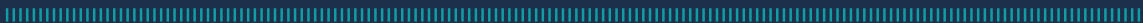


PROTOCOLO ■■■
PROVINCIAL DE CIBERSEGURIDAD

Estándar de Gestión de Cuentas / Control de Acceso

02
CAPÍTULO



Estándar de Gestión de Cuentas / Control de acceso

1.0 Propósito y Beneficios

El propósito de esta norma es establecer las reglas y procesos para crear, mantener y controlar el acceso de una identidad digital (cuenta) a las aplicaciones y recursos de una organización, como medio para proteger sus sistemas de información.

2.0 Alcance

Este estándar cubre todos los sistemas desarrollados por o en nombre de la entidad que requieren acceso autenticado. Esto incluye todos los sistemas de desarrollo, pruebas, control de calidad, producción y otros sistemas ad hoc.

3.0 Declaración de información

La gestión de cuentas y el control de acceso incluyen el proceso de solicitar, crear, emitir, modificar y deshabilitar cuentas de usuario; habilitar y deshabilitar el acceso a recursos y aplicaciones; establecer condiciones para la pertenencia a grupos y roles; seguimiento de cuentas y sus respectivas autorizaciones de acceso; y gestionar estas funciones.

3.1 FUNCIONES DE GESTIÓN DE CUENTAS/CONTROL DE ACCESO

La gestión de cuentas y el control de acceso requieren que los roles de propietario de la información, administrador general de cuentas y, opcionalmente, administradores de cuentas, estén definidos y asignados para cada recurso y aplicación. Se debe documentar y mantener una lista de usuarios autorizados en estos roles. Las tareas y responsabilidades asociadas a cada función se describen a continuación. Cada rol puede pertenecer a una o más personas según la aplicación. En algunos casos, a un solo individuo o grupo se le puede asignar más de uno de estos roles.

- a. **Propietario de la información:** Son personas en el nivel gerencial dentro de una entidad, que:

1. Delegan funciones operativas a los administradores generales de cuentas, para garantizar que se proporcione el nivel adecuado de acceso a la información. La delegación puede realizarse a usuarios individuales, grupos y/o terceros (por ejemplo, otra entidad).
 2. Definen roles y grupos, así como el nivel correspondiente de acceso a los recursos para ese rol o grupo.
 3. Determinan quién debería tener acceso.
 4. Determinan el nivel de garantía de las identidades para el acceso a aplicación y/o los datos. (ver estándar de autenticación tokens)
 5. Revisan que las cuentas y los controles de acceso sean proporcionales a la función operativa general y que los permisos asociados se hayan asignado adecuadamente, como mínimo, anualmente.
 6. Exigen a las unidades organizativas o reparticiones, con acceso a recursos protegidos, que notifiquen a los administradores de cuentas cuando las cuentas ya no sean necesarias, como cuando los usuarios son dados de baja o transferidos y cuando cambian los requisitos de acceso individual.
- b. Administrador general de cuentas:** Gestiona las cuentas. Es el custodio delegado de los datos protegidos. El administrador general de cuentas:
1. Mantiene niveles apropiados de comunicación con los propietarios de la información, para determinar el nivel o grado de acceso otorgado a un individuo.
 2. Determina las especificaciones técnicas necesarias para establecer privilegios de acceso.
 3. Delega funciones de gestión de cuentas a administradores de cuentas.
 4. Crea y mantiene los procedimientos utilizados en la gestión de cuentas.
 5. Realiza todas las tareas de administradores de cuentas según sea necesario.
- c. Administradores de cuentas:** Son un subconjunto opcional de la función de administrador general de cuentas. No determinan procedimientos. El administrador general de cuentas les asigna los derechos y/o responsabilidades del sistema. Todas las responsabilidades de los administradores de cuentas están contenidas en la función de administrador general de cuentas, en caso de que no existan administradores

de cuentas. Se podrá asignar un subconjunto de funciones del administrador general de cuentas, según corresponda. Por ejemplo, es posible que exista una función para restablecer contraseñas únicamente para los empleados de la mesa de entrada. Además, algunas de estas responsabilidades pueden permanecer en el administrador general de cuentas, si éste determina que es necesario. Para la gestión de cuentas, el administrador podrá:

1. Mantener toda la información necesaria que respalde las actividades de administración de cuentas, incluidas las solicitudes y aprobaciones de administración de cuentas.
 2. Inscribir nuevos usuarios.
 3. Activar/desactivar cuentas de usuario.
 4. Crear y mantener roles y grupos de usuarios.
 5. Asignar derechos y privilegios a un usuario o grupo.
 6. Recopilar datos para revisar periódicamente las cuentas de usuario y sus derechos asociados.
 7. Asignar nuevos tokens de autenticación (por ejemplo, restablecimiento de contraseñas).
- d. Administrador de permisos:** Son un subconjunto opcional de la función de administrador de cuentas. Los permisos y/o responsabilidades les son definidos por el titular de la información (o sus delegados) y generalmente incluyen:
1. Asignar derechos y privilegios a un usuario, grupo o rol.
 2. Recopilar datos para revisar periódicamente las cuentas de usuario y sus permisos asociados.
 3. Mantener toda la información necesaria que respalde las actividades de administración de cuentas, incluidas las solicitudes y aprobaciones de administración de cuentas.

3.2 TIPOS DE CUENTAS

Los tipos de cuentas incluyen: individual, privilegiada, de servicio, compartida, invitada/anónima, de emergencia y temporal. Todos los tipos de cuentas deben cumplir con todas las reglas aplicables según lo definido en el Estándar de tokens de autenticación.

- a. Cuentas individuales:** una cuenta individual es una cuenta única, emitida para un solo usuario. La cuenta permite al usuario autenticarse en sistemas con una identidad digital. Después de autenticar a un usuario, se le autoriza o se le niega el acceso al sistema, según los permisos que se le asignan directa o indirectamente (permisos heredados).
- b. Cuentas privilegiadas:** una cuenta privilegiada es una cuenta que proporciona mayor acceso y requiere autorización adicional, por ejemplo, cuentas de administradores de red, de sistema o de seguridad. Solo se puede proporcionar una cuenta privilegiada a agentes y funcionarios que la requieran para cumplir con sus débitos laborales. El uso de cuentas privilegiadas debe cumplir con el principio de privilegio mínimo. El acceso se restringirá únicamente a aquellos programas o procesos específicamente necesarios para realizar tareas operativas autorizadas y nada más. Hay dos tipos de cuentas privilegiadas: cuentas administrativas y cuentas privilegiadas predeterminadas.
- 1. Cuentas administrativas:** Cuentas concedidas a un usuario que le otorgan el derecho de modificar la configuración del sistema operativo o de la plataforma, o aquellas que permiten modificaciones de otras cuentas. Estas cuentas deben:
 - i. Estar en un nivel de garantía de identidad acorde con los recursos protegidos a los que acceden.
 - ii. No poseer un ID de usuario que proporcione indicios acerca del nivel de privilegio del mismo, por ejemplo, supervisor, gerente, administrador o cualquier tipo aplicable.
 - iii. Ser identificables internamente como cuentas administrativas según una convención de nomenclatura estandarizada.
 - iv. Ser revocadas de acuerdo con los requisitos organizacionales.
 - 2. Cuentas privilegiadas predeterminadas:** las cuentas privilegiadas predeterminadas (por ejemplo, administrador o root) se proporcionan con un sistema en particular y no se pueden eliminar sin afectar la funcionalidad del sistema. Las cuentas privilegiadas predeterminadas deben:
 - i. Deshabilitarse si no está en uso o cambiarse de nombre si es técnicamente posible.
 - ii. Utilizarse únicamente para la instalación inicial del sistema o para realizar tareas de mantenimiento. Cuando sea técnicamente posible, deben emitirse alertas al personal apropiado, cuando éstas sean utilizadas para iniciar sesión.

- iii. Poseer una contraseña que no sea la predeterminada o inicialmente asignada por el sistema.
 - iv. Poseer una contraseña conocida o accesible por al menos dos personas dentro de la organización.
- c. Cuentas de servicio:** una cuenta de servicio no está destinada a ser otorgada a un usuario, sino que se proporciona para la ejecución de un proceso, usualmente automatizado. Debe usarse en situaciones tales como permitir que un sistema ejecute trabajos y servicios independientemente de la interacción del usuario. Las cuentas de servicio deben:
1. Tener un propietario asignado, responsable de documentar y administrar la cuenta.
 2. Restringirse a dispositivos y horarios específicos cuando sea posible.
 3. Ser gestionadas, de forma tal, que su utilización no se realice de manera interactiva por un usuario, para ningún propósito que no sea la instalación inicial del sistema o, si es absolutamente necesario, para la resolución de problemas o mantenimiento del sistema. Siempre que sea técnicamente posible, los administradores deben aprovechar mecanismos de “cambio de usuario” o “ejecutar como” para lanzar procesos mediante cuentas de servicio.
 4. Utilizarse únicamente para propósitos circunscriptos a su alcance inicial.
 5. Ser identificables internamente, cuando sea posible, como cuentas de servicio según una convención de nomenclatura estandarizada.
 6. Estar exentas de cronogramas estandarizados y/o forzados de rotación de credenciales. Sin embargo, si un integrante de la organización, con conocimiento de dicha contraseña, abandonara la entidad, dichas credenciales deberán ser cambiadas inmediatamente.
 7. Poseer una contraseña conocida o accesible por al menos dos personas dentro de la organización.
- d. Cuentas compartidas:** una cuenta compartida es cualquier cuenta en la que más de una persona conoce la contraseña y/o utiliza el mismo token de autenticación. El uso de cuentas compartidas solo se permite cuando existe una limitación del sistema o de la operación que impide el uso de cuentas individuales. Estos casos deben ser documentados por el propietario de la información y revisados por el responsable de

seguridad designado. Se deben implementar controles compensatorios adicionales para confirmar que se mantiene la rendición de cuentas. Las cuentas compartidas deben:

1. Restablecer los tokens (por ejemplo, la contraseña) cuando alguno de sus usuarios ya no necesite acceso, o de otro modo de acuerdo con el Estándar de Tokens de Autenticación.
2. Restringirse a dispositivos y horarios específicos, cuando sea posible.
3. Siempre que sea técnicamente posible, hacer que sus usuarios inicien sesión en el sistema con sus cuentas individuales y “cambien de usuario” (SU) o “ejecuten como” la cuenta compartida.
4. Contar con permisos estrictamente limitados y acceso solo a los sistemas requeridos.

e. Cuentas predeterminadas sin privilegios: la cuenta predeterminada sin privilegios (invitado o usuario anónimo) es una cuenta para personas que no tienen cuentas individuales. Un ejemplo de dónde esto podría ser necesario es en una red Wi-Fi pública. Este tipo de cuentas deben:

1. Desactivarse hasta que sea necesario.
2. Poseer restricciones y permisos limitados.
3. Permitirse únicamente luego de una evaluación de riesgos.
4. Tener controles compensatorios que incluyan acceso restringido a la red.
5. Tener asignada una contraseña que el usuario no pueda cambiar, pero que se actualice por un administrador, como mínimo, mensualmente.
6. Prohibir sean delegadas a otra cuenta.
7. Mantener un registro de usuarios a quienes se les proporciona la contraseña.

f. Cuentas de emergencia: Las cuentas de emergencia están destinadas a un uso de corto plazo e incluyen restricciones de creación, punto de origen y uso (por ejemplo, hora del día, día de la semana). El Oficial de Seguridad de la Información (ISO)/representante de seguridad designado, puede establecer cuentas de emergencia en respuesta a situaciones de crisis. Por lo tanto, la activación de emergencia de las

cuentas, pueden eludir los procesos normales de autorización de las mismas. Las cuentas de emergencia deben desactivarse automáticamente después de 24 horas.

- g. Cuentas temporales:** Las cuentas temporales están destinadas a un uso de corto plazo e incluyen restricciones de creación, punto de origen, uso (por ejemplo, hora del día, día de la semana) y deben tener fechas pautadas de inicio y finalización para su desactivación. Una Unidad de Organización puede establecer cuentas temporales como parte de los procedimientos normales de activación de cuentas, cuando existe la necesidad de cuentas de corto plazo y no existe la exigencia de inmediatez en la activación de la misma. Estas cuentas deben tener permisos y accesos estrictamente limitados a los sistemas requeridos.

3.3 FUNCIONES DE GESTIÓN DE CUENTAS Y CONTROL DE ACCESO

En caso de ser posible, se deben emplear mecanismos automatizados para monitorear el uso y la gestión de las cuentas. Estos mecanismos deben permitir el monitoreo del uso y emitir notificaciones, en caso de uso atípico de las mismas. Los umbrales para las alertas deben establecerse según la importancia del sistema o el nivel de seguridad de la cuenta.

Se debe notificar al personal que desempeña las funciones apropiadas de administración de cuentas/control de acceso, cuando se realicen actividades de administración de cuentas, como, por ejemplo, cuando las cuentas ya no sean necesarias, los usuarios sean eliminados, dados de baja o transferidos. Estas actividades deberían automatizarse, siempre que sea técnicamente posible.

Dentro de los sistemas, deben existir políticas de control de acceso automatizadas, siempre que sea posible, que hagan cumplir las autorizaciones aprobadas para la información y los recursos del sistema. Estas políticas de control de acceso podrán basarse en identidad, rol o atributos.

De forma predeterminada, nadie debe contar con acceso a los sistemas de información, a menos que esté autorizado.

El Nivel de Garantía de Identidad (NGI) de un sistema, determina el grado de certeza requerido al verificar la identidad de un usuario. La siguiente tabla describe el nivel de confianza asociado con cada NGI:

Nivel de garantía de identidad	Descripción
1	Confianza baja o nula en la validez de la identidad afirmada
2	Confianza en la validez de la identidad afirmada.
3	Alta confianza en la validez de la identidad afirmada.

La Tabla 1 refleja los estándares para la gestión de cuentas en cada nivel de aseguramiento.

Tabla 1: Estándares de gestión de cuentas por nivel de garantía de identidad

Categoría	Niveles de garantía de identidad		
	1	2	3
Cuenta desactivada automáticamente después de x días de inactividad	1096	90	90
Enviar notificación x días antes de que la cuenta se deshabilite	30	30	14
Cuenta bloqueada después de x número de intentos fallidos consecutivos de inicio de sesión	10	5	3
La creación de una cuenta requiere un atributo autorizado que vincule al usuario a su cuenta. Por ejemplo, podría ser una identificación de empleado, una identificación de licencia de conducir, una identificación fiscal o una dirección de correo electrónico individual única.	No	Sí	Sí

Categoría	Niveles de garantía de identidad		
	1	2	3
Se enviará una notificación por correo electrónico al usuario para los siguientes eventos: <ul style="list-style-type: none"> • Cambio de token (contraseña, token de conocimiento pre-registrado, información del token fuera de banda (OOB)) • Cuenta inhabilitada debido a intentos no válidos • Se ha emitido una identificación de usuario (UID) olvidada • Cambio de atributo de cuenta (por ejemplo, cambio de nombre) • Reactivación de cuenta 	Si se sabe	Sí	Sí
Funcionalidad de autoservicio permitida	Sí	Sí	No

Para todos los niveles de garantía, se debe cumplir lo siguiente.

- a. **Creación de cuentas nuevas:** para crear una cuenta, debe haber una autorización de acceso válida basada en una justificación operativa aprobada y debe realizarse una solicitud formal para crear la cuenta.
- b. **Modificación de los atributos de la cuenta (es decir, cambiar los nombres de los usuarios, datos demográficos, etc.):** Las modificaciones solo deben ser realizadas por el usuario autenticado o un administrador de cuentas autorizado.
- c. **Habilitación de acceso:** El acceso se otorga, según el principio de privilegio mínimo, con una autorización de acceso válida.
- d. **Modificación de acceso:** Las modificaciones de acceso deben incluir una autorización válida. Cuando haya un cambio de rol, función o cargo (sin incluir desvinculación), el acceso debe revisarse inmediatamente y se suspende/elimina cuando ya no es necesario.
- e. **Deshabilitar cuentas/eliminar acceso:**
 1. **Basado en eventos/riesgos (desactivación administrativa):** cuando una cuenta presenta o tiene el potencial de representar un riesgo significativo, la cuenta se deshabilita y/o los atributos de acceso se eliminan al descubrir el riesgo. Es esencial una estrecha coordinación entre los propietarios de la información, los administradores/responsables de cuentas, las partes interesadas legales, de respuesta a incidentes y los responsables de recursos humanos para

ejecutar oportunamente la eliminación o restricción del acceso de los usuarios. Los usuarios que representan un riesgo significativo para las organizaciones incluyen personas para quienes evidencia o inteligencia confiable indican la intención de utilizar el acceso autorizado a los sistemas de información para causar daño o a través de quienes los adversarios causarán daño. El daño incluye posibles impactos adversos a las operaciones y activos de la repartición, a los individuos y a otras organizaciones. Se requiere un identificador de cuenta para identificar estas cuentas y evitar una reactivación inapropiada de la cuenta/acceso. Volver a habilitar la cuenta requiere la aprobación explícita de la repartición. No se pueden utilizar mecanismos de autoservicio para volver a habilitar la cuenta.

2. Desactivación tras la desvinculación: todas las cuentas de usuario (incluidas las privilegiadas) deben desactivarse inmediatamente después de la desvinculación. Además, las credenciales deben revocarse de acuerdo con los requisitos de la repartición y se deben eliminar los atributos de acceso. No se podrán utilizar mecanismos de autogestión para volver a habilitar la cuenta o sus permisos.

3. Deshabilitación por inactividad: cuando una cuenta se deshabilita debido a inactividad, los atributos de acceso pueden permanecer sin cambios si el propietario de la información lo considera apropiado. La reactivación será a través de su respectiva vía administrativa.

f. Revisión de cuentas y acceso:

1. Los propietarios de la información deben revisar todas las cuentas anualmente (como mínimo) para determinar si todavía son necesarias.
2. El acceso a cuentas privilegiadas debe revisarse cada seis meses (como mínimo) para determinar si todavía son necesarias o no.
3. Los propietarios de la información deben revisar las autorizaciones de cuentas y/o las asignaciones de acceso de los usuarios anualmente (como mínimo) para determinar si aún se necesita todo el acceso.
4. Las cuentas o registros de la cuenta deben archivarlos después de 5 años de inactividad o después de que se cumplan propósitos de auditoría específicos.

g. Desbloqueo de cuentas de usuario: Para que un administrador o técnico de soporte informático desbloquee una cuenta para un usuario, el

usuario debe ser examinado mediante tokens de conocimiento pre-registrados según el Estándar de Autenticación Tokens.

- h. Procedimientos de inicio de sesión seguro:** cuando sea técnicamente posible, el acceso debe controlarse mediante procedimientos de inicio de sesión seguro de la siguiente manera:
 1. No debe mostrar los tokens (por ejemplo, contraseña, PIN) que se ingresan.
 2. Debe mostrar la siguiente información al completar un inicio de sesión exitoso:
 - i. Fecha y hora del inicio de sesión exitoso anterior; y
 - ii. Detalles de cualquier intento fallido de inicio de sesión desde el último inicio de sesión exitoso.
- i. Bloqueo de inactividad de sesión:** las sesiones deben bloquearse después de un período máximo de inactividad de 15 minutos. Los bloqueos de inactividad de sesión son acciones temporales que se toman cuando los usuarios dejan de trabajar y se alejan de su entorno inmediato, pero no quieren cerrar sesión debido a la naturaleza temporal de sus ausencias. Los usuarios deben volver a autenticarse para desbloquear la sesión.
- j. Tiempo de espera de sesión activas:** las sesiones deben finalizar automáticamente después de 18 horas o después de condiciones “predefinidas”, como respuestas específicas a ciertos tipos de incidentes.
- k. Registro/Auditoría/Monitoreo:** toda la actividad de la cuenta debe registrarse y auditarse de acuerdo con el Estándar de Registro de Seguridad. La capacidad de modificar o eliminar registros de auditoría debe evitarse tanto como sea posible y limitarse a un conjunto específico de cuentas privilegiadas. Cualquier modificación de los atributos de acceso debe registrarse y rastrearse hasta un solo individuo.

4.0 Cumplimiento

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y administrativas. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

5.0 Excepciones de Política

Las solicitudes de excepciones a esta política serán revisadas por el Director de Ciberseguridad (DC) y la Secretaría de Innovación Pública (SIP) o Encargado de Información. Los departamentos que soliciten excepciones deberán proporcionarle dichas solicitudes. La solicitud debe indicar específicamente el alcance de la excepción junto con la justificación para otorgar la excepción, el posible impacto o riesgo asociado al otorgar la excepción, las medidas de mitigación de riesgos que debe tomar el Departamento de TI, iniciativas, acciones y un cronograma para lograr el nivel mínimo de cumplimiento de las políticas aquí establecidas. El DC revisará dichas solicitudes y concederá al departamento solicitante dejando asentada la excepción.

6.0 Departamento Responsable

Oficina principal de información y propietarios de sistemas de información.

7.0 Historial de revisiones

Fecha	Descripción de Cambio	Revisado por
27-05-2024	Draft final del documento	Alejandro Castro Pablo Zalazar
29-05-2024	Cambios en puntos 5, 6 y 7, para unificar formato con anterior documento.	Alejandro Castro Pablo Zalazar

8.0 Documentos relacionados

- Estándar de tokens de autenticación
- Estándar de registro de seguridad
- Publicación especial del NIST 800-63-3 Pautas de identidad digital