NOR-003 – Norma de Criação e Utilização de Senhas

Sumário

1. Objetivo

Estabelecer diretrizes, critérios, responsabilidades e procedimentos relacionados a criação e utilização de senhas, que permitem o gerenciamento e acesso para estações de trabalho, servidores, aplicativos e serviços em geral.

2. Âmbito de Aplicação

2.1. A presente norma aplica-se ào GRUPO LUFTe às empresas controladas ou a ela afiliadas, cada qual doravante individualmente designada “Empresa”.

2.2. As regras definidas neste documento aplicam-se a todas as estações de trabalho, servidores, aplicativos, dispositivos móveis e serviços que se relacionam com as Informações da Empresa, abrangendo as senhas para todos os tipos de contas, ou seja, contas do sistema, contas de Usuários, contas de serviço e qualquer outro tipo de conta necessária para acessar qualquer tipo de Informação.

3. Considerações Gerais

3.1. O conteúdo desta norma é propriedade da Empresa, e é destinado para uso interno. Para garantir que seja sempre considerada a versão mais atualizada, não é recomendado que este documento seja reproduzido, armazenado ou transmitido, em qualquer formato ou por quaisquer meios, sejam eletrônicos ou físicos.

3.2. O conteúdo desta norma deve ser conhecido e observado por todos os funcionários e terceiros que trabalhem internamente nos ambientes da empresa, sendo o seu descumprimento passível de aplicação de medidas legais e disciplinares.

3.3. Com o objetivo de proteger suas informações e validar se o comportamento de seus colaboradores está de acordo com a política e normas, ao GRUPO LUFT efetua o monitoramento de todos os ativos da informação e ativos de tecnologia.

3.4. Durante o monitoramento, ao GRUPO LUFT, sem qualquer notificação ou aviso poderá interceptar, registrar, ler, bloquear, redirecionar, retransmitir, copiar e divulgar a pessoas autorizadas qualquer tipo de informação relacionada ou contida nos recursos ou serviços de tecnologia da informação.

3.5. Em caso de dúvidas sobre a aplicação adequada das diretrizes constantes da presente norma, os Funcionários devem consultar o seu Gestor imediato e/ou a Área de Compliance.

3.6. A infração a esta norma estará sujeita às regras estabelecidas na Norma de Penalidades.

3.7. Os casos omissos serão decididos pelo Comitê de Conduta.

4. Vínculos

PS01 - Política de Segurança da Informação

5. Conceitos

5.1 Conta de Funcionário – Conta aberta em nome de um Funcionário no âmbito dos Recursos de Tecnologia da Informação da Empresa.

5.2 Conta de Terceiro – Conta aberta em nome de um Terceiro no âmbito dos Recursos de Tecnologia da Informação da Empresa, em decorrência da celebração de um Contrato e a pedido do respectivo Gestor do Contrato.

5.3 Conta de Usuário – Significa uma Conta de Funcionário ou uma Conta de Terceiro.

5.4 Senha de administrador – Senha de usuários privilegiados, isto é, que possuem acesso administrador a sistemas e ambientes da empresa e permissão de execução de tarefas críticas que podem comprometer a confidencialidade, disponibilidade e integridade de serviços e informações da a empresa.

5.5 Contrato – Significa, para fins deste instrumento normativo, todo e qualquer tipo de proposta, contrato, instrumento particular de aditamento, cessão e transferência, carta de renovação, distrato, termo, notificação, declaração, memorando de entendimentos, fatura, nota promissória, instrumentos de dívida, contratos, acordos ou atos societários, e assemelhados de quaisquer um destes itens, que envolve a Empresa, e que tenha sido devidamente formalizado e tenha força obrigacional.

5.6 Funcionário – Refere-se a todo e qualquer conselheiro, administrador, diretor e funcionário que compõe o quadro da Empresa.

5.7 Gestor da Conta de Usuário – É aquele que é o responsável por gerenciar as Informações ou Informações Confidenciais, bem como sua distribuição e autorizações de acesso para dada Conta de Usuário, sendo que no caso de uma Conta de Funcionário será o seu gestor imediato e no caso de uma Conta de Terceiro será o Gestor do Contrato.

5.8 Gestor do Contrato – Funcionário solicitante de um Contrato, o qual é responsável pela administração do respectivo objeto contratual, além da solicitação de abertura, manuseio e encerramento de uma Conta de Terceiro.

5.9 Informação – É todo e qualquer dado, informe, elemento, notícia, comunicação, material, instrução ou direção que sejam disponibilizados por escrito, oralmente ou de qualquer outra forma, gravados ou não com a expressão “confidencial”, em decorrência do desenvolvimento das atividades profissionais da Empresa.

5.10 Informação Confidencial – Constituem Informações Confidenciais:

a) Dados ou informações da Empresa (ainda que não sejam de propriedade da Empresa, mas que a Empresa tenha recebido em razão de uma oportunidade de negócio, por exemplo) ou desenvolvidos pela Empresa ou por Terceiro contratado pela Empresa, os quais o Funcionário venha a tomar conhecimento por qualquer forma, incluindo, mas não se limitando a, informações de natureza técnica, comercial, financeira, jurídica, estratégica, tecnológica, know-how, desenhos, modelos, dados, cadastros, especificações, relatórios, compilações, análises, previsões, estudos, reproduções, sumários, comunicados, fórmulas, patentes, dados financeiros e econômicos, informações relacionadas a clientes, fornecedores atuais ou potenciais,

operações financeiras, planos comerciais, demonstrações ou planos financeiros, estratégias de marketing e outros negócios, contratos, produtos existentes ou futuros e quaisquer outras informações de propriedade da Empresa reveladas em confiança para o Funcionário;

b) Outros dados ou informações necessárias para o exercício das funções do Funcionário relativos à Empresa, incluindo, mas não se limitando aos dados de natureza societária, objetivos de investimentos, estrutura jurídica e segredos de negócio;

c) Todas as anotações, análises, compilações, estudos, materiais ou quaisquer outros documentos elaborados pela Empresa e/ou por qualquer de seus Funcionários ou Terceiros contratados, que contenham ou reflitam de outra maneira Informações Confidenciais.

5.11 Recursos de Tecnologia da Informação ("TI") – São ferramentas de tecnologia da informação disponibilizadas ao Funcionário ou Terceiro para utilização a serviço da Empresa, tais como, mas não se limitando a: internet, intranet, rede corporativa com seus respectivos diretórios, correio eletrônico (e-mail), notebooks, computadores, impressoras, scanners, softwares e sistemas aplicativos.

5.12 Terceiro – Refere-se, mas não está limitado, a toda e qualquer pessoa física ou jurídica, que a Empresa se relacione ou venha a se relacionar, prestador de serviços, fornecedor, consultor, cliente, parceiro de negócio, terceiro contratado ou subcontratado, locatário, cessionário de espaço comercial, independentemente de contrato formal ou não, incluindo aquele que utiliza o nome da Empresa para qualquer fim ou que presta serviços, fornece materiais, interage com Funcionário Público, com o Governo ou com outros Terceiros em nome da Empresa.

5.13 Usuário – Qualquer Funcionário, Terceiro ou qualquer outra pessoa que venha a ter acesso à Informação ou Informação Confidencial que transitam no âmbito dos Recursos de Tecnologia da Informação da Empresa, seja através de uma Conta de Usuário ou de uma Conta de Terceiro.

6. Diretrizes

6.1 Gerais

a) São responsabilidades relacionadas a esta norma:

- Cada Usuário é responsável pela memorização de sua própria senha;
- A equipe de TI não deverá possuir acesso às senhas dos Usuários;
- A senha não pode ser compartilhada, divulgada, anotada em papel ou em sistema visível ou de acesso não protegido
- As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), ou meios compreensíveis por linguagem humana (não criptografados);

- As senhas não devem ser baseadas em informações pessoais, tais como o próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento;

- As senhas não devem ser constituídas de combinações óbvias de teclado, tais como “abcdefgh”, “87654321”; e

- O extravio, roubo ou perda da senha de acesso pelos Usuários, deverá ser comunicado imediatamente para a equipe de TI a fim de que possam bloqueá-la e disponibilizar nova senha de acesso.

b) É de inteira responsabilidade do Usuário qualquer prejuízo e dano que venha a sofrer ou que cause à instituição e/ou a terceiros, em decorrência do uso inadequado ou indevido de sua senha, seja por culpa ou dolo.

6.2 Características das senhas

a) Qualquer senha utilizada para se autenticar em uma estação de trabalho, um servidor, um aplicativo, um sistema ou qualquer serviço que se relacione com à Informação ou Informação Confidencial que transite no âmbito dos Recursos de Tecnologia da Informação da Empresa, deve possuir um nível de segurança mínimo para garantir autenticação e identidade do seu respectivo usuário. Para este fim, as características das senhas devem utilizar as considerações apresentadas a seguir:

- Possuir no mínimo 12 (doze) caracteres e utilizar os 4 (quatro) elementos apresentados a seguir:

  - Caracteres numéricos 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
  - Caracteres utilizando letras maiúsculas do alfabeto
  - Caracteres utilizando letras minúsculas do alfabeto
  - Caracteres especiais: !,”,#,$,%,&,’,(,),*,+,- ,.,/,[,\,],@,^,_,{,|,},~.

- Será mantido um histórico de senhas utilizadas pelos Usuários, não sendo permitida a reutilização das últimas 12(doze)

- O intervalo máximo para alteração de senha será de 90 (noventa) dias. Expirado esse prazo, o Usuário irá receber notificação de troca de senha e fazê-lo obrigatoriamente no próximo Logon.

- A senha deverá ser modificada a cada 90 dias para Conta de Serviço

- O número máximo de tentativas de autenticação de senha será de 5 (cinco). Sempre que o Usuário ultrapassar o número máximo de tentativas, a sua conta será bloqueada.

6.3 Ativação inicial e desbloqueio (ou reinicialização) de conta:

a) No caso de bloqueio devido a tentativas malsucedidas de inserção de senhas de acesso à rede, as Contas de Usuários gerenciadas pelo serviço de diretório corporativo serão desbloqueadas automaticamente após 30 minutos, oportunidade em que os Usuários deverão tentar inserir a senha correta novamente.

b) Para sistemas de acesso a aplicativos que possuírem a opção de desbloqueio através de solicitação do respetivo Usuário, seja via sistema ou abertura de Chamado, somente após a solicitação, o Usuário receberá um e-mail com instruções que deverão ser seguidas e permitirão a troca de senha e o desbloqueio da conta que estava bloqueada.

c) No caso de bloqueio de contas de Usuários devido a outros casos que não os acima listados, as contas só poderão ser desbloqueadas ou reiniciadas por um administrador devidamente autorizado pela área de Recursos Humanos, ou pelo Gestor responsável pelo Funcionário ou, ainda, pelo Gestor do Contrato em caso de uma Conta de Terceiro.

d) Cabe a Área de TI orientar regularmente os Usuários sobre as melhores práticas de criação e memorização de senha, de maneira a coibir que as senhas sejam muito fáceis a ponto de poderem ser descobertas ou de serem muito complexas a ponto de precisarem ser anotadas.

6.4 Gerenciamento de senhas de administrador

a) As senhas de administrador que precisarem ser armazenadas em soluções como cofres virtuais de senhas, deverão seguir as considerações abaixo:

- As senhas de administrador deverão ser armazenadas usando um algoritmo de *hash* moderno e criptograficamente forte;
- As senhas de administrador não podem ser armazenadas usando um protocolo de criptografia reversível; e
- A senha de administrador nunca deverá ser armazenada em texto puro.

6.5 Contas geradas durante a instalação de aplicativos/sistemas

a) As contas criadas automaticamente durante o processo de instalação de aplicativos/sistemas devem ser desativadas ou ter sua senha padrão alterada antes de entrarem em produção.

6.6 Mecanismos de autenticação adicionais

a) Sempre que tecnicamente possível, a Empresa solicitará, além da senha de acesso à conta, soluções extras de autenticação (ex. token) complementar para proteção das contas de Usuários, aplicativos, sistemas e serviços que se relacionam com as informações da Empresa.

7. Procedimentos

7.1. Usuários

a) Criar e memorizar suas senhas de acesso individual seguindo as diretrizes desta norma.

b) Não fornecer a senha de acesso para outra pessoa.

c) Comunicar à equipe de TI se houver extravio, roubo ou perda da senha.

7.2. Equipe de TI

a) Manter as regras de segurança e complexidades das senhas atualizadas.

b) Bloquear e disponibilizar nova senha de acesso num evento de extravio, roubo ou perda da senha de funcionários.

c) Desbloquear a Conta de Funcionário, via autorização da área de Recursos Humanos ou do seu Gestor imediato, caso o bloqueio não seja devido a tentativa malsucedida de acesso.

d) Desbloquear a Conta de Terceiro, via autorização do Gestor do Contrato, caso o bloqueio não seja devido a tentativa malsucedida de acesso

7.3. Área de Recursos Humanos

a) Autorizar o desbloqueio de Conta de Funcionário, caso o bloqueio não seja devido a tentativa malsucedida de acesso.

7.4. Gestor do Funcionário

a) Autorizar o desbloqueio de Conta de Funcionário, caso o bloqueio não seja devido a tentativa malsucedida de acesso.

7.5. Gestor do Contrato / Terceiros

b) Autorizar o desbloqueio de Conta de Terceiro, caso o bloqueio não seja devido a tentativa malsucedida de acesso.

8. Disposições Finais

Esta norma entrará em vigor na data de sua divulgação, revogando e substituindo qualquer comunicação anterior sobre o assunto.

9. Controle e histórico de versões

Data	Versão	Sumário
01/07/2021	001	Criação do instrumento normativo

10. Aprovações

Código	Descrição	Versão	Vigência
NOR-003	Norma de criação e utilização de senhas	001	01/07/2021

Emissor(es): TI Corporativo, Grupo Gemina e Juridico Corporativo.

Revisor(es):

Aprovador(es):