1. Introdução

A Connecta Contabilidade lida diariamente com o ativo mais crítico de seus clientes: seus dados financeiros e pessoais (CPFs, CNPJs, balanços, declarações fiscais).

Um incidente de segurança, como um vazamento de dados ou um ataque de ransomware, não resultaria apenas em prejuízo financeiro, mas em uma quebra de confiança irreparável.

Este documento estabelece um conjunto fundamental de políticas de segurança. Elas não são projetadas para burocratizar, mas para criar uma linha de base de defesa que proteja a reputação da Connecta, a privacidade de seus clientes e a continuidade de seus negócios.

2. Política de Acesso e Controle de Usuários

Objetivo: Garantir que apenas pessoas autorizadas acessem as informações e que elas acessem apenas o que é necessário para seu trabalho.

2.1 Política 1.1 – Identificação Única e Intransferível

Diretriz: Cada funcionário receberá uma conta de usuário (login) única e pessoal para todos os sistemas (computador, e-mail, sistema contábil). O compartilhamento de senhas ou contas (ex: "atendimento@") é estritamente proibido.
Justificativa: *Rastreabilidade e responsabilização.* Caso uma ação indevida ocorra, é necessário identificar quem a executou. Contas compartilhadas impossibilitam auditorias e diluem a responsabilidade individual.

2.2 Política 1.2 – Senhas Fortes e Autenticação Multifator

Diretriz: Senhas devem conter no mínimo 12 caracteres. Além disso, a Autenticação Multifator (MFA) — como um código recebido por SMS ou aplicativo autenticador — é obrigatória para todos os serviços expostos à internet (e-mail, acesso à nuvem, VPN).
Justificativa: *Proteção contra invasões.* Estudos apontam que 99% dos ataques de roubo de credenciais são frustrados pelo uso do MFA. Mesmo que a senha de um funcionário vaze, o invasor não conseguirá logar sem o segundo fator (o celular do funcionário).

2.3 Política 1.3 – Princípio do Menor Privilégio

Diretriz: Cada funcionário terá acesso apenas aos arquivos e sistemas estritamente necessários para o desempenho de suas funções. Um analista júnior, por exemplo, não terá acesso às pastas da diretoria ou de clientes de outro analista, salvo autorização expressa.
Justificativa: *Contenção de danos.* Caso a conta de um funcionário seja

comprometida, o acesso limitado impede que o invasor obtenha dados sensíveis de toda a empresa.

2.4 Política 1.4 – Processo de Desligamento

Diretriz: No último dia de trabalho de um funcionário, todas as suas contas de acesso (e-mail, sistemas, VPN) devem ser desativadas ou revogadas até o final do expediente.
Justificativa: *Prevenção de acessos indevidos.* A desativação imediata evita possíveis ações maliciosas de ex-funcionários ou o uso indevido de contas inativas.

3. Política de Uso de Dispositivos Móveis e Redes

Objetivo: Proteger os dados da empresa quando estes saem do perímetro físico do escritório (em notebooks e celulares), além de proteger a rede interna contra dispositivos inseguros.

3.1 Política 2.1 – Dispositivos Pessoais (BYOD – Bring Your Own Device)

Diretriz: É permitido o uso de smartphones pessoais para acessar o e-mail e o calendário corporativo, desde que o dispositivo:
(a) Tenha senha de bloqueio (PIN ou biometria) ativa;
(b) Esteja com o sistema operacional atualizado; e
(c) Possua software de gerenciamento (MDM) que permita à Connecta apagar dados corporativos remotamente em caso de perda ou roubo.
Justificativa: *Mitigação de vazamento físico.* O maior risco em dispositivos móveis é a perda ou roubo. A capacidade de apagar e-mails e dados remotamente evita o vazamento de informações de clientes.

3.2 Política 2.2 – Redes Wi-Fi Seguras e VPN

Diretriz: É proibido conectar notebooks corporativos a redes Wi-Fi públicas (aeroportos, cafés, hotéis) sem o uso de uma VPN fornecida pela empresa.
Justificativa: *Proteção contra interceptação.* Em redes públicas, invasores podem "escutar" o tráfego e interceptar dados sensíveis. A VPN cria um túnel criptografado, tornando as comunicações ilegíveis para terceiros.

3.3 Política 2.3 – Segmentação da Rede Interna

Diretriz: O escritório manterá duas redes Wi-Fi distintas:

1. **CONNECTA_CORP – para notebooks e servidores da empresa.**
2. **CONNECTA_VISITANTE – para celulares pessoais e dispositivos de visitantes.**
   As duas redes não devem se comunicar entre si.
   Justificativa: *Isolamento de risco.* Caso um dispositivo pessoal seja infectado, o malware não poderá se propagar para os sistemas corporativos.

4. Diretrizes para Resposta a Incidentes de Segurança

Objetivo: Definir um plano de ação claro para quando um incidente ocorrer, minimizando o pânico, o tempo de inatividade e os danos financeiros.

4.1 Diretriz 3.1 – Relate Imediatamente (Sem Culpa)

Diretriz: Qualquer funcionário que suspeitar de incidente — como clicar em link suspeito, receber e-mail de phishing ou notar atividade anormal — deve reportar imediatamente ao gestor ou responsável de TI. A política é de "não culpabilização"; o foco é a resposta rápida.
Justificativa: *Tempo é fator crítico.* Atrasar o relato pode transformar um incidente isolado em um ataque generalizado.

4.2 Diretriz 3.2 – Conter e Isolar o Dispositivo

Diretriz: Ao identificar um dispositivo comprometido, deve-se desconectá-lo da rede (remover cabo ou desligar Wi-Fi), mas não desligar o computador.
Justificativa: *Preservação de evidências.* Manter o equipamento ligado preserva dados na memória RAM, essenciais para investigação.

4.3 Diretriz 3.3 – Comunicação Controlada

Diretriz: Em incidentes graves (como vazamento de dados), apenas o sócio/diretor designado será o porta-voz oficial. Nenhum outro funcionário deve comunicar o ocorrido a clientes ou parceiros.
Justificativa: *Evita pânico e desinformação.* A comunicação deve ser precisa, controlada e, se necessário, orientada juridicamente.

5. Política de Backup e Recuperação de Desastres

Objetivo: Garantir que a Connecta Contabilidade possa restaurar seus dados e retomar suas operações rapidamente após eventos críticos (ataque de ransomware, incêndio, falha física etc.).

5.1 Política 4.1 – Regra de Ouro "3-2-1"

Diretriz: Todos os dados críticos seguirão a regra 3-2-1:

- **3 cópias dos dados;**
- **2 mídias diferentes (ex: servidor local + HD externo);**
- **1 cópia fora do local (off-site), preferencialmente em nuvem segura.**
  Justificativa: *Padrão de mercado.* Protege contra falhas de hardware, desastres físicos e ataques cibernéticos.

5.2 Política 4.2 – Backup de Dados em Nuvem

Diretriz: Além dos backups locais, será contratado serviço específico de backup para e-mails e arquivos em nuvem (Microsoft 365 / Google Workspace).
Justificativa: *Prevenção contra exclusão acidental.* Fornecedores de nuvem

garantem disponibilidade, mas não recuperação de dados apagados pelo usuário.

5.3 Política 4.3 – Testes de Restauração Periódicos

Diretriz: Trimestralmente, o responsável pela TI deve realizar testes de restauração, recuperando arquivos de exemplo para validar o processo. Justificativa: *Confiabilidade do backup.* Backups não testados são inúteis em emergências reais.

6. Nota Final dos Consultores

A implementação dessas políticas representa apenas o primeiro passo para uma postura de segurança robusta. O sucesso deste plano depende de duas ações contínuas:

1. **Investimento em Ferramentas: Aquisição de soluções adequadas (MFA, software de backup, VPN).**
2. **Treinamento Contínuo: Funcionários devem compreender as políticas e receber treinamentos anuais sobre phishing, boas práticas e uso seguro de senhas.**