

PACKS SERVIÇOS EM INFRAESTRUTURA DE TI



Pack
**PROTEÇÃO DE DADOS
É COISA SÉRIA**

COMO VOCÊ PROTEGE OS DADOS DA SUA EMPRESA?

- Usa um antivírus gratuito?
- Se tiver algo suspeito chama o pessoal do TI?
- Reza para não clicar em nada errado?



A FunctionOne tem três pacotes de segurança definitiva para sua empresa:



NÍVEL BÁSICO

Ativação das configurações básicas de segurança do ambiente
Microsoft 365

NÍVEL INTERMEDIÁRIO

Ativação de configurações de segurança do ambiente **Microsoft 365** para empresas que possuem pelo menos o plano 1 do **Azure AD Premium**.

NÍVEL AVANÇADO

Ativação de configurações avançadas de segurança do ambiente
Microsoft 365

Controles avançados de acesso / Monitoramento constante do ambiente de nuvem / Gestão de acessos / Monitoramento de informações enviadas para externos / Segurança de e-mails / Anti-Spam / Anti-phishing / Anti-Malware /

Pack PROTEÇÃO DE DADOS É COISA SÉRIA

ESCOPO

- Configuração da política de complexidade e expiração de senhas ;
- Configurar acesso administrativo por funções;
- Habilitar padrões de Segurança do Azure Active Directory;
- Configurar a Integridade do serviço do Portal Admin Center;
- Configuração do centro de mensagens do Portal Admin Center;
- Configuração de acesso anônimos em reuniões do Teams;
- Configuração de acesso externo ao SharePoint Online e OneDrive;
- Configuração do serviço de Anti-Spam de entrada e saída com regras padrão;
- Configuração do serviço de Anti-phishing com regras padrão;
- Configuração do serviço de Anti-Malware com regras padrão;
- Configuração das políticas de alerta no Painel de conformidade;
- Ativação dos logs de auditoria do Painel de Conformidade do Microsoft 365;
- Configuração do serviço de autenticação Multi-Fator para todos os usuários.
- Configuração do acesso condicional para controle de login dos usuários (Até 3 políticas) ;
- Ativação do serviço de Password Write Back (Para ambientes configurados com Azure AD Connect)
- Ativação do portal Self Service Password Reset
- Orientação sobre acesso e consulta dos logs de auditoria do Azure Active Directory
- Orientação e criação de grupos de acesso dinâmico (Até 5 grupos)
- Configuração de 1 política de Prevenção Contra Perda de Dados para RG, CPF e CNPJ
- Configuração de uma política de Anexos Seguros.
- Configuração de uma política de Links Seguros.
- Configuração dos rótulos de Confidencialidade para proteger e-mails e documentos (Configuração de 4 rótulos de confidencialidade).
- Orientação para baixar o Cliente dos rótulos de Confidencialidade.
- Orientação para utilizar o Cliente dos rótulos de Confidencialidade.
- Ativação do Microsoft 365 no Cloud app Security.
- Configuração das métricas do Microsoft 365 no Cloud app Security.
- Configuração do relatório de dados no Cloud app Security.



PACKS SERVIÇOS EM INFRAESTRUTURA DE TI

PREMISSAS

Até 300 usuários

- Já possuir um Tenant do Microsoft 365 configurado e funcional, com os usuários provisionados no Azure AD ;
- Possuir licenças básicas do Azure Active Directory ;
- Sem configuração do Windows Defender;
- Possuir licenças do Azure Active Directory Premium (Plano 1) ;
- Requisito mínimo para o Azure Write Back – Nível funcional de domínio Windows Server 2016;
- Possuir licenças do Microsoft Defender for Office 365;
- Licenças que contemplem rótulos de confidencialidade e Cloud App Security.