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

Este documento quando impresso ou salvo em local indevido é considerado Cópia Não Controlada.

1 Introdução

O propósito deste documento é explicar as políticas para gerenciamento de Contas, Identidade e Senhas.

2 IDENTIFICAÇÃO/CONTAS

Um identificador único deve ser atribuído para todos os usuários capazes de acessar componentes do ambiente do ISMS primariamente associado com infraestrutura de clientes e serviços de produção e gerenciamento (Servidores, equipamento de rede, aplicações ou interfaces administradoras e etc).

Nenhuma conta genérica deverá ser utilizada para administração dos sistemas e das bases de dados.

Em adição, somente contas nominativas providenciadas com rastreabilidade precisa deverão ser utilizadas nos sistemas e componentes de ISMS.

Finalmente, é estritamente proibido compartilhar usuários.

3 AUTENTICAÇÃO

Os métodos de autenticação são utilizados da maneira a seguir:

Sistemas / Aplicações	Mecanismo de Controle de Acesso	Método de Autenticação
VPN	Autenticação Local	Usuário + Senha
Firewall Cisco ASA	Autenticação Centralizada	Usuário + Senha
Switches	Autenticação Centralizada	Usuário + Senha
WAF Imperva	Autenticação Externa	Usuário + Senha + MFA
VSphere / VCenter / ESX	Autenticação Centralizada	Usuário + Senha
Windows Servers	Autenticação Local	Usuário + Senha
Linux Servers	Autenticação Centralizada	Usuário + Senha
DRAC	Autenticação Local	Usuário + Senha
AWS	Autenticação Externa	Usuário + Senha + MFA
New Relic	Autenticação Externa	Usuário + Senha

Esse documento é propriedade da Ecritel. Ele não pode ser reproduzido ou comunicado a terceiros sem prévia autorização.
Este documento quando impresso ou salvo em local indevido é considerado Cópia Não Controlada.
Ecritel do Brasil Ltda. Rua Abaçaí, 60 Brooklin Paulista, São Paulo CEP 04570-030 Brasil Tel.: +55 11 5505-0525 www.ecritel.com

DYN	Autenticação Externa	Usuário + Senha
Nagios	Autenticação Local	Usuário + Senha
CDN Services	Autenticação Externa	Usuário + Senha
DevOps Portals	Autenticação Centralizada	Usuário + Senha
Si Ecritel	Autenticação Centralizada	Usuário + Senha

4 COMPLEXIDADE DAS SENHAS

Para sistemas de produção e acesso de sistemas web:

De maneira a evitar acesso fraudulento através do descobrimento de senhas triviais ou com ataques de “força bruta”, senhas para acesso as contas para componentes ISMS devem cumprir as seguintes regras:

- O comprimento da senha deve ser maior ou igual a 10 caracteres;
- A senha deve ser complexa. No mínimo deve conter uma letra maiúscula, uma letra minúscula, um número e um caractere especial;
- A senha deve ser gerada randomicamente.

5 PROTEÇÃO DE CONTAS E SENHAS

Como forma de reforçar a proteção das contas e suas senhas, o seguintes mecanismos precisam ser implementados em todos os componentes e sistemas ISMS:

- Senhas padrões de equipamento devem sempre ser alteradas antes do equipamento ser colocado no ambiente de produção;
- As senhas dos usuários devem sempre ser renovadas no mínimo a cada 6 meses. Em sistemas de uso geral (ex. Google Drive) usuários são forçados a mudar sua senha seguindo as regras de senha segura do sistema AD.
- Novas senhas devem ser diferentes das senhas antigas;
- Após 6 tentativas de autenticação malsucedidas com uma conta, a mesma deve ser bloqueada automaticamente por pelo menos 30 minutos (quando este recurso estiver disponível).
- Qualquer sessão deverá ser suspensa após 15 minutos de inatividade. De maneira que o usuário deverá entrar com sua senha novamente de modo a recuperar a sessão quando este recurso esta disponível

Esse documento é propriedade da Ecritel. Ele não pode ser reproduzido ou comunicado a terceiros sem prévia autorização.
Este documento quando impresso ou salvo em local indevido é considerado Cópia Não Controlada.
Ecritel do Brasil Ltda. Rua Abaçaí, 60 Brooklin Paulista, São Paulo CEP 04570-030 Brasil Tel.: +55 11 5505-0525 www.ecritel.com

- A senha definida no momento de criação da conta ou renovação de senha deve ser aleatória, de uso único, e diferente entre os usuários. O usuário deverá alterar a senha após o seu primeiro uso

Em caso de suspeita de alguma senha frágil, deve ser feita a renovação imediatamente.

Se algum usuário solicitar a renovação de senha de modo remoto (telefone, e-mail, chamado, etc), a identidade do mesmo deve ser verificada antes da renovação.

Quando algo além das senhas é utilizado (token, chave, certificado), a senha deve ser atribuída a um usuário e não para o grupo do mesmo. Não deverá ser compartilhada por mais de uma pessoa e não pode ser usada para autorizar acesso pelo seu usuário.

6 TRANSMISSÃO E ARMAZENAMENTO DE SENHAS

Senhas devem ser armazenadas na forma de um KeePassX [AES 256bit] se armazenados localmente, ou na plataforma SI.

Na hora de mudar ou atribuir uma senha, o Dpto de Ti faz o procedimento em pessoa com o dono da conta em questão para evitar a transmissão de senhas pela internet. Se precisar fazer o procedimento a distância, pode enviar uma senha temporária por email usando KeePassX com senha de acesso por outro meio de comunicação.

7 DESATIVANDO SENHAS / CONTAS

As contas de funcionários que deixam a empresa devem ser revogadas imediatamente, o RH notifica o Dpto. Ti, fazendo um pedido de exclusão de contas por e-mail em antecedência do desligamento.

No caso onde tem uma senha ou conta comprometida, o Dpto. de Ti é o primeiro a ser avisado, pois ele tem habilidade de revogar contas ou trocar senhas.

8 CERTIFICADOS SSL

Informações relacionadas a certificados SSL estão na “INT-PL05-Politica de Controle de Criptografia”

9 RECUPERAÇÃO DE CHAVES PERDIDAS OU CORROMPIDAS

Recuperação de chaves não é feita em nenhum dos nossos sistemas. Quando uma chave é perdida ou corrompida, outra é gerada para tomar o seu lugar. Se a chave Administradora de um sistema importante e perdida, outra instância do sistema com uma chave nova e gerada para tomar seu lugar. Em casos onde a senha é armazenada externamente (ex. Google Drive) chave nova e gerada entrando em contato com a empresa caso recuperação de senha não seja possível.

Esse documento é propriedade da Ecritel. Ele não pode ser reproduzido ou comunicado a terceiros sem prévia autorização.
Este documento quando impresso ou salvo em local indevido é considerado Cópia Não Controlada.
Ecritel do Brasil Ltda. Rua Abaçaí, 60 Brooklin Paulista, São Paulo CEP 04570-030 Brasil Tel.: +55 11 5505-0525 www.ecritel.com