PRESIDÊNCIA

PORTARIA Nº 184/2026/APPA

O Diretor Presidente da Administração dos Portos de Paranaguá e Antonina, no uso de suas atribuições conferidas pelo artigo 33 do Estatuto Social da APPA, aprovado na 1ª Assembleia Geral Extraordinária realizada em 20 de maio de 2020,

RESOLVE:

Art 1º ESTABELECER o procedimento de Revisão Periódica de Contas de Usuários e Direitos de Acesso que encontra-se disponível no endereço eletrônico www.portosdoparana.pr.gov.br/Pagina/Procedimento-de-Revisao-Periodica-de-Contas-de-Usuarios-e-Direitos-de-Acesso .

Art 2º Esta Portaria entra em vigor na data de sua publicação.

Gabinete da Presidência, em 4 de novembro de 2026.

LUIZ FERNANDO GARCIA DA SILVA:32960264878

Assinado digitalmente por LUIZ FERNANDO GARCIA DA SILVA:32960264878
ND: C=BR, O=ICP-Brasil, OU=Secretaria da Receita Federal do Brasil - RFB, OU=RFB e-CPF A3, OU=(EM BRANCO), OU=34028316000103, OU=videoconferencia, CN=LUIZ FERNANDO GARCIA DA SILVA:32960264878
Razão: Eu concordo com os termos definidos por minha assinatura neste documento
Localização:
Data: 2026.11.04 10:51:33-03'00'
Foxit PDF Reader Versão: 2025.2.0

(assinado digitalmente)
LUIZ FERNANDO GARCIA DA SILVA
Diretor Presidente

PRESIDÊNCIA

PORTARIA Nº 184/2026/APPA

ANEXO

ÍNDICE DE REVISÕES		
REV.	**DATA**	**DESCRIÇÃO E/OU FOLHAS ATINGIDAS**
0	04/11/2026	Emissão inicial
Requisito(s): Capítulo VI da Resolução CONPORTOS nº 53/2020; itens 16.5, 16.59.2 e 16.61.5 do ISPS Code (SOLAS 74/78, Decreto nº 9.988/2019); e item 5.34 do Parecer Técnico da CESPORTOS.		
Prazo máximo para revisão: 16/11/2027		

ELABORAÇÃO:	ANÁLISE CRÍTICA:	APROVAÇÃO:
Coordenadoria de Sistemas	Gerência de Tecnologia da Informação	Diretoria de Desenvolvimento Empresarial

PORTARIA Nº 184/2026/APPA

PROCEDIMENTOS DE REVISÃO PERIÓDICA DE CONTAS DE USUÁRIOS E DIREITOS DE ACESSO

1. OBJETIVOS

Estabelecer o procedimento padrão para a revisão, validação e recertificação periódica das contas de usuários e seus respectivos privilégios e direitos de acesso aos sistemas de informação, redes e infraestrutura de TI da Administração dos Portos de Paranaguá e Antonina (APPA), assegurando o cumprimento dos princípios da necessidade de conhecer e do menor privilégio, em conformidade com os *frameworks* ISO/IEC 27001:2022 e SOC 2 (*Trust Services Criteria*).

2. CAMPO DE APLICAÇÃO

Todas as contas de acesso (individuais, genéricas, *privileged*/privilegiadas, de serviço ou temporárias) criadas e ativas nos ambientes de tecnologia da informação e comunicação (TIC) mantidos ou geridos pela APPA, abrangendo empregados públicos, terceirizados, estagiários, prestadores de serviço e parceiros externos.

3. DOCUMENTOS DE REFERÊNCIA

I – ABNT ISO 27001 (Controle A.5.15, A.5.18, A.8.2, A.8.3): Foco na gestão de direitos de acesso e autenticação robusta;
II – SOC 2 (Critérios CC6.1, CC6.2 e CC6.3): Foco na lógica, credenciais de usuário e revisão de acessos;
III – ISPS Code – Código Internacional para Proteção de Navios e Instalações Portuárias (Parte A e B);
IV – Resolução CONPORTOS nº 53/2020 e demais regulamentações vigentes; e
V – LGPD – Lei Geral de Proteção de Dados Pessoais.

4. DEFINIÇÕES E SIGLAS

Conta de Usuário: Identificador digital único atribuído a uma pessoa física ou jurídica/serviço para acesso a recursos computacionais.

Direitos de Acesso: Conjunto de permissões (leitura, escrita, execução, administração) concedidas a uma conta de usuário dentro de um sistema ou repositório.

Necessidade de Conhecer (*Need-to-Know*): O acesso é limitado a informações necessárias para o desempenho de tarefas específicas.

PORTARIA Nº 184/2026/APPA

Princípio do Menor Privilégio (*Least Privilege*): Um usuário deve ter apenas as permissões e os recursos exatos necessários para concluir a tarefa atribuída, e nada mais.

Recertificação: Processo auditável de revisão formal promovido pela gestão de área de tecnologia da informação para aprovação, alteração ou revogação dos acessos vigentes.

UASP: Unidade Administrativa de Segurança Portuária.

GTEC: Gerência de Tecnologia da Informação.

5. DISPOSIÇÕES NORMATIVAS

5.1 GESTÃO DO CICLO DE VIDA DO ACESSO

5.1.1 Concessão: O acesso deve ser solicitado formalmente e aprovado pelo gestor da área e pelo dono do sistema, utilizando os critérios de menor privilégio e necessidade de conhecer como balizadores para a solicitação.

5.1.2 Revisão Periódica: As permissões de acesso devem ser revisadas semestralmente para garantir que permaneçam adequadas ou sejam corrigidas, sem prejuízo do dever do Gestor da Área de solicitar alterações nestas permissões sempre que se faça necessário.

5.1.3 Revogação: O acesso deve ser desativado imediatamente (em até 24 horas) após a comunicação à GTEC do desligamento ou mudança de função do colaborador.

5.2 RESPONSABILIDADES

Papel/Unidade	Responsabilidades Principais
GTEC (Tecnologia da Informação)	Extrair relatórios de acessos, consolidar dados, executar os bloqueios/revogações solicitados e manter o arquivo de evidências.
Gestores de Área / Chefias Imediatas	Analisar os relatórios de recertificação de sua equipe, validar a pertinência dos privilégios e formalizar a manutenção, ajuste ou revogação em prazo hábil.
Unidade de Recursos Humanos (RH) / Gestores de Contratos	Notificar imediatamente a GTEC sobre desligamentos, transferências, suspensões ou término de contratos de trabalho/prestação de serviços.
UASP	Acompanhar os níveis de proteção ISPS e solicitar auditorias pontuais de acessos em cenários de risco elevado ou emergencial.

Tabela 1 – Quadro de Responsabilidades

5.3 MONITORAMENTO E AUDITORIA

Logs de acesso (*logins* bem-sucedidos e tentativas falhas) devem ser coletados, protegidos contra alteração e revisados regularmente para detectar atividades suspeitas, conforme exigido pelos critérios de monitoramento do SOC 2.

6. DISPOSIÇÕES OPERACIONAIS

6.1 PLANEJAMENTO E EXECUÇÃO DA REVISÃO DE ROTINA (SEMESTRAL)

I – Início do Processo: A revisão será iniciada semestralmente, até o 10º dia útil do mês subsequente ao semestre;

II – Extração e Consolidação: A GTEC gerará os relatórios consolidados de contas ativas, perfis e permissões dos ambientes e sistemas críticos;

III – Envio para Validação (até o 10º dia útil): A GTEC enviará as listas de contas para a respectiva chefia/gestor da unidade administrativa;

IV – Análise Crítica e Resposta (até o 20º dia útil): Os gestores analisarão o relatório e formalizarão o retorno (via sistema de chamados/ITSM ou processo administrativo digital) confirmando a manutenção dos acessos existentes ou solicitando ajustes nas permissões; e

V – Execução das Correções (até 10 dias úteis após o retorno): A GTEC aplicará as revogações e adequações solicitadas e encerrará o ciclo de revisão semestral.

6.2 REGRAS ESPECÍFICAS DE SEGURANÇA

I – Contas Inativas: Contas sem *log* de autenticação nos últimos 60 (sessenta) dias serão suspensas/bloqueadas. Contas inativas por mais de 120 (cento e vinte) dias deverão ser desativadas/excluídas conforme política de retenção;

II – Contas Genéricas e de Serviço: Devem possuir justificativa formal aprovada pela GTEC, com responsável nomeado, escopo restrito ou conforme necessidade de segurança; e

III – Acessos Privilegiados / Administradores: Devem ser revisados com prioridade alta, limitando-se estritamente ao pessoal técnico autorizado.

6.3 TRATAMENTO DE NÃO CONFORMIDADES DE ACESSO

PORTARIA Nº 184/2026/APPA

6.3.1 Qualquer divergência identificada (privilégio excessivo, conta ativa de colaborador desligado, acúmulo indevido de funções) será registrada como Não Conformidade de Acesso (NCA).

6.3.2 O gestor imediato será notificado para apresentar justificativa técnica ou formalizar a correção no prazo improrrogável de 5 (cinco) dias úteis.

6.3.3 A GTEC aplicará as correções (bloqueio, remoção de grupos, alteração de perfis) e registrará a ação.

6.3.4 Na ausência de resposta do gestor no prazo limite, a GTEC aplicará o bloqueio preventivo da conta/perfil não confirmado até a manifestação formal da chefia.

6.3.5 Todos os registros de concessão, alteração, revogação, relatórios de recertificação e justificativas deverão ser mantidos arquivados de forma auditável.