CHILQUINTA energía	**GRUPO DE EMPRESAS CHILQUINTA** **GERENCIA DE TECNOLOGÍA**		
Identificación: CS GT SGTI ET 05	**Fecha Creación:** 20/10/2011	**Fecha Revisión/Modificación:** 07-08-2025	**Versión:** 1
ESPECIFICACIÓN TÉCNICA **ADMINISTRACIÓN DE CONTRASEÑAS** **PASSWORD MANAGEMENT**			

Revisado por: ALFREDO MARTINEZ Fecha: 07-08-2025	Aprobado por: FANGJIAN SHANG Fecha: 07-08-2025

1. OBJETIVO

El propósito del documento es establecer los parámetros globales de seguridad de contraseñas en la plataforma tecnológica del grupo de empresas Chilquinta.

2. ALCANCE

La información contenida en este documento debe ser aplicada en la gestión de las contraseñas de todos los sistemas que administra la Subgerencia de Telecomunicaciones y Tecnologías de Información

3. DEFINICIONES Y ABREVIACIONES

No Aplica.

4. RESPONSABILIDAD Y AUTORIDAD

CARGO	DESCRIPCIÓN (Ejecución de labores/Revisiones y/o aprobaciones)
Ingeniero de Sistemas	Responsables de ejecutar lo contenido en este documento.

5. DIAGRAMA DE FLUJO

No Aplica.

6. CONTENIDO

6.1. Forzar la generación de un historial de las contraseñas

Política de Configuración

Default Domain Controller Security Settings\Security Settings\Account Policies\Password Policy\Enforce History

Descripción

Determina el número de las nuevas contraseñas únicas que tienen que ser asociadas a una cuenta del usuario antes de que una vieja contraseña pueda ser reutilizada. El valor debe estar entre 0 y 24 contraseñas.

Por defecto, este ajuste es definido en el objeto de la política del grupo del dominio del defecto (GPO) y en la política local de la seguridad de sitios de trabajo y de servidores con un valor de 1.

Esta política permite a los administradores aplicar seguridad asegurándose de que las viejas contraseñas no están reutilizadas continuamente. Para el grupo empresas Chilquinta está configurada con un valor de 10.

6.2. Edad máxima de la contraseña

Política de Configuración

Default Domain Controller Security Settings\Security Settings\Account Policies\Password Policy\Maximum Password Age

Descripción

Determina el período de tiempo (en días) que una contraseña puede ser utilizada antes de que el sistema requiera al usuario cambiarla. Es posible fijar contraseñas para expirar después de un número de días entre 1 y 999, o especificar que las contraseñas nunca expiran fijando el número de días a 0.

Por defecto, este ajuste es definido en el objeto de la política del grupo del dominio del defecto (GPO) y en la política local de la seguridad de sitios de trabajo y de servidores con un valor de 42. Para el grupo empresas Chilquinta está configurada con un valor de 90.

Para las cuentas de administración y servicio la parametrización es el valor 0, es decir, no aplica.

6.3. Edad mínima de la contraseña

Política de Configuración

Default Domain Controller Security Settings\Security Settings\Account Policies\Password Policy\Minimum Password Age

Descripción

Determina el período de tiempo (en días) que una contraseña debe ser utilizada antes de que el usuario pueda cambiarla. Es posible fijar valores entre 1 y 999 días, o permitir cambios inmediatamente fijando el número de días a 0.

Por defecto, este ajuste es definido en el dominio GPO y en la política local de la seguridad de sitios de trabajo y de servidores con un valor de 0, que permite que las contraseñas sean cambiadas inmediatamente. Para el grupo empresas Chilquinta está configurada con un valor de 1.

6.4. Longitud mínima de la contraseña

Política de Configuración

Default Domain Controller Security Settings\Security Settings\Account Policies\Password Policy\Minimum Password Length

Descripción

Determina el número mínimo de caracteres que la contraseña de una cuenta del usuario puede contener. Es posible fijar valores entre 1 y 14 caracteres, o establecer que no se requiere ninguna contraseña fijando el número de caracteres a 0.

Por defecto, este ajuste es definido en el objeto de la política del grupo del dominio del defecto (GPO) y en la política local de la seguridad de sitios de trabajo y de servidores con un valor de 0.

Para el grupo empresas Chilquinta está configurada con un valor de 8.

6.5. Complejidad de la Contraseña

Política de Configuración

Default Domain Controller Security Settings\Security Settings\Account Policies\Password Policy\Password Must Meet Complexity Requirements Descripción

Descripción

Esta configuración de seguridad determina si las contraseñas deben cumplir los requerimientos de complejidad. Requisitos de complejidad se aplican cuando las contraseñas se cambian o crean.

Las contraseñas no deben contener todo o parte del Nombre de cuenta.

6.5.1. Contraseña de Usuario

Es una combinación de letras mayúsculas, minúsculas, números y caracteres, no contiene una palabra exacta del diccionario, no contiene el nombre de usuario, el nombre real o el nombre de la empresa y es significativamente diferente de otras contraseñas anteriores.

Según lo definido en las políticas de seguridad, los usuarios del grupo Empresas Chilquinta Energía S.A., cada 3 meses deben cambiar sus contraseñas sistemas y/o Aplicaciones de acuerdo a las siguientes buenas prácticas.

1. Largo Mínimo 8 caracteres.
2. La contraseña debe contener 3 de las 4 siguientes categorías
    - Letras mayúsculas
    - Letras minúsculas
    - Números
    - 4. Caracteres alfanuméricos: Ejemplos (? ~. @ # $% ^ & * + _- = `| \ () {} [] :;" '<>, /)
3. La complejidad es obligatoria
4. No utilizar caracteres consecutivos (12345678, ABCDEFGH).
5. Usar palabras distintas a las relacionadas con su trabajo.
6. No utilizar nombres o apellidos suyos o de familiares.
7. Usar códigos que no estén asociados a fechas de cumpleaños, direcciones, teléfonos, fichas orgánicas, Rut.
8. Cuidar la privacidad de su clave y evite compartirlas con terceros.
9. Contraseña debe ser distinta a las ultimas 10 contraseñas utilizadas.
10. Evitar llevar su clave en anotaciones, es mejor memorizarla.
11. El sistema exigirá cambio de clave cada 90 días.

Estas recomendaciones, están orientadas a mantener los niveles de seguridad de los sistemas computacionales y de la información contenida en ellos.

- Las responsabilidades de la seguridad de estas contraseñas son de cada usuario, lo que significa que son personales e intransferibles.

- En caso de olvido o bloqueo de una de estas contraseñas, se debe llamar a la mesa de ayuda, la cual gestionará la solución con el administrador de plataforma o sistema correspondiente. Para el caso de cuentas de SAP y OSF, es posible utilizar el sistema Web de autoatención de cambio de clave, ver el “Instructivo portal de Cambio de Contraseña de SAP u OSF”.

- En periodo de vacaciones o ausencia laboral es responsabilidad del usuario dejar informado mediante respuesta automática (fuera de la oficina) en su cuenta de correo quien lo reemplazará en sus funciones o a quien se deberá contactar.

- Lista de palabras no permitidas en ninguna parte de la contraseña
    - acceso
    - casablanca
    - chilquinta
    - clave
    - linares
    - litoral

- parral
- password
- prueba
- tecnored
- test
- abc123
- password

- Ejemplos de contraseñas correctas:
  - Elinvierno.Esfrio
  - 3Nv32rN4 (esto significa invierno reemplazando las vocales por números del 1 al 5)
  - 1Nv23rn4 (Esto significa invierno reemplazando las vocales por números)

6.5.2. Contraseña de Administrador

Según lo definido en las políticas de seguridad, los usuarios Administradores, cada 3 meses deberán cambiar sus contraseñas de acuerdo a las siguientes buenas prácticas.

- Largo Mínimo 10 caracteres.
- La contraseña debe contener 3 de las 4 siguientes categorías
  - Letras mayúsculas
  - Letras minúsculas
  - Números
  - 8. Caracteres alfanuméricos: Ejemplos (? ~. @ # $% ^ & * + _- = `| \ () {} [] :;" '<>, /)
- La complejidad es obligatoria
- No utilizar caracteres consecutivos (12345678, ABCDEFGH).
- Usar palabras distintas a las relacionadas con su trabajo.
- No utilizar nombres o apellidos suyos o de familiares.
- Usar códigos que no estén asociados a fechas de cumpleaños, direcciones, teléfonos, fichas orgánicas, Rut.
- Cuidar la privacidad de su clave y evite compartirlas con terceros.
- Contraseña deberá ser distinta a las ultimas 10 contraseñas utilizadas
- Doble autenticación
- Se exigirá cambio de clave cada 90 días.
- Las responsabilidades de la seguridad de estas contraseñas son de cada usuario administrador, lo que significa que son personales e intransferibles.
- Lista de palabras no permitidas en ninguna parte de la contraseña
  - acceso
  - casablanca
  - chilquinta
  - clave
  - linares
  - litoral
  - parral
  - password
  - prueba
  - tecnored

- test
- abc123
- password

6.5.3. Contraseña de Servicios

Las cuentas de servicio son utilizadas por aplicaciones, procesos automatizados o integraciones entre sistemas, y no son accedidas de forma interactiva por usuarios humanos. Se deben establecer sus contraseñas de acuerdo con las siguientes buenas prácticas.

- Largo Mínimo 10 caracteres.
- La contraseña debe contener 3 de las 4 siguientes categorías
    - Letras mayúsculas
    - Letras minúsculas
    - Números
    - 8. Caracteres alfanuméricos: Ejemplos (? ~. @ # $% ^ & * + _- = `| \ () {} [] :;" '<>, /)
- La complejidad es obligatoria
- No utilizar caracteres consecutivos (12345678, ABCDEFGH).
- Usar palabras distintas a las relacionadas con su trabajo.
- No utilizar nombres o apellidos o de familiares del ingeniero encargado de la creación.
- Usar códigos que no estén asociados a fechas de cumpleaños, direcciones, teléfonos, fichas orgánicas, Rut.
- Cuidar la privacidad de la clave y evitar compartirlas con terceros.
- Contraseña deberá ser distinta a las ultimas 10 contraseñas utilizadas
- Evitar llevar la clave en anotaciones, es mejor memorizarla.
- Lista de palabras no permitidas en ninguna parte de la contraseña
    - acceso
    - casablanca
    - chilquinta
    - clave
    - linares
    - litoral
    - parral
    - password
    - prueba
    - tecnored
    - test
    - abc123
    - password

6.6. Bloqueo de la contraseña

Política de Configuración

Default Domain Controller Security Settings\Security Settings\Account Policies\Account Lockout Policy\ Account Lockout threshold

Descripción

Define el número de intentos fallidos para bloqueo de cuentas de usuario. Para el grupo de empresas Chilquinta está definida con 6 intentos.

Para las cuentas de administración y servicio la parametrización es el valor 0, es decir, no aplica.

El medio de desbloqueo de las cuentas de sistemas es a través de los administradores del área de Sistemas e Infraestructura, para lo cual el usuario debe llamar a la mesa de ayuda, generar ticket vía Service Desk o mediante el sistema de AutoServicio para el caso de SAP.

6.7. Duración del bloqueo de la contraseña

Política de Configuración

Default Domain Controller Security Settings\Security Settings\Account Policies\Account Lockout Policy\ Account Lockout Duration

Descripción

Define el tiempo de bloqueo de la cuenta de usuario. Por defecto son 30 minutos es decir luego de 30 minutos la cuenta se desbloquea sola. Si se desea que nunca se desbloquee y que se desbloquee de forma manual por un administrador se debe escribir 0. Para el grupo empresas Chilquinta está definida en 45 minutos. Esta política aplica solo a cuentas de red.

6.8. Reiniciar conteo de intentos fallidos

Política de Configuración

Default Domain Controller Security Settings\Security Settings\Account Policies\Account Lockout Policy\ reset account lockout counter after

Descripción

Define el tiempo en el que el valor Badpwdcount es reseteado, por defecto es 30 minutos, es decir en 30 minutos el valor no debe exceder el valor definido en el Account Lockout Threshold, de lo contrario la cuenta se bloquea. Para el grupo empresas Chilquinta está definida en 10 minutos.

Para las cuentas de administración y servicio la parametrización es el valor 0, es decir, no aplica.

6.9. Cambio de Contraseñas de Administrador

Se realiza el cambio de contraseñas de manera procedimental cada 90 días para las siguientes plataformas:

- Infraestructura
  - DBA
    - Sybase
    - MSSqlserver
    - Oracle
    - MySql
    - Postgress
    - Sap IQ
    - SAP
  - Ingeniería
    - Servidores Red DMZ
    - Servidores Red SCADA
    - Servidores Red Corporativa
    - Servidores Dominio
    - Plataforma Storage
    - Plataforma F5
    - Plataforma VMware
    - Plataforma Huawei
    - Relay
  - TTI
    - ServiceDesk
    - Plataforma MDM
- Telecomunicaciones IT
  - Switch CORE Miraflores - Cisco Catalyst 9600
  - Switch CORE Curauma - Cisco Catalyst 9400
  - Switch CORE Aldunate - Cisco Catalyst 9400
  - Plataforma NAC
- Telecomunicaciones OT
  - Firewalls Scada
- Ciberseguridad
  - CORTEX
  - SIEM
  - Nessus

Las contraseñas deberán quedar disponibles en la bóveda de contraseñas corporativas, la cual cuenta deberá contar con MFA y cifrado. La bóveda debe permitir el acceso a estas contraseñas al Jefe de Sistemas e Infraestructura y el Arquitecto de Infraestructura.

6.10. Excepciones

- Para las cuentas que sea requerido cambio en alguna de las parametrizaciones distinta a lo especificado en este documento, debe enviarse la solicitud con el detalle del motivo de la necesidad al jefe de Infra y/o al Subgerente de TyTI para su autorización.
- El cambio de contraseñas, expiración, complejidad, re-intententos y bloqueos se implementan de forma procedimental a las cuentas de administración y servicios. No se establecen política/parámetros para su cumplimiento. Lo anterior con el propósito de evitar fallos en servicios críticos.

6.11. Comentarios y/o Consultas

CONTACTO
1. Mesa de ayuda
2. Ingeniero de Sistema
3. Jefe de Sistemas e Infraestructura

7. NORMATIVA VIGENTE

No Aplica.

8. REFERENCIAS

No Aplica.

9. ASUNTOS ÉTICOS

Consultas o inquietudes relacionadas con temas éticos pueden ser realizadas al oficial de cumplimiento (Gerente Legal) al fono: 322452429.

10. HISTORIAL DE REVISIONES Y MODIFICACIONES

Nº Versión	Fecha Vigencia	Comentario	Elaborado por	Revisado por	Aprobado por
0	20-10-2011	Creación documento			
0	02-08-2024	Adecuación procedimiento control documental corporativo	Alfredo Martinez	Alfredo Martinez	Fangjian Shang
1	07-08-2025	Excepciones cuentas de administración y servicios.	Jesús Ayala	Alfredo Martinez	Fangjian Shang

11. ANEXOS Y REGISTROS

Registros: Los registros digitales se almacenarán según se indique en la planilla de gestión de configuración del área de Sistemas e Infraestructura.

CHILQUINTA energía	CHILQUINTA GROUP OF COMPANIES		
Identification: CS GT SGTI ET 05	**Creation date:** 20-10-2011	**Review/Modification date:** 07-08-2025	**Version:** 1
TECHNICAL SPECIFICATION **PASSWORD MANAGEMENT** **ADMINISTRACIÓN DE CONTRASEÑAS**			

Reviewed by: ALFREDO MARTINEZ Date:07-08-2025	Approved by: FANGJIAN SHANG Date: 07-08-2024

1. OBJECTIVE

The purpose of the document is to establish the global password security parameters in the technological platform of the Chilquinta group of companies.

2. SCOPE

The information contained in this document must be applied in the management of passwords of all the systems managed by the Sub-Management of Telecommunications and Information Technologies.

3. DEFINITIONS AND ABBREVIATIONS

Does not apply.

4. RESPONSIBILITY AND AUTHORITY

POST	DESCRIPTION (Execution of tasks/Reviews and/or approvals)
Systems Engineer	Responsible for executing what is contained in this document.

5. FLOWCHART

Does not apply.

6. CONTENT

6.1. Force generation of a password history

Configuration Policy

Default Domain Controller Security Settings\Security Settings\Account Policies\Password Policy\Enforce History

Description

Determines the number of new unique passwords that have to be associated with a user's account before an old password can be reused. The value must be between 0 and 24 passwords.

By default, this setting is defined in the default domain group policy object (GPO) and in the local workstation and server security policy with a value of 1.

This policy allows administrators to enhance security by ensuring that old passwords are not continually reused. For the Chilquinta group of companies it is configured with a value of 10.

6.2. Maximum password age

Configuration Policy

Default Domain Controller Security Settings\Security Settings\Account Policies\Password Policy\Maximum Password Age

Description

Determines the period of time (in days) that a password can be used before the system requires the user to change it. It is possible to set passwords to expire after a number of days between 1 and 999, or specify that passwords never expire by setting the number of days to 0.

By default, this setting is defined in the default domain group policy object (GPO) and in the local workplace and server security policy with a value of 42. For the Chilquinta group of companies it is configured with a value of 90.

For administration and service accounts, the parameterization is set to 0, meaning it does not apply.

6.3. Minimum password age

Configuration Policy

Default Domain Controller Security Settings\Security Settings\Account Policies\Password Policy\Minimum Password Age

Description

Determines the period of time (in days) that a password must be used before the user can change it. It is possible to set values between 1 and 999 days, or allow changes immediately by setting the number of days to 0.

By default, this setting is defined in the domain GPO and in the local workstation and server security policy with a value of 0, which allows passwords to be changed immediately. For the Chilquinta group of companies it is configured with a value of 1.

6.4. Minimum password length

Configuration Policy

Default Domain Controller Security Settings\Security Settings\Account Policies\Password Policy\Minimum Password Length

Description

Determines the minimum number of characters that a user's account password can contain. It is possible to set values between 1 and 14 characters, or set that no password is required by setting the number of characters to 0.

By default, this setting is defined in the default domain Group Policy Object (GPO) and in the local security policy of workstations and servers with a value of 0.

For the Chilquinta group of companies it is configured with a value of 8.

6.5. Password Complexity

Configuration Policy

Default Domain Controller Security Settings\Security Settings\Account Policies\Password Policy\Password Must Meet Complexity Requirements Description

Description

This security setting determines whether passwords must meet complexity requirements. Complexity requirements apply when passwords are changed or created.

Passwords must not contain all or part of the Account Name.

6.5.1. User Password

It is a combination of uppercase and lowercase letters, numbers, and characters, does not contain an exact dictionary word, does not contain the username, real name, or company name, and is significantly different from previous passwords.

As defined in the security policies, users of the Empresas Chilquinta Energía SA group must change their system and/or Application passwords every 3 months in accordance with the following good practices.

1. Minimum length 8 characters.
2. Password must contain 3 of the following 4 categories

    - Capital letters
    - Lowercase letters
    - Numbers
    - 4. Alphanumeric characters: Examples (? ~. @ # $% ^ & * + _- = `| \ () {} [] :;" '<>, /)
3. Complexity is mandatory
4. Do not use consecutive characters (12345678, ABCDEFGH).
5. Use words other than those related to your work.
6. Do not use your or family names or surnames.
7. Use codes that are not associated with birthday dates, addresses, telephone numbers, organic records, Rut.
8. Take care of the privacy of your password and avoid sharing it with third parties.
9. Password must be different from the last 10 passwords used.
10. Avoid carrying your password in notes, it is better to memorize it.
11. The system will require a password change every 90 days.

These recommendations are aimed at maintaining the security levels of computer systems and the information contained in them.

- The responsibilities for the security of these passwords rest with each user, which means that they are personal and non-transferable.

- If you forget or lock one of these passwords, you should call the help desk, which will manage the solution with the corresponding platform or system administrator. For SAP and OSF accounts, you can use the self-service web system for password change, see the “SAP or OSF Password Change Portal Instructions”.

- During vacation periods or absence from work, it is the user's responsibility to inform by automatic response (out of the office) in their email account who will replace them in their duties or who should be contacted.

- List of words not allowed anywhere in the password
    - casablanca
    - chilquinta
    - linares
    - Luzlinares
    - Parral
    - Luzparral
    - Litoral
    - Chilquintaservicios
    - Chilquintadistribucion
    - Chilquintaenergia
    - Enerquinta
    - Litoraltransmision
    - Luzparraltransmision
    - Transquinta
    - Eletrans
    - Eletrans1
    - Eletrans2
    - Eletrans3
    - Gesan

        - ctng
        - tecnored
        - acceso
        - clave
        - password
        - prueba
        - test
        - abc123
        - password

- Examples of correct passwords:
    - Winter is cold
    - 3Nv32rN4 (this means winter by replacing the vowels with numbers 1 to 5)
    - 1Nv23rn4 (This means winter by replacing the vowels with numbers)

6.5.2. Administrator Password

As defined in the security policies, Administrator users must change their passwords every 3 months according to the following good practices.

- Minimum length 10 characters.
- Password must contain 3 of the following 4 categories
    - Capital letters
    - Lowercase letters
    - Numbers
    - 8. Alphanumeric Characters: Examples (? ~. @ # $% ^ & * + _- = `| \ () {} [] :;" '<>, /)
- Complexity is mandatory
- Do not use consecutive characters (12345678, ABCDEFGH).
- Use words other than those related to your work.
- Do not use your or family names or surnames.
- Use codes that are not associated with birthday dates, addresses, telephone numbers, organic records, Ruth.
- Take care of the privacy of your password and avoid sharing it with third parties.
- Password must be different from the last 10 passwords used
- Double authentication
-
- It is required password change every 90 days.
- The responsibilities for the security of these passwords rest with each administrator user, which means that they are personal and non-transferable.
- List of words not allowed anywhere in the password
    - access
    - admin
    - casablanca
    - chilquinta
    - clue
    - linares
    - litoral
    - parral

- password
- proof
- technored
- test
- abc123
- password

6.5.3. Services Password

Service accounts are used by applications, automated processes, or integrations between systems, and are not accessed interactively by human users. Their passwords must be set according to the following best practices:

- Minimum length of 10 characters.
- The password must contain 3 of the following 4 categories:
  - Uppercase letters
  - Lowercase letters
  - Numbers
  - Alphanumeric characters: Examples (? ~. @ # $% ^ & * + _- = `| \ () {} [] :;" '<>, /)
- Complexity is mandatory.
- Do not use consecutive characters (12345678, ABCDEFGH).
- Use words other than those related to your work.
- Do not use your or family names or surnames.
- Use codes that are not associated with birthdays, addresses, phone numbers, organic records, Rut.
- Protect the privacy of your password and avoid sharing it with third parties.
- The password must be different from the last 10 passwords used.
- Avoid writing down your password; it is better to memorize it.
- List of words not allowed in any part of the password:
  - acceso
  - casablanca
  - chilquinta
  - clave
  - linares
  - litoral
  - parral
  - password
  - prueba
  - tecnored
  - test
  - abc123
  - password

6.6. Password lock

Configuration Policy

Default Domain Controller Security Settings\Security Settings\Account Policies\Account Lockout Policy\ Account Lockout threshold

Description

Defines the number of failed attempts to lock user accounts. For the Chilquinta group of companies it is defined with 6 attempts.

For administration and service accounts, the setting is 0, meaning it does not apply.

System accounts can be unlocked through the Systems and Infrastructure administrators. To do this, the user must call the help desk, generate a ticket via the Service Desk, or use the Self-Service system in the case of SAP.

6.7. Password lock duration

Configuration Policy

Default Domain Controller Security Settings\Security Settings\Account Policies\Account Lockout Policy\ Account Lockout Duration

Description

Defines the user account lockout time. By default it is 30 minutes, that is, after 30 minutes the account unlocks itself. If you want it to never be unlocked and to be unlocked manually by an administrator, you must write 0. For the Chilquinta group of companies it is defined in 45 minutes This policy apply only to a network accounts..

6.8. Reset failed attempt count

Configuration Policy

Default Domain Controller Security Settings\Security Settings\Account Policies\Account Lockout Policy\ reset account lockout counter after

Description

Defines the time in which the Badpwdcount value is reset, by default it is 30 minutes, that is, in 30 minutes the value must not exceed the value defined in the Account Lockout Threshold , otherwise the account is locked. For the Chilquinta group of companies it is defined as 10 minutes.

For administration and service accounts, the setting is 0, meaning it does not apply.

6.9. Administrator Password Change

Passwords are changed procedurally every 90 days for the following platforms:

- Infraestructura
  - DBA
    - Sybase
    - MSSqlserver
    - Oracle
    - MySql
    - Postgress
    - Sap IQ
    - SAP
  - Ingeniería
    - Servidores Red DMZ
    - Servidores Red SCADA
    - Servidores Red Corporativa
    - Servidores Dominio
    - Plataforma Storage
    - Plataforma F5
    - Plataforma VMware
    - Plataforma Huawei
    - Relay
  - TTI
    - ServiceDesk
    - Plataforma MDM
- Telecomunicaciones IT
  - Switch CORE Miraflores - Cisco Catalyst 9600
  - Switch CORE Curauma - Cisco Catalyst 9400
  - Switch CORE Aldunate - Cisco Catalyst 9400
  - Plataforma NAC
- Telecomunicaciones OT
  - Firewalls Scada
- Ciberseguridad
  - CORTEX
  - SIEM
  - Nessus

Passwords must be stored in the corporate password vault, which must have MFA and encryption. The vault must allow access to these passwords to the Head of Systems and Infrastructure and the Infrastructure Architect

6.10. Exceptions

- For accounts requiring a change in any parameter different from what is specified in this document, a request detailing the reason for the need must be submitted to the Head of Infrastructure and/or the Deputy Manager of Technology and Information for authorization.
- The change of passwords, expiration, complexity, retries, and locks are implemented procedurally for administration and service accounts. Policies/parameters are not established for their compliance. This is done to avoid failures in critical services.

6.11. Comments and/or Queries

CONTACT
1. Help Desk
2. System Engineer
3. Head of Systems and Infrastructure

7. REGULATIONS IN FORCE

Does not apply.

8. REFERENCES

Does not apply.

9. ETHICAL ISSUES

Queries or concerns related to ethical issues can be made to the compliance officer (Legal Manager) at phone number: 322452429.

10. HISTORY OF MODIFICATIONS AND CHANGES

Version No.	Effective date	Comment	Produced by	reviewed by	Approved by
0	20-10-2011	Document creation			
1	02-08-2024	Adaptation of corporate documentary control procedure	Alfredo Martinez	Alfredo Martinez	Fangjian Shang

2	07-08-2025	Exceptions for administration and services accounts.	Jesús Ayala	Alfredo Martinez	Fangjian Shang

11. ANNEXES AND RECORDS

Records: The digital records will be stored as indicated in the configuration management form of the Systems and Infrastructure area.