



Política de Segurança da Informação GWS

GWS-ISI-001 · Versão 1.0

Uso Institucional Emissão 09/03/2026

SUMÁRIO

CONTROLE DO DOCUMENTO.....	1
OBJETIVO.....	2
APLICABILIDADE.....	3
PRINCÍPIOS DE SEGURANÇA.....	4
CLASSIFICAÇÃO DA INFORMAÇÃO.....	5
CONTROLE DE ACESSO.....	6
COMPARTILHAMENTO INTERNO E EXTERNO.....	7
AMBIENTES DE CLIENTE E DOCUMENTOS RESTRITOS.....	8
SENHAS, MFA E DISPOSITIVOS.....	9
BACKUP, RETENÇÃO E DESCARTE.....	10
INCIDENTES DE SEGURANÇA.....	11
RESPONSABILIDADES DOS USUÁRIOS.....	12
TREINAMENTO E RESPONSABILIZAÇÃO.....	13
VIGÊNCIA E REVISÃO.....	14



CONTROLE DO DOCUMENTO

Campo	Valor
Código	GWS-ISI-001
Versão	1.0
Emissão	09/03/2026
Revisão	09/03/2026
Aprovador	Direção GWS
Responsável	Governança Institucional
Classificação	Uso Institucional
Idioma	Português

Esta Política estabelece os controles mínimos para proteger a confidencialidade, a integridade, a disponibilidade e a rastreabilidade das informações sob responsabilidade da GWS. A empresa atua com documentos técnicos, comerciais, contratuais e estratégicos ligados a relações institucionais sensíveis, diligências e mandatos comerciais e, por isso, exige disciplina informacional compatível com esse contexto e com a criticidade dos dados tratados.

01

OBJETIVO

Definir regras básicas para o uso, o armazenamento, o compartilhamento, a proteção e o descarte de informações e documentos da GWS e de seus clientes, parceiros e interlocutores.

02

APLICABILIDADE

Esta Política aplica-se a:

- sócios e dirigentes;
- empregados e estagiários;
- consultores e representantes;
- terceiros autorizados a acessar informações ou ambientes da GWS;
- documentos físicos e digitais sob guarda da empresa.

03

PRINCÍPIOS DE SEGURANÇA

As informações da GWS devem ser tratadas conforme os seguintes princípios:

- **confidencialidade:** acesso apenas por quem precisa conhecer;
- **integridade:** preservação da exatidão e da consistência;
- **disponibilidade:** acesso adequado quando necessário;
- **rastreabilidade:** possibilidade de identificar uso, versões e fluxos relevantes;
- **proporcionalidade:** controles compatíveis com o nível de sensibilidade.

04

CLASSIFICAÇÃO DA INFORMAÇÃO

As informações devem ser classificadas de forma simples e objetiva:

Classe	Uso esperado
Pública	Pode ser divulgada sem risco relevante
Interna	Uso restrito ao ambiente de trabalho da GWS
Confidencial	Acesso controlado, com impacto relevante em caso de divulgação indevida
Restrita	Acesso limitado e controle reforçado

Documentos de cliente, diligências, oportunidades não públicas, contratos, estudos técnicos e ambientes de projeto devem ser tratados, como regra, no mínimo como confidenciais.

05

CONTROLE DE ACESSO

O acesso a informações e sistemas deve seguir o princípio do menor privilégio.

Isso significa que:

- cada pessoa recebe apenas o acesso necessário ao seu papel;
- credenciais são pessoais e intransferíveis;
- acessos devem ser revistos quando houver mudança de função, projeto ou desligamento;
- informações restritas exigem controle reforçado.

Os responsáveis por ambiente, pasta, sistema ou projeto devem zelar pela coerência entre os acessos concedidos e a necessidade funcional efetiva.

06

COMPARTILHAMENTO INTERNO E EXTERNO

Toda circulação de informação deve observar necessidade, adequação e canal apropriado.

Não é permitido:

- compartilhar documentos confidenciais sem base funcional;
- enviar arquivos sensíveis por canais inadequados;
- armazenar documentos relevantes em ambientes não autorizados;
- manter cópias desnecessárias de informações restritas.

Sempre que houver compartilhamento externo de informação confidencial ou restrita, deve haver base funcional legítima, controle mínimo de destinatários e preferência por ambientes com permissão gerenciável.

07

AMBIENTES DE CLIENTE E DOCUMENTOS RESTRITOS

Documentos de cliente e ambientes restritos devem, sempre que possível, observar:

- autenticação reforçada;
- controle de permissão por usuário ou projeto;
- registro de versões;
- trilha de auditoria para acessos relevantes;
- expiração ou revisão periódica de acessos.

08

SENHAS, MFA E DISPOSITIVOS

Todos devem adotar cuidados mínimos com credenciais e equipamentos utilizados em atividades da GWS.

Regras mínimas:

- senhas fortes e não compartilhadas;
- ativação de MFA quando disponível para ambientes críticos;
- bloqueio de tela e proteção básica dos dispositivos;
- uso responsável de equipamentos pessoais em contexto profissional.

Em acessos remotos, redes compartilhadas ou uso de equipamento pessoal, o usuário deve adotar cautela reforçada para evitar visualização indevida, captura não autorizada ou permanência de arquivos fora de ambiente controlado.

09

BACKUP, RETENÇÃO E DESCARTE

Informações relevantes devem seguir critério razoável de retenção, recuperação e descarte.

Sempre que aplicável:

- documentos ativos devem permanecer em ambiente controlado;
- arquivos obsoletos ou duplicados devem ser eliminados de forma segura;
- materiais sensíveis não devem permanecer indefinidamente sem necessidade;
- o descarte deve considerar a classificação da informação.

10

INCIDENTES DE SEGURANÇA

Incidentes ou suspeitas de incidente devem ser reportados imediatamente.

Exemplos:

- envio indevido de documento;
- acesso não autorizado;
- perda de dispositivo com informações da GWS;
- vazamento ou suspeita de vazamento;
- alteração indevida de arquivo relevante.

Toda ocorrência deve ser registrada e tratada de forma proporcional à criticidade do caso.

Sempre que cabível, a resposta a incidente deve contemplar contenção inicial, preservação de evidências, avaliação de impacto, comunicação aos responsáveis e definição de medidas de correção.

11

RESPONSABILIDADES DOS USUÁRIOS

Toda pessoa com acesso a informações da GWS deve:

- observar a classificação aplicável ao documento ou ambiente;
- manter organização mínima de pastas, versões e nomenclaturas;
- reportar acessos indevidos, fragilidades percebidas ou dúvidas relevantes;
- encerrar ou devolver acessos, arquivos e materiais quando cessar a necessidade de uso.

12

TREINAMENTO E RESPONSABILIZAÇÃO

As pessoas sujeitas a esta Política devem receber orientação adequada sobre o tratamento das informações em seu contexto de trabalho.

O descumprimento das regras desta Política pode gerar medida corretiva, restritiva, disciplinar ou contratual, conforme a gravidade do caso.

13

VIGÊNCIA E REVISÃO

Esta Política entra em vigor na data de sua aprovação e deve ser revista periodicamente ou sempre que houver mudança material no ambiente operacional, tecnológico ou regulatório da GWS.

Uso interno e institucional da GWS. Documento sujeito a revisão periódica.



**Conectando o Brasil ao mundo,
com governança que sustenta
confiança.**

www.gwscons.com gws@gwscons.com