IT-ONE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

PC11 - Política de Controle de Acesso

1. HISTÓRICO DE VERSÕES

DATA	VERSÃO	DESCRIÇÃO	AUTOR
02/06/21	1.0	Criação do documento	Peterson Pires

INTRODUÇÃO

O controle de acesso ao ambiente tecnológico da IT-One, com base nos princípios fundamentais da Segurança da Informação, remete a autenticação como mecanismo para certificar as credenciais de acesso (conta de usuário e senha). Dentro deste princípio, essas credenciais permitem que um usuário seja logicamente identificado, autenticado e autorizado a acessar um determinado ambiente, inclusive as dependências da empresa. Assim, esta política vem estabelecer padrões de segurança alinhados com as melhores práticas de mercado no controle de acesso ao ambiente tecnológico da IT-One.

OBJETIVO

Definir um padrão mínimo de controle, que garanta que pessoas não autorizadas tenham seus acessos negados, evitando atividades indevidas e acesso a informações que não sejam públicas; estabelecer atribuições e rotinas de controle para concessão e cancelamento de acesso, minimizando os riscos nas criações e manutenções das credenciais de autenticação

ABRANGÊNCIA

Esta política se aplica a todos os colaboradores da IT-One, quais sejam: funcionários servidores ou comissionados, estagiários, menor aprendiz, terceirizados ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, infraestrutura ou informações da IT-One. Todos esses colaboradores serão tratados nesta política como usuários

DIRETRIZES DE CONTROLE DE ACESSO

1. Diretrizes para Acesso Lógico

1.1 Acesso lógico de Usuário

a) Deve ser estabelecido um processo e controle de concessão, alteração e cancelamento de acesso para os colaboradores em todo e qualquer ambiente;

b) Os gestores das áreas são responsáveis por assegurar que as credenciais de acesso dos respectivos colaboradores sejam disponibilizadas e utilizadas em conformidade com as necessidades funcionais do trabalho, por meio de

formulário específico de solicitação de acesso e abertura de chamado junto a Central de Serviços;

c) Toda concessão de acesso aos sistemas de informações deve ser controlada por um método que envolva identificação, autenticação e autorização;

d) Os usuários devem cadastrar e utilizar suas respectivas senhas de acesso aos sistemas de informações em conformidade com a Política de Uso de Senhas;

e) Ao serem disponibilizadas as credenciais de acesso com os respectivos logins e senhas, o colaborador passa a ser usuário do ambiente tecnológico da IT-One;

f) O Acesso Lógico dos Usuários ao ambiente tecnológico da IT-One deve ser feito mediante a utilização de Contas de Acesso;

g) O usuário terá uma única credencial de acesso em cada ambiente que seja necessário o credenciamento. Esta credencial será válida pelo período de vínculo ativo de trabalho com a IT-One e não deve ser reaproveitada para outros usuários, mesmo após o término da necessidade de uso inicial;

h) As atividades realizadas por meio de determinada credencial de acesso são de responsabilidade do respectivo usuário;

i) É proibido aos Usuários compartilharem suas credenciais de acesso, bem como realizarem qualquer ação utilizando a credencial de Acesso individual ou de grupo para a qual não tenham sido autorizados;

j) Não é permitida a criação nem utilização de contas genéricas (exemplo: temp, quest, usuario, teste, userit...);

k) O gestor de área ou superior deve abrir um chamado junto a central de serviços para solicitar o bloqueio das credenciais de acesso dos respectivos usuários afastados ou desligados;

l) Nos casos em que o usuário afastado é um colaborador terceirizado, o gestor responsável pelo contrato do terceirizado deve abrir um chamado junto à central de serviços para solicitar o bloqueio do respectivo acesso do usuário;

m) Área de Tecnologia da Informação fará o bloqueio automático das credenciais de acesso dos usuários que não realizaram acesso por mais de 90 dias;

n) Todas as pessoas que acessam fisicamente as instalações, mas que não possuem vínculo de trabalho com a IT-One, são considerados visitantes. Neste caso, elas terão acesso lógico a um ambiente tecnológico da IT-One separado, controlado e monitorado, quer seja em meio móvel (wi-fi) ou fixo;

o) Os registros de atividades com a respectiva identificação dos responsáveis pela requisição, aprovação, concessão, comprovação e revogação de Acesso devem ser armazenados para fins de análise de segurança da informação e auditoria.

1.2 Gerenciamento de Privilégio

a) As credenciais de acesso privilegiado, que correspondem ao acesso a atividades de administrador de sistemas ou ativos físicos do ambiente tecnológico, devem ser atribuídas, conforme aprovação do gestor de área ou superior ao colaborador, com base na sua respectiva função e na necessidade de conhecimento da Informação para as atividades do trabalho;

b) O compartilhamento do uso de credenciais de acesso privilegiado deve ser individual e restrito. Contudo, quando essas credenciais precisarem ser compartilhadas por questões técnicas, estas devem ser apenas para equipe habilitada, autorizadas pelo gestor da área de Tecnologia da Informação ou superior e registradas para fins de auditoria;

c) As credenciais de acesso privilegiado devem ser necessariamente trocadas quando houver desligamento ou substituição de qualquer membro da equipe;

d) Todos os usuários que utilizam credenciais de acesso privilegiadas para execução de atividades específicas para este fim devem também possuir credenciais não privilegiadas para atividades do dia a dia. De maneira que a utilização de credenciais de acesso privilegiado só ocorra quando for estritamente necessário.

1.3 Revisão dos Direitos de Acesso

a) Os direitos de acesso devem ser revisados periodicamente pela área de Tecnologia da Informação da IT-One, conforme processo determinado, e validados pelos respectivos gestores de área ou superiores;

b) As requisições geradas devem ser prontamente atendidas e documentadas pela Área de Tecnologia da Informação da IT-One;

c) Mensalmente, o Departamento Pessoal da IT-One deverá encaminhar à Área de Tecnologia da Informação da IT-One uma relação dos colaboradores afastados e dos estagiários desligados há mais de 90 dias, para que sejam verificados possíveis acessos que deveriam estar desabilitados.

1.4 Revisão dos Direitos de Acesso

a) As Contas de Serviço devem ter individualmente um responsável pela sua manutenção, bem como pela alteração de sua senha. O responsável não deve utilizar a Conta do Serviço para outros fins que não seja para o qual foi criado, conforme sua definição;

b) Sistemas e dispositivos devem ser configurados, quando tecnicamente possível, de modo a prevenir Acesso remoto por meio de Contas de Serviço;

c) Contas de Acesso privilegiado que não se enquadram em Contas de Serviço terão suas senhas expiradas em observância ao mesmo processo adotado para contas de Acesso não privilegiado.

2. Diretrizes para Acesso Físico

a) Os controles de Acesso físico visam restringir o Acesso a equipamentos, documentos e suprimentos do ambiente tecnológico da IT-One e a proteção dos recursos computacionais, permitindo-lhes acesso apenas de pessoas autorizadas;

b) Os recursos computacionais críticos da IT-One devem ser mantidos em ambientes reservados, monitorados e com acesso físico controlado, permitido apenas para pessoas autorizadas;

c) Periodicamente a Área de Tecnologia da Informação da IT-One deve revisar os acessos aos ambientes tecnológicos reservados, restringindo o acesso apenas a pessoas autorizadas.