RELATÓRIO DE SEGURANÇA E AUDITORIA DE SISTEMAS

Empresa: Jaguara SAS

Data: [16/06/2025]

Responsável pelo Relatório: [João Pedro, Lucas Ciacci, Ingryd, Victor, Vinícius, Matheus]

# 1. Infraestrutura Tecnológica – Inventário Geral

Foi realizado um levantamento técnico do ambiente de tecnologia da informação da empresa. Identificaram-se os seguintes ativos:

| Nome do Equipamento | Categoria | Domínio | Observações | Quantidade |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| Notebooks | Hardware | TI | SO: Windows | 8 |
| Modem | Rede | TI | Vivo | 1 |

**Pontos de atenção**:

* Racks abertos e desorganizados.
* Cabeamento exposto e mal acondicionado.
* Falta de servidor dedicado para arquivos.
* Ausência de controle de acesso físico aos equipamentos.
* Equipamentos de rede e elétricos em instalações improvisadas.

# 2. Vulnerabilidades Identificadas

As ameaças foram identificadas a partir de análises diretas no ambiente, cruzadas com as respostas dos formulários e observações feitas in loco. A responsabilidade pelo levantamento de dados foi da equipe de auditoria de segurança da informação do projeto.

**Principais vulnerabilidades e impactos:**

| **Processo / Recurso** | **Vulnerabilidade** | **Impacto Potencial** |
| --- | --- | --- |
| Controle de acesso ao sistema | Compartilhamento de senhas | Vazamento de dados e acessos não autorizados |
| Gerenciamento de senhas | Senhas fracas e reutilizadas | Invasão de sistemas via ataques de força bruta |
| Desativação de contas | Falta de alinhamento entre RH e TI | Ex-funcionários com acesso ativo |
| Infraestrutura física | Equipamentos e cabeamentos expostos | Danos físicos e acesso não autorizado |
| Estações de trabalho | Computadores desbloqueados e desatendidos | Uso indevido de sistemas |
| Armazenamento e backup | Sem rotina centralizada de backup | Perda irreversível de dados |
| Logs e auditoria de sistemas | Falta de logs detalhados | Dificuldade em identificar responsáveis |
| Acesso de terceiros (desenvolvedora) | Acesso total ao código-fonte e banco de dados | Vazamento de informações estratégicas |

# 3. Sugestões de Correções

Para mitigar e corrigir as vulnerabilidades levantadas, recomenda-se:

* **Controle de senhas:** Implantar política obrigatória de senhas fortes e autenticação multifator.
* **Desativação de contas:** Criar fluxo automatizado entre RH e TI para exclusão imediata de acessos.
* **Segurança física:** Trancar racks, reorganizar cabeamento e restringir o acesso a áreas críticas.
* **Estação de trabalho:** Configurar bloqueio automático de tela após 5 minutos de inatividade.
* **Backups:** Implementar backup automático diário e testes de restauração periódicos.
* **Monitoramento:** Ativar logs de sistema e implementar ferramentas SIEM para análise em tempo real.
* **Acesso de terceiros:** Revisar contratos e limitar o acesso externo com autenticação controlada.

# 4. Oportunidades de Melhoria da Infraestrutura Tecnológica

Além das correções necessárias, existem oportunidades que trarão maior segurança e eficiência:

* **Aquisição de servidor dedicado** para armazenamento e backup de dados.
* **Implantação de firewall e VPN** para proteção de tráfego de rede.
* **Capacitação dos colaboradores** com treinamentos regulares sobre boas práticas.
* **Implementação de um rack de rede fechado** com controle de acesso físico.
* **Padronização do parque tecnológico**, reduzindo riscos e otimizando a manutenção.

# 5. Sugestão de Política de Segurança da Informação

A política de segurança da informação da empresa deve conter as seguintes diretrizes:

* **Controle de Acesso:** Acesso individual e intransferível a todos os sistemas.
* **Gestão de Senhas:** Exigir senhas complexas, trocas periódicas e impedir reutilização.
* **Classificação da Informação:** Categorizar os dados por criticidade e restringir acessos.
* **Proteção Física:** Proteger fisicamente os ativos de TI com acesso controlado.
* **Backups e Continuidade:** Realizar backups regulares e manter plano de recuperação de desastres.
* **Auditoria e Monitoramento:** Registrar e monitorar ações dos usuários nos sistemas.
* **Treinamento e Conscientização:** Treinamentos periódicos e campanhas internas.
* **Gestão de Incidentes:** Plano de resposta a incidentes com equipe responsável.

# 6. Conclusão

A empresa Jaguara SAS apresenta vulnerabilidades críticas que exigem ação imediata para garantir a segurança das suas operações. A implementação das soluções e políticas propostas elevará o nível de maturidade da segurança da informação e reduzirá significativamente os riscos técnicos e operacionais.