ELABORADOR/ APROVADOR		
RESPONSAVEL		**DATA**
ELABORADOR	Luc Salmon	25/02/2021
APROVADOR	Henri Le Rasle	26/02/2021

Histórico de revisão

Versão	Date	Descrição
1.0	23/02/2021	Versão inicial

1 Introdução

O documento tem como objetivo apresentar a política de controle de acesso remoto, de forma a mitigar riscos e padronizar o uso remoto de sistemas.

2 Acceso Remoto

Este documento trata do acesso remoto à produção do cliente e aos sistemas e aplicativos de computador da Ecritel para operações, departamentos de suporte e outros departamentos.

DEFINIÇÃO DE TRABALHO REMOTO : refere-se a todas as formas de trabalho fora do escritório, incluindo ambientes de trabalho não tradicionais, como aqueles referidos como: "ambientes de *telecommuting*", "local de trabalho flexível", "trabalho remoto" e "trabalho virtual".

1.1 Política de controle de acesso remoto

Apenas os três protocolos a seguir têm permissão para iniciar sessões de acesso remoto para fins de TI:

- RDP (Remote Desktop Protocol)
- SSH (Secure SHell)
- HTTPS (HyperText Transfer Protocol Secure)

O uso de qualquer outro protocolo é estritamente proibido.

1.2 Equipe técnica

Para ter acesso aos sistemas de produção da Ecritel ou de seus clientes, a equipe técnica deve utilizar uma VPN segura para ter acesso, a partir da qual podem se autenticar por SSH / RDP /HTTPS em qualquer sistema. Uma conta única está disponível para cada usuário.

1.3 Equipe de Apoio

Os membros da Equipe de Suporte não precisam acessar regularmente os Sistemas Ecritel remotamente, mas em circunstâncias atenuantes, eles podem fazê-lo. No caso que precisam, a equipe do suporte deve utilizar uma VPN segura para ter acesso, a partir da qual podem se autenticar por SSH / RDP / HTTPS em qualquer sistema que tenham acesso. Uma conta única está disponível para cada usuário.

1.4 Outros Departamentos

Aqueles que trabalham em outros departamentos não precisam de RDP ou acesso remoto aos sistemas Ecritel, pois podem trabalhar usando o Google Drive/Google Docs onde todo funcionário tem acesso, e um navegador da web.

1.5 Como Proteger as informações e Equipamentos

As informações acessadas remotamente são protegidas pelas configurações feitas nos computadores pelo dpto. Ti, e pela infraestrutura do Google. Usuários são responsáveis pelo uso apropriado do equipamento seguindo as próximas guias:

1. Sempre deixar o computador com tela travada quando não está em uso
2. Não usar o equipamento em local onde outros possam ver a tela
3. Não compartilhar o uso do equipamento da empresa com terceiros(inclui familiares)
4. Não deixar o equipamento desprotegido em locais públicos
5. Imediatamente avisar o dpto. Ti caso haja perca ou furto de equipamento
6. Manutenção e Suporte são dados pelo Dpto. Ti a través de email e Slack

1.6 Controle e segurança dos acessos remotos

Controle dos acessos aos sistemas Google e de Produção são feitos pelo Dpto. Ti. Acessos são distribuídos baseado em cargo dos funcionários.
Medidas de segurança são implementadas pelo Dpto. Ti, e descritas no procedimento de Ti Interno.
Os únicos com acesso aos sistemas de produção são o Dpto. Ti, e Tecnico. O acesso é feito através de uma VPN para garantir segurança.
Auditoria é feita nos Equipamentos de uso remoto