Política de Segurança da Informação

Como o OperSyncro protege o acesso ao sistema e os dados de empresas, obras e colaboradores.

Documento	Política de Segurança da Informação do OperSyncro
Abrangência	Site opersyncro.com.br, aplicativo em app.opersyncro.com.br e serviços de apoio
Responsável pelo sistema	OperSyncro - identificação completa a completar após a formalização da empresa (CNPJ)
Contato de segurança	A completar após a formalização da empresa (CNPJ)
Versão	BETA
Vigência	BETA - aguardando CNPJ

Versão BETA - aguardando CNPJ: os dados de identificação da empresa (razão social, CNPJ, endereço e contato oficial) ficam sem preenchimento até a formalização. A data de vigência definitiva será indicada quando o CNPJ for emitido.

1. Objetivo e escopo

Esta política define as medidas de segurança adotadas pelo OperSyncro para proteger a confidencialidade, a integridade e a disponibilidade das informações tratadas no sistema. Ela vale para o site, para o aplicativo usado por administradores, executores e usuários básicos, e para os serviços que sustentam o funcionamento do sistema.

A política se aplica a todos os dados cadastrados e gerados no uso do sistema, incluindo dados de empresas, obras e colaboradores, registros de presença, documentos e prazos de saúde ocupacional, mensagens internas e registros de auditoria. Ela complementa a Política de Privacidade e deve ser lida junto com ela.

2. Princípios

- **Menor privilégio:** cada usuário acessa somente as empresas, as obras e as funções de que precisa para o seu trabalho.
- **Segurança desde a concepção:** novas funções nascem com controle de acesso e registro de auditoria, e não recebem esses controles depois.
- **Defesa em camadas:** nenhuma proteção depende de uma única barreira; acesso, criptografia, auditoria e revisão se somam.
- **Preservação do que funciona:** correções de segurança não substituem mecanismos em funcionamento sem decisão expressa do responsável pelo sistema.
- **Responsabilidade compartilhada:** o OperSyncro protege a plataforma; cada empresa e cada usuário protegem suas credenciais e dispositivos.

3. Responsabilidades

Papel	Responsabilidades de segurança
Responsável pelo sistema (Master)	Administra a plataforma, concede e revoga acessos de maior privilégio, aprova mudanças relevantes de segurança, atende a incidentes e mantém esta política atualizada.
Administrador da empresa (CLIENT_ADMIN)	Administra os usuários e os dados da própria empresa, concede acessos dentro do seu escopo e comunica ao responsável pelo sistema qualquer uso suspeito.
Administradores	Usam somente as permissões liberadas no seu perfil, uma a uma, e respondem pelas ações feitas com a sua conta.
Executores	Operam as obras atribuídas, registram presença e movimentações e protegem o dispositivo usado no canteiro.
Usuários básicos	Acessam a interface simplificada apenas com as ações liberadas para o seu perfil e para as suas obras.
Empresas clientes	Indicam quem pode ser cadastrado, mantêm atualizada a lista de responsáveis e pedem a revogação imediata do acesso de quem sair da empresa ou mudar de função.

Não há, neste momento, um encarregado de proteção de dados (DPO) formalmente nomeado. Pedidos e comunicações sobre segurança e proteção de dados são tratados pelo responsável pelo sistema, pelo contato da primeira página.

4. Controle de acesso e autenticação

O acesso ao OperSyncro é individual e protegido por credencial. Não existem contas compartilhadas: cada login identifica uma pessoa, e as ações feitas no sistema ficam vinculadas a ela no registro de auditoria.

- **Senha individual:** o acesso principal é por senha pessoal. A senha é guardada de forma protegida no servidor e nunca é exibida em tela nem enviada por e-mail pelo sistema.
- **Reconhecimento facial como opção:** quando habilitado para o usuário, o acesso facial funciona como forma adicional de entrada, com as proteções descritas na seção 5.
- **Perfis e permissões:** as funções são liberadas por perfil e por permissão. Funções sensíveis, como limpar a base de uma empresa, ficam desligadas por padrão e só são liberadas de forma expressa.
- **Isolamento por empresa e obra:** o usuário enxerga apenas as empresas liberadas no seu perfil e as obras do seu escopo. Sem empresa liberada, nenhum dado de empresa é exibido.
- **Sessão controlada:** a sessão identifica o usuário durante o uso e é encerrada ao sair do sistema, sem apagar o registro das ações anteriores.
- **Recuperação de acesso:** pedidos de redefinição de senha seguem fluxo controlado pelo responsável pelo sistema, com entrega do código por canal externo ao aplicativo.
- **Funções em implantação:** módulos não liberados ficam bloqueados por configuração para todos os perfis, incluindo o Master, até a liberação expressa.

5. Biometria facial

O OperSyncro usa reconhecimento facial como opção de acesso e de registro de presença. O funcionamento foi desenhado para não transformar o rosto em uma senha reutilizável:

- **Template, não foto solta:** no cadastro, o sistema gera um vetor numérico de 512 dimensões (template biométrico) a partir do rosto. É esse vetor, e não uma senha derivada da imagem, que é comparado nas verificações seguintes.
- **Proteção do template:** os templates são mantidos no servidor, com acesso restrito aos serviços que fazem a comparação, e não são exibidos nas telas do sistema.
- **Limiares de decisão:** a entrada por reconhecimento facial e o registro de presença usam limiares próprios de similaridade, mais exigentes no acesso ao sistema do que no registro de presença.
- **Travas contra falso aceite:** a decisão não depende de uma única captura. O sistema exige consenso entre capturas, margem mínima sobre o segundo colocado e recusa a verificação quando as capturas são insuficientes.
- **Motor atual:** a detecção e a comparação usam modelos executados para essa finalidade (detecção YuNet e representação AdaFace 512D). A troca do motor biométrico depende de decisão expressa do responsável pelo sistema.
- **Uso limitado:** o template é usado somente para confirmar a identidade dentro do OperSyncro. Ele não é vendido, compartilhado para publicidade ou usado para identificar pessoas fora do sistema.
- **Exclusão:** quando o cadastro do colaborador ou do usuário é encerrado, o template associado pode ser excluído a pedido da empresa ou do titular, observado o registro necessário para auditoria.

Como todo sistema biométrico, o reconhecimento facial tem margem de erro. Por isso ele convive com o acesso por senha e com a revisão humana: uma recusa do reconhecimento não bloqueia o trabalho, e um aceite suspeito pode ser verificado no registro de auditoria.

6. Criptografia e proteção de dados

- **Em trânsito:** toda a comunicação entre o navegador ou o aplicativo e os servidores do OperSyncro é feita por conexão segura (HTTPS/TLS), incluindo login, cadastros, fotos e registros de presença.
- **Em repouso:** os dados ficam armazenados nos serviços de nuvem descritos na seção 7, com as proteções de armazenamento da plataforma. Credenciais de serviços integrados, como a senha do servidor de e-mail, são guardadas cifradas, e não em texto puro.
- **Segredos fora do código:** chaves e senhas de infraestrutura são mantidas em gerenciador de segredos da nuvem, e não no código-fonte nem em arquivos do aplicativo.
- **Dados sensíveis com acesso restrito:** dados de saúde ocupacional, como datas e resultados ligados ao Atestado de Saúde Ocupacional (ASO), e dados biométricos têm acesso limitado aos perfis e às obras que precisam deles. Avisos de vencimento são enviados aos responsáveis pela obra, e não ao colaborador, quando essa é a regra do evento.
- **Minimização:** o sistema pede e mantém somente os dados necessários para a gestão da obra e para as obrigações trabalhistas acompanhadas pela empresa.

7. Infraestrutura e nuvem

O OperSyncro roda em infraestrutura de nuvem gerenciada. O aplicativo é servido pelo Google Cloud Run, com acesso público pelo domínio app.opersyncro.com.br por meio do Firebase Hosting, e os dados são mantidos no banco de dados em nuvem do Firebase (Firestore), sob as regras de segurança da plataforma.

- O acesso direto ao banco de dados é restrito aos serviços autorizados do sistema; as telas do aplicativo não acessam dados fora do escopo do usuário logado.
- Configurações sensíveis do servidor são espelhadas na nuvem para sobreviver a atualizações e reinícios, sempre na forma cifrada quando envolvem credenciais.
- Arquivos grandes necessários ao funcionamento, como o modelo de reconhecimento facial, são servidos pela mesma origem oficial do aplicativo, para evitar fontes externas não controladas.
- Atualizações de infraestrutura seguem o mesmo controle de versão e de publicação descrito na seção 11.

8. Registro, monitoramento e auditoria

O sistema mantém um registro de auditoria (log) das ações relevantes, como acessos, cadastros, alterações, transferências, exclusões e registros de presença, com identificação de quem fez a ação e de quando ela ocorreu.

- O log serve para rastrear a origem de cada registro, investigar divergências e atender a pedidos das empresas clientes sobre as suas próprias informações.
- O acesso ao log é restrito aos perfis de administração, dentro do escopo de cada empresa.
- Falhas de salvamento são sinalizadas ao usuário na tela, para que nenhum registro seja perdido em silêncio: o dado permanece no dispositivo até que o salvamento seja concluído ou tratado.
- Sinais de uso indevido, como acessos fora do padrão ou tentativas repetidas de entrada, devem ser comunicados ao responsável pelo sistema pelo contato de segurança.

9. Cópias de segurança, disponibilidade e continuidade

A disponibilidade do OperSyncro se apoia na infraestrutura em nuvem descrita na seção 7, que mantém o serviço com capacidade mínima ativa e escala conforme a demanda. Os dados gravados na nuvem permanecem disponíveis após atualizações do sistema e reinícios do serviço.

As empresas podem exportar as suas informações a partir das telas do sistema e devem manter as suas próprias cópias dos documentos trabalhistas que a lei exige guardar. Em caso de indisponibilidade prolongada, o responsável pelo sistema comunicará as empresas afetadas pelo canal de contato cadastrado, com a previsão de retorno quando ela existir.

10. Resposta a incidentes de segurança

Incidente de segurança é qualquer evento que comprometa, ou possa comprometer, o acesso ao sistema ou os dados nele tratados - por exemplo, uso de uma conta por outra pessoa, perda de um dispositivo com sessão aberta, acesso indevido a dados de uma empresa ou indisponibilidade causada por ataque.

Como o OperSyncro responde

- **1. Detecção e aviso:** o incidente pode ser percebido pelo monitoramento, pelo registro de auditoria ou pelo aviso de uma empresa ou usuário. Qualquer pessoa pode comunicar um incidente pelo contato de segurança indicado na primeira página.
- **2. Contenção:** a primeira medida é conter o problema - revogar acessos, encerrar sessões, trocar credenciais ou bloquear a função afetada.
- **3. Avaliação:** em seguida, são apurados quais dados, empresas e pessoas foram afetados e qual é o risco para os titulares.
- **4. Comunicação:** as empresas e os titulares afetados são comunicados quando o incidente puder gerar risco ou dano relevante. Quando a lei exigir, a Autoridade Nacional de Proteção de Dados (ANPD) também é comunicada, nos termos do artigo 48 da Lei Geral de Proteção de Dados Pessoais (LGPD - Lei n. 13.709/2018).
- **5. Correção e registro:** a causa é corrigida, a correção é verificada e o incidente fica registrado, com as medidas tomadas, para revisão desta política.

Quem perceber um incidente não deve tentar resolver por conta própria apagando registros: a preservação das evidências faz parte da resposta.

11. Desenvolvimento seguro e atualizações

- **Versionamento:** cada versão do sistema é identificada e registrada, e a versão em uso aparece no próprio aplicativo.
- **Testes antes de publicar:** mudanças passam por verificação técnica e por conferência no endereço oficial após a publicação, incluindo login, salvamento e sincronização.
- **Publicação controlada:** nenhuma versão entra no ar sem autorização do responsável pelo sistema.
- **Escopo fechado:** cada atualização corrige ou acrescenta o que foi aprovado. Mecanismos que funcionam, como o motor de reconhecimento facial e as regras de acesso, não são substituídos por uma correção de outro ponto.
- **Dependências:** bibliotecas e modelos usados pelo sistema são mantidos em versões identificadas, servidos a partir da origem oficial sempre que possível.

12. Uso aceitável e deveres dos usuários

- Não compartilhar a senha nem permitir que outra pessoa use a sua conta, inclusive por reconhecimento facial cadastrado em seu nome.
- Manter o celular, o tablet ou o computador de acesso com bloqueio de tela e sistema atualizado, e sair da conta ao terminar o uso em aparelho compartilhado.
- Cadastrar somente dados verdadeiros e de pessoas ligadas às obras da sua empresa. O sistema cruza cadastros com a base importada da empresa e exige uma obra real como destino.
- Não tentar acessar dados de outra empresa, outra obra ou outro perfil, nem usar o sistema para finalidade diferente da gestão das suas obras.
- Não extrair listas de colaboradores para uso fora do trabalho sem autorização da empresa responsável pelos dados.
- Comunicar de imediato ao administrador da empresa, ou ao responsável pelo sistema, qualquer perda de dispositivo, suspeita de uso da conta por terceiros ou erro que exponha dados de outra pessoa.

O descumprimento destes deveres pode levar à revogação do acesso, sem prejuízo das responsabilidades previstas em lei e no contrato com a empresa cliente.

13. Revisão, vigência e contato

Esta política está em versão BETA, aguardando o CNPJ, e vale por prazo indeterminado a partir da sua disponibilização. A vigência definitiva será formalizada quando o CNPJ for emitido. Ela será revisada quando houver mudança relevante no sistema, na infraestrutura ou na legislação, e sempre que um incidente mostrar a necessidade de uma nova medida. A versão vigente fica disponível para as empresas clientes e, quando publicada no site, substitui a anterior.

Dúvidas, pedidos e comunicações de segurança devem ser enviados ao responsável pelo sistema do OperSyncro, pelo contato de segurança indicado na primeira página - a completar após a formalização da empresa (CNPJ).

Documentos relacionados	Política de Privacidade do OperSyncro (LGPD) - documento complementar, que descreve os dados coletados, as finalidades e os direitos dos titulares.
Base legal principal	Lei n. 13.709/2018 (LGPD), especialmente os artigos 46 (segurança), 47 (sigilo) e 48 (comunicação de incidente).

Versão BETA - aguardando CNPJ.

OperSyncro
Responsável pelo sistema - identificação a completar após a formalização (CNPJ)