**INSTRUÇÃO DE TRABALHO (IT)**

Esta instrução de trabalho visa orientar o analista a realizar a criação de usuário no sistema SISTEMA Y

a. Pré-requisitos:

a) Acesso ao SISTEMA X;

b) Acesso ao SISTEMA Z.

a. Revisão Semestral de Acessos

a) Regularmente os acessos ao Sistemas deverão ser revisados pelo Gestor do time de GQ-Digital.

b) A lista de acessos ativos no sistema será gerada pelo time de Digital - Acessos

c) A lista deve ser respondida pelo Gestor de Negócio validando a lista ativa ou informando quais inativações deverão ser realizadas

d) O time de Digital - Acessos registrará as alterações a partir de chamados no Sistema de ITSM de Digital em nome do Gestor de GQ-Digital.

e) O time de Digital - Acessos executará a atualização e finalizará o chamado com status de resolvido.

Não há referências.

3.1. Pelo navegador Internet Explorer digite o endereço: HTTP://XXXXXX

3.1.1. Acesse a pasta SISTEMAS:

3.1.2. Em seguida, acesse a pasta SISTEMA Y:

3.1.3. Na pasta SISTEMA Y contém as opções de acesso:

• Easy SmartClient – PRD (Ambiente de Produção).

• Easy SmartClient – QAS (Ambiente de Qualidade e Desenvolvimento).

Observação: Primeiramente cria o grupo no ambiente de qualidade e realiza os testes com o mesmo. Quando confirmado o acesso, solicitação é encaminhada para a equipe de Controles Internos e, após a aprovação deste que é criado no ambiente de produção.

3.1.4. Abra o Smart Client no ambiente que necessitar (Produção ou Qualidade).

3.1.4.1. O Programa Inicial virá configurado como: SIGAEIC (Easy Import Control):

3.1.4.2. Para criação do usuário, deve-se alterar a configuração do Programa Inicial manualmente para: SIGACFG (Modo de Configuração):

Observação: Os Parâmetros Iniciais possuem 03 campos, que são:

• Programa Inicial: É indicado o módulo de conexão do Protheus, será utilizado o SIGACFG que é o módulo configurador, onde é atribuído acesso ao usuário, criação de grupos, reset de senha, bloqueio de acesso e outros.

• Comunicação no Cliente: Indica o ambiente para conexão.

• Ambiente no Servidor: Indica o ambiente para conexão dentro do servidor.

3.2. Digite seu usuário e senha e clique em “Acessar Protheus”.

3.2.1. Na próxima tela clique em “Entrar”.

3.3. No menu do Configurador, acesse as opções “Usuário > Senhas > Grupos” que abrirá a tela de Criação de usuários.

3.3.1. Em seguida, acesse a opção “Incluir” para abrir as opções de criação do grupo.

3.3.2. Na aba “Grupo”, é necessário preencher o nome do Grupo e a sua descrição. Os demais parâmetros de configuração não são alterados.

3.3.2. Em seguida, clique nas abas “Restrições de Acessos > Filiais > Grupo de empresas”, selecione a filial que o novo grupo deverá ter o acesso permitido e clique em “OK”. Para cadastrar nova filial, deve-se repetir o processo.

Observação: Ao cadastrar nova filial, é necessário inserir nova linha, clicando na seta para baixo do teclado.

3.3.3. Em seguida, clique na aba “Ambientes” e selecione o módulo do Easy: SIGAEIC – Easy Import Control.

3.3.3.1. Em seguida, atribua o menu criado para o grupo, alterando o campo “Arquivo”. Segue abaixo o passo a passo:

3.3.3.1.1. Clique no mechcode para abrir a caixa de seleção:

3.3.3.1.2. Selecione a pasta “System”.

3.3.3.1.2. Selecione o arquivo do menu e clique em “Abrir”:

3.3.4. Clique em “Confirmar” para salvar as alterações.

3.4. Para controle de acesso liberado no sistema Comex, é necessário que atualize a planilha “Controle\_Grupos\_de\_Acessos\_Comex”, que encontra-se disponível no endereço: g:\xxxxx

Não há anexos.

INSTRUÇÃO DE TRABALHO (IT)

SISTEMA Y - Criação de Menus de Acesso

Esta instrução de trabalho visa orientar o analista a realizar a criação de usuário no SISTEMA Y

b. Pré-requisitos:

c) Acesso ao SISTEMA X;

d) Acesso ao SISTEMA Z;

e) Planilha “IT - SISTEMA Y\_Criação de Menus” preenchida pelo usuário com o tipo de acesso a ser atribuído no Menu.

◦ Revisão Semestral de Acessos

a) Regularmente os acessos ao Sistemas deverão ser revisados pelo Gestor do time de GQ-Digital.

b) A lista de acessos ativos no sistema será gerada pelo time de Digital - Acessos

c) A lista deve ser respondida pelo Gestor de Negócio validando a lista ativa ou informando quais inativações deverão ser realizadas

d) O time de Digital - Acessos registrará as alterações a partir de chamados no Sistema de ITSM de Digital em nome do Gestor de GQ-Digital.

e) O time de Digital - Acessos executará a atualização e finalizará o chamado com status de resolvido.

Não há referências.

Para criação do Menu, é encaminhada ao usuário a planilha “IT - SISTEMA Y\_Criação de Menus”, onde deve ser mapeado os acessos que precisará. Após o preenchimento da mesma, seguiremos o ítem 3.1.

3.1. Pelo navegador Internet Explorer digite o endereço: HTTPS://XXXXXXXXXXXXX

3.1.1. Acesse a pasta SISTEMAS:

3.1.2. Em seguida, acesse a pasta SISTEMA Y:

3.1.3. Na pasta SISTEMA Y contém as opções de acesso:

• SISTEMA Y SmartClient – PRD (Ambiente de Produção).

• SISTEMA Y SmartClient – QAS (Ambiente de Qualidade e Desenvolvimento).

3.1.4. Abra o SISTEMA Z no ambiente que necessitar (Produção ou Qualidade).

3.1.4.1. O Programa Inicial virá configurado como: SIGAEIC (SISTEMA Y Import Control):

3.1.4.2. Para criação do usuário, deve-se alterar a configuração do Programa Inicial manualmente para: SIGACFG (Modo de Configuração):

Observação: Os Parâmetros Iniciais possuem 03 campos, que são:

• Programa Inicial: É indicado o módulo de conexão do Protheus, será utilizado o SIGACFG que é o módulo configurador, onde é atribuído acesso ao usuário, criação de grupos, reset de senha, bloqueio de acesso e outros.

• Comunicação no Cliente: Indica o ambiente para conexão.

• Ambiente no Servidor: Indica o ambiente para conexão dentro do servidor.

3.2. Digite seu usuário e senha e clique em “Acessar SISTEMA x”.

3.2.1. Na próxima tela clique em “Entrar”.

3.3. No menu do Configurador, acesse as opções “Usuário > Cadastros > Menus” que abrirá a tela de Criação e Edição de Menus.

3.3.1. Para criação de novo menu, temos como base o menu inicial do Ambiente SISTEMA Y Import Control (EIC).

3.3.2. Clique em “Adicionar” os itens serão disponibilizados para o modo edição no “Novo Menu”.

3.3.3. Na tela “Configuração de Menus”, em “Novo Menu” são carregadas todas as telas presentes no ambiente EIC, nelas devemos aplicar as restrições conforme mapeamento da planilha. Segue abaixo descrição da tela para configuração das restrições:

3.3.3.1. Adicionar: Carrega o Menu para o modo edição;

3.3.3.2. Remover: Remove o Menu do modo edição;

3.3.3.3. Novo Grupo: Adiciona uma nova pasta ao meu;

3.3.3.4. Novo Item: Adiciona um novo campo;

3.3.3.5. Detalhes: Selecionado o Item do Menu, podemos editar os acessos ao item;

3.3.3.6. Mover para Cima: Move o item de posição;

3.3.3.7. Mover para Baixo: Move o item de posição;

3.3.3.8. Pesquisar;

3.3.3.9. Gerar: Gravar o Menu do Sistema;

3.3.3.10. Fechar: Fecha sem salvar as alterações.

3.4. Para restringir o acesso selecione o ítem que irá modificar, e clique no botão “Detalhes”.

3.4.1. Abrirá a tela abaixo para configuração do Menu:

3.4.1.1. Descrição: Informe o nome do ítem;

3.4.1.2. Programa: Selecione “EICZCC” para o nome do programa;

3.4.1.3. Status: Selecione o status do menu:

3.4.1.3.1. Habilitado: Menu terá acesso a configuração do ítem;

3.4.1.3.2. Desabilitado: Menu não terá acesso a configuração do ítem e o visualizará.

3.4.1.3.3. Inibido: Menu terá acesso a configuração do ítem e não o visualizará.

3.4.1.4. Rotinas do browser: Opções devem ser selecionadas de acordo com o preenchimento da planilha “XX- SISTEMA Y\_Criação de Menus”.

3.4.2. Após configuração do Menu, clique no botão “Gerar”. Salve o Menu com o mesmo nome. Em seguida clique em “Gerar” e logo após em “Fechar”.

Exemplo: M\_ACESSOS

3.5. Para controle de acesso liberado no sistema SISTEMA Y, é necessário que atualize a planilha “Controle\_Grupos\_de\_Acessos\_ SISTEMA Y”, que encontra-se disponível no endereço:

Anexo I - SISTEMA Y\_Criação de Menus

FIELD – SISTEMA Y – ANDROID

Este documento tem por objetivo orientar o time de FieldService na padronização de móveis destinado ao público Android Xxxxx.

Pré-requisitos:

◦ Realizar previamente o cadastro do SN do dispositivo no portal SISTEMA Y pelo link htttxxxxxxxxxx..

◦ Perfil destinado a todos os cargos até gerencia.

• ND

Após realizar o HardReset, selecione o idioma e clique em Iniciar. Em seguida no lugar do e-mail insira o valor afw#setup e clique em Próxima

Siga com a instalação do Android Device Policy e aceite os termos.

Aponte a câmera para o QRCode. Caso apresente erro na leitura você pode inserir o código RUCNJNUC.

Aceite os termos novamente e faça logon com a conta Da EMPRESA X do colaborador.

Clique em entrar e faça logon novamente com a conta Da EMPRESA X do colaborador.

Finalizado, basta aguardar que os aplicativos e demais configurações sejam aplicados automaticamente.

1. ND

INSTRUÇÃO DE TRABALHO (IT) Docnix - Alteração de Acessos

1. Introdução / Pré-requisitos para execução da IT

Esta instrução de trabalho descreve a atividade de Troca de perfil de Usuário no SISTEMA Y.

1.1 Pré-requisitos:

· Ambiente que usuário deseja alterar acesso (DEV, QA, PROD):

· Nome completo do usuário que terá o perfil alterado;

· Login de rede do usuário que terá o perfil alterado;

· Nome do perfil que deverá ser adicionado ao usuário;

· Aval da área do A EMPRESA X (pesquisas com consumidor). Responsáveis:

· XXXX (XXXX@XXXX.COM)

1.1 Revisão Semestral de Acessos

a) Regularmente os acessos ao Sistemas deverão ser revisados pelo Gestor do time de GQ-Digital.

b) A lista de acessos ativos no sistema será gerada pelo time de Digital - Acessos

c) A lista deve ser respondida pelo Gestor de Negócio validando a lista ativa ou informando quais inativações deverão ser realizadas

d) O time de Digital - Acessos registrará as alterações a partir de chamados no Sistema de ITSM de Digital em nome do Gestor de GQ-Digital.

e) O time de Digital - Acessos executará a atualização e finalizará o chamado com status de resolvido.

2. Referências

· PROCEDIMENTO:

3. Descrição das Atividades

Para acessar ao APLICATIVO de Voluntários:

· Acesse o browser de acordo com o ambiente solicitado:

· (Desenvolvimento);

· (Homologação);

· (Produção).

· Informe o e-mail corporativo e clique em "Avançar".

Execute os seguintes passos:

· Clique no botão > "Configurações" > "Segurança", conforme demonstrado abaixo:

· Clique em "Usuários".

· Pesquise e selecione o usuário desejado. Confira a "Unidade de Negócios".

NOTA: Caso o usuário acesse outros Aplicativos além de “Voluntários”, OBRIGATORIAMENTE este usuário deve ser mantido na Unidade de Negócio “A EMPRESA X”, do contrário não terá acesso aos registros desta unidade de negócio.

· Para alterar os direitos de Acesso, clique em ‘Gerenciar Funções’ e selecione os itens de acordo com a nova função informada pelo usuário:

· Se função é “Gerente”, selecionar os itens abaixo:

· [VOL] - Administração

· [VOL] - APP

· [VOL] - Survey

· Se função é “Coordenador”, selecionar os itens abaixo:

· [VOL] - Administração

· [VOL] - APP

· [VOL] - Survey

· Se outras funções, selecionar os itens abaixo:

· [VOL] - Perfil A

· [VOL] - APP

· Mantenha o usuário selecionado e clique em "Mais Comandos" > "Abrir Caixa de Correio" para sua configuração.

· Configure os campos de "Método de Sincronização" conforme abaixo e clique em "Salvar" .

Anexos

Não há anexos.

CS - SAP - ZBO103 ATUALIZAR DADOS DA BU

Introdução

Quando um colaborador DA EMPRESA X entrar em contato comunicado que agora seu e-mail deixará de ser DA EMPRESA X e se tornará DA EMPRESA X ou DA EMPRESA X(por exemplo). O analista N1 deve realizar as orientações descritas nessa IT.

a. Revisão Semestral de Acessos

• Regularmente os acessos ao Sistema deverão ser revisados pelo Gestor do time de GQ-Digital.

• A lista de acessos ativos no sistema será gerada pelo time de Digital - Acessos

• A lista deve ser respondida pelo Gestor de Negócio validando a lista ativa ou informando quais inativações deverão ser realizadas

• O time de Digital - Acessos registrará as alterações a partir de chamados no Sistema de ITSM de Digital em nome do Gestor de GQ-Digital.

• O time de Digital - Acessos executará a atualização e finalizará o chamado com status de resolvido.

Referências

Palavras chaves: domínio, e-mail. ZBO103, AD, mudança no domínio.

Descrição

N1-Outros em posse dos requisitos, realiza a troca do E-mail na ZBO103, campo E-mail.

3.1 Inicia a edição

3.2 edita o campo e-mail

3.3 Preenche o campo motivo, com o número do chamado e no campo Nr chamado colocar apenas o número da TASK.

3.4 Após alterado e colocado os dados, precisa gravar como apontado abaixo

3.5 Evidencia a alteração na ZBO103 e AD dos campos de Email (General e Account) no chamado

Requisito da atividade:

2 Aval gerencial

3 Motivo:

4 De: user@xxxxxxxxx.com.br

5 Para: user@yyyyyyyyyy.com.br

Obs: Antes de concluir esse 1 chamado, abra um novo chamado e com as mesmas evidências e aval enviar para Equipe X para que realizem a alteração do novo e-mail no AD e informe o número desse 2° chamado no 1° chamado aberto para o concluir corretamente.

Anexos

Sem anexos

SYSTEMA Y - Ativar, Inativar Acesso e transferir licenças

Introdução / Pré-requisitos para execução da IT

Esta instrução de trabalho orienta o passo a passo para ativar ou inativar acesso de usuário no SISTEMA Y

1.1 Pré-requisitos para Ativação

a) Nome do colaborador;

b) Usuário do SISTEMA Y;

c) Solicitar aval do keyuser xxxxxx ou xxxxxxxxx;

Revisão Semestral de Acessos

1 Regularmente os acessos ao Sistema deverão ser revisados pelo Gestor do time de GQ-Digital.

2 A lista de acessos ativos no sistema será gerada pelo time de Digital - Acessos

3 A lista deve ser respondida pelo Gestor de Negócio validando a lista ativa ou informando quais inativações deverão ser realizadas

4 O time de Digital - Acessos registrará as alterações a partir de chamados no Sistema de ITSM de Digital em nome do Gestor de GQ-Digital.

5 O time de Digital - Acessos executará a atualização e finalizará o chamado com status de resolvido.

1.2 Pré-requisitos para Inativação

a) Nome do colaborador;

b) Usuário do SISTEMA Y;

c) Motivo da inativação do usuário;

d) Solicitar aval do keyuser XXXXXXXXX ou XXXXXXXXXX;

e) O RH ou gerente imediato (para colaborador terceiro) poderá solicitar a inativação do usuário sem necessidade do aval anexado.

1.3 Pré-requisitos para Inativação com transferência de Licença

a) Nome do colaborador;

b) Usuário do SISTEMA Y que terá a licença removida;

c) Usuário do SISTEMA Y que terá a licença atribuída;

d) Solicitar aval do keyuser XXXXXX ou XXXXXXXXX;

Referências

Não há referências.

Descrição das Atividades

3.1 Ativar ou inativar acesso de usuário

Para esse procedimento, o usuário está criado. Portanto, o mesmo pode ser ativado ou inativado seguindo os passos abaixo.

Ao acessar o SISTEMA Y, selecione a opção Manage Users:

O sistema abrirá a tela de help desk, acessar com usuário e senha:

Será aberta a página de gerenciamento de usuário:

Selecione o usuário por uma das seguintes formas:

1. Digite o usuário do SISTEMA Y e clique em “Apply Filter”;

2. Selecione o usuário na tela de usuário:

3. Clicar em “Edit User”:O parâmetro que define um usuário como ativo ou não é o parâmetro Enabled¸ caso o mesmo esteja marcado o usuário está ativo, caso esteja desmarcado o usuário está inativo.

Anexos

Não há anexos.

INFRA - SYSTEMA Y - LIBERAÇÃO DE ACESSO SYSTEMA Y

Liberação de acesso ao SYSTEMA Y

Pré-requisitos:

• Aval do Gerente responsável com CDC.

Após central de serviços coletar os pré-quesitos irá recategorizar o chamado para fila do time de “X”.

Categoria: A

Subcategoria: B

Sintoma: C

Qualificação Sintoma: D

Não há referências.

Procedimento de liberação de acesso ao SYSTEMA Y

Validação de Licença, verificar se existe licença E5 publicada para colaborador (M365 XXXXXXX XXX) no Active Directory.

Incluir usuário no grupo de liberação da ferramenta Azure Virtual desktop (AVD) “G-XXXXXX- SYSTEMA Y”.

Métodos de acesso.

• Cliente Área de Trabalho do Windows (recomendado - 01):

• Cliente Microsoft Store (recomendado - 02)

• Cliente para área de trabalho MacOS.

• Cliente WEB (recomendado somente em último caso por não apresentar total performance)

Não há anexos.

Criação de Perfil no SISTEMA Y

1. Introdução / Pré-requisitos para execução da IT

Esta instrução de trabalho descreve a atividade de Troca de perfil de Usuário no SISTEMA Y.

6

6.1 Pré-requisitos:

f) Ambiente (DEV, QA, PROD)

g) Nome do perfil que deseja criar;

h) Tipo de Acesso que o perfil deverá ter;

i) Aval da área do XXX (pesquisas com consumidor). Responsáveis:

j) XXXXXX (XXXX@XXXX)

a. Revisão Semestral de Acessos

1. Regularmente os acessos ao Sistema deverão ser revisados pelo Gestor do time de GQ-Digital.

2. A lista de acessos ativos no sistema será gerada pelo time de Digital - Acessos

3. A lista deve ser respondida pelo Gestor de Negócio validando a lista ativa ou informando quais inativações deverão ser realizadas

4. O time de Digital - Acessos registrará as alterações a partir de chamados no Sistema de ITSM de Digital em nome do Gestor de GQ-Digital.

5. O time de Digital - Acessos executará a atualização e finalizará o chamado com status de resolvido.

2. Referência

• PROCEDIMENTO:

3. Descrição das Atividades

1

2

3

3.1 Para acessar ao APLICATIVO de Voluntários:

a) Acesse o browser de acordo com o ambiente solicitado:

• (Desenvolvimento);

• (Homologação);

• (Produção).

• Informe o e-mail corporativo e clique em "Avançar".

3.2 Execute os seguintes passos:

• Clique no botão > "Configurações" > "Segurança", conforme demonstrado abaixo:

• Clique em "Direitos de Acesso".

• Clique no botão “Novo”

• Preencha o campo “Nome da Função” com o valor informado nos pré-requisitos. No campo “Unidade de Negócio”, o valor deverá ser “GESTAO\_AMBIENTE”

• Encontrar nas abas abaixo as entidades que o novo perfil terá acesso, de acordo com os pré-requisitos e selecionar a ação do perfil para aquela entidade. Clique em “Salvar e Fechar”

3.3 Classificação do chamado: - Criação de Perfil no SISTEMA Y.

4. Anexos

Não há anexos.

CS- SAP PORTAL – DESBLOQUEIO DE USUÁRIO

Introdução / Pré-requisitos para execução da IT

Esta instrução de trabalho tem como objetivo orientar os analistas no processo de desbloqueio de usuário no sistema SAP e Portal SAP.

1.1 Pré-requisitos:

7

7.1 Nome completo do usuário;

7.2 Login do usuário nos sistemas SAP e Portal SAP;

7.3 Acesso ao SAP Solution Manager;

7.4 Acesso ao Portal SAP;

7.5 Chamado deve ser solicitado/registrado pelo próprio usuário ou pelo gestor imediato.

◦ Revisão Semestral de Acessos

1. Regularmente os acessos ao Sistema deverão ser revisados pelo Gestor do time de GQ-Digital.

2. A lista de acessos ativos no sistema será gerada pelo time de Digital - Acessos

3. A lista deve ser respondida pelo Gestor de Negócio validando a lista ativa ou informando quais inativações deverão ser realizadas

4. O time de Digital - Acessos registrará as alterações a partir de chamados no Sistema de ITSM de Digital em nome do Gestor de GQ-Digital.

5. O time de Digital - Acessos executará a atualização e finalizará o chamado com status de resolvido.

Referências

Não há referências.

Descrição das Atividades

Para desbloquear acesso do usuário no sistema SAP e Portal SAP, siga os passos abaixo:

k) Para usuários terceiros, caso a solicitação seja registrada pelo gestor imediato, é necessário seguir os passos abaixo:

Realize a comparação do gestor que respondeu o e-mail com o gestor cadastrado na transação ZBO103 e siga orientações abaixo:

• Caso seja o mesmo gestor, prossiga com o passo 3.2.

• Caso sejam gestores diferentes, faça:

◦ Abra chamado relacionado para Correção de dados cadastrais

◦ Realize a alteração do gestor responsável pela abertura do chamado.

◦ Prossiga o atendimento da solicitação conforme passo 3.2.

Observação: Deve ser considerado Gestor imediato para terceiro: Coordenador, Gerente e Diretor.

Acesse o sistema SAP, no ambiente 06) SAP Solution Manager:

Digite a transação “SU01” e tecle “Enter”:

Clique no matchcode :

Informe o nome do usuário e clique no botão ou tecle “Enter” para realizar a Busca.

Selecione o usuário e clique no botão ou tecle “Enter”.

Em seguida, clique no botão para realizar o desbloqueio:

Clique no botão .

Informe o número do chamado e clique em ou tecle “Enter”.

Para desbloquear acesso no SAP Portal é necessário acessar o endereço do ambiente desejado, informe usuário, senha e clique em “Logon”:

3.10.1 Endereços do SAP Portal:

b. Ambiente de Produção: https://xxxxxxxxxxxxxx

c. Ambiente de desenvolvimento: https://xxxxxxxxxxxxxx

d. Ambiente de qualidade: https://xxxxxxxxxxxxxx

6. Selecione a aba “Administração de Usuário”, informe o usuário que deseja realizar desbloqueio e tecle “Enter”.

3.12 Selecione o usuário, em “Detalhes para Usuário” clique na aba “Informações sobre a conta” e certifique que o campo “Senha bloqueada” está selecionado. Clique em “Modificar”:

Clique na aba “Informações gerais”, informe a senha nos campos “Definir senha” e “Confirmar senha” e clique em “Gravar”:

Certifique que o campo “Senha bloqueada”, na aba “Informações sobre a conta” não está selecionado.

Anexos

Não há anexos.

CS - SAP – PRORROGAÇÃO E REVOGAÇÃO DE ACESSO DE TERCEIRO

Introdução / Pré-requisitos para execução da IT

Esta instrução de trabalho visa orientar o assistente da Central de Serviços na prorrogação e revogação de acessos de terceiros no sistema SAP.

Pré-requisitos:

2.

a. Acesso à caixa de e-mail “Suporte”;

b. Acesso às transações: ZBO103, ZBO104 e ZBO127;

c. Para Prorrogação de Acesso de Terceiro:

2.

◦ Validação/resposta do gestor (GER/DIR) para prorrogação do acesso;

◦ Prazo máximo para prorrogação de acesso é de 90 dias (o SAP não aceita mais do que 90 dias)

6.

a. Para Revogação de Acesso de Terceiro

1.

◦ Validação/resposta do gestor para revogação programada ou imediata de acesso

1.1 Revisão Semestral de Acessos

a) Regularmente os acessos ao Sistema deverão ser revisados pelo Gestor do time de GQ-Digital.

b) A lista de acessos ativos no sistema será gerada pelo time de Digital - Acessos

c) A lista deve ser respondida pelo Gestor de Negócio validando a lista ativa ou informando quais inativações deverão ser realizadas

d) O time de Digital - Acessos registrará as alterações a partir de chamados no Sistema de ITSM de Digital em nome do Gestor de GQ-Digital.

e) O time de Digital - Acessos executará a atualização e finalizará o chamado com status de resolvido.

Referências

n/a

Descrição das Atividades

O sistema SAP envia automaticamente e-mail de “Acessos de Terceiros a Vencer – Ambiente ECP” para o gestor responsável quando faltam 05 dias para vencimento dos acessos.

Por meio deste, os acessos são prorrogados ou revogados.

Quando no ato de revogar/prorrogar acessos, o time CS tem visibilidade do COUPA, SAP PRD, QAS e DEV.

Quando for aberto um chamado para o atendimento do time de ACESSOS SAP, deve-se abrir 1 chamado para qualquer uma ou para todas as frentes SAP como COUPA, SAP PRD, QAS e ou DEV.

I- PRORROGAÇÃO DE ACESSO DE TERCEIRO

Os acessos são prorrogados quando, no período das 05 notificações diárias, via e-mail, o gestor solicita a renovação dos acessos.

Caso gestor autorize a prorrogação de acesso, siga os passos abaixo:

1.

2.

1. Realize a comparação do gestor que respondeu o e-mail com o gestor cadastrado na transação ZBO103 e siga orientações abaixo:

3. Caso seja o mesmo gestor, prossiga com o passo 3.1.2.

4. Caso sejam gestores diferentes, faça:

I. Abra chamado relacionado para Correção de dados cadastrais

II. Realize a alteração do gestor imediato responsável pela resposta do e-mail.

III. Prossiga o atendimento da solicitação conforme passo 3.1.2

1.

1. Anexe o e-mail de resposta do gestor;

2. Classifique o chamado: - Prorrogação/Revogação de Acesso de Terceiro;

3. EQUIPE: N1 - OUTROS

4. Na aba Especificação preencha no atributo “Nome do Serviço” o valor “Prorrogação”.

5. Siga os passos abaixo para tratativa da solicitação:

I-ZBO103 – Identidades

Acesse a transação ZBO103 e realize a prorrogação do acesso do usuário conforme informação do gestor.

Clique em “Alterar” através do botão

I. Preencha o Nr. Chamado;

II. Informe o “Motivo” como: Prorrogação de Acessos;

III. Informe a nova “Data de Desligamento” e clique em “Salvar

II-ZBO104 – Administração de Contas de Sistema

• A CENTRAL DE SERVIÇOS executa prorrogação apenas de REDE

• O time N1-ACESSOS SAP realiza a prorrogação do SAP-SAP ECC CORPORATIVO (SOLMAN/GRC)

II-REVOGAÇÃO DE ACESSO DE TERCEIRO

Há três situações de revogação de acesso:

a. O gestor responde o e-mail solicitando a revogação do acesso de imediato.

b. O gestor responde o e-mail solicitando a revogação do acesso programada para a data fim informada.

c. Caso não haja retorno do gestor, neste período, o sistema SAP JOB revoga os acessos de forma automática para os demais sistemas que usuário possui cadastrado na ZBO104.

• Para Inativar apenas 1 sistema/ambiente da ZBO104 e não o user de rede AD, deve ser feito manualmente e não usar ZBO127.

• A ZBO127 inativa automaticamente o SAP e o AD

• Caso o SAP não seja inativado automaticamente, deve realizar manualmente na ZBO104

• Toda revogação deve possuir a evidência da ZBO104 mostrando Rede e SAP inativos

• Não revogar RDV/Paytrack, Docnix, Dynamics e etc, quando a ZBO127 é realizada, o JOB automaticamente abre chamados e direciona para os times que os revogarão.

Para registrar o motivo da revogação de acessos, realize os seguintes passos:

2. Realize a comparação do gestor que respondeu o e-mail com o gestor cadastrado na ZBO103 e siga as orientações abaixo:

3. Caso seja o mesmo gestor, prossiga com o passo 3.2.2

4. Caso sejam gestores diferentes faça:

I. Abra chamado relacionado para Correção de dados cadastrais

II. Realize a alteração do gestor imediato responsável pela resposta do e-mail.

III. Prossiga o atendimento da solicitação conforme passo 3.2.2

1.

1.

1. Anexe o e-mail do SAP JOB;

2. EQUIPE: N1- OUTROS

3. Classifique o chamado: - Prorrogação/Revogação de Acesso de Terceiro;

4. Na aba Especificação preencha no atributo “Nome do Serviço” o valor “Revogação”.

Para o item "b", selecione a flag “Revogação programada”, na ZBO103, para bloquear o envio de e-mail do SAP JOB para o gestor até a data fim do contrato.

Acesse a transação ZBO103 e clique em “Alterar” através do botão

I. Selecione a flag “Revogação Programada”;

II. Clique em “Salvar” .

Para os itens "b" e "c", a revogação dos acessos ocorrerá automaticamente, um dia após a data de desligamento.

Para esclarecimento de dúvidas quanto à operação da ZBO127, acessar a IT- ZBO127\_Inativação de usuário pelo RH.

Sistemas revogados automaticamente pelo JOB da ZBO127 IT - ZBO104 \_ Ativar e inativar conta de usuário de sistema

Anexos

Não há anexo.

ZBO104 - ATIVAR E INATIVAR CONTA DE USUÁRIO DE SISTEMA

Introdução / Pré-requisitos para execução da IT

Esta instrução de trabalho visa orientar analista/assistente das áreas: Central de Serviços, Satélite e Operação, a ativar ou inativar uma conta de sistema no cadastro único de usuários do SAP.

Pré-requisitos:

8

8.1 Número da Identidade do usuário no SAP, ou número do CPF;

8.2 Dados da conta do sistema;

8.3 Acesso à transação ZBO104 e ao sistema específico;

8.4 Possuir Login cadastrados e ativos dos SYSTEMA Y e SAP na transação ZBO104 para a própria identidade que irá realizar a ativação/ inativação, caso a solicitação seja para esses sistemas.

3.1 Revisão Semestral de Acessos

a) Regularmente os acessos ao Sistema deverão ser revisados pelo Gestor do time de GQ-Digital.

b) A lista de acessos ativos no sistema será gerada pelo time de Digital - Acessos

c) A lista deve ser respondida pelo Gestor de Negócio validando a lista ativa ou informando quais inativações deverão ser realizadas

d) O time de Digital - Acessos registrará as alterações a partir de chamados no Sistema de ITSM de Digital em nome do Gestor de GQ-Digital.

e) O time de Digital - Acessos executará a atualização e finalizará o chamado com status de resolvido.

Referências

Descrição das Atividades

• Responsabilidades da Central de serviços para revogação dos sistemas: SYSTEMA Y e SAP.

• Responsabilidades de Acessos para revogação do sistema: SYSTEMA Y.

• Responsabilidades da Operação para revogação do sistema: AD (Usuário de rede).

Para inativar os acessos dos sistemas descritos acima, siga os passos abaixo:

Passo 01: Abra o SAP Logon e clique duas vezes no ambiente “02) SAP ERP Produção”.

Passo 02: Digite o número da identidade ou o CPF do colaborador, clique no mechcode executar ou tecle “Enter”.

Passo 03: Para inativar uma conta, selecione a conta, clique no mechcode “Ativar/inativar Conta” ou tecle “F6”.

Observação: Caso a conta a ser Ativada/Inativada seja dos sistemas SYSTEMA Y, ir para o “Passo 05”.

3.1. Clique no mechcode para finalizar a alteração.

Passo 04: Após finalizar a alteração, verifique se o campo “Status cta” está de acordo com o solicitado.

Observação: “A” para Ativo e “I” para Inativo.

Passo 05: Para inativar uma conta do SYSTEMA Y, selecione a conta e clique no mechcode “Ativar/inativar Conta” ou clique em “F6” conforme o “Passo 3”.

5.1. Clique no mechcode para sair do log de execução SM49.

Observação: Se na tela aparecer a informação “1 rows affected”, a inativação foi realizada com sucesso. Caso apareça a informação “0 rows affected”, não houve inativação, siga o “Passo 8”.

Passo 5.2: Clique no mechcode para finalizar a alteração.

Passo 06: Após finalizar a alteração, verifique se o campo “Status cta” está de acordo com o solicitado.

Observação: “A” para Ativo e “I” para Inativo.

Passo 07: Caso apareça a tela abaixo ao desativar os SYSTEMA Y e SAP, clique no mechcode para sair do log de execução SM49.

Observação: Conforme o “Passo 6.1”, caso apareça “0 rows affected”, significa que a inativação não foi realizada.

7.1: Como mostra a mensagem de erro no canto inferior da tela, o usuário não foi encontrado no sistema. E como mostra o campo “Status cta”, o status da conta não foi alterado.

Observação: Caso tenha ocorrido o processo acima, será necessário ir ao sistema correspondente e procurar pelo funcionário. Se o login for encontrado e estiver cadastrado errado, será necessário excluir e cadastrar a conta novamente para a identidade conforme as IT‘s.

Anexos

Não há anexos.

CS - SAP PORTAL - RESET DE SENHA

1. Introdução / Pré-requisitos para execução da IT

Esta instrução de trabalho tem como objetivo orientar os analistas no processo de alteração de senha do usuário nos sistemas SAP e Portal SAP.

Pré-requisitos:

a) Nome completo do usuário;

b) Login do usuário nos sistemas SAP e Portal SAP;

c) Acesso ao SAP Solution Manager;

d) Acesso ao Portal SAP;

e) Chamado deve ser solicitado/registrado pelo próprio usuário ou pelo gestor imediato.

8.1 Revisão Semestral de Acessos

a) Regularmente os acessos ao Sistema deverão ser revisados pelo Gestor do time de GQ-Digital.

b) A lista de acessos ativos no sistema será gerada pelo time de Digital - Acessos

c) A lista deve ser respondida pelo Gestor de Negócio validando a lista ativa ou informando quais inativações deverão ser realizadas

d) O time de Digital - Acessos registrará as alterações a partir de chamados no Sistema de ITSM de Digital em nome do Gestor de GQ-Digital.

e) O time de Digital - Acessos executará a atualização e finalizará o chamado com status de resolvido.

2. Referências

Não há referências.

3. Descrição das Atividades

Para alterar senha do usuário no sistema Portal SAP, siga os passos abaixo:

3.1 Para realizar alteração de senha do usuário no SAP Portal é necessário acessar o endereço do ambiente desejado, informe usuário, senha e clique em “Logon”:

3.1.1 Endereços do SAP Portal:

a) Ambiente de Produção: https://xxxxxxxxxxxxxxxxxxxxxx

b) Ambiente de desenvolvimento: https://xxxxxxxxxxxxxxxxxxxxxx

c) Ambiente de qualidade: https://xxxxxxxxxxxxxxxxxxxxxx

3.2 Selecione a aba “Administração de Usuário”, informe o usuário que deseja realizar alteração de senha, tecle “Enter”, selecione o usuário e clique em “Modificar”.

3.3 Na aba “Informações Gerais”, altere a senha através dos campos “Definir Senha” e “Confirmar Senha”. Em seguida, clique em “Gravar”.

4. Anexo

N/A

Manutenção de Perfil no SISTEMA Y

Introdução / Pré-requisitos para execução da IT

Este documento estabelece o procedimento para os analistas de Acesso criar, alterar e/ou modificar Perfil e Funções no SISTEMA Y (SISTEMA Y e Pagamento aos Distribuidores e Redes) que podem ser acessados através do endereço do ambiente de produção https://xxxxxxxxxxxxxxxx

Para os demais ambientes, os endereços são:

DEV: https://xxxxxxxxxxxxxxxx

QAS: https://xxxxxxxxxxxxxxxx

Pré-requisitos:

a) O usuário precisa estar cadastrado no AD.

b) O acesso ao sistema Web poderá ser pelo Google Chrome e Internet Explorer (IE).

Ter e-mail de autorização da responsável pelo negócio, que atualmente a responsável é a XXXX . Na sua ausência, a responsável será a XXXX

8.1 Revisão Semestral de Acessos

a) Regularmente os acessos ao Sistema deverão ser revisados pelo Gestor do time de GQ-Digital.

b) A lista de acessos ativos no sistema será gerada pelo time de Digital - Acessos

c) A lista deve ser respondida pelo Gestor de Negócio validando a lista ativa ou informando quais inativações deverão ser realizadas

d) O time de Digital - Acessos registrará as alterações a partir de chamados no Sistema de ITSM de Digital em nome do Gestor de GQ-Digital.

e) O time de Digital - Acessos executará a atualização e finalizará o chamado com status de resolvido.

Referências

Não há referências.

Descrição das Atividades

Perfil

Tela para cadastrar perfis.

· Descrição: informar o perfil.

Após o perfil informado, para gravar clicar em

Observação: Todo registro criado é gravado com o status Ativo.

Além das funcionalidades de excluir e editar existe a funcionalidade de alterar status, Uma vez clicado nesta opção, o sistema abrirá um pop-up informando se realmente deseja alterar o status, se clicar em, o sistema alterará o status do perfil. Se tiver ativo, desativará e se estiver desativado, ativará.

Exemplo:

Perfil Administrador está ativo, clicando em , aparecerá a seguinte mensagem:

Ao clicar em, o sistema alterará o status.

Na funcionalidade excluir, caso o perfil já esteja associado a uma função e usuário, o sistema não permitirá a exclusão, exibindo a seguinte mensagem de erro: Função

NOTA: O Cadastro de função será realizado pela equipe de Web. A associação da função ao perfil que é de responsabilidade da equipe de Acesso.

Tela para cadastrar funções.

Para adicionar uma nova função, clicar em.

· Código: informar um código. Nesse campo deve ser informado um objeto de desenvolvimento. Para o nome do código, segue as recomendações dadas pelo fornecedor.

· Descrição: informar uma descrição da função.

Para gravar os dados informados, clicar em

Observação: Todo registro criado é gravado com o status Ativo.

Além das funcionalidades de excluir e editar existe a funcionalidade de alterar status, . Uma vez clicado nesta opção, o sistema abrirá um pop-up informando se realmente deseja alterar o status, se clilcar em , o sistema alterará o status do perfil. Se tiver ativo, desativará e se estiver desativado, ativará.

Exemplo:

A função pgnAgrpLinhaProduto está ativo, clicando em, aparecerá a seguinte mensagem:

Na funcionalidade excluir, caso a função já esteja associado a um perfil, o sistema não permitirá a exclusão, exibindo a seguinte mensagem de erro:

Anexos

Não há anexos.

IT Sistema SISTEMA Y

Introdução / Pré-requisitos para execução da IT

Este documento foi preparado para orientar a Gestão de Acessos – TI Aplicações quanto ao cadastramento de usuários no SYSTEMA Y utilizado pela equipe do Financeiro.

Link de acesso: https://xxxxxxxxxxxx

8.1 Revisão Semestral de Acessos

a) Regularmente os acessos ao Sistema deverão ser revisados pelo Gestor do time de GQ-Digital.

b) A lista de acessos ativos no sistema será gerada pelo time de Digital - Acessos

c) A lista deve ser respondida pelo Gestor de Negócio validando a lista ativa ou informando quais inativações deverão ser realizadas

d) O time de Digital - Acessos registrará as alterações a partir de chamados no Sistema de ITSM de Digital em nome do Gestor de GQ-Digital.

e) O time de Digital - Acessos executará a atualização e finalizará o chamado com status de resolvido.

Referências

Não há referências.

Descrição das Atividades

Segue abaixo, a descrição do procedimento para criação / alteração de usuário no sistema.

3.1 – Cadastro de usuários.

Requisitos:

a) Nome completo do usuário;

b) CPF;

c) RG;

d) Login de rede do usuário;

e) Perfil a ser atribuído ou usuário cópia;

f) Ambiente que deseja acesso (DEV, QA e PRD);

g) Aval do Gerente (para acesso ao ambiente PRD);

h) Validação de Controles Internos.

Abra o navegador e digite o endereço HTTPS://XXXXXXX.

A página de login aparecerá, digite o nome de usuário e senha de um perfil Gestão de acessos e entre no sistema. Clicar em novo usuário.

Preencher com os dados solicitados, clicar em próximo.

Determinar o perfil a ser utilizado, lembrando que o perfil beneficiário não poderá ser concedido pela equipe de acessos, clicar em próximo.

Na próxima tela preencher com os dados solicitados e clicar em finalizar o cadastro clicando no botão Cadastrar Usuários. Após aparecerá a mensagem abaixo, confirmando a finalização do cadastro. · Retornar para o usuário informando que o cadastro foi finalizado e informar a senha provisória.

3.2 – Alteração de Cadastro de usuários.

Requisitos:

a) Nome completo do usuário;

b) Login de rede do usuário;

c) Ambiente que deseja acesso (DEV, QA e PRD);

d) Aval do Gerente (para acesso ao ambiente PRD).

Abra o navegador e digite o endereço HTTPS://XXXX

A página de login aparecerá, digite o nome de usuário e senha de um perfil Gestão de acessos e entre no sistema. Clicar em atualizar informação.

Selecionar o tipo de usuário.

Clicar no botão Alterar os campos solicitados. Apenas os campos são disponibilizados para alteração.

· Nome;

· RG;

· CPF;

· Empresa;

· Cargo;

· E-mail;

· Órgão administrativo. Após isso clicar no botão confirmar. A alteração será finalizada.

Anexos

Não há anexos.

SISTEMA Y - Alterar Perfil de Acesso

1. Introdução / Pré-requisitos para execução da IT

Esta instrução de trabalho orienta o passo a passo para atribuição de grupos de acesso ao SISTEMA Y, para a atribuição do mesmo é necessário que os seguintes questionamentos tenham sido respondidos via chamado. Com autorização gerencial em anexo.

1.1 Pré-requisitos

a) Nome do colaborador;

b) Usuário do Sistema SISTEMA Y;

c) Motivo da alteração do perfil;

d) Tipo e Grupo de acesso ou usuário cópia;

e) Autorização gerencial.

8.1 Revisão Semestral de Acessos

a) Regularmente os acessos ao Sistema deverão ser revisados pelo Gestor do time de GQ-Digital.

b) A lista de acessos ativos no sistema será gerada pelo time de Digital - Acessos

c) A lista deve ser respondida pelo Gestor de Negócio validando a lista ativa ou informando quais inativações deverão ser realizadas

d) O time de Digital - Acessos registrará as alterações a partir de chamados no Sistema de ITSM de Digital em nome do Gestor de GQ-Digital.

e) O time de Digital - Acessos executará a atualização e finalizará o chamado com status de resolvido.

2. Referências

Não há referências.

3. Descrição das Atividades das Atividades

3.1 Atribuir perfil de acesso ao SISTEMA Y

Após o usuário está criado é necessário que o mesmo seja atribuído a um perfil de acesso. Seguindo os passos abaixo.

Clique em "Users" e todos os usuários cadastrados no sistema serão exibidos.

Obs.: Existem três grupos de usuários: Ativos, Inativos ou Removidos.

Ativos (Active): São usuários ativos no sistema, é possível acesso ao sistema de acordo com o seu nível de permissão de acesso e grupo de acesso atribuído;

Inativos (Disable): São usuários inativos no sistema, não sendo possível a sua conexão no sistema independentemente do nível de acesso ou grupo atribuído.

Obs.: O status Inativo é utilizado em caso de férias, ou ausência do usuário por um período X de dias. Neste cenário somente o usuário solicitará sua reativação.

Removidos (Removed): São usuários removidos do sistema, não sendo possível a sua conexão no sistema independentemente do nível de acesso ou grupo atribuído.

Obs.: Esta opção é utilizada para colaboradores que foram desligados da companhia ou que não utilizarão o Empower em suas atividades.

O perfil de aceso deve ser o mesmo em “Allowed User Types”e “Default User Type”.

Como próximo passo, marque o chekbox "Password Required"

Em Default User Interface, selecione a opção “Pro”

Nos checkbox da caixa “Allowed Interfaces”

Deixe marcado somente “Pro Interfaces”

Recapitulando, após todas as configurações, a tela deve ser idêntica à tela abaixo. Somente os campos User Name, Full Name, Allowed User Types e Default User Types devem ser modificados de acordo com os requisitos que foram enviados pelo usuário.

Anexos

Não há anexos.

SISTEMA Y- Alteração de Acessos

1. Introdução / Pré-requisitos para execução da IT

Esta Instrução de Trabalho visa orientar na atividade de alteração de acesso do usuário no sistema SISTEMA Y.

1.1 Pré-requisitos

a) Ter acesso ao sistema SISTEMA Ycom permissão para alterar acesso.

b) Nome completo do usuário;

c) Tipo da alteração de acesso (Perfil);

d) O chamado deverá ser aberto ou possuir anexo de autorização das colaboradoras:

Obs.: Caso o usuário seja da localidade Anápolis/Brainfarma será válido o aval da documentação técnica:

X

8.1 Revisão Semestral de Acessos

a) Regularmente os acessos ao Sistema deverão ser revisados pelo Gestor do time de GQ-Digital.

b) A lista de acessos ativos no sistema será gerada pelo time de Digital - Acessos

c) A lista deve ser respondida pelo Gestor de Negócio validando a lista ativa ou informando quais inativações deverão ser realizadas

d) O time de Digital - Acessos registrará as alterações a partir de chamados no Sistema de ITSM de Digital em nome do Gestor de GQ-Digital.

e) O time de Digital - Acessos executará a atualização e finalizará o chamado com status de resolvido.

2. Referências

Não há referências.

3. Descrição das Atividades

3.1. Para alterar acessos de usuários no sistema SISTEMA Y acesse o sistema no link:

http://xxxxxxxxxxxxxxxx

3.1.1. Logar no sistema com seu “Login” e “Senha”, após clicar em “Enviar”.

3.1.2. No menu “Administração” escolher a opção “Controle de Acesso”.

3.1.3. No menu “Controle” clique na opção “Usuário”.

3.1.4. Em “Lista de Usuários” inserir o nome completo do usuário que necessita alterar o tipo de acesso e clicar em Listar, em seguida clicar no nome do mesmo.

3.1.5. Com o cadastro do usuário aberto, clicar em “Ação > Editar Usuário”:

3.1.6. Em seguida, clique em “Pertence aos grupos”, onde abrirá a janela “Lista de grupos” para marcar o grupo que o usuário pertencerá:

3.1.7. Após, clique em “Atribuições”, onde abrirá a janela “Lista de Atribuições” para selecionar o acesso que o usuário terá:

3.1.8. Com o acesso do usuário alterado, clicar em “Ação > Salvar Usuário”: