este período de transición.

9. Responsabilidades

Cuando se demuestre un uso incorrecto o no aceptable con respecto a lo especificado en este documento, o cuando se reciba un aviso de incidencia, el SGTI podrá proceder al bloqueo temporal o indefinido del usuario dependiendo de la gravedad y reiteración del incidente, siendo responsable el usuario titular.

10. Cumplimiento de la Política

10.1. Medidas de Cumplimiento

El equipo de la Sub Gerencia de Tecnologías de la Información verificará el cumplimiento de esta política a través de diversos métodos, incluyendo, pero no limitado a, revisiones periódicas caminando (walk- thru), video vigilancia (si fuera el caso), informes de la herramienta de negocio, auditorías internas y externas, así como la retroalimentación al dueño de la política.

10.2. Excepciones

Cualquier excepción a la norma debe ser aprobada por el Equipo de la Sub Gerencia de las Tecnologías de la Información con antelación.

10.3. Incumplimiento

Un empleado que se haya encontrado que ha violado esta política puede estar sujeto a medidas disciplinarias, hasta e incluyendo la terminación del empleo.

11. Criterios en la construcción de contraseñas seguras

Una contraseña segura deberá cumplir con las siguientes características:

- La longitud debe ser al menos de 8 caracteres.
- Contener caracteres tanto en mayúsculas como en minúsculas.
- Tener al menos un símbolo (cualquier otro carácter que no sea alfabético o numérico: `~! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /).
- No debe ser una palabra por sí sola, en ningún lenguaje, dialecto, jerga, etc.
- No debe ser un palíndromo (ejemplo: agasaga)
- No debe ser basada en información personal, nombres de familia, etc.
- Procurar construir contraseñas que sean fáciles de recordar o deducir.
- Algunos ejemplos de contraseñas NO seguras por sí solas:
- Nombres de familiares, mascotas, amigos, compañeros de trabajo, personajes, etc.
- Cualquier palabra de cualquier diccionario, términos, sitios, compañías, hardware, software, etc.
- Cumpleaños, aniversarios, información personal, teléfonos, códigos postales, etc.
- Patrones como 1234?, aaabbb, qwerty, zyxwvuts, etc.
- Composiciones simples como: MINOMBRE1, 2minombre, etc.

Además de la anterior política de contraseñas aplicada a los UVMPCH, el usuario podrá observar las siguientes recomendaciones:

- Modificar la contraseña que le entreguen antes de hacer uso de ella, aunque no esté obligado a hacerlo.
- Los usuarios no deben usar la misma contraseña para acceso a cuentas de la municipalidad que para otro tipo de accesos no relacionados con la municipalidad (por ejemplo, cuentas de Correo personal, Redes Sociales, etc.).
- Siempre que sea posible, los usuarios no deben usar la misma contraseña para diferentes necesidades de acceso de la municipalidad.
- Las cuentas de usuario que tengan privilegios concedidos a nivel de sistema a través de la pertenencia a grupos o programas como SUDO deben tener una contraseña única y diferente de todas las demás cuentas de dicho usuario con los privilegios de acceso a nivel de sistema.
- Cuando se utilice SNMP (Simple Network Management Protocol), el nombre de la comunidad debe definirse como algo diferente de los valores default estándar tales como "public", "private" y "system" así como deben ser diferentes de las contraseñas utilizadas para conectarse de forma interactiva. Los nombres de comunidades SNMP deben de cumplir con las especificaciones de construcción contraseñas.
- Todas las contraseñas de nivel de sistema (por ejemplo, usuario root, admin, administrador, cuentas de administrador de aplicaciones, etc.) debe de ser cambiadas al menos cada trimestre.

- Todas las contraseñas de nivel de usuario (por ejemplo: de Correo Electrónico, Navegación Web, Computadoras de Escritorio, etc.) deben cambiarse al menos cada seis meses. El intervalo de cambio recomendado es cada cuatro meses.
- El Equipo de la SGTI pueden realizar crackeos o tratar de adivinar contraseñas de forma periódica o aleatoria. Si una contraseña es adivinada o Crackeada durante una de estas exploraciones, se le solicitará al usuario que la cambie para estar en conformidad con los lineamientos de construcción de contraseñas.

12. Historial de Revisiones

Fecha de Cambio	Responsable	Resumen de cambios
Febrero 2021	Sub Gerente de Tecnologías de la Información	Creación

ANEXO: Acrónimos y glosario de términos

TIC

Tecnologías de la Información y las Comunicaciones. Dispositivos que permiten trabajar el ciclo de vida completo de la información, es decir, crear, almacenar, tratar, enviar o borrar información.

UVMPCH

Usuario Virtual de la Municipalidad Provincial de Chachapoyas.

VPN

Virtual Private Network (Red Privada Virtual) es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que los ordenadores que usan esta tecnología envíen y reciban datos sobre redes públicas con toda la funcionalidad, seguridad y políticas de gestión de una red privada.