POSITIVO

CONCESSÃO DE ACESSO A SISTEMAS E REDE INTERNA

SUMÁRIO

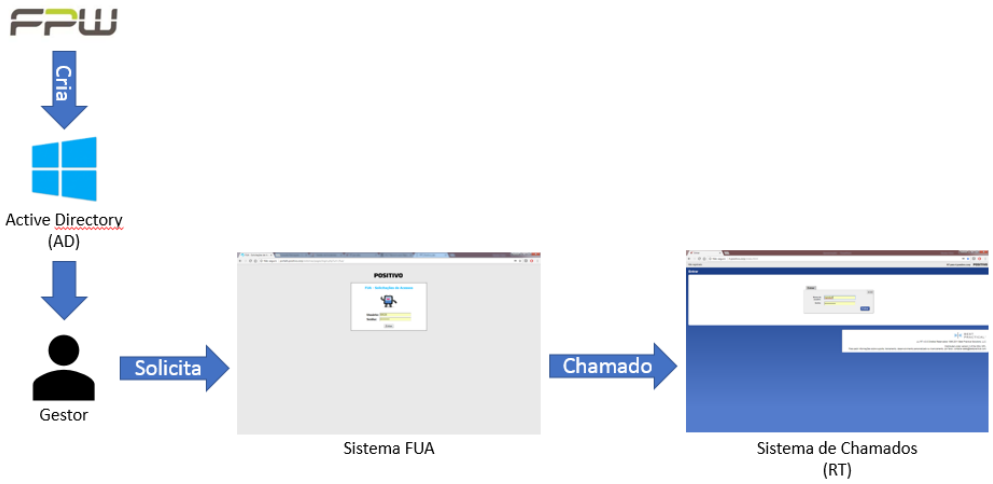
1 DEFINIÇÕES DAS ABREVIATURAS

Ambiente Informatizado da Empresa: Conjunto composto pelas redes de dados externas e internas, aplicações (ex.: SAP), computadores e demais recursos disponibilizados pelo departamento de Informática da Positivo para os seus Colaboradores e Prestadores de Serviços desenvolverem atividades de negócio relevantes para a Empresa.
Assist: Sistema voltado à administração dos processos e gestão de Assistências Técnicas Positivo (ATP).
Identificador de registro: um identificador de registro é a identificação que o usuário do ambiente informatizado recebe do departamento de Tecnologia da Informação e que individualiza o usuário (login ou user id).
Outlook Express: Aplicativo de correio eletrônico.
Sistema de Folha de Pagamento FPW: Sistema de controle dos processos de Folha de Pagamento, cujo suporte de primeiro nível é fornecido pelo TI da Central Administrativa do Grupo Positivo.
Sistema de Gestão Fiscal Synchro: Sistema de registro e apuração de informações fiscais e gerador de arquivos e informações para atendimento às exigências dos órgãos governamentais, cujo suporte de primeiro nível é fornecido pelo TI da Central Administrativa do Grupo Positivo.
Sistema de Gestão SAP: Sistema integrado de informações da Positivo Tecnologia, cujo suporte é fornecido pelo TI da Positivo Tecnologia.
Sharepoint: Sistema utilizado para a requisição de mudanças no cadastro de materiais, clientes e fornecedores no ambiente SAP.
Sistema RT: Sistema de gerenciamento de tickets de serviços e incidentes.
Sistema Ronda Acesso: Sistema responsável pelo controle de acesso físico às sedes da Positivo Tecnologia.
Softway: Sistema de gerenciamento das operações de importação.
SPAM: Mensagem eletrônica indesejada enviada em massa.
TI: Tecnologia da Informação.
VPN: Acesso remoto e seguro aos sistemas e diretório da rede de dados.
FUA: Sistema responsável por gerenciar as solicitações de acessos aos principais sistemas da companhia.
SESMT: Área de Serviço Especializado em Engenharia de Segurança e em Medicina do Trabalho.

2 DESCRIÇÃO DAS ETAPAS DO PROCESSO

2.1 Autorização de acesso a sistemas

FLUXO DE CRIAÇÃO DE USUÁRIO E CONCESSÃO DE ACESSO(S) - NOVO COLABORADOR



1) Todo colaborador novo cadastrado no FPW é automaticamente criado no AD, sem acesso e desativado;
2) O gestor deverá solicitar acesso ao novo colaborador através do sistema FUA;
3) No final do processo de aprovação(ões) o FUA abrirá automaticamente um chamado no sistema RT

2.1.1 Rede interna e correio eletrônico

A solicitação de acessos à rede e correio eletrônico para novos colaboradores e prestadores de serviço deve ser realizada por meio do sistema FUA disponível em http://portalti.positivo.corp/sistemas/pages/login.php?url=/fua/. O FUA fará todo o fluxo de aprovações necessárias e ao final do processo irá gerar automaticamente um ticket no sistema RT.
A área de TI é responsável por analisar as solicitações, suas justificativas e identificar os custos envolvidos para atendimento da solicitação.
O acesso sistêmico aos terceiros será concedido de acordo com a validade do contrato fixada no sistema Ronda. Os terceiros cadastrados no Ronda são geridos pela equipe do SESMT.
A renovação da validade não é automática devendo o gestor do contrato solicitar através do FUA a renovação dos acessos pelo novo período.
Maiores informações sobre concessões de acesso a terceiros em: http://gsi.positivo.corp/procedimentos/solicitacao-de-acesso-terceiro/

2.1.2 Disponibilização de pastas no servidor de arquivos

O perfil de acesso padrão aos diretórios da rede de dados contempla uma pasta particular e uma pública, demais acessos serão concedidos de acordo com a definição do superior imediato.
Os acessos específicos devem ser solicitados à área de Suporte Técnico de TI, via e-mail (FrontendJB@positivo.com.br, frontendmao@positivo.com.br, frontendsp@positivo.com.br) pelo superior imediato e/ ou pelo responsável pela informação.
Os acessos serão concedidos somente mediante aprovação do colaborador responsável pelo diretório (proprietário da informação).

Após analise o Front End irá encaminhar para a equipe de infraestrutura o qual concederá o acesso.

2.1.3 Sistemas Synchro e FPW

A solicitação deve ser feita pelo usuário, através da abertura de chamado para a área de TI da Central do Grupo Positivo, informando os dados do novo usuário e um perfil (matrícula) a ser considerada como base para a criação do novo acesso.
A aprovação da solicitação de acesso deve ser feita pelo Gestor da Área Solicitante, através de comprovação via e-mail.
Caso o acesso solicitado envolva funcionalidades de outras áreas da empresa, que não sejam de controle da área solicitante, o Gestor da área "proprietária" da informação também deve aprovar o acesso através de comprovação via e-mail.
O sistema de chamado da TI da Central do Grupo Positivo poderá ser acessado através do link: http://csc.positivo.com.br/site/index.html

2.1.4 Sistema Softway

A solicitação de acesso ao sistema Softway deve ser encaminhada pelo gestor da área de Comércio Exterior para área de TI (suportesoftwayti@positivo.com.br), através de e-mail e formulário de acesso.

2.1.5 Sistemas SAP

Verifique no Sistema de Documentação o procedimento “Concessão acesso a sistemas SAP”.

2.1.6 Sharepoint

A solicitação de acesso às aplicações desenvolvidas no Sharepoint administradas pela TI da Positivo Tecnologia, deverá ser feita através do sistema FUA.
São essas as aplicações:

- Sistema para solicitação de criação e alteração de dados de clientes ou fornecedores;
- Sistema para solicitação de criação e alteração de dados de cadastro de material.

2.1.7 VPN

Todas as informações necessárias para solicitação de acesso a VPN encontram-se publicadas na intranet da segurança da informação em:
http://gsi.positivo.corp/procedimentos/solicitacao-de-acesso-vpn/

2.1.8 Internet

Todas as informações necessárias para solicitação de acesso à Internet encontram-se publicadas na intranet da segurança da informação em:
http://gsi.positivo.corp/procedimentos/solicitacoes-de-acesso-internet/

2.1.9 WhatsApp Web

Todas as informações necessárias para solicitação de acesso ao WhatsApp via web encontram-se publicadas na intranet da segurança da informação em:
http://gsi.positivo.corp/procedimentos/solicitacao-de-acesso-a-whatsapp-web/

2.1.10 Armazenamento em Nuvem

Todas as informações necessárias para solicitação de acesso a armazenamento em nuvem encontram-se publicadas na intranet da segurança da informação em:
http://gsi.positivo.corp/procedimentos/solicitacao-de-acesso-a-aplicativos-de-arquivos-em-nuvem/

2.1.11 Mídias removíveis

Todas as informações necessárias para solicitação de acesso a mídias removíveis encontram-se publicadas na intranet da segurança da informação em:
http://gsi.positivo.corp/procedimentos/solicitacao-de-acesso-a-midias-removiveis/

2.1.12 Skype

Todas as informações necessárias para solicitação de acesso ao Skype encontram-se publicadas na intranet da segurança da informação em:
http://gsi.positivo.corp/procedimentos/solicitacao-de-acesso-ao-skype/

2.2 Administração de senhas

A senha é o principal mecanismo de segurança do sistema informatizado. A divulgação de senhas é proibida.

Todos os usuários de sistemas informatizados devem obrigatoriamente proteger as informações sob sua responsabilidade através do uso de senhas.

As senhas são de uso individual e não devem ser impressas, armazenadas em documentos eletrônicos ou físicos, fornecidas ou compartilhadas com qualquer pessoa.

Na criação de senhas não é recomendado à utilização de termos ou palavras fáceis, como por exemplo: Positivo, nome do próprio usuário, nome da esposa ou dos filhos, mês em curso, senhas contínuas com número de revisão (mes1, mes2,...), datas de aniversários, RG, CPF ou qualquer informação de fácil dedução. As senhas devem ser alfanuméricas, ou seja, combinação de letras, números e caracteres especiais. No entanto, devem ser de fácil memorização para que não necessitem ser anotadas. Como medida de segurança todas as aplicações devem ser configuradas para exigir identificador de registro e senha para autenticação do acesso.

Como medida de segurança e para proteger nossas informações e arquivos, a cada 90 dias o sistema de usuários (AD) solicita automaticamente a substituição de senha. Deverá ser feito de forma que a nova senha contenha, no mínimos três, dos itens a seguir:

1) Letras minúsculas;
2) Letras maiúsculas;
3) Caracteres especiais;
4) Números;

O sistema não permite:

1) Que as três últimas senhas sejam utilizadas novamente;
2) Conter parte do nome, nome da empresa ou sequencias de fácil adivinhação;
3) Alterar a senha mais que uma vez em 24h;

2.3 Compartilhamento de Informações

As informações armazenadas nos diretórios da rede de dados devem ser organizadas de acordo com o assunto e grau de confidencialidade sendo que as permissões de acessos podem ser:

- Somente para leitura (permite cópia e impressão);

- Acesso completo (permite impressão, cópia, alteração, gravação, deleção e cancelamento).

Cada Usuário é responsável por assegurar o bom uso do ambiente sem comprometer a segurança das informações. O "e-mail" enviado na "internet" e "intranet" expressa somente a opinião individual do remetente, cabendo a este total responsabilidade sobre as consequências das informações divulgadas. O Compartilhamento de informações via e-mail devem seguir as regras estabelecidas na Política de Segurança da Informação. Os usuários com acesso privilegiado aos sistemas manterão sigilo dessas informações, bem como, estarão cientes da responsabilidade e das penalidades da divulgação e/ou uso inadequado da informação.
A concessão de acesso privilegiado ao ambiente informatizado é restrita e os colaboradores, com este acesso, devem manter sigilo das informações conforme Termo de Adesão a Política de Segurança da Informação.

3 DESCRIÇÃO DAS RESPONSABILIDADES

3.1 TI (Tecnologia da Informação)

- Implementar e manter as medidas de segurança estabelecidas pela empresa, em conjunto com a Diretoria das áreas usuárias.

- Incluir novos usuários, alterar e excluir acessos ao ambiente Informatizado de acordo com as informações providas pelos gestores e RH.

- Monitorar periodicamente o uso do ambiente informatizado e a aderência do mesmo com a Política de Segurança da Informação.

3.2 Gestores

- Solicitar/Aprovar a inclusão/alteração/exclusão de acessos de usuários para a área de TI.

- Solicitar/Aprovar a inclusão/alteração/exclusão de acessos a transações críticas para a área de TI.

- Informar as áreas de TI e Segurança da Informação sobre o término de contrato de prestadores de serviços, terceiros, temporários e menores aprendizes, mesmo que estes tenham sido transferidos de departamento.

3.3 Usuários

- Salvaguardar suas senhas de acesso ao ambiente informatizado.

- Utilizar o ambiente informatizado para fins profissionais, seguindo as definições contidas na Política de Segurança da Informação.