N° de revisión	N°. de paginas	Fecha (dd/mm/año)	Descripción del Cambio/Modificación
0	7	01/09/2025	Creación del documento
1	20	25/11/2025	Actualización de contenidos y redacción del capítulo 6 Políticas. Incluyendo ajustes en sus numerales del 6.1 al 6.18.

USO INTERNO

ELABORADO POR	**REVISADO POR**	**APROBADO POR**
CARLOS ANDRES GARZON	MONICA MONTOYA ALVEREZ	DAVID FLOREZ
ANALISTA LIDER TI	**COORDINADORA SGI**	**ANALISTA INTELIGENCIA DE NEGOCIOS**

Este documento pertenece a CONHYDRA S.A. E.S.P, Aguas de La Prosperidad S.A.S. E.S.P y GESCOMER S.A.S, por lo cual, se prohíbe su reproducción total o parcial en cualquier medio, sin previa autorización escrita del Gerente.

Este documento impreso en cualquier medio se considera **"COPIA NO CONTROLADA"**

Contenido

1 Introducción 4
2 Objetivo 4
3 Alcance....5
4 Definiciones clave 5
5 Roles y responsabilidades....6
6 Políticas....7
6.1 Acceso responsable a la información 7
6.2 Clasificación de la Información....7
6.3 Riesgos 8
6.4 Gestión de incidentes o problemas de seguridad 8
6.5 Responsabilidad de seguridad de la información 9
6.6 Propiedad de los recursos 9
6.7 Uso aceptable de los recursos....10
6.8 Estaciones de trabajo y equipos móviles 11
6.9 Usuarios y contraseñas....12
6.10 Uso de internet....13
6.11 Transferencia de información 14
6.12 Respaldo de la información 15
6.13 Equipos desatendidos....16

USO INTERNO

ELABORADO POR	**REVISADO POR**	**APROBADO POR**
CARLOS ANDRES GARZON	MONICA MONTOYA ALVEREZ	DAVID FLOREZ
ANALISTA LIDER TI	**COORDINADORA SGI**	**ANALISTA INTELIGENCIA DE NEGOCIOS**

Este documento pertenece a CONHYDRA S.A. E.S.P, Aguas de La Prosperidad S.A.S. E.S.P y GESCOMER S.A.S, por lo cual, se prohíbe su reproducción total o parcial en cualquier medio, sin previa autorización escrita del Gerente.
Este documento impreso en cualquier medio se considera **"COPIA NO CONTROLADA"**

6.14 Omisión de procedimientos o evasión de controles de seguridad 17

6.15 Cumplimiento normativo 18

6.16 Monitoreo.....18

6.17 Cumplimiento y sanciones.....19

6.18 Excepciones 19

USO INTERNO

ELABORADO POR	**REVISADO POR**	**APROBADO POR**
CARLOS ANDRES GARZON	MONICA MONTOYA ALVEREZ	DAVID FLOREZ
ANALISTA LIDER TI	**COORDINADORA SGI**	**ANALISTA INTELIGENCIA DE NEGOCIOS**

Este documento pertenece a CONHYDRA S.A. E.S.P, Aguas de La Prosperidad S.A.S. E.S.P y GESCOMER S.A.S, por lo cual, se prohíbe su reproducción total o parcial en cualquier medio, sin previa autorización escrita del Gerente.

Este documento impreso en cualquier medio se considera **"COPIA NO CONTROLADA"**

1 Introducción

La seguridad de la información es esencial para proteger los activos de la empresa, garantizar la confidencialidad, integridad y disponibilidad de los datos, y asegurar el cumplimiento de las normativas aplicables. Esta política se fundamenta en un enfoque basado en riesgos, que exige evaluar y tratar de forma periódica los riesgos de seguridad de la información, así como revisarlos ante cambios relevantes en los procesos, la tecnología o el contexto de la organización.

La organización se compromete a definir, comunicar y revisar objetivos de seguridad de la información que estén alineados con el contexto y la estrategia del negocio. La Alta Dirección garantizará los recursos necesarios, impulsará el cumplimiento y la mejora continua, y promoverá la difusión, comprensión y aplicación de esta política en todos los niveles de la organización, asegurando su adecuada socialización entre los colaboradores y demás partes interesadas.

Este documento utiliza cómo referente el estándar internacional ISO/IEC 27001:2022, otras metodologías de gestión y procedimientos internos establecidos por la empresa.

2 Objetivo

Proteger los datos de Conhydra contra accesos no autorizados, pérdida, manipulación o divulgación indebida, garantizando la confidencialidad, integridad y disponibilidad (CIA) de la información. Adicionalmente, esta política establece el marco para gestionar del riesgo de seguridad de la información y su tratamiento, definir objetivos de seguridad medibles y su seguimiento; y la mejora continua. Aplica a todos los datos en medios digitales, físicos, en tránsito y en almacenamiento, incluyendo nubes públicas y privadas.

USO INTERNO

ELABORADO POR	**REVISADO POR**	**APROBADO POR**
CARLOS ANDRES GARZON	MONICA MONTOYA ALVEREZ	DAVID FLOREZ
ANALISTA LIDER TI	**COORDINADORA SGI**	**ANALISTA INTELIGENCIA DE NEGOCIOS**

Este documento pertenece a CONHYDRA S.A. E.S.P, Aguas de La Prosperidad S.A.S. E.S.P y GESCOMER S.A.S, por lo cual, se prohíbe su reproducción total o parcial en cualquier medio, sin previa autorización escrita del Gerente.

Este documento impreso en cualquier medio se considera **"COPIA NO CONTROLADA"**

3 Alcance

Esta política aplica a toda la información digital y física que Conhydra gestiona, incluyendo bases de datos corporativas, archivos en la nube, documentos impresos, comunicaciones electrónicas y respaldos, en todas las ubicaciones y procesos. Abarca a colaboradores internos, contratistas y proveedores que tengan acceso a los datos de la organización.

4 Definiciones clave

- Seguridad de la información: Conjunto de prácticas, procesos y controles destinados a proteger la confidencialidad, integridad y disponibilidad de los datos frente a accesos no autorizados, alteraciones, pérdidas o divulgación indebidas.
- Confidencialidad: Principio que asegura que la información solo esté disponible para personas con autorización expresa.
- Integridad: Propiedad que garantiza que los datos se mantienen completos, coherentes y sin alteraciones no autorizadas.
- Disponibilidad: Capacidad de que la información esté accesible y utilizable en el momento en que se requiera.
- Acceso autorizado: Permiso concedido a usuarios o sistemas para consultar, modificar o administrar información, conforme a roles y responsabilidades definidas.
- Riesgo de seguridad de la información: Efecto de la incertidumbre sobre los objetivos de seguridad; se gestiona mediante evaluación y tratamiento documentados.
- Incidente de seguridad: Evento que compromete o puede comprometer la confidencialidad, integridad o disponibilidad de la información (ej. accesos indebidos, fugas, alteraciones o pérdidas de datos).

USO INTERNO

Este documento pertenece a CONHYDRA S.A. E.S.P, Aguas de La Prosperidad S.A.S. E.S.P y GESCOMER S.A.S, por lo cual, se prohíbe su reproducción total o parcial en cualquier medio, sin previa autorización escrita del Gerente.

Este documento impreso en cualquier medio se considera **"COPIA NO CONTROLADA"**

- Control de acceso: Conjunto de mecanismos y procedimientos que aseguran que solo las personas autorizadas accedan a los recursos de información según el principio de mínima necesidad.
- Autenticación: Proceso de verificar la identidad de un usuario, dispositivo o sistema antes de permitir el acceso a los recursos de información.
- Amenaza: Cualquier circunstancia, acción o evento que pueda explotar una vulnerabilidad y poner en riesgo la seguridad de la información.
- Phishing: Técnica fraudulenta utilizada por atacantes para engañar a los usuarios y obtener información sensible mediante correos electrónicos, mensajes o enlaces falsos.

5 Roles y responsabilidades

- Gerencia General: Es responsable de aprobar esta política, proveer los recursos necesarios para su implementación y demostrar liderazgo y compromiso con la seguridad de la información.
- Responsable de Seguridad de la Información (RSI): Será la persona encargada de supervisar la implementación, el mantenimiento y la mejora continua de la gestión de seguridad de la información.
- Todos los Empleados: Son responsables de conocer y cumplir esta política y los procedimientos asociados. Deben reportar cualquier incidente de seguridad de la información de manera inmediata

USO INTERNO

ELABORADO POR	**REVISADO POR**	**APROBADO POR**
CARLOS ANDRES GARZON	MONICA MONTOYA ALVEREZ	DAVID FLOREZ
ANALISTA LIDER TI	**COORDINADORA SGI**	**ANALISTA INTELIGENCIA DE NEGOCIOS**

Este documento pertenece a CONHYDRA S.A. E.S.P, Aguas de La Prosperidad S.A.S. E.S.P y GESCOMER S.A.S, por lo cual, se prohíbe su reproducción total o parcial en cualquier medio, sin previa autorización escrita del Gerente.
Este documento impreso en cualquier medio se considera **"COPIA NO CONTROLADA"**

6 Políticas

6.1 Acceso responsable a la información

La organización establece que el acceso a la información y a los recursos tecnológicos se otorgue y utilice de manera responsable, limitado a lo estrictamente necesario para el desempeño de las funciones de cada colaborador y en coherencia con los principios de confidencialidad, integridad y disponibilidad.

Todo acceso a la información y a los sistemas deberá estar previamente autorizado, basado en el rol y en el principio de "mínima necesidad". Asimismo, los usuarios son responsables de proteger los medios que utilicen para acceder a la información (equipos, dispositivos móviles, aplicaciones, cuentas en la nube), incluyendo el bloqueo de pantalla, el cierre de sesión y el resguardo físico de los dispositivos.

6.2 Clasificación de la Información

Cada activo de información tendrá un propietario responsable de su clasificación, etiquetado y manejo. La información debe ser clasificada en las siguientes categorías:

- Confidencial: su divulgación no autorizada puede causar daño a la empresa; requiere controles reforzados y acceso restringido.
- Interna: Información que es de uso interno y no debe ser divulgada al público.
- Pública: Información que puede ser compartida sin restricciones.

USO INTERNO

Este documento pertenece a CONHYDRA S.A. E.S.P, Aguas de La Prosperidad S.A.S. E.S.P y GESCOMER S.A.S, por lo cual, se prohíbe su reproducción total o parcial en cualquier medio, sin previa autorización escrita del Gerente.

Este documento impreso en cualquier medio se considera **"COPIA NO CONTROLADA"**

6.3 Riesgos

La protección adecuada de la información de la organización se basa en la identificación, evaluación y tratamiento oportuno de los riesgos de seguridad, así como en la implementación de controles proporcionales a dichos riesgos. Cualquier acción que impida la aplicación oportuna de estos controles puede poner en riesgo la información importante de la compañía.

Los colaboradores deberán evitar exponer la información de la organización utilizando únicamente los sistemas, aplicaciones y repositorios autorizados por la empresa para almacenar y gestionar los datos de los procesos y proyectos, absteniéndose de usar medios personales o no aprobados.

Todo suceso ocurrido en la que la información pueda verse en riesgo por aspectos cómo pérdida, acceso no autorizado, uso indebido, modificación o divulgación no autorizada deberá ser reportada de manera inmediata al correo informatica@conhydra.com.

6.4 Gestión de incidentes o problemas de seguridad

La organización establece que todo incidente o problema de seguridad de la información, real o sospechado (como accesos no autorizados, pérdida de información, malware, uso indebido de cuentas o dispositivos, entre otros), debe ser reportado de manera inmediata al responsable de seguridad de la información.

Los colaboradores deben abstenerse de actuar por cuenta propia para “resolver” el incidente, evitando acciones que puedan agravar la situación, borrar evidencias o dificultar el análisis. La organización realiza esfuerzos para proporcionar y mantener los medios, procedimientos y herramientas necesarios para registrar, atender,

USO INTERNO

Este documento pertenece a CONHYDRA S.A. E.S.P, Aguas de La Prosperidad S.A.S. E.S.P y GESCOMER S.A.S, por lo cual, se prohíbe su reproducción total o parcial en cualquier medio, sin previa autorización escrita del Gerente.

Este documento impreso en cualquier medio se considera **“COPIA NO CONTROLADA”**

investigar y cerrar los incidentes de seguridad, promoviendo la mejora continua de los controles y la reducción de riesgos asociados.

Adicionalmente, la organización mantendrá un proceso formal para la gestión de incidentes de seguridad de la información que contemple su registro, clasificación, análisis de causa raíz y definición de acciones correctivas y preventivas, así como la comunicación a las partes interesadas pertinentes.

6.5 Responsabilidad de seguridad de la información

La seguridad de la información es una responsabilidad de toda la organización y no recae exclusivamente en el área de tecnología. La Alta Dirección debe establecer, asignar y comunicar claramente los roles y responsabilidades relacionados con la seguridad de la información, asegurando que todos los colaboradores y partes interesadas que acceden a la información conozcan y cumplan las políticas.

Cada colaborador es responsable de proteger la información a la que tiene acceso, utilizar de forma adecuada los activos de información, cumplir las directrices definidas en esta política y reportar oportunamente cualquier incidente, debilidad o situación que pueda comprometer la seguridad. Los responsables de procesos, dueños de la información y administradores de sistemas deberán, además, velar por la correcta aplicación de los controles, la actualización de la información bajo su custodia y el apoyo permanente a las actividades de mejora continua.

6.6 Propiedad de los recursos

Todos los activos y recursos de información de la empresa, incluyendo equipos, sistemas, aplicaciones, cuentas de usuario, documentación, redes, datos y demás herramientas tecnológicas son propiedad exclusiva de la organización.

USO INTERNO

ELABORADO POR	**REVISADO POR**	**APROBADO POR**
CARLOS ANDRES GARZON	MONICA MONTOYA ALVEREZ	DAVID FLOREZ
ANALISTA LIDER TI	**COORDINADORA SGI**	**ANALISTA INTELIGENCIA DE NEGOCIOS**

Este documento pertenece a CONHYDRA S.A. E.S.P, Aguas de La Prosperidad S.A.S. E.S.P y GESCOMER S.A.S, por lo cual, se prohíbe su reproducción total o parcial en cualquier medio, sin previa autorización escrita del Gerente.

Este documento impreso en cualquier medio se considera **"COPIA NO CONTROLADA"**

Todas las personas que interactúan con estos recursos, incluyendo empleados, contratistas, proveedores y terceros, deben utilizarlos únicamente para actividades laborales autorizadas y en cumplimiento de las políticas y procedimientos internos establecidos por la empresa.

Para los recursos se prohíbe cualquier uso personal excesivo, indebido, no autorizado o que comprometa la información. El incumplimiento de estas disposiciones podrá generar acciones disciplinarias, contractuales o legales según corresponda.

6.7 Uso aceptable de los recursos

El uso de los recursos tecnológicos y de información de la empresa, incluyendo equipos, redes, aplicaciones, plataformas, servicios internos y especialmente el correo electrónico corporativo debe realizarse de manera responsable, ética y conforme a las funciones asignadas por la organización.

Todos los empleados, contratistas, proveedores y terceros con acceso a estos recursos deben:

- Seguir los procedimientos operativos y lineamientos internos establecidos por la empresa.
- Evitar el uso personal innecesario o inapropiado.
- No enviar, recibir o almacenar información ilegal, ofensiva, no relacionada con la labor o que afecte la imagen de la empresa.
- No instalar software o herramientas no autorizadas.
- No acceder a sitios o plataformas que no tengan relación con las funciones laborales.

USO INTERNO

Este documento pertenece a CONHYDRA S.A. E.S.P, Aguas de La Prosperidad S.A.S. E.S.P y GESCOMER S.A.S, por lo cual, se prohíbe su reproducción total o parcial en cualquier medio, sin previa autorización escrita del Gerente.

Este documento impreso en cualquier medio se considera **"COPIA NO CONTROLADA"**

Cualquier incidente, sospecha de uso indebido, acceso no autorizado o actividad que pueda comprometer la seguridad debe reportarse de inmediato al correo institucional **informatica@conhydra.com.**

6.8 Estaciones de trabajo y equipos móviles

Con el fin de mitigar el impacto ante pérdida o robo, todos los equipos portátiles corporativos deberán contar con cifrado de disco completo activado.

Todos los empleados, contratistas, proveedores y terceros que utilicen estos dispositivos deben garantizar su uso responsable y seguro, manteniendo la protección de la información que manejan y evitando prácticas que puedan comprometer los activos de la organización.

Las siguientes directrices aplican a toda persona con acceso a estos recursos:

- Mantener los equipos bloqueados cuando no estén en uso o cuando el usuario se ausente de su puesto.
- No instalar software, aplicaciones o herramientas no autorizadas por la empresa.
- No conectar dispositivos externos (USB, discos duros, celulares, etc.) sin aprobación o sin haber sido verificados para evitar malware.
- Reportar inmediatamente cualquier pérdida, daño, robo o sospecha de manipulación no autorizada del equipo.
- Evitar el uso personal excesivo o actividades que puedan afectar el rendimiento, seguridad o disponibilidad de los equipos.
- Asegurar que la información almacenada en dispositivos móviles se maneje con especial cuidado, protegiéndola contra accesos no autorizados, extravíos o exposición indebida.

USO INTERNO

Este documento pertenece a CONHYDRA S.A. E.S.P, Aguas de La Prosperidad S.A.S. E.S.P y GESCOMER S.A.S, por lo cual, se prohíbe su reproducción total o parcial en cualquier medio, sin previa autorización escrita del Gerente.

Este documento impreso en cualquier medio se considera **"COPIA NO CONTROLADA"**

- Mantener actualizados los sistemas operativos, antivirus y demás mecanismos de protección.

El uso inadecuado de estaciones de trabajo o equipos móviles podrá generar sanciones disciplinarias o contractuales, según corresponda.

6.9 Usuarios y contraseñas

Las credenciales de acceso asignadas por la empresa, incluyendo usuarios, contraseñas, tokens, claves temporales y cualquier otro mecanismo de autenticación, son de carácter personal e intransferible. Para garantizar un nivel superior de protección, la organización exige el uso de Autenticación Multifactor (MFA) para cuentas administrativas y acceso a servicios en la nube críticos.

Cada persona es responsable de su custodia, del uso adecuado de las mismas y de evitar cualquier acción que pueda poner en riesgo la seguridad de la información o de los sistemas corporativos.

Todos los empleados, contratistas, proveedores y terceros deben mantener sus contraseñas en absoluta confidencialidad, crear claves robustas que cumplan los lineamientos definidos por la organización, y cambiarlas cuando el sistema lo solicite o exista sospecha de compromiso. Asimismo, deberán abstenerse de almacenar contraseñas en archivos accesibles, notas visibles, correos electrónicos u otros medios inseguros, de reutilizar credenciales de servicios personales en entornos corporativos y de ignorar intentos de suplantación, accesos indebidos o cualquier anomalía relacionada con el uso de sus credenciales, los cuales deberán ser reportados de inmediato por los canales establecidos.

El uso inadecuado, intercambio, divulgación, préstamo o exposición de credenciales se considera una falta grave, ya que compromete la seguridad de la organización y de

Este documento pertenece a CONHYDRA S.A. E.S.P, Aguas de La Prosperidad S.A.S. E.S.P y GESCOMER S.A.S, por lo cual, se prohíbe su reproducción total o parcial en cualquier medio, sin previa autorización escrita del Gerente.

Este documento impreso en cualquier medio se considera **"COPIA NO CONTROLADA"**

USO INTERNO

sus activos de información. Estas conductas podrán derivar en la aplicación de medidas disciplinarias o contractuales, de acuerdo con el reglamento interno y la normatividad vigente.

6.10 Uso de internet

El servicio de Internet proporcionado por la empresa es un recurso corporativo destinado exclusivamente al cumplimiento de funciones laborales. Su uso está estrictamente regulado y en ninguna circunstancia podrá utilizarse para fines personales, recreativos o distintos a las responsabilidades asignadas.

La empresa se reserva el derecho de supervisar el uso de sus recursos tecnológicos, incluyendo el monitoreo del tráfico de Internet y el registro de accesos, descargas y utilización de plataformas. En caso de incumplimiento de las disposiciones establecidas, podrán aplicarse sanciones disciplinarias o contractuales de acuerdo con la gravedad de la falta. El uso del servicio de Internet por parte de los colaboradores implica la aceptación de estos mecanismos de supervisión y control.

Se establece que cualquier usuario de la red corporativa está obligado a cumplir las siguientes reglas:

- El acceso a Internet debe emplearse únicamente para consultar información relacionada con las funciones laborales, utilizar plataformas, aplicaciones y servicios previamente autorizados por la empresa, acceder a herramientas aprobadas para la ejecución de procesos internos y comunicaciones corporativas.

- Está estrictamente prohibido utilizar el servicio de Internet corporativo para acceder a páginas con contenido ilegal, violento, discriminatorio, pornográfico

USO INTERNO

Este documento pertenece a CONHYDRA S.A. E.S.P, Aguas de La Prosperidad S.A.S. E.S.P y GESCOMER S.A.S, por lo cual, se prohíbe su reproducción total o parcial en cualquier medio, sin previa autorización escrita del Gerente.

Este documento impreso en cualquier medio se considera **"COPIA NO CONTROLADA"**

o de apuestas, así como a plataformas de servicios de streaming, videojuegos u otros sitios que no estén relacionados con las funciones laborales.

- Está prohibido descargar archivos, programas, videos o herramientas que no hayan sido autorizadas, instalar aplicaciones, extensiones o software sin aprobación formal.

- Cualquier interacción con plataformas de IA (como asistentes de IA, chatbots, generadores de contenido, entre otros) no podrá implicar el ingreso de información confidencial, personal, interna o estratégica de la empresa.

6.11 Transferencia de información

La información debe transferirse de forma segura de acuerdo con su categoría y nivel de sensibilidad. Cada colaborador es responsable de asegurarse de que los datos se compartan únicamente con destinatarios autorizados y mediante los canales institucionales aprobados.

Para la transferencia de información se deberán utilizar exclusivamente los medios seguros definidos por la empresa, como el correo corporativo, las plataformas internas o los servicios expresamente autorizados, validando siempre la identidad del destinatario antes de enviar cualquier dato. Queda prohibido el uso de aplicaciones, cuentas o dispositivos personales para transferir información corporativa.

Solo deberá compartirse la información estrictamente necesaria para el propósito previsto, respetando su ciclo de vida y su nivel de sensibilidad. Aunque la información alojada en las plataformas institucionales cuenta con controles y respaldos

USO INTERNO

Este documento pertenece a CONHYDRA S.A. E.S.P, Aguas de La Prosperidad S.A.S. E.S.P y GESCOMER S.A.S, por lo cual, se prohíbe su reproducción total o parcial en cualquier medio, sin previa autorización escrita del Gerente.

Este documento impreso en cualquier medio se considera **"COPIA NO CONTROLADA"**

establecidos, la protección de los datos durante su envío, recepción y manejo sigue siendo responsabilidad de cada usuario.

6.12 Respaldo de la información

La información de la empresa es un activo crítico y debe ser protegida mediante mecanismos formales de respaldo que garanticen la continuidad operativa y eviten la pérdida de datos. Todos los empleados, contratistas y terceros que gestionen información corporativa deben cumplir estas directrices y colaborar con las medidas definidas por la organización para la protección de la información.

La empresa cuenta con dos mecanismos oficiales de respaldo:

- **Servidor físico de respaldos:** encargado de realizar copias de seguridad periódicas de los sistemas y archivos almacenados en la infraestructura local.
- **Respaldo en la nube:** toda la información alojada servicios cloud cuenta con respaldos, garantizando disponibilidad y recuperación.

El respaldo y la conservación de los datos se rigen por el ciclo de vida de la información, que comprende las etapas de creación, uso, retención, archivo y disposición final. El dueño del dato es responsable de definir los tiempos de retención y los requisitos legales u operativos asociados a su conservación, así como de determinar qué información requiere ser preservada y bajo qué criterios. Los usuarios, por su parte, deben guardar la información únicamente en los repositorios aprobados por la organización, de modo que pueda ser incluida de forma adecuada en los procesos de copia y recuperación.

El área encargada de la administración de respaldos ejecuta y supervisa las copias de seguridad del servidor y garantiza la correcta aplicación de los esquemas de retención automatizada. Está prohibido almacenar información corporativa en

USO INTERNO

Este documento pertenece a CONHYDRA S.A. E.S.P, Aguas de La Prosperidad S.A.S. E.S.P y GESCOMER S.A.S, por lo cual, se prohíbe su reproducción total o parcial en cualquier medio, sin previa autorización escrita del Gerente.

Este documento impreso en cualquier medio se considera **"COPIA NO CONTROLADA"**

dispositivos personales, unidades USB, correos privados o cualquier otro medio no autorizado. La pérdida de información por no utilizar los repositorios oficiales, el borrado no autorizado o el almacenamiento en ubicaciones no aprobadas se considera una falta grave y puede derivar en sanciones disciplinarias o contractuales, de acuerdo con las políticas internas y la normatividad vigente.

6.13 Equipos desatendidos

Los colaboradores, contratistas y terceros deben aplicar las medidas necesarias para evitar el uso no autorizado de los equipos cuando deban ausentarse, incluso por periodos cortos de tiempo. La protección de la información y de los recursos tecnológicos es responsabilidad de todos, sin excepción.

Para este propósito, se establecen las siguientes disposiciones:

- Bloquear la sesión de inmediato al retirarse del puesto de trabajo, independientemente de la duración de la ausencia.
- Guardar o cerrar documentos que contengan información sensible antes de abandonar el equipo.
- Evitar dejar dispositivos móviles, portátiles u otros medios de almacenamiento expuestos o accesibles para personas no autorizadas.
- Asegurar que, al finalizar la jornada o en ausencias prolongadas, los equipos se apaguen o queden protegidos según las directrices emitidas por el área responsable.
- No permitir que terceros utilicen el equipo asignado, salvo autorización expresa de la organización.

El incumplimiento de estas prácticas representa una falta grave, ya que expone la información corporativa a pérdida, alteración o uso indebido.

USO INTERNO

ELABORADO POR	**REVISADO POR**	**APROBADO POR**
CARLOS ANDRES GARZON	MONICA MONTOYA ALVEREZ	DAVID FLOREZ
ANALISTA LIDER TI	**COORDINADORA SGI**	**ANALISTA INTELIGENCIA DE NEGOCIOS**

Este documento pertenece a CONHYDRA S.A. E.S.P, Aguas de La Prosperidad S.A.S. E.S.P y GESCOMER S.A.S, por lo cual, se prohíbe su reproducción total o parcial en cualquier medio, sin previa autorización escrita del Gerente.
Este documento impreso en cualquier medio se considera **"COPIA NO CONTROLADA"**

6.14 Omisión de procedimientos o evasión de controles de seguridad

Queda estrictamente prohibido omitir o evadir cualquiera de los procedimientos, lineamientos o controles de seguridad establecidos por la organización. Estas directrices existen para proteger la información, los recursos tecnológicos y la continuidad de las operaciones, por lo que su cumplimiento es obligatorio para todos los colaboradores, contratistas y terceros que interactúen con los sistemas o con la información institucional.

Estas conductas vulneran la integridad, disponibilidad y confidencialidad de la información corporativa y pueden generar impactos operativos, legales y reputacionales, por lo que serán tratadas con la máxima severidad disciplinaria.

Se considera falta grave cualquier acción u omisión que implique:

- Compartir o eludir mecanismos de autenticación
- Ignorar procedimientos documentados o instrucciones oficiales relacionadas con la seguridad de la información.
- Deshabilitar, modificar o evitar controles técnicos, tales como bloqueos automáticos, actualizaciones, antivirus, autenticaciones, registros de auditoría, o mecanismos de protección.
- Utilizar medios o prácticas no autorizadas para realizar tareas laborales, con el fin de eludir supervisión o restricciones establecidas.
- Facilitar o permitir, directa o indirectamente, que otros evadan los controles definidos.

USO INTERNO

Este documento pertenece a CONHYDRA S.A. E.S.P, Aguas de La Prosperidad S.A.S. E.S.P y GESCOMER S.A.S, por lo cual, se prohíbe su reproducción total o parcial en cualquier medio, sin previa autorización escrita del Gerente.

Este documento impreso en cualquier medio se considera **"COPIA NO CONTROLADA"**

6.15 Cumplimiento normativo

La organización se compromete a cumplir con la legislación y la normativa aplicable en materia de protección de datos personales, propiedad intelectual, derechos de autor, así como con cualquier otra disposición legal, reglamentaria o contractual relacionada con la seguridad de la información.

Todos los colaboradores deben respetar las leyes vigentes y las políticas de la organización, evitando cualquier acción que pueda vulnerar la legalidad o generar sanciones legales, contractuales o impactos reputacionales para la empresa. La organización promoverá la sensibilización sobre estos aspectos, promoviendo una cultura de responsabilidad.

6.16 Monitoreo

La organización se reserva el derecho de monitorear el uso de los servicios y recursos tecnológicos con el fin de identificar situaciones irregulares, detectar posibles vulnerabilidades y prevenir incidentes de seguridad de la información. Este monitoreo podrá incluir la revisión de registros de acceso, actividades en los sistemas, uso de aplicaciones y tráfico de red, entre otros mecanismos que se consideren necesarios y proporcionales para proteger los activos de información.

Dado que los servicios y recursos tecnológicos son propiedad de la compañía, en cualquier momento en que se detecte una posible vulnerabilidad, uso indebido o incidente que pueda comprometer la información, la organización podrá rastrear el origen del evento, analizar las evidencias disponibles y tomar las acciones correctivas,

USO INTERNO

Este documento pertenece a CONHYDRA S.A. E.S.P, Aguas de La Prosperidad S.A.S. E.S.P y GESCOMER S.A.S, por lo cual, se prohíbe su reproducción total o parcial en cualquier medio, sin previa autorización escrita del Gerente.

Este documento impreso en cualquier medio se considera **"COPIA NO CONTROLADA"**

preventivas o disciplinarias que correspondan, respetando la normativa vigente y las políticas internas.

Adicionalmente, la organización garantizará que las actividades de monitoreo se realicen de manera transparente, documentada y con fines exclusivamente relacionados con la seguridad de la información y la continuidad del negocio.

6.17 Cumplimiento y sanciones

El cumplimiento de esta Política de Seguridad de la Información es obligatorio para todos los colaboradores, contratistas y terceros que tengan acceso a los datos y activos de información de la organización. La empresa realizará actividades de monitoreo, auditorías internas y revisiones periódicas por parte de la dirección, con el fin de evaluar la eficacia de los controles, verificar el cumplimiento de la política y medir el logro de los objetivos establecidos.

Las no conformidades identificadas serán gestionadas mediante acciones correctivas y de mejora continua, buscando reducir la probabilidad de recurrencia y fortalecer el sistema de gestión de la seguridad de la información. Cualquier incumplimiento de las disposiciones aquí establecidas podrá dar lugar a la aplicación de medidas disciplinarias o contractuales, de acuerdo con el reglamento interno, los acuerdos vigentes y la normatividad aplicable.

6.18 Excepciones

Cualquier excepción a lo establecido en esta Política de Seguridad de la Información deberá ser gestionada de manera formal enviando la solicitud al correo informatica@conhydra.com, indicando claramente la necesidad, el alcance y la

USO INTERNO

Este documento pertenece a CONHYDRA S.A. E.S.P, Aguas de La Prosperidad S.A.S. E.S.P y GESCOMER S.A.S, por lo cual, se prohíbe su reproducción total o parcial en cualquier medio, sin previa autorización escrita del Gerente.

Este documento impreso en cualquier medio se considera **"COPIA NO CONTROLADA"**

duración estimada. La solicitud será evaluada por el responsable de seguridad de la información y, de ser necesario, será escalada a los entes directivos correspondientes para su análisis y aprobación.

Las excepciones autorizadas deberán quedar documentadas, incluir las medidas de mitigación de riesgos que apliquen y tendrán una vigencia limitada, sujeta a revisión periódica. Una vez superada la causa que dio origen a la excepción, deberán restablecerse las condiciones normales definidas en la política.

USO INTERNO

ELABORADO POR	**REVISADO POR**	**APROBADO POR**
CARLOS ANDRES GARZON	MONICA MONTOYA ALVEREZ	DAVID FLOREZ
ANALISTA LIDER TI	**COORDINADORA SGI**	**ANALISTA INTELIGENCIA DE NEGOCIOS**

Este documento pertenece a CONHYDRA S.A. E.S.P, Aguas de La Prosperidad S.A.S. E.S.P y GESCOMER S.A.S, por lo cual, se prohíbe su reproducción total o parcial en cualquier medio, sin previa autorización escrita del Gerente.

Este documento impreso en cualquier medio se considera **"COPIA NO CONTROLADA"**