Questionário de Avaliação de Risco ITGC

Cliente:

Data base: 31.12.2024

CARACTERÍSTICAS DO APLICATIVO DE TI

1 - Autenticação de usuário complexa

Este aplicativo de TI tem algum dos seguintes itens?

Login único, onde é usado não apenas para autenticação do usuário, mas também para controle de acesso e autorização?

Gerenciamento central de direitos?

Sistema complexo com vários níveis de funções com diferentes atribuições de direitos (por exemplo, um grande número de funções diferentes)?

Resposta: Atualmente não contamos com um login único (SSO). Para o Sistema Windows o sistema para gerenciamento central de permissionamento é o AD (Active Directory) e para o pacote Office é o Centro de administração do Office 365. Para o sistema ERP Protheus não é diferente, não utiliza login único (SSO), sendo necessário que cada usuário realize autenticação individual por meio de credenciais próprias (login e senha). O controle de acesso é realizado diretamente no próprio ERP, por meio de um modelo de perfis e funções configurado com base nos cargos e responsabilidades dos usuários.

*Tanto o Windows quanto o Office 365 e ERPs, possuem um **nível intermediário de complexidade**, com múltiplos perfis e grupos de permissões que restringem o acesso a menus, rotinas e transações específicas, conforme o departamento e função do colaborador. O gerenciamento de direitos de acesso é realizado pela equipe de TI, com base em solicitações aprovadas pelas lideranças das áreas usuárias gerenciadas através de sistema de chamados.*

2 - Mudanças em programas

A entidade tem a capacidade (direta ou indiretamente por meio do fornecedor de software ou consultor) para fazer o seguinte para este aplicativo de TI:

Modificar o aplicativo (fazer alterações de programa no sistema)? Modificar as definições de configuração com impacto financeiro significativo?

Resposta: Sim, a entidade possui capacidade para realizar modificações no aplicativo ERP Protheus, tanto por meio da equipe interna de TI quanto com o suporte de consultores e equipe de suporte da TOTVS. Essas modificações podem incluir alterações de programa (customizações) e parametrizações com impacto financeiro.

*No entanto, **nenhum membro da equipe de TI, tampouco qualquer consultor externo, está autorizado a realizar modificações no sistema sem consentimento formal prévio**. Todo e qualquer ajuste deve obrigatoriamente **passar por aprovação da gestão responsável e estar vinculado a um chamado formal registrado no sistema de suporte interno**.*

O processo segue os princípios de gestão de mudanças (change management) conforme as boas práticas da ITIL, garantindo controle, rastreabilidade e validação das alterações. As mudanças são documentadas, testadas em ambiente separado (homologação) e validadas pelas áreas usuárias antes de sua aplicação em ambiente produtivo, minimizando riscos operacionais e impactos indevidos sobre os dados financeiros.

3 - Processamento de dados

A entidade possui processamento automatizado de dados entre diferentes sistemas ou módulos de aplicativos em relação a este aplicativo de TI, tais como:

As interfaces personalizadas entre os aplicativos de TI e o cliente não estão verificando substancialmente as transferências de dados usando controles manuais? Processamento em lote (ou seja, processamento de um grupo (lote) de transações/arquivos de uma só vez de acordo com um cronograma predefinido. Isso geralmente não inclui itens como contas a pagar ou processamento em lote de folha de pagamento pelo qual o processo é iniciado por um usuário)? Uso de armazenamento de dados para suportar relatórios financeiros? Complexidade tecnológica para o processamento de transações (por exemplo, online, em tempo real, EDI, Blockchain, etc.)?

Resposta: Atualmente, o processamento de dados da organização é conduzido exclusivamente por meio do sistema ERP Protheus (TOTVS), que centraliza as operações administrativas, contábeis e financeiras da empresa. Todas as inserções de dados (input) são realizadas manualmente pelos usuários de cada área, conforme seus respectivos níveis de acesso e permissões previamente definidos de acordo com suas funções, e registros (históricos) no próprio sistema de cada operação executada.

Não existem integrações automatizadas entre diferentes sistemas ou módulos externos, tampouco são utilizados processos de automação ou rotinas de processamento em lote. O fluxo de informações ocorre internamente no próprio ERP, sem a utilização de interfaces de terceiros, middleware ou EDI. Além disso, a organização não faz uso de data warehouses, somente de repositórios auxiliares (pasta de rede compartilhadas) com controle de acessos, para apoio, e não exclusivo para fins de reporte financeiro, sendo todos os relatórios extraídos diretamente do ERP quando necessário, assegurando a rastreabilidade e integridade das informações no ambiente de origem.

4 - Conversão de dados

Tratava-se de uma nova aplicação implementada no período auditado, que contemplaria alguma das seguintes situações:

Novo aplicativo de TI? Grande atualização do sistema? Migração de dados para um novo sistema?

Resposta: Durante o período auditado, ***não houve implantação de novos aplicativos de TI, nem atualizações de grande porte ou processos de migração de dados****. As operações continuaram sendo executadas integralmente no ERP Protheus, sem alterações estruturais no ambiente de tecnologia que impactassem o processamento ou integridade dos dados.*

ANÁLISE DE RISCOS DE TI E ITGCS RELEVANTES PARA ESTE APLICATIVO DE TI

1 - AAR1 Privilégios de acesso do usuário ao aplicativo de TI para usuários novos e modificados não são autorizados pelo gerenciamento (provisionamento)

AAC1 A gerência aprova a natureza e a extensão dos privilégios de acesso do usuário para acesso de usuário novo e modificado, incluindo perfis/funções de aplicativos padrão, transações críticas de relatórios financeiros e segregação de funções?

Resposta: A concessão e a modificação de privilégios de acesso ao ERP Protheus seguem um processo formal de aprovação, alinhado às melhores práticas de governança de TI. Todos os acessos de novos usuários, bem como alterações de perfis, são solicitados pelas áreas

demandantes através do sistema de chamados e aprovados pela gestão imediata e pelo setor de TI, considerando a natureza e extensão dos privilégios.

Perfis e permissões são atribuídos com base em funções predefinidas, de acordo com a segregação de funções. Transações críticas para o processo financeiro são restritas a perfis específicos de acordo com cada função.

Esse processo está em conformidade com os princípios da ITIL (Gerenciamento de Acesso.

2 - AAR2 O acesso ao sistema de TI não é encerrado ou modificado em tempo hábil (Desprovisionamento)

AAC2 O acesso para usuários encerrados ou transferidos é removido ou modificado em tempo hábil?

Resposta: A empresa possui um processo formal para desprovisionamento de acessos no ERP Protheus. Sempre que ocorre o desligamento de um colaborador, a área de Recursos Humanos informa imediatamente a equipe de TI por meio de chamado formal, e o acesso é revogado no mesmo dia. Em casos de movimentações internas, os acessos antigos são revisados e ajustados conforme a nova função do colaborador, com validação e aprovação da gestão da área envolvida.

Esse procedimento está alinhado às boas práticas da ITIL (Gerenciamento de Acesso), garantindo o controle adequado sobre o ciclo de vida dos acessos aos sistemas corporativos.

3 - AAR3 Os administradores de segurança ou proprietários de dados não revisam, testam e documentam periodicamente as listas de usuários ativos nos sistemas de TI quanto à razoabilidade e precisão com base na segregação de funções, e o acesso conflitante ao sistema de TI não é removido ou mapeado (revisões e autorização de acesso do usuário)

AAC3 Os administradores de segurança ou proprietários de dados revisam, testam e documentam periodicamente as listas de usuários ativos nos sistemas de TI para razoabilidade e precisão com base na segregação de funções, e o acesso conflitante é removido ou mapeado para controles de mitigação?

Resposta: A empresa adota um processo formal de gestão de acessos no sistema ERP Protheus, no qual as ***alterações de permissionamento são realizadas exclusivamente mediante solicitação formal****, registrada por meio de chamado técnico e com aprovação da liderança da área demandante, pois o mesmo deve ser feito por ela.*

Sempre que ocorre uma solicitação de inclusão, alteração ou exclusão de acesso, é realizada uma ***revisão pontual e individualizada*** *dos privilégios atribuídos, garantindo que estejam adequados à função do usuário, em conformidade com o princípio do mínimo privilégio e com a política de segregação de funções.*

Dado que não há alterações de acesso sem demanda formal e aprovada, a empresa ***não realiza revisões periódicas da lista de usuários ativos****, por entender que o processo atual já garante a acuracidade e a rastreabilidade dos acessos. Esse procedimento é suficiente para assegurar o controle e a mitigação de riscos, em alinhamento com as boas práticas de governança de TI.*

4 - AAR4 O acesso a nível de privilégios (por exemplo, configuração, administradores de dados e segurança) ao aplicativo de TI não é autorizado e adequadamente restrito (acesso privilegiado)

AAC4 Acesso de administrador de aplicativo/superusuário - o acesso a nível privilegiado (por exemplo, configuração, administradores de dados e/ou segurança) ao aplicativo de TI é autorizado e adequadamente restrito?

Resposta: O acesso privilegiado ao sistema ERP Protheus, como funções administrativas e de configuração (por exemplo, administradores de dados, segurança ou superusuários), é ***estritamente controlado e concedido apenas a membros autorizados da equipe de TI*** *com base em necessidade operacional justificada.*

Toda concessão de privilégio elevado é ***realizada mediante solicitação formal e aprovação da gestão****, com registro em chamado técnico. O número de usuários com esse tipo de acesso é mantido no mínimo necessário para operação e suporte, respeitando o princípio do* ***menor privilégio****.*

Além disso, as atividades realizadas por usuários com acesso privilegiado estão sujeitas a ***monitoramento, trilha de auditoria e controle por parte da área de TI****, garantindo rastreabilidade e conformidade com as boas práticas de governança de TI (como ITIL)*

5 - AAR5 O acesso aos arquivos/bancos de dados de aplicativos de TI não está limitado a pessoal autorizado, e tal acesso não é aprovado pela administração. Portanto, alterações inadequadas podem ser feitas diretamente nos dados financeiros por outros meios que não as transações do aplicativo. (Controles de configuração de segurança)

AAC5 Administrador de banco de dados/acesso formal - O acesso a arquivos de dados de aplicativos ou objetos/tabelas/dados é limitado a pessoal autorizado, com base em suas responsabilidades e função atribuída, e esse acesso é aprovado pela administração?

Resposta: O acesso direto ao banco de dados e arquivos do sistema ERP Protheus, incluindo tabelas, objetos e dados financeiros, é ***estritamente limitado ao pessoal autorizado da área de TI****, conforme a função técnica exercida. Esse tipo de acesso é* ***restrito a administradores de banco de dados (DBAs)*** *e técnicos responsáveis,* ***mediante aprovação formal da gestão*** *e registro por meio de chamado técnico.*

A empresa ***não permite alterações manuais nos dados diretamente no banco de dados****, salvo em casos excepcionais, mediante autorização expressa e controle rígido. Toda intervenção é documentada, validada pela área demandante e, sempre que possível, acompanhada por* ***trilha de auditoria*** *ou logs de execução.*

Esse procedimento visa assegurar a ***integridade, rastreabilidade e segurança dos dados****, em conformidade com as boas práticas de controles gerais de TI (ITGCs) e ITIL.*

6 - AAR6 Os parâmetros de senha ou outros métodos de autenticação não atendem aos padrões da empresa ou do setor (por exemplo, comprimento e complexidade mínimos da senha, expiração e histórico, bloqueio de conta etc.) e, portanto, não são adequados para impedir o acesso não autorizado ao sistema (Autenticação)

AAC6 Autenticação de usuário: O acesso é autenticado por meio de IDs de usuário e senhas exclusivos ou outros métodos como um mecanismo para validar se os usuários estão autorizados a obter acesso ao sistema. Os parâmetros de senha ou outros métodos de autenticação atendem aos padrões da empresa ou do setor (por exemplo, comprimento e complexidade mínimos da senha, validade e histórico, bloqueio de conta, etc.)?

*Resposta: O sistema ERP Protheus utiliza **IDs de usuário e senhas exclusivos** para autenticação de acesso, sendo as credenciais atribuídas individualmente a cada colaborador autorizado. Os parâmetros de senha seguem os padrões definidos pela política interna de segurança da informação, contemplando:*

- *Comprimento mínimo de caracteres;*
- *Requisitos de complexidade (letras maiúsculas, minúsculas, números e caracteres especiais);*
- *Expiração periódica das senhas com histórico para impedir reutilização recente;*
- *Bloqueio automático do usuário após múltiplas tentativas de login malsucedidas.*

*O acesso é restrito a usuários devidamente provisionados por meio de processo formal, e os controles de autenticação são alinhados às **boas práticas de mercado**.*

CARACTERÍSTICAS DO AMBIENTE DE TI QUE PODEM DAR ORIGEM A RISCOS DE TI E ENVOLVIMENTO DE ESPECIALISTA EM AUDITORIA DE SI

1 - Sistema operacional

O sistema operacional tem uma ou mais das seguintes características:

Login único?

Quaisquer ligações diretas com terceiros por meio de aplicativos baseados na web, comércio eletrônico, troca eletrônica de dados (EDI) relacionados aos sistemas de TI relevantes identificados?

O sistema operacional é complexo (algo além do Windows, como AS400, Unix, etc.)?

*Resposta: O ambiente de TI da empresa opera predominantemente em sistema operacional **Microsoft Windows Server**, com gerenciamento centralizado pela equipe interna de TI. Não há utilização de sistemas operacionais complexos como AS400, Unix ou similares.*

*O ambiente **não utiliza login único (SSO)**, sendo exigida autenticação individualizada por usuário e sistema. Além disso, **não existem conexões diretas com terceiros via aplicativos web, comércio eletrônico ou EDI** nos sistemas críticos avaliados. O ERP Protheus utiliza sistema em Cloud Compunting da Própria TOTVS, sendo assim todo acesso fica ainda mais restritivo. Todo nosso ambiente é considerado de complexidade operacional moderada, não exigindo envolvimento de auditor especializado em infraestrutura de TI neste momento.*

2 - Segurança da rede

A entidade tem maior probabilidade de problemas de segurança de rede resultarem em risco de distorção relevante? Por exemplo:

Servidores externos (ambiente sem servidor)?

Acesso direto a terceiros – aplicativos baseados na web, comércio eletrônico sofisticado, EDI?

Estrutura de rede complexa com várias localidades?

*Resposta: A estrutura de rede da empresa adota um modelo híbrido de infraestrutura. Toda a camada de ERP e banco de dados opera na **infraestrutura em nuvem da TOTVS, por meio***

***do T-Cloud**, assegurando alta disponibilidade, segurança gerenciada e suporte especializado para os sistemas críticos, como o ERP Protheus.*

*Internamente, a empresa mantém **servidor local com sistema operacional Windows Server**, utilizado para serviços complementares de rede e aplicações de menor criticidade. A infraestrutura física compreende **cabeamento estruturado, racks, switches, access points (APs)** e demais ativos de rede, todos mantidos e administrados pela equipe interna de TI.*

*O acesso remoto a pastas de rede compartilhadas é realizado de forma segura por meio de **VPN corporativa da Sophos**, configurada em dispositivos móveis autorizados, garantindo criptografia de tráfego e autenticação protegida. Não há integrações diretas com terceiros via EDI, e-commerce ou APIs externas conectadas diretamente ao ERP ou banco de dados.*

*Para a suíte de produtividade, é utilizado o **Office 365 da Microsoft**, com gerenciamento centralizado via **Portal Microsoft 365**, permitindo controle granular de licenças, políticas de segurança, autenticação e monitoramento de atividades.*

*A estrutura da empresa é considerada de **complexidade moderada**, com controle centralizado de acessos, rede segmentada e políticas de segurança bem definidas. Com isso, o ambiente apresenta **baixo risco de distorções financeiras decorrentes de problemas de segurança de rede**, estando em conformidade com as boas práticas de governança de TI e segurança da informação.*

3 - Backup de dados

Com base em seu entendimento sobre o ambiente de TI, houve algum problema com os processos de backup e/ou restauração/recuperação de dados durante o período auditado?

*Resposta: Durante o período auditado, **não foram registrados incidentes ou falhas nos processos de backup, restauração ou recuperação de dados**. Os procedimentos de backup seguem uma rotina definida pela equipe de TI, com políticas de retenção e agendamento adequados para garantir a segurança e a disponibilidade das informações.*

*Os dados relacionados ao ERP Protheus, hospedado no ambiente T-Cloud da TOTVS, são respaldados diretamente pela infraestrutura da TOTVS, que realiza **backups automáticos em nuvem com redundância e gestão profissional**.*

*Já os dados armazenados localmente em servidores internos são **submetidos a backups periódicos**, com registros de execução mantidos pela equipe de TI e testes pontuais de restauração para validação da integridade.*

Com isso, o ambiente é considerado seguro em relação à continuidade operacional, estando alinhado às boas práticas de governança de TI e planos de recuperação em caso de incidente.