



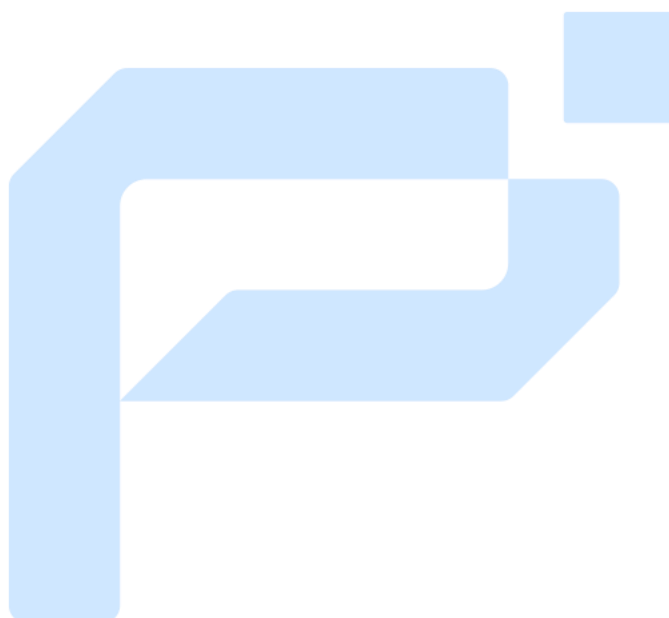
MANUAL DE CONFIGURAÇÃO DE 2FA/MFA NO GLPI PETA

Autenticação Multifator



HISTÓRICO DE REVISÕES

Versão	Data	Resumo das alterações	Elaborado por	Aprovado por
1.0	18/08/2026	Criação do documento	Bruno Mendes	Mayra Farias





SUMÁRIO

HISTÓRICO DE REVISÕES.....	0
INTRODUÇÃO AO 2FA	3
Por que usar MFA?.....	3
Como funciona o TOTP	3
Pré-requisitos.....	3
GOOGLE AUTHENTICATOR.....	3
Instalação.....	4
Configuração no GLPI Peta	4
Utilização diária	5
MICROSOFT AUTHENTICATOR	5
Instalação.....	6
Configuração no GLPI Peta	6
Recursos avançados.....	7
TWILIO AUTHY AUTHENTICATOR.....	7
Instalação.....	8
Configuração inicial da conta Authy	8
Configuração no GLPI Peta	8
Recursos exclusivos do Authy	9
SOLUÇÃO DE PROBLEMAS.....	9
Código de verificação não funciona.....	10
Perda ou troca de smartphone.....	10
O aplicativo não gera códigos.....	11
Erro de sincronização de horário	11
BOAS PRÁTICAS DE SEGURANÇA	12
CONTATO COM O SUPORTE	12
LINKS DOS APLICATIVOS	12
Google Authenticator	12
Microsoft Authenticator	13
Twilio Authy Authenticator.....	13
GLOSSÁRIO.....	13
REFERÊNCIAS	14



INTRODUÇÃO AO 2FA

A autenticação multifator (MFA) é um método de segurança que exige dois ou mais fatores de verificação de identidade antes de conceder acesso. Além da senha (algo que você sabe), o MFA exige um segundo fator, como um código gerado no smartphone (algo que você tem), garantindo que somente usuários legítimos acessem suas contas.

Atenção: a configuração do MFA é obrigatória no GLPI Peta desde 11/08/2026. No primeiro acesso ao sistema após essa data, você será automaticamente redirecionado para a tela de configuração do MFA. Enquanto não concluir a configuração, não será possível acessar o sistema.

Os aplicativos autenticadores (Google Authenticator, Microsoft Authenticator e Twilio Authy) geram códigos de 6 dígitos que mudam a cada 30 segundos. Esses códigos são gerados localmente no dispositivo, sem necessidade de internet após a configuração inicial. Este manual explica como configurar o MFA no GLPI Peta (<https://glpi.petacorp.com.br/>) com cada um desses três aplicativos.

Por que usar MFA?

Senhas sozinhas não são suficientes para proteger contas. Mais de 80% das violações de dados envolvem credenciais comprometidas. O MFA adiciona uma camada crítica de proteção: mesmo que um invasor obtenha sua senha, ainda precisará do segundo fator para acessar a conta.

Como funciona o TOTP

O protocolo TOTP (Time-based One-Time Password) gera códigos numéricos de uso único baseados em uma chave secreta compartilhada (via QR Code) e o horário atual. A cada 30 segundos, um novo código é calculado localmente tanto no servidor quanto no seu dispositivo, sem necessidade de comunicação de rede. Se os códigos coincidirem, o acesso é concedido.

Pré-requisitos

Para configurar o MFA em sua conta, você precisa de um smartphone com Android ou iOS, acesso à conta que deseja proteger, um aplicativo autenticador instalado (Google Authenticator, Microsoft Authenticator ou Authy) e acesso a um computador ou outro dispositivo para realizar o login durante a configuração.

GOOGLE AUTHENTICATOR

O Google Authenticator é um dos aplicativos autenticadores mais populares e amplamente utilizados no mundo. Desenvolvido pelo Google, está disponível gratuitamente para Android e iOS e oferece uma interface simples e direta para gerar códigos TOTP de 6 dígitos. Sua principal vantagem é a simplicidade: não requer cadastro



de conta no Google para funcionar e suporta múltiplas contas de diferentes serviços simultaneamente.

Instalação

Android

1. Abra a Google Play Store no seu dispositivo Android.
2. Toque na barra de pesquisa e digite "Google Authenticator".
3. Localize o aplicativo desenvolvido pelo Google LLC e toque em "Instalar".
4. Aguarde o download e a instalação serem concluídos. O ícone aparecerá na sua tela de aplicativos.

iOS (iPhone/iPad)

1. Abra a App Store no seu iPhone ou iPad.
2. Toque no ícone de busca e digite "Google Authenticator".
3. Localize o aplicativo oficial do Google e toque em "Obter" ou no ícone de download.
4. Confirme a instalação com Face ID, Touch ID ou senha do Apple ID.
5. Após a instalação, o aplicativo estará disponível na sua tela de aplicativos.

Dica: verifique se o desenvolvedor é realmente o Google LLC para evitar instalação de aplicativos falsos que possam comprometer sua segurança.

Configuração no GLPI Peta

A configuração do Google Authenticator com o sistema GLPI Peta envolve duas etapas principais: preparar o aplicativo e vincular sua conta do GLPI ao autenticador. Siga cada passo com atenção para garantir que a vinculação seja feita corretamente.

Passo a passo

1. Acesse o sistema GLPI Peta em <https://glpi.petacorp.com.br/> e faça login com suas credenciais habituais (usuário e senha). No primeiro acesso após 11/08/2026, o sistema automaticamente redirecionará você para a tela de configuração do 2FA.
2. O sistema exibirá um QR Code específico para a sua conta. Caso não seja redirecionado automaticamente, navegue até as configurações da sua conta (menu superior > seu nome de usuário > "Preferências") e procure a seção de autenticação em dois fatores.
3. Abra o Google Authenticator no seu smartphone. Toque no ícone "+" (ou "Adicionar conta") no canto inferior direito da tela.
4. Selecione a opção "Escanear código QR". A câmera do dispositivo será ativada automaticamente.



5. Aponte a câmera para o QR Code exibido na tela do GLPI Peta. Certifique-se de que o QR Code esteja completamente visível e dentro da área de escaneamento.
6. Após o escaneamento, o aplicativo adicionará automaticamente a conta GLPI Peta e começará a gerar códigos de 6 dígitos que mudam a cada 30 segundos.
7. Volte ao GLPI Peta e insira o código de 6 dígitos atualmente exibido no Google Authenticator no campo de verificação. Isso confirma que a vinculação foi feita corretamente.
8. O sistema pode exibir códigos de backup (recovery codes). Anote e guarde esses códigos em um local seguro, pois eles permitem acessar a conta caso você perca o acesso ao smartphone.

Atenção: não pule o passo de salvar os códigos de backup. Sem eles, a perda ou danificação do smartphone pode resultar em bloqueio permanente da conta.

Utilização diária

Após a configuração, cada vez que você fizer login no GLPI Peta, o sistema solicitará o código de verificação após a inserção da senha. Abra o Google Authenticator, localize a entrada correspondente ao GLPI Peta na lista de contas e insira o código de 6 dígitos exibido na tela de login. Os códigos mudam a cada 30 segundos, indicado por um indicador circular ou barra de progresso próximo ao código.

Se o código expirar antes de você digitá-lo completamente, simplesmente aguarde o próximo código ser gerado. Não tente usar um código expirado, pois ele será rejeitado pelo servidor. Se você tiver dificuldades com a sincronia dos códigos, verifique se o relógio do seu smartphone está sincronizado corretamente com o horário de rede, pois o TOTP depende de precisão temporal.

Dica: no Android, você pode copiar o código tocando nele e depois colar diretamente no navegador, sem precisar digitar manualmente.

MICROSOFT AUTHENTICATOR

O Microsoft Authenticator é o aplicativo de autenticação da Microsoft, disponível gratuitamente para Android e iOS. Além de gerar códigos TOTP padrão, oferece recursos avançados como aprovação push (notificação para aprovar ou negar o login com um toque), autenticação biométrica (Face ID, impressão digital) e backup em nuvem das contas configuradas.



Instalação

Android

1. Abra a Google Play Store no seu dispositivo Android.
2. Pesquise por "Microsoft Authenticator" na barra de busca.
3. Identifique o aplicativo publicado pela Microsoft Corporation e toque em "Instalar".
4. Aguarde a conclusão da instalação. O aplicativo estará pronto para uso após o download.

iOS (iPhone/iPad)

1. Abra a App Store no seu iPhone ou iPad.
2. Toque no ícone de busca e digite "Microsoft Authenticator".
3. Localize o aplicativo oficial da Microsoft Corporation e toque em "Obter".
4. Confirme a instalação com Face ID, Touch ID ou senha do Apple ID.
5. Após a instalação, abra o aplicativo e conceda as permissões necessárias (câmera para escanear QR Codes e notificações para aprovações push).

Configuração no GLPI Peta

O processo de configuração do Microsoft Authenticator segue a mesma lógica do Google Authenticator, com a diferença de que o aplicativo da Microsoft oferece funcionalidades adicionais de backup e recuperação que podem ser muito úteis em caso de perda ou troca de dispositivo.

Passo a passo

1. Acesse o GLPI Peta em <https://glpi.petacorp.com.br/> e faça login com suas credenciais. No primeiro acesso após 11/08/2026, o sistema automaticamente redirecionará você para a tela de configuração do 2FA.
2. O sistema exibirá um QR Code para vinculação com o autenticador. Caso não seja redirecionado, vá até as configurações de sua conta e procure a seção de autenticação em dois fatores.
3. Abra o Microsoft Authenticator no seu smartphone. Toque no ícone "+" ou em "Adicionar conta" no canto superior.
4. Selecione a opção "Outra conta" (ou "Other account"), pois o GLPI não é um serviço Microsoft. Para contas do ecossistema Microsoft (Outlook, Office 365), selecione "Conta de trabalho ou escola" ou "Conta pessoal Microsoft".
5. Escolha "Escanear código QR" e aponte a câmera para o QR Code exibido no GLPI Peta. O aplicativo processará o código automaticamente.
6. A conta GLPI Peta será adicionada à lista de contas no Microsoft Authenticator e os códigos TOTP começarão a ser gerados imediatamente.



7. Insira o código de verificação atual no campo correspondente do GLPI Peta para confirmar a vinculação.
8. Salve os códigos de backup exibidos pelo GLPI em um local seguro.

Recursos avançados

Backup em nuvem

O Microsoft Authenticator permite fazer backup das contas configuradas na nuvem, usando sua conta Microsoft pessoal. Isso significa que, se você perder o dispositivo ou trocar de smartphone, poderá restaurar todas as suas contas de autenticação no novo dispositivo sem precisar reconfigurar cada conta individualmente. Para ativar o backup, acesse as configurações do aplicativo e ative a opção "Backup em nuvem" (Cloud backup). O backup é criptografado e armazenado de forma segura.

Aprovação por notificação push

Para contas do ecossistema Microsoft (não aplicável ao GLPI Peta com TOTP), o aplicativo pode receber notificações push solicitando aprovação de login. Em vez de digitar um código, você simplesmente aprova ou nega a solicitação com um toque. Para contas de terceiros como o GLPI Peta, o método utilizado é o código TOTP padrão de 6 dígitos.

Verificação biométrica

O aplicativo pode exigir verificação biométrica (Face ID ou impressão digital) antes de exibir os códigos de autenticação. Isso adiciona uma camada extra de proteção: mesmo que alguém tenha acesso físico ao seu dispositivo desbloqueado, não poderá ver os códigos sem passar pela verificação biométrica. Para ativar, acesse as configurações do aplicativo e ative "Bloqueio de aplicativo" ou "App lock".

Dica: ative o backup em nuvem e o bloqueio biométrico assim que configurar o aplicativo. Esses recursos salvam tempo em caso de troca de dispositivo e protegem seus códigos de acessos não autorizados.

TWILIO AUTHY AUTHENTICATOR

O Twilio Authy Authenticator, agora parte do ecossistema Twilio, é um aplicativo autenticador que se destaca por oferecer backup criptografado em nuvem, suporte a múltiplos dispositivos simultaneamente e uma interface intuitiva. Diferente do Google Authenticator, o Authy requer a criação de uma conta com número de telefone durante a configuração inicial, o que permite a sincronização das contas entre dispositivos e a recuperação de acesso em caso de perda do smartphone. Essa abordagem equilibra



segurança com conveniência, sendo especialmente útil para usuários que utilizam múltiplos dispositivos ou que precisam de uma solução de recuperação mais robusta.

Instalação

Android

1. Abra a Google Play Store no seu dispositivo Android.
2. Pesquise por "Authy Authenticator" ou "Twilio Authy" na barra de busca.
3. Identifique o aplicativo publicado pela Twilio Authy Inc. e toque em "Instalar".
4. Aguarde a conclusão da instalação e abra o aplicativo.

iOS (iPhone/iPad)

1. Abra a App Store no seu iPhone ou iPad.
2. Busque por "Authy Authenticator" ou "Twilio Authy".
3. Localize o aplicativo oficial da Twilio Authy Inc. e toque em "Obter".
4. Confirme a instalação e abra o aplicativo após o download.

Configuração inicial da conta Authy

Diferente dos outros autenticadores, o Authy requer a criação de uma conta vinculada ao seu número de telefone celular. Isso é necessário para o funcionamento do backup em nuvem e da sincronização entre dispositivos. Ao abrir o aplicativo pela primeira vez, você será solicitado a inserir seu número de telefone com código do país (ex: +55 para Brasil). O Authy enviará um código de verificação via SMS ou chamada telefônica para confirmar o número. Após a verificação, você definirá uma senha ou biometria para proteger o aplicativo localmente.

Atenção: use um número de telefone celular que você controle permanentemente. O número é a base para a recuperação de conta e sincronização entre dispositivos.

Configuração no GLPI Peta

Passo a passo

1. Acesse o GLPI Peta em <https://glpi.petacorp.com.br/> e faça login com suas credenciais. No primeiro acesso após 11/08/2026, o sistema automaticamente redirecionará você para a tela de configuração do 2FA.
2. O sistema exibirá um QR Code para vinculação. Caso não seja redirecionado, navegue até as configurações de sua conta e ative a autenticação em dois fatores (2FA/MFA).
3. Abra o Authy no seu smartphone. Toque no ícone "+" ou em "Add Account" (Adicionar conta).



4. Selecione a opção "Scan QR Code" (Escanear QR Code). A câmera será ativada.
5. Aponte a câmera para o QR Code exibido na tela do GLPI Peta. O Authy processará o código e adicionará a conta automaticamente.
6. Você pode personalizar o nome da conta (ex: "GLPI Peta") e escolher um ícone para facilitar a identificação.
7. Volte ao GLPI Peta e insira o código de 6 dígitos gerado pelo Authy para confirmar a vinculação.
8. Salve os códigos de backup (recovery codes) do GLPI em local seguro.

Recursos exclusivos do Authy

Backup criptografado em nuvem

O Authy sincroniza automaticamente todas as contas configuradas com a nuvem da Twilio, protegidas por criptografia. Isso significa que, ao instalar o Authy em um novo dispositivo e fazer login com seu número de telefone, todas as contas de autenticação estarão disponíveis imediatamente, sem necessidade de reconfiguração individual. O backup utiliza criptografia de ponta a ponta, garantindo que nem mesmo a Twilio tenha acesso às suas chaves secretas.

Múltiplos dispositivos

O Authy permite que você use o mesmo conjunto de contas de autenticação em vários dispositivos simultaneamente (smartphone, tablet, desktop). Essa funcionalidade é particularmente útil para profissionais que trabalham em diferentes estações ou que desejam ter um dispositivo de backup para gerar códigos. Cada dispositivo autorizado gera códigos independentes, mas sincronizados, para as mesmas contas.

Aplicação desktop

O Authy oferece uma aplicação para desktop (Windows, macOS e Linux) que permite gerar códigos diretamente no computador, sem necessidade de consultar o smartphone. Isso é extremamente conveniente para quem trabalha primariamente no computador e prefere não alternar entre dispositivos durante o login. A aplicação de desktop sincroniza automaticamente com a versão mobile através da conta Authy.

Dica: instale o Authy também no computador de trabalho. Ter os códigos disponíveis no desktop agiliza o processo de login e evita interrupções para consultar o smartphone.

SOLUÇÃO DE PROBLEMAS

Mesmo com uma configuração correta, situações inesperadas podem ocorrer durante o uso do MFA. Esta seção apresenta os problemas mais comuns relatados por



usuários e suas soluções detalhadas, permitindo que você resolva a maioria das situações sem necessidade de contatar o suporte técnico.

Código de verificação não funciona

Se o código de 6 dígitos gerado pelo autenticador é rejeitado pelo GLPI Peta, as causas mais prováveis são problemas de sincronização de horário ou erro de digitação. O protocolo TOTP depende de que o relógio do dispositivo e o do servidor estejam sincronizados com precisão. Uma diferença de mais de 30 segundos pode resultar em códigos inválidos.

Solução

1. Verifique se o relógio do seu smartphone está configurado para atualização automática (fuso horário e horário de rede). Em Android, vá em Configurações > Sistema > Data e hora > Ativar "Data e hora automáticas". Em iOS, vá em Ajustes > Geral > Data e hora > Ativar "Ajustar automaticamente".
2. Certifique-se de digitar o código exatamente como aparece, sem espaços ou caracteres adicionais. Códigos TOTP são exclusivamente numéricos.
3. Se o código está prestes a expirar (indicador circular quase no final), aguarde o próximo código antes de inserir. Nunca use códigos expirados.
4. Tente reiniciar o aplicativo autenticador e gerar um novo código.

Perda ou troca de smartphone

A perda, roubo ou troca do smartphone é uma das situações mais críticas relacionadas ao MFA, pois o dispositivo é o segundo fator de autenticação. A abordagem para recuperação varia conforme o aplicativo utilizado e as medidas preventivas adotadas.

Com códigos de backup (todos os apps)

Use um dos códigos de backup (recovery codes) que você salvou durante a configuração inicial. Cada código de backup geralmente pode ser usado apenas uma vez. Após usar um código de backup para fazer login, configure o MFA novamente no novo dispositivo e gere novos códigos de backup.

Com Microsoft Authenticator

Se você ativou o backup em nuvem, instale o Microsoft Authenticator no novo dispositivo, faça login com sua conta Microsoft e restaure o backup. Todas as contas configuradas serão recuperadas automaticamente, sem necessidade de reconfiguração individual.

Com Authy



Instale o Authy no novo dispositivo e faça login com seu número de telefone. Após a verificação de identidade, todas as contas sincronizadas estarão disponíveis imediatamente, pois o Authy mantém backup criptografado em nuvem por padrão.

Sem nenhuma opção de recuperação

Se você não possui códigos de backup, não ativou backup em nuvem e perdeu o dispositivo, será necessário contatar o administrador do sistema GLPI Peta para desativar temporariamente o MFA da sua conta e reconfigurar do zero (*veja detalhes na sessão 7 deste documento: Contato com o suporte*). Este processo envolve verificação de identidade adicional por parte da equipe de TI.

Atenção: sempre salve os códigos de backup em local seguro (gerenciador de senhas, cofre físico) e ative backup em nuvem quando disponível. Isso evita situações de bloqueio irreversível.

O aplicativo não gera códigos

Se o aplicativo autenticador não está gerando códigos ou a conta do GLPI não aparece na lista, isso pode indicar que a vinculação foi perdida ou corrompida. As possíveis causas incluem atualização do aplicativo que resetou dados locais, limpeza de cache do sistema operacional, ou falha durante o escaneamento do QR Code original.

Solução

1. Verifique se a conta do GLPI Peta ainda aparece na lista do autenticador. Se não aparecer, será necessário reconfigurar a vinculação.
2. Para reconfigurar, faça login no GLPI Peta usando um código de backup, vá até as configurações de MFA e desative/reactive a autenticação em dois fatores. Isso gerará um novo QR Code.
3. Escaneie o novo QR Code com o autenticador para restabelecer a vinculação.
4. Se o problema persistir, tente desinstalar e reinstalar o aplicativo autenticador, depois reconfigure a conta.

Erro de sincronização de horário

O TOTP é sensível à sincronização temporal. Se o horário do seu dispositivo está dessincronizado com o servidor, os códigos gerados serão diferentes dos esperados pelo servidor, resultando em falha de autenticação mesmo que o código pareça correto.



Solução

1. Android: Vá em Configurações > Sistema > Data e hora. Ative "Data e hora automáticas" e "Fuso horário automático". Se já estiverem ativos, desative e reative para forçar a resincronização.
2. iOS: Vá em Ajustes > Geral > Data e hora. Ative "Ajustar automaticamente". Se necessário, altere manualmente o fuso horário e volte ao automático.
3. Para verificação, compare o horário do dispositivo com um serviço de horário oficial como <https://time.is/>. A diferença deve ser inferior a 5 segundos.

BOAS PRÁTICAS DE SEGURANÇA

- Guarde os códigos de backup de cada serviço em um local seguro, como um gerenciador de senhas ou cofre físico.
- Nunca compartilhe os códigos de autenticação com outras pessoas.
- Mantenha o aplicativo autenticador atualizado.
- Ao trocar de celular, transfira suas contas antes de apagar o aparelho antigo, utilizando as funções de exportação ou backup disponíveis no aplicativo.

Dica: a prevenção é sempre mais rápida e menos estressante que a recuperação.

CONTATO COM O SUPORTE

Se nenhuma das soluções acima resolver o problema, contate a equipe de suporte técnico do GLPI Peta através do próprio sistema, utilizando o link <https://glpi.petacorp.com.br/Form/Render/6047> ou envie um e-mail para itsm@petacorp.com.br, fornecendo as seguintes informações para agilizar o atendimento: seu e-mail cadastrado no GLPI, descrição detalhada do problema, aplicativo autenticador utilizado, etapas já tentadas para resolver e, se possível, capturas de tela do erro.

LINKS DOS APLICATIVOS

Todos esses apps são gratuitos e oferecem autenticação em dois fatores (2FA) para proteger suas contas online.

Google Authenticator

iOS: <https://apps.apple.com/us/app/google-authenticator/id388497605>



Android:

<https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator>
2

Microsoft Authenticator

iOS: <https://apps.apple.com/us/app/microsoft-authenticator/id983156458>

Android: <https://play.google.com/store/apps/details?id=com.azure.authenticator>

Twilio Authy Authenticator

iOS: <https://apps.apple.com/us/app/twilio-authy/id494168017>

Android: <https://play.google.com/store/apps/details?id=com.authy.authy>

GLOSSÁRIO

Autenticação biométrica: verificação de identidade via Face ID, impressão digital ou reconhecimento de íris. No contexto do manual, é usada como camada extra de proteção no aplicativo autenticador antes de exibir os códigos.

Authenticator: software que gera códigos TOTP. Neste manual: Google Authenticator, Microsoft Authenticator e Twilio Authy.

Backup em nuvem: funcionalidade do Microsoft Authenticator e do Twilio Authy que criptografa e sincroniza as contas configuradas na nuvem, permitindo restaurá-las em um novo dispositivo.

Chave secreta: sequência alfanumérica compartilhada entre o servidor (GLPI Peta) e o aplicativo autenticador no momento do escaneamento do QR Code. É a base matemática para a geração dos códigos TOTP.

Código de verificação: código TOTP de 6 dígitos exibido pelo aplicativo autenticador, válido por 30 segundos. Deve ser inserido na tela de login do GLPI Peta após a senha.

Códigos de backup: conjunto de códigos de uso único (geralmente 10) fornecidos pelo GLPI Peta durante a configuração do 2FA. Permitem acesso emergencial caso o smartphone seja perdido ou danificado.

GLPI: plataforma de gerenciamento de ativos de TI e service desk de código aberto. O GLPI Peta (<https://glpi.petacorp.com.br/>) é a instância utilizada pela Peta.

MFA: método de segurança que exige dois ou mais fatores de verificação de identidade para conceder acesso a um sistema.



Push notification: notificação enviada pelo servidor ao dispositivo do usuário solicitando aprovação ou negação de um login. Disponível no Microsoft Authenticator para contas do ecossistema Microsoft (não aplicável ao GLPI Peta com TOTP).

QR Code: código bidimensional usado para transmitir a chave secreta TOTP do servidor para o aplicativo autenticador de forma visual, sem digitação manual.

RFC 6238: documento de padronização da IETF que define o algoritmo TOTP. Especifica como gerar senhas de uso único baseadas em tempo a partir de uma chave secreta compartilhada.

Sincronização temporal: alinhamento do relógio do dispositivo com o horário de rede (NTP). Essencial para o funcionamento correto do TOTP, pois códigos dessincronizados serão rejeitados pelo servidor.

TOTP: senha de uso único baseada em tempo (RFC 6238). Algoritmo que gera códigos numéricos de 6 dígitos a cada 30 segundos, usando uma chave secreta compartilhada e o relógio do sistema.

2FA: caso específico do MFA com exatamente dois fatores (ex.: senha + código TOTP). É o que está obrigatório no GLPI Peta.

REFERÊNCIAS

GLPI — Documentação oficial

- GLPI NETWORK. **Documentation.** Disponível em: <https://glpi-project.org/documentation/>.
- GLPI INSTALL. **Documentação sobre configuração de 2FA/TOTP no GLPI.** Disponível em: <https://glpi-install.readthedocs.io/>.

Google Authenticator — Documentação oficial

- GOOGLE. **Fazer login com a verificação em duas etapas.** Disponível em: <https://support.google.com/accounts/answer/1066447>.

Microsoft Authenticator — Documentação oficial

- MICROSOFT. **Informações sobre o aplicativo Microsoft Authenticator.** Disponível em: <https://support.microsoft.com/pt-br/account-billing/info-about-the-microsoft-authenticator-app>.

NIST SP 800-63B — Digital Identity Guidelines

- JANSEN, W.; SCARFONE, K. **Digital Identity Guidelines: Authentication and Lifecycle Management.** NIST, 2024. Disponível em: <https://pages.nist.gov/800-63-3/sp800-63b.html>.

RFC 4226 — HOTP

- M'RAIHI, D. et al. **RFC 4226: An HMAC-Based One-Time Password Algorithm.** IETF, dez. 2005. Disponível em: <https://datatracker.ietf.org/doc/html/rfc4226>.

RFC 6238 — TOTP

- M'RAIHI, D. et al. **RFC 6238: TOTP: Time-Based One-Time Password Algorithm.** IETF, maio 2011. Disponível em: <https://datatracker.ietf.org/doc/html/rfc6238>.

Twilio Authy — Documentação oficial



- TWILIO. **Authy Help**. Disponível em: <https://authy.com/help/>.

Verizon — Data Breach Investigations Report (DBIR)

- VERIZON. **Data Breach Investigations Report (DBIR)**. Disponível em: <https://www.verizon.com/business/resources/reports/data-breach-investigations-report/>.

