UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE GESTÃO E NEGÓCIOS
CURSO DE GRADUAÇÃO EM GESTÃO DA INFORMAÇÃO

DOUGLAS DOS SANTOS FERREIRA

CONTROLE DE ACESSO A DADOS E INFORMAÇÕES EM EMPRESAS DE BASE TECNOLÓGICA: UMA PROPOSIÇÃO DE SOLUÇÃO

UBERLÂNDIA

2023

DOUGLAS DOS SANTOS FERREIRA

CONTROLE DE ACESSO A DADOS E INFORMAÇÕES EM EMPRESAS DE BASE TECNOLÓGICA: UMA PROPOSIÇÃO DE SOLUÇÃO

Monografia apresentada ao Curso de Graduação em Gestão da Informação, da Universidade Federal de Uberlândia, como exigência parcial para a obtenção do título de Bacharel em Gestão da Informação.

Orientador Profa. Dra. Janaína Maria Bueno.

Banca de Avaliação:

Prof. Dra. Janaína Maria Bueno – Professora Orientadora – FAGEN/UFU

Prof. Dra. Camila Araújo – FAGEN/UFU

Prof. Dra. Maria Adriana Vidigal de Lima – FACOM/UFU

UBERLÂNDIA
2023

RESUMO

O presente artigo tecnológico tem como objetivo analisar a problemática do controle de acessos e permissões em ambientes digitais e apresentar a solução oferecida com o desenvolvimento do software Ex.it a partir da experiência com a empresa Alfa (nome fictício). Este trabalho teve abordagem qualitativa, do tipo descritivo com base em um estudo de caso. Como coleta de dados foi utilizada a pesquisa bibliográfica e entrevistas com três gestores de três empresas diferentes que enfrentam o problema da falta de controle de acessos de seus funcionários aos diferentes sistemas das empresas. A partir desses dados, foi possível identificar que a gestão de acessos é uma tarefa complexa e que empresas enfrentam desafios em garantir a segurança de seus dados e informações confidenciais. Os principais resultados estão relacionados à análise de funcionalidades de um sistema que centraliza as permissões e simplifica processos que incluem a necessidade de monitorar e gerenciar os acessos de funcionários a ferramentas e sistemas tecnológicos. Ainda, o uso do Ex.it pode melhorar significativamente a segurança de dados, permitindo que as empresas cumpram as regulamentações específicas do setor e evitem possíveis prejuízos. As principais conclusões deste trabalho são que o controle de acessos é fundamental para garantir a segurança de dados e informações confidenciais em empresas de todos os setores. A proposta de software oferece uma solução tecnológica eficaz para esse problema, permitindo que as empresas simplifiquem a gestão de acessos e cumpram as regulamentações do setor. Também, o desenvolvimento e o uso do Ex.it podem trazer benefícios tanto para os profissionais que lidam com a segurança de dados, quanto para as empresas como um todo, que podem se destacar no mercado ao oferecer um grau adequado de proteção de informações confidenciais. Este estudo pretende contribuir para o aprimoramento das estratégias de segurança de dados em empresas, permitindo que essas organizações sejam mais eficientes, assertivas e seguras em relação ao controle de acessos e gerenciamento de dados.

Palavras-chaves: Controle de Acessos, Segurança da Informação, Sistemas, Rotatividade, Gestão, Dados e Informações, Privacidade.

SUMÁRIO

1. INTRODUÇÃO

A tecnologia se tornou uma parte fundamental das nossas vidas, transformando a forma como vivemos, trabalhamos e nos comunicamos. No entanto, essa onipresença também traz uma série de desafios e preocupações, especialmente relacionados à segurança de dados e informações confidenciais. Empresas de todos os setores enfrentam o desafio de controlar o acesso de seus funcionários a ferramentas tecnológicas, visando proteger informações sensíveis e garantir que estejam em mãos autorizadas. Esse desafio é ainda maior no cenário de desenvolvimento de sistemas onde, frequentemente, são armazenadas informações confidenciais, como dados pessoais de clientes e informações financeiras. Mascarenhas Neto e Araújo (2019) afirmam que as empresas precisam assumir um comportamento dinâmico em relação à segurança de informações, ressaltam que comportamentos letárgicos não são aceitáveis para a atualidade, pois vivemos um momento de transposição comportamental, em que a interação contínua, sem fronteiras e baseada nas relações de conectividade impõe diferentes desafios para as empresas do Século XXI e, principalmente para a área de segurança da informação, que assume o papel de proteger os ambientes informacionais das diferentes formas de ataques, exposições existentes.

Ademais, os profissionais que atuam no desenvolvimento dos sistemas, muitas vezes, precisam ter acesso a informações confidenciais para criar os sistemas e solucionar problemas. No entanto, o controle de acessos pode ser uma tarefa complexa, especialmente para empresas com muitos funcionários ou com uma alta rotatividade no seu quadro pessoal. Processos manuais correm o risco de erros humanos, como atrasos na remoção de acessos de ex-funcionários ou a concessão de permissões inadequadas, que podem levar à exposição de informações confidenciais, comprometendo a segurança da empresa e a confiança do cliente. Em setores altamente regulamentados, como os de saúde e finanças, a proteção de informações é ainda mais crítica, com multas pesadas para as empresas que não cumprem as leis e regulamentações.

É neste contexto que surgem soluções tecnológicas como a que é proposta neste estudo, o software ora denominado de Ex.it, que se trata de uma plataforma de gestão de acessos que centraliza as permissões e simplifica a tarefa de monitorar e gerenciar os acessos de funcionários a ferramentas e sistemas tecnológicos. A expectativa é de que a utilização do Ex.it melhore significativamente a segurança de dados, permitindo que as empresas cumpram as

regulamentações específicas do setor e evitem possíveis penalidades, além de contribuir com insumos através de informações validadas para tomadas de decisões estratégicas.

O presente artigo tecnológico tem como objetivo analisar a problemática do controle de acessos em empresas e apresentar a solução oferecida com o desenvolvimento do software Ex.it a partir da experiência com a empresa Alfa (nome fictício). Além disso, serão discutidos os possíveis benefícios que essa tecnologia pode trazer para estudantes, profissionais e empresas da área de tecnologia. Com isso, espera-se contribuir para o avanço da segurança de dados e conscientização sobre a importância de investir em soluções de controle de acessos para garantir a proteção de informações sensíveis.

2. CONTEXTO E REALIDADE INVESTIGADA

A empresa Alfa, fundada nos anos 2000, é especializada em soluções de tecnologia. Com uma equipe experiente em diferentes setores, como telecomunicações, atacado, finanças e indústria, a Alfa colabora de perto com seus clientes, oferecendo tecnologias de qualidade e um atendimento personalizado para atender às necessidades específicas de cada um. Ao longo dos últimos anos, a empresa passou por transformações significativas, conquistando clientes de grande porte e estabelecendo parcerias estratégicas. Os valores da Alfa residem nas pessoas que compõem sua equipe, que compartilham a missão de promover inovações tecnológicas com base na ética e no desenvolvimento do bem comum. O objetivo da empresa é otimizar negócios e melhorar a vida das pessoas, com a visão de se tornar uma referência em inovação, serviço e responsabilidade social.

A empresa possui experiência e entrega resultados na área de tecnologia, combinando conhecimento de negócio com capacidade técnica em todo o ciclo de vida de desenvolvimento de software. Além disso, oferece serviços de mobilidade totalmente adaptados à realidade atual da mobilidade Digital, utilizando as melhores e mais atuais tecnologias, tais como Swift para iOS, Java para Android, Apache Cordova para desenvolvimento híbrido e HTML5, CSS e JS para as progressive web apps. A empresa também está envolvida na sustentação de sistemas, reconhecendo que as empresas precisam manter o foco na inovação de seus produtos e serviços. A decisão de investir em Sustentação surge como uma opção capaz de garantir as condições de tempo e foco para atender as necessidades das organizações, apoiada em metodologias como ITIL (Information Technology Infrastructure Library), que é um conjunto de melhorias práticas para o gerenciamento de serviços de tecnologia da informação; e com uma equipe de

profissionais com todo o domínio técnico e do negócio de seus clientes, garantindo altos níveis de satisfação e sucesso.

Recentemente, a Alfa começou a investir em uma nova abordagem: a gamificação. Essa técnica consiste em aplicar elementos de jogos em contextos não lúdicos, com o objetivo de tornar as tarefas mais interessantes e motivadoras. A gamificação pode ser aplicada de diversas formas, como por exemplo, com o uso de sistemas de pontuação, desafios, recompensas e rankings. O investimento está relacionado na implementação de uma plataforma de gestão de projetos e pessoas com o uso da gamificação, com a expectativa de aumentar a produtividade e o engajamento dos seus funcionários, incentivando a competitividade saudável e a busca por resultados. Para isso, a empresa está contando com a colaboração de várias equipes, cada uma com sua responsabilidade específica. A equipe de desenvolvimento de software, por exemplo, é responsável por criar e implementar as funcionalidades da plataforma. Eles trabalham em conjunto para garantir que o produto esteja em conformidade com as expectativas da empresa e atenda às necessidades dos usuários.

Já a equipe de marketing é responsável por promover a plataforma e atrair novos clientes. Eles criam manual de uso, campanhas publicitárias e estratégias de divulgação para que a plataforma seja conhecida pelo seu público-alvo. A equipe de processos é responsável por garantir que a plataforma funcione de maneira eficiente e que os processos de negócios estejam integrados. Eles monitoram os fluxos de trabalho e identificam possíveis gargalos, trabalhando para solucioná-los e melhorar continuamente a experiência do usuário, também são responsáveis por garantir a comunicação transparente entre todas as equipes e apresentar as entregas parciais dos sistemas.

A Figura 1 retrata, em linhas gerais, o organograma da empresa Alfa quando do levantamento de dados para este trabalho.

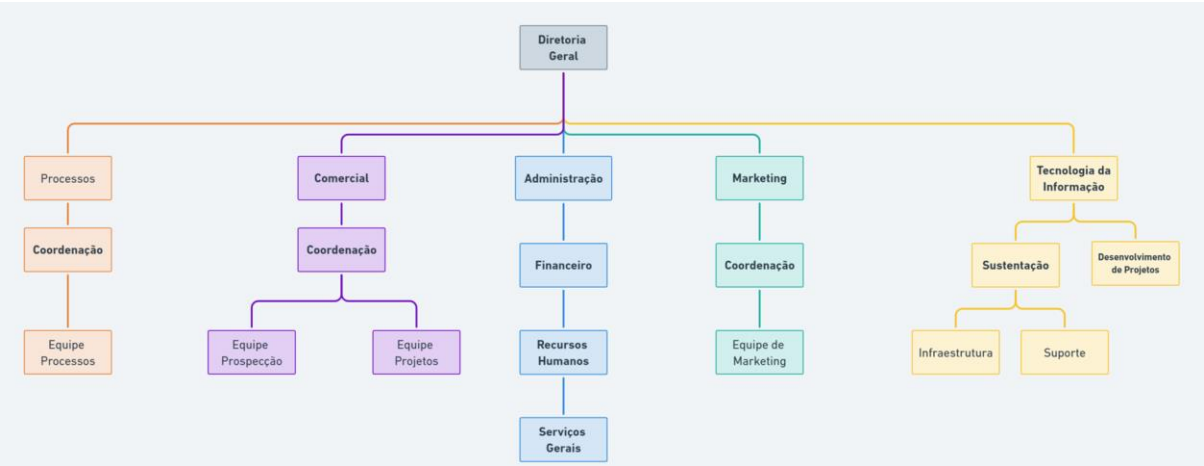


Figura 1 – Estrutura organizacional da empresa Alfa.

Fonte: dados da pesquisa.

Os gestores da empresa acreditam que essa abordagem inovadora pode trazer resultados positivos para a empresa e seus colaboradores. Além das equipes mencionadas anteriormente, a Alfa também está envolvendo outras equipes em diferentes fases do novo projeto chave, como a equipe de recursos humanos, responsável por acompanhar a adoção da plataforma pelos colaboradores, organizar dinâmicas com premiações e oferecer suporte para eventuais dúvidas e problemas, e a equipe de qualidade, que irá testar e validar a plataforma para garantir a sua qualidade.

A colaboração e envolvimento de todas as equipes é fundamental para o sucesso do projeto. Cada equipe tem um papel específico e importante na construção e implementação da plataforma, contribuindo com suas habilidades, experiências e conhecimentos para garantir que a plataforma seja eficiente, fácil de usar e incentivadora para as pessoas. Além disso, o envolvimento de diversas equipes no projeto também contribui para a disseminação da cultura de gamificação na empresa. Ao trabalharem juntas, visualizando os benefícios da gamificação na prática, as equipes se tornam defensoras da abordagem, consequentemente podem incentivar outros setores da empresa que são mais resistentes a mudanças, a adotarem a gamificação em suas atividades.

2.1. Entendimento Do Problema A Ser Tratado

A análise das equipes envolvidas na implementação da plataforma de gamificação na empresa Alfa revelou a gestão de acessos ineficiente e insegura, devido à realização manual do controle de acessos. Esse cenário se tornava ainda mais desafiador devido à presença de funcionários em regime de tempo parcial e provisório, tornando complexo o gerenciamento adequado dos acessos individuais. Além disso, a concessão de acessos privilegiados, como a capacidade de modificações em bancos de dados, representava um desafio adicional para garantir a segurança e o controle adequado. Contudo, a ausência de um sistema automatizado de controle de acesso agravava ainda mais essa complexidade operacional.

Um outro problema identificado estava relacionado à manutenção de acessos de ex-funcionários a determinados arquivos e informações mesmo após suas saídas da empresa. Isso incluía documentos em drives compartilhados em nuvem, links de apresentações, contas de e-mail e plataformas de comunicação, como Teams, Discord, Slack e Skype. Essa situação levantava sérias preocupações quanto à segurança, uma vez que informações confidenciais poderiam ser acessadas por pessoas não autorizadas, mesmo após o desligamento do

funcionário. Neste sentido, também tinha o risco de a empresa perder documentações de processos internos, de requisitos de sistemas ou até mesmo de acordos comerciais.

Além dos desafios mencionados, a observação das equipes da empresa Alfa indicou outras questões decorrentes da falta de um sistema adequado de controle de acesso. Por exemplo, havia dificuldades em gerenciar as permissões de acesso de acordo com a hierarquia organizacional de cada funcionário. Frequentemente, as permissões eram concedidas de forma genérica, sem levar em consideração a posição e as responsabilidades específicas de cada indivíduo. Isso resultava em pessoas possuindo acesso a informações irrelevantes, desnecessárias para suas funções, enquanto outras não tinham acesso a informações importantes para a realização de suas tarefas.

Mais um fator associado à ausência de um sistema eficiente de controle de acesso era a impossibilidade de monitorar e auditar as ações dos funcionários. Sem um registro adequado das atividades dos usuários, não era possível identificar quem acessou determinadas informações e quando, dificultando a detecção de possíveis violações de segurança ou comportamentos inadequados.

Destaca-se ainda um incidente no qual um ex-funcionário continuou recebendo e-mails da empresa, incluindo detalhes sobre atualizações da plataforma de gamificação, mesmo dois meses após sua saída. Acrescentando a isso, o ex-funcionário recebia regularmente notificações semanais contendo atas completas de reuniões gerais da empresa, que incluíam informações confidenciais e sensíveis sobre projetos em andamento, estratégias de negócios e dados de clientes. Essa situação é extremamente preocupante, pois evidencia uma falha grave na segurança dos dados corporativos. Ao deixar a organização, é essencial revogar imediatamente todas as permissões de acesso de um funcionário (WHITMAN; MATTORD, 2017).

É evidente que a segurança de dados e informações desempenha um papel fundamental no sucesso de qualquer organização. A exposição de informações confidenciais pode causar danos irreparáveis à reputação empresarial (LIMA, 2019) e prejudicar significativamente seus resultados financeiros. Portanto, é imprescindível que as empresas invistam em sistemas de controle de acesso eficientes e implementem políticas sólidas de segurança da informação, a fim de garantir a proteção dos dados e informações confidenciais.

Esse conjunto de problemas aponta para a importância de ter um sistema de controle de acesso eficiente, que permita gerenciar de forma detalhada as permissões de acesso e garantir que cada funcionário tenha acesso apenas às informações necessárias para o desempenho de suas funções. Adicionalmente, um sistema de controle de acesso adequado permite monitorar

e auditar as ações dos usuários, fornecendo informações valiosas para a prevenção e detecção de violações de segurança ou de comportamentos inadequados.

3. ANÁLISE DO PROBLEMA

3.1. Procedimentos Metodológicos

O presente trabalho consiste em um artigo tecnológico com abordagem qualitativa, utilizando o método de estudo de caso para analisar detalhadamente uma situação específica em uma empresa. Essa abordagem qualitativa permitiu coletar informações ricas e significativas, proporcionando uma compreensão abrangente dos problemas enfrentados pela empresa devido à ausência de um sistema eficiente de controle de acessos. Para o desenvolvimento no formato de artigo tecnológico, foram utilizadas as recomendações de Marcondes et al. (2017) e de Motta (2022).

Buscou-se identificar e compreender os detalhes do problema relacionado ao controle de acesso, bem como simular e avaliar uma solução proposta para esse problema. Para atingir esses objetivos, foram adotadas técnicas de coleta de dados, incluindo observação participante e entrevistas abertas com indivíduos-chave da organização e de outras empresas.

Na primeira etapa da coleta de dados, foram realizadas observações das rotinas das equipes que fazem uso de ferramentas internas e externas. Essa abordagem com duração de três meses, permitiu uma imersão na realidade das equipes e possibilitou identificar os problemas relacionados ao controle de acesso, bem como, compreender em profundidade o impacto desses problemas no desempenho das equipes. Durante essa fase, foram registradas anotações detalhadas, capturando os principais pontos de dificuldade encontrados.

Na segunda etapa, foram conduzidas entrevistas com os gestores das equipes de Processos, Marketing, Comercial, Recursos Humanos e Tecnologia da Informação, totalizando a participação de cinco gestores. O propósito dessas entrevistas foi compreender, a partir da percepção dos gestores, como e se a falta de controle de acessos estava afetando o trabalho das equipes. As entrevistas foram no formato aberto (sem um roteiro estruturado de perguntas), permitindo que os gestores compartilhassem suas percepções, experiências e desafios enfrentados nesse contexto específico em suas rotinas.

Na terceira e última etapa, foram conduzidas mais três entrevistas com gestores de outras empresas distintas. Essas entrevistas visavam a compreensão das dificuldades enfrentadas por essas organizações ao controlar o acesso de seus funcionários a ferramentas e aplicativos, além da preocupação com a segurança de dados e informações diante do fluxo e

rotatividade de colaboradores. Essa comparação entre diferentes empresas permitiu ampliar a compreensão do problema em estudo, agregando perspectivas adicionais e enriquecendo a análise da situação específica da empresa em foco.

A combinação das técnicas de observação participante e entrevistas proporcionou uma coleta abrangente de dados, permitindo uma análise aprofundada do problema do controle de acesso, em diferentes contextos organizacionais. A partir dessas informações, foi possível identificar as principais dificuldades enfrentadas e propor soluções adequadas com embasamento sólido.

3.2. Mapeamento do Problema

Com base nas informações levantadas das empresas que colaboraram para este estudo, evidenciou-se que no cotidiano das empresas de base tecnológica é destacado desafios diários no que está relacionado ao controle de acessos/permissões de funcionários nas ferramentas virtuais utilizadas para a realização de suas devidas atividades. Essas ferramentas podem ser sistemas ou aplicativos que são utilizados em dispositivos eletrônicos, como computadores, smartphones ou tablets, que disponibilizam funcionalidades e recursos para prover suporte em diversas situações: comunicação - os principais exemplos são aplicativos de videoconferência, e-mails, chats e plataformas de compartilhamento de arquivos permitem a comunicação remota entre indivíduos; gestão de projetos - são ferramentas que auxiliam no gerenciamento de atividades, prazos e entregas, permitindo a visualização do progresso, as respectivas responsabilidades e etc; armazenamento em nuvem - possibilitam guardar, compartilhar arquivos e documentos; produtividade - podem colaborar na organização de agendas, compromissos, lista de tarefas, rascunhos, anotações e etc; desenvolvimento de software - ferramentas para programação, repositório de códigos, controle de versão; análise de dados - análise e visualização de dados, ajudam na geração de ideias, informações validades para tomada de decisão.

No dia a dia dessas empresas, as equipes são envolvidas em projetos dinâmicos, com prazos apertados e estimativas de entregas contínuas, sendo comum que procedimentos de gerenciamento de acessos sejam negligenciados ou enfraquecidos, uma vez que o foco principal está na satisfação dos clientes. A urgência em atender às demandas do mercado, muitas vezes, leva a práticas emergenciais que não estão alinhadas, como o compartilhamento de senhas, arquivos, documentos ou a concessão de permissões excessivas, o que aumenta significativamente os riscos de segurança de dados e informações.

Além disso, em empresas iniciantes de base tecnológica, as estruturas organizacionais estão em constante mudanças, pois buscam se adaptar ao mercado, implementando novas metodologias de gestão se tornando cada vez mais flexíveis (BLANK; DORF, 2012). A definição clara de papéis e responsabilidades pode ser um problema, especialmente quando as equipes são reduzidas e têm de lidar com múltiplas tarefas. Isso dificulta o estabelecimento e o monitoramento adequado dos acessos às ferramentas. A falta de processos bem definidos e mapeados (documentados) resulta em gargalos na concessão e revogação de acessos, tornando o gerenciamento mais difícil e suscetível a erros.

Adicionalmente, a falta de conscientização sobre segurança da informação que inclusive, Pipkin (2000) ressalta como passo indispensável, por parte dos colaboradores também pode representar um obstáculo significativo no gerenciamento de acessos. Ainda sobre as empresas iniciantes, onde a cultura de segurança ainda está em desenvolvimento, os funcionários podem não compreender plenamente a importância de seguir os procedimentos de controle de acesso ou as consequências de práticas negligentes. A falta de treinamento e educação em segurança da informação contribui para comportamentos de risco, como o compartilhamento indiscriminado de informações sensíveis. As empresas de grande porte e com longa trajetória também enfrentam desafios significativos no que se refere ao gerenciamento de acessos e segurança da informação. Embora essas organizações possuam estruturas mais consolidadas e recursos dedicados à proteção, elas ainda lidam com questões complexas relacionadas à rotatividade de funcionários e à crescente utilização de tecnologias e sistemas que exigem autenticação por meio de login de usuários e senhas.

A rotatividade de funcionários é uma realidade presente em todas as empresas, independentemente de seu tamanho ou setor de atuação. Essa entrada e saída frequente de colaboradores demanda um cuidadoso controle dos acessos às ferramentas virtuais. No momento em que um funcionário deixa a empresa, é essencial garantir o cancelamento imediato de suas permissões e acessos, a fim de prevenir riscos potenciais, como vazamento de informações confidenciais ou uso indevido das ferramentas.

Como já citado anteriormente, nas empresas de grande porte, que contam com um considerável número de colaboradores, o desafio se amplia. É necessário estabelecer processos eficientes de gerenciamento de identidade e acesso, que permitam a rápida provisão e desativação de contas de usuários, além de garantir que os acessos sejam concedidos de acordo com as necessidades específicas de cada função. Isso requer um trabalho maior de uma coordenação efetiva entre as equipes e o setor de Recursos Humanos, a fim de assegurar uma

manutenção adequada dos acessos durante as etapas de contratação, desligamento e alterações de função.

Ademais, o crescente uso intensivo de tecnologias e sistemas que requerem login de usuários e senhas adiciona complexidade ao gerenciamento de acessos. As empresas de grande porte geralmente possuem uma variedade ampla de sistemas, aplicativos e plataformas, cada um com suas próprias políticas de segurança e requisitos de autenticação. Realizar o gerenciamento de forma eficaz, garantir a conformidade com as políticas de segurança e evitar a reutilização de senhas são desafios constantes que demandam atenção contínua e uma abordagem cuidadosa.

Diante desses desafios, é fundamental que as empresas de tecnologia da informação adotem medidas para aprimorar o gerenciamento de acessos (SILVA NETTO; SILVEIRA, 2007). Isso inclui a implementação de políticas claras de segurança da informação (FONTES, 2012), a adoção de processos formais de concessão e revogação de acessos, o estabelecimento de treinamentos periódicos para os colaboradores e a criação de uma cultura organizacional que valorize a segurança como um componente essencial das atividades diárias. Por meio dessas ações é possível minimizar os riscos de acessos não autorizados, vazamentos de informações sensíveis e outros comprometimentos de segurança, preservando a confiança dos clientes, a reputação da empresa e até mesmo evitando prejuízos financeiros.

Os estudos sobre segurança de dados e informações têm se tornado cada vez mais relevantes para as empresas, afinal, a perda ou roubo de informações sensíveis pode ter graves consequências. Hintzbergen *et al*. (2018) afirmam que as organizações precisam definir questões internas e externas que são relevantes para seus propósitos e que afetam suas habilidades de conquistar resultados pretendidos dos seus sistemas de gerenciamento de segurança da informação.

4. IMPLEMENTAÇÃO DA SOLUÇÃO

Ao observar o trabalho das equipes na Empresa Alfa, foi constatado que cada uma delas tinha diferentes tipos de ferramentas para realizar suas atividades, o que é comum em empresas com processos complexos e diversificados. Entretanto, a diversidade de ferramentas também gerava um problema de controle de acesso, uma vez que cada pessoa na empresa possuía diferentes níveis de acesso às ferramentas utilizadas pela equipe, dependendo de sua função, equipe ou nível hierárquico. O resultado desse cenário implicava diretamente, pois muitas pessoas com diferentes níveis de acesso a informações confidenciais externas e internas da

empresa. Ademais, foi comprovado que quando alguém deixava a empresa, muitas vezes ainda mantinha seus acessos ativos às ferramentas utilizadas pelas equipes, o que criava um risco de segurança significativo.

Durante as entrevistas com gestores da Alfa, eles destacaram alguns dos principais desafios que as equipes estavam enfrentando. Um dos principais problemas era o fato de que muitos funcionários tinham acesso a informações sensíveis, mesmo sem necessidade. Um fator preocupante, pois isso aumentava o risco de vazamento de informações importantes, comprometendo a segurança da empresa. Além disso, os gestores também mencionaram que a falta de controle de acessos dificultava a identificação de problemas de desempenho e produtividade das equipes. Sem um controle adequado, era difícil rastrear quem estava acessando quais sistemas e aplicativos, o que tornava mais complicado monitorar o desempenho das equipes.

Outra questão levantada pelos gestores foi a falta de padronização nos processos de acesso. Sem um controle adequado, cada equipe tinha sua própria forma de gerenciar os acessos aos sistemas e aplicativos, o que tornava o processo completamente desorganizado.

Já com relação aos dados levantados com as outras três empresas, o gestor da Empresa Beta relatou que sua equipe tem muita autonomia no uso de ferramentas, o que torna difícil o controle de acesso. Ele mencionou que os funcionários muitas vezes compartilham senhas e acessos sem autorização, o que representa um risco de segurança para a empresa. Ele também destacou que possui consciência da importância de manter o controle de acesso atualizado e garantir que apenas os funcionários que necessitam de acesso às informações confidenciais tenham suas devidas permissões.

O gestor complementou dizendo que a ausência de um controle adequado pode dificultar a avaliação das atividades dos funcionários, tornando a auditoria um processo mais complexo. Isso pode representar um grande problema para a empresa em termos de conformidade com regulamentações e leis aplicáveis, já que a empresa pode ser obrigada a demonstrar que segue determinados padrões de segurança e privacidade das informações. Sem um controle adequado de acesso, a empresa pode estar em risco de não cumprir essas obrigações regulatórias, o que pode resultar em sanções ou penalidades financeiras, além de danificar a reputação da empresa perante o mercado.

O gestor da empresa Gama mencionou que tem dificuldades em controlar o acesso às ferramentas utilizadas na empresa, pois não possui conhecimento técnico na área de tecnologia da informação. Ele reconhece que muitas vezes não compreende completamente as ferramentas e depende da equipe de desenvolvimento para auxiliá-lo nas configurações do controle de

acessos. Ele também enfatizou que é crucial garantir que somente os funcionários autorizados tenham acesso a informações confidenciais e que, quando um funcionário deixar a empresa, seus acessos devem ser imediatamente desativados para minimizar riscos de segurança.

E destacou a importância de garantir a integridade dos dados e a disponibilidade das ferramentas e aplicativos usados pela empresa. Ele ressaltou que falhas de segurança podem comprometer a integridade dos dados e prejudicar o desempenho da organização como um todo. Por isso, é essencial ter medidas de segurança adequadas em vigor para evitar tais falhas e garantir a continuidade dos projetos da empresa.

Por fim, o gestor da Empresa Delta compartilhou sua experiência com um ex-funcionário que costumava armazenar documentos e informações importantes da empresa em um repositório em nuvem, porém, utilizava o seu e-mail pessoal como forma de acesso a essa plataforma. Infelizmente, após a saída do funcionário, a empresa não conseguiu mais ter acesso a essas informações, já que estavam vinculadas à conta de e-mail pessoal do ex-funcionário, que foi desativada. Ele explicou que uma ferramenta unificada e dedicada ao controle de acesso seria uma solução mais eficiente e segura para a empresa.

Além disso, ele pontuou a importância de investir em treinamento e conscientização dos funcionários sobre a segurança da informação e a necessidade de garantir que apenas funcionários autorizados tenham acesso às informações confidenciais. Ele destacou a importância de um controle de acesso rígido, especialmente em relação a informações sensíveis e estratégicas da empresa, para evitar possíveis perdas e vazamentos de informações.

O gestor da Empresa Delta, após a entrevista sugeriu que a equipe de Recursos Humanos preparasse um treinamento sobre a importância da segurança de dados e informações, de forma remota para que todos da empresa pudessem participar.

Diante desse cenário, surgiu a ideia do sistema Ex.it em resposta à crescente necessidade de aprimorar a segurança da informação e otimizar o controle e a gestão de acessos a ferramentas digitais no contexto empresarial. O Ex.it foi concebido para abordar os desafios relacionados ao vazamento de informações em todas as fases do ciclo de emprego, desde a contratação, encerramento de contrato ou até o desligamento dos funcionários.

O Ex.it foi iniciado com a criação de uma documentação de requisitos e, paralelamente, pesquisas de mercado e análises de tendências foram conduzidas para compreender as necessidades emergentes no campo da segurança da informação. Em seguida, técnicas de modelagem de dados foram empregadas para elaborar uma representação estruturada dos elementos de dados que o sistema seria responsável por gerenciar. A modelagem de processos desempenhou um papel fundamental no projeto, com o desenvolvimento de diagramas de fluxo

de processos. Esses diagramas forneceram uma representação ilustrativa das interações do Ex.it com os usuários e sistemas externos, permitindo uma compreensão mais clara das etapas envolvidas no gerenciamento de acessos.

A prototipagem foi um passo adicional, com a criação do protótipo interativo do Ex.it. Essa abordagem permitiu que as partes interessadas (gestores) visualizassem como o sistema se pareceria e funcionaria na prática. O protótipo foi essencial para a obtenção de comentários valiosos e na validação de conceitos antes de se pensar em seu desenvolvimento em larga escala. Vale ressaltar que o Ex.it não está vinculado exclusivamente à empresa Alfa, sendo uma ideia independente que busca atender a diversas organizações.

O Ex.it é um software de segurança da informação pensado para a redução e eliminação de vazamentos de informações desde a contratação, alocação até o desligamento de funcionários. Ele é projetado para atender às necessidades dos clientes, fornecendo segurança de dados e informações da empresa, controlando o turnover e automatizando processos de gestão e manutenção de acessos.

Uma das principais funções do Ex.it é bloquear automaticamente de forma adequada o acesso dos funcionários que estão deixando a empresa ou mudando de área, projetos e atividades. Isso garante que as informações confidenciais e dados da empresa sejam protegidos.

O sistema também oferece funcionalidades com o uso de mineração de dados e inteligência de negócios que ajudam os usuários a tomar decisões estratégicas. Com essas funcionalidades, é possível fornecer aos usuários indicadores importantes que os ajudam a entender melhor o desempenho da empresa.

Outra configuração importante do Ex.it é a emissão de relatórios com informações validadas de pessoas, projetos e acessos. Esses relatórios fornecem uma visão detalhada dos funcionários e projetos em que estiveram envolvidos, permitindo que os usuários tenham uma melhor compreensão da segurança da informação e da eficiência operacional da empresa.

Para garantir a qualidade do software, durante o processo de criação do Ex.it, foi realizada uma auditoria com possíveis clientes para entender quais são os problemas que devem ser resolvidos e quais os parâmetros de qualidade necessários que a equipe de desenvolvimento deve seguir para a criação do escopo e seus respectivos usuários.

Com foco nas áreas de segurança e players (funcionários), o Ex.it envolve estratégias e preparação para a realidade produtiva desde o início do software em desenvolvimento. Além disso, o projeto inclui a infraestrutura de tecnologia da informação e a padronização dos processos com a criação de requisitos funcionais e não funcionais, fluxos, atores e interfaces.

É importante ressaltar que o acesso ao Ex.it será restrito apenas aos gestores de equipes, membros do RH ou diretores que possuam a devida autorização. Isso se deve ao fato de que a plataforma contém informações sensíveis e confidenciais, cujo acesso deve ser controlado e limitado a pessoas devidamente autorizadas. Para garantir a segurança das informações e o controle de acessos, a plataforma contará com um sistema de autenticação seguro e com níveis de acesso pré-definidos para cada usuário. Além disso, também terá a funcionalidade de rastrear e registrar todas as atividades realizadas pelos usuários na plataforma, permitindo identificar qualquer possível violação de segurança ou uso indevido.

Vale destacar que será necessário integrar o Ex.it com as ferramentas virtuais para melhor aproveitamento das funcionalidades, as ferramentas de gestão de pessoas, por exemplo, que muitas das vezes já são utilizadas e armazenam os registros dos funcionários, deverão ser integradas para evitar o retrabalho manual de ter que recadastrar todos os funcionários manualmente, mesmo que esta opção também esteja disponível, caso alguma ferramenta virtual seja limitada a integração.

Em relação a funcionalidade chave do sistema, a de bloqueio, manutenção e controle de acessos, será necessário um trabalho de análise e configuração da plataforma com as ferramentas utilizadas pelas empresas, a fim de garantir a compatibilidade e o pleno funcionamento. Caso alguma ferramenta seja incompatível com a possibilidade de ações instantâneas, o Ex.it terá a funcionalidade de enviar notificações automáticas de alerta ao gestor responsável pelo funcionário, assim ele será informado para que complete a ação desejada diretamente na ferramenta em questão.

A implementação do Ex.it é uma solução eficiente e inovadora, o poderoso sistema é capaz de trazer autonomia incomparável, sem comentar que o layout conta com elementos modernos e descontraídos, com o objetivo de deixar o processo intuitivo, assertivo, além de ser um forte aliado para os usuários nas suas rotinas e desafios.

Figura 2 – Tela de Login do Ex.it
Fonte: dados da pesquisa.

A tela de login do Ex.it, mostrada na Figura 2, é a primeira etapa para acessar todas as funcionalidades do software. Nesta tela, é necessário preencher o campo de e-mail e senha previamente cadastrados pelos gestores de equipe, RH ou diretores autorizados a acessar o sistema. Após inserir as informações de login, o usuário será direcionado para a página inicial do Ex.it, onde será possível visualizar todas as opções disponíveis para controle e gestão de dados e informações da empresa. Essa etapa é fundamental para garantir a segurança dos dados e a privacidade das informações contidas no software, permitindo que apenas usuários autorizados possam acessar o sistema.

Além disso, para aumentar ainda mais a segurança do Ex.it, é importante que os usuários criem senhas fortes e mantenham a confidencialidade de suas informações de login, evitando o compartilhamento com terceiros e possíveis violações de segurança.

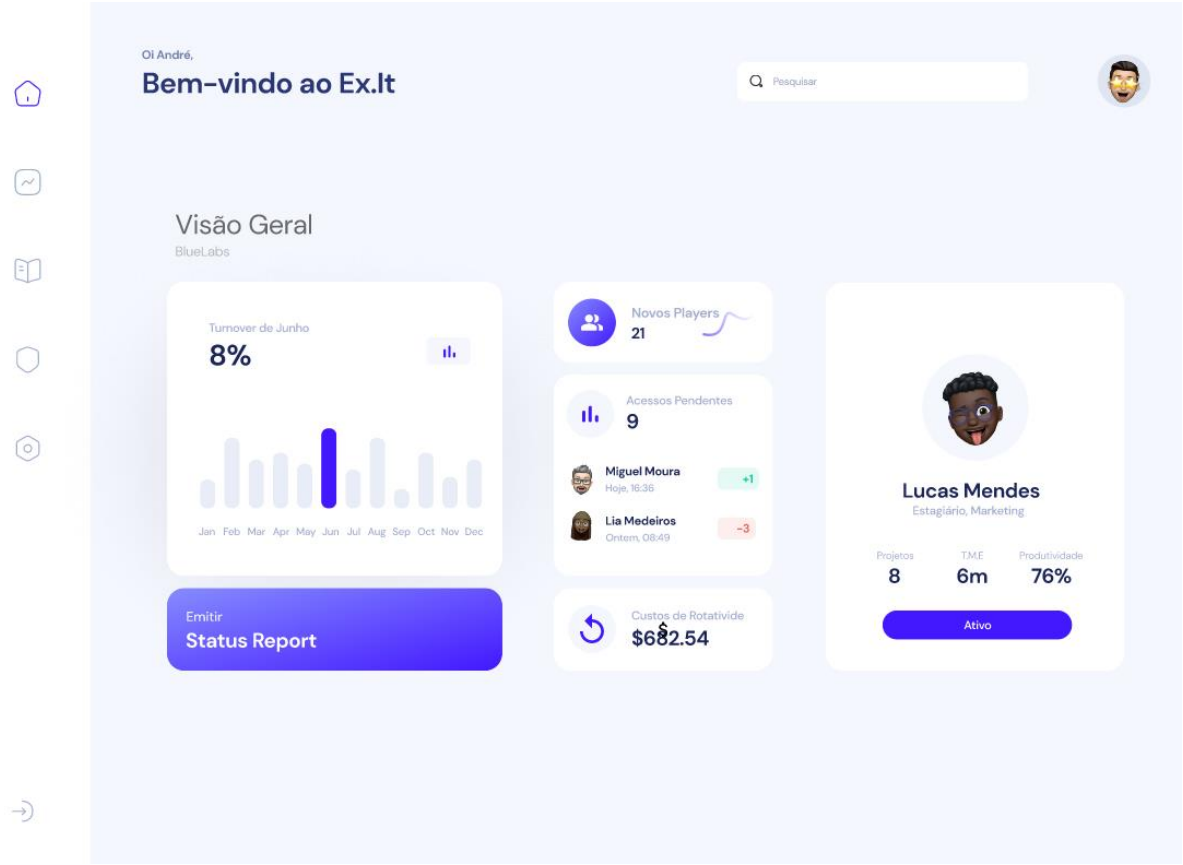


Figura 3 – Tela Principal do Ex.it

Fonte: dados da pesquisa.

Após o login, o usuário será direcionado para a tela principal do Ex.it, conforme Figura 3, que exibirá uma mensagem de boas-vindas personalizada com o nome do usuário e a data atual. Na parte superior da tela, haverá um gráfico de visão geral que apresentará um resumo das informações de rotatividade dos funcionários da empresa, permitindo que o gestor tenha uma visão clara e objetiva do cenário atual.

Na tela principal, o usuário também terá a funcionalidade de emitir um Status Report, que permitirá gerar um arquivo em PDF com informações específicas de sua escolha. Essas informações podem ser filtradas por período, setor ou tipo de funcionário, por exemplo. Haverá um indicador de novos players (funcionários) na empresa, que será atualizado automaticamente sempre que um novo funcionário for contratado. Além disso, o usuário poderá visualizar uma lista de acessos pendentes que precisam ser aprovados ou negados.

Outro indicador importante na tela principal será o custo de rotatividade, que permitirá que o gestor tenha uma ideia clara do impacto financeiro causado pela rotatividade dos funcionários. Inclusive, um estudo feito Ruiz, Perroca e Jericó (2015) destacou essa importância do gerenciamento do custo da rotatividade de colaboradores e o impacto financeiro

do custo do desligamento, que representou três vezes o salário médio de uma equipe de enfermagem estudada. Ainda na tela principal, haverá informações sobre um usuário filtrado como exemplo, no caso o funcionário Lucas Mendes, estagiário de marketing, que está alocado em 8 projetos, possui 6 meses na empresa e tem 76% de produtividade. Essa informação é útil para o gestor ter uma visão mais detalhada do desempenho de cada funcionário.

A tela principal do Ex.it fornecerá um panorama completo das informações dos players, permitindo que o gestor tome decisões mais informadas e estratégicas para a empresa.

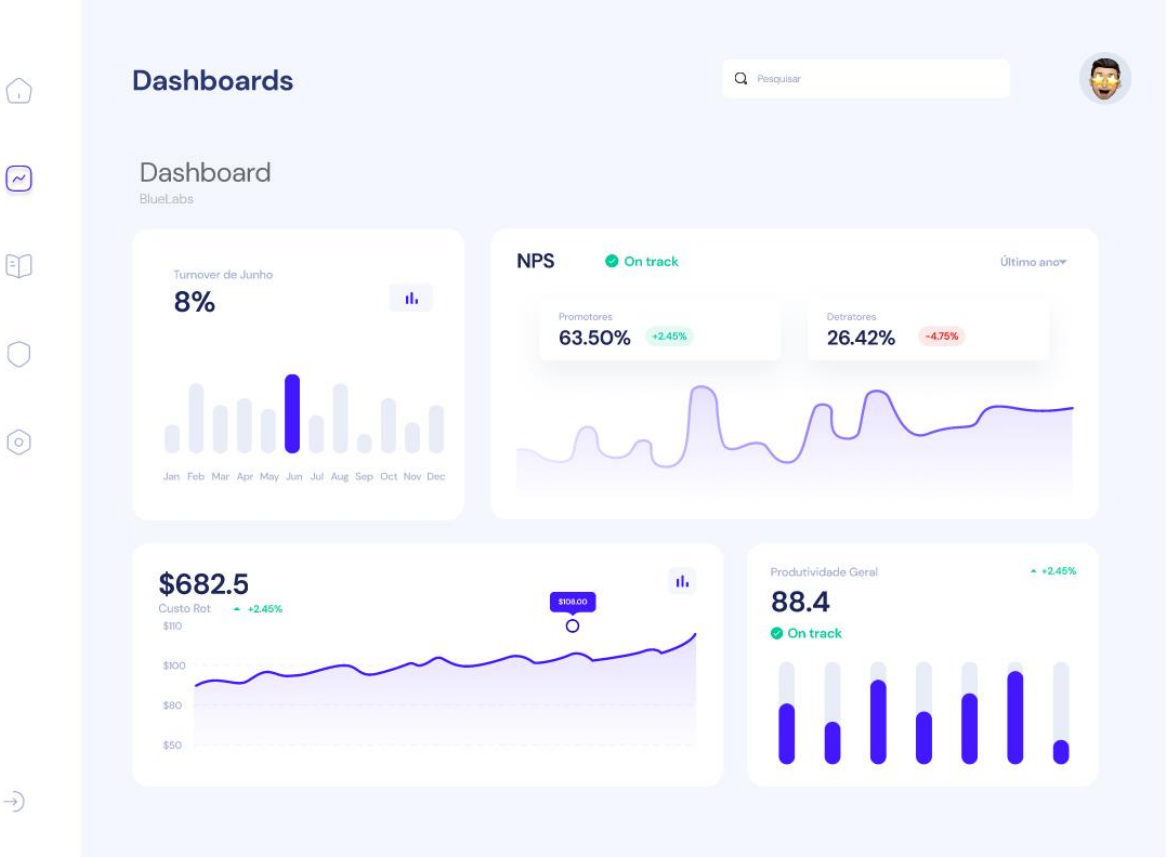


Figura 4 – Tela de Dashbords do Ex.it

Fonte: dados da pesquisa.

A tela de Dashboards do Ex.it, apresentada na Figura 4, é uma ferramenta essencial para o monitoramento dos indicadores mais importantes de uma empresa. Nela, é possível visualizar de forma clara e objetiva informações sobre o Turnover, NPS, Custo de Rotatividade e Produtividade Geral da Empresa. Segundo Chiavenato (2010, p. 88) o *turnover* é o índice de rotatividade de funcionários em uma empresa, ou seja, a quantidade de saídas de colaboradores em relação ao número total de funcionários. É um indicador importante para medir a satisfação e a retenção de talentos.

O NPS é o Net Promoter Score, uma métrica utilizada para avaliar a satisfação dos clientes em relação à empresa. É uma medida de como os clientes recomendariam a empresa para outras pessoas (Reichheld, 2003). E o Custo de Rotatividade é o valor gasto pela empresa em processos de demissão, contratação e treinamento de novos funcionários. É um fenômeno destrutivo, que traz muitos custos para a organização e situa-se na faixa de 25% a 75% da equipe das organizações de varejo (FEINBERG; JEPPESON, 2000).

A Produtividade Geral da Empresa é o indicador que mede a eficiência na conversão de recursos em bens econômicos, isto é, é a relação entre o que é produzido (bens e/ou serviços) e recursos que são usados para produzi-los (WAINER, 2002). É um indicador que ajuda a avaliar a eficácia dos processos e métodos de trabalho.

Através da tela de Dashboards do Ex.it, é possível ter uma visão geral sobre a situação desses indicadores, o que ajuda na tomada de decisões estratégicas. Dashboard trata-se de um display visual das informações mais importantes necessárias para alcançar um ou mais objetivos, consolidados e organizados em uma única tela para que a informação possa ser monitorada rapidamente (FEW, 2006). Os dados são apresentados de forma clara e objetiva em gráficos e tabelas, facilitando a interpretação e análise dos resultados.

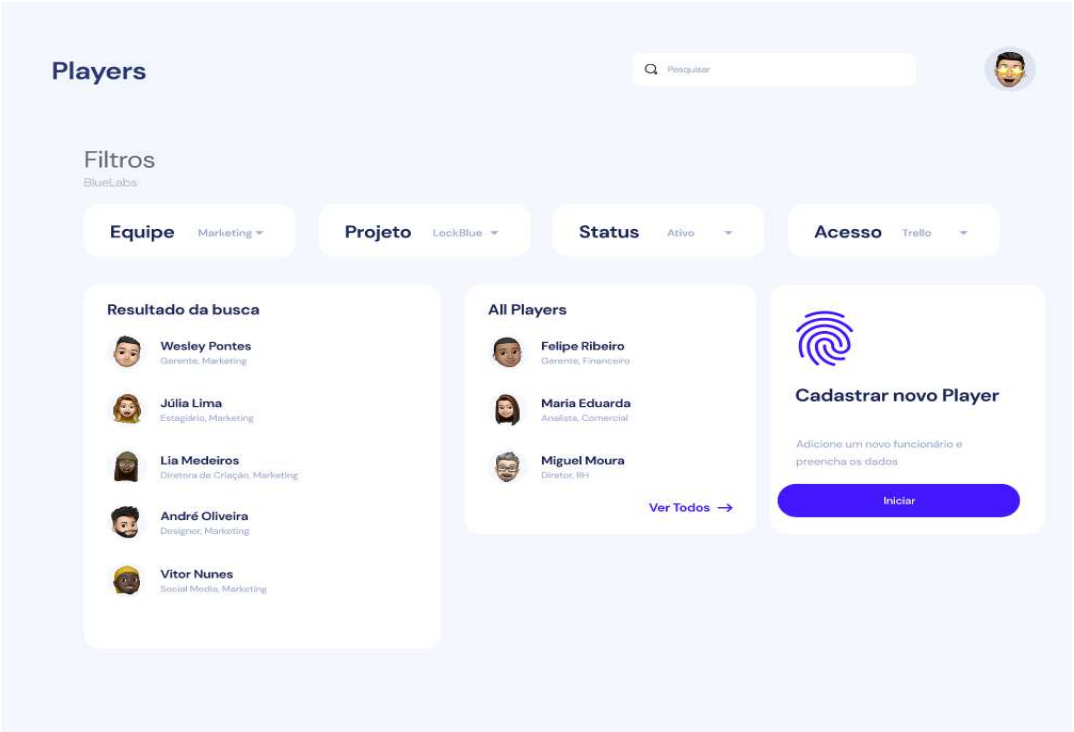


Figura 5 – Tela de Player do Ex.it

Fonte: dados da pesquisa.

A tela de Player no Ex.it é uma das mais importantes, de acordo com a Figura 5, pois permite que os gestores e o RH tenham acesso a informações completas e atualizadas sobre

todos os colaboradores da empresa. A tela conta com diversos filtros para facilitar a busca de informações, tais como: equipe, projeto, status e acesso.

O filtro de equipe permite que o usuário selecione a equipe específica que deseja visualizar, como por exemplo, a equipe de marketing, a equipe de processos, entre outras. Já o filtro de projeto permite que o usuário selecione o projeto específico em que o colaborador está ou foi alocado. O filtro de status permite que o usuário filtre os colaboradores de acordo com seu status na empresa, como ativo, inativo, entre outros. Por fim, o filtro de acesso permite que o usuário filtre os colaboradores de acordo com as ferramentas utilizadas e cadastradas, como por exemplo, Trello (ferramenta visual que possibilita ao time o gerenciamento de qualquer tipo de projeto, fluxo de trabalho ou monitoramento de tarefas), Miro (plataforma visual colaborativa em formato de lousa online que pode unir suas equipes a qualquer hora, de qualquer lugar), entre outras. Com seus devidos níveis de acessos, como por exemplo, colaboradores que possuem acesso total, acesso restrito, ou nenhum acesso.

Ao realizar a busca, é possível visualizar todos os funcionários que correspondem aos filtros selecionados, com informações detalhadas como nome, cargo, equipe, projeto, status, data de admissão, entre outras informações importantes. Além disso, a tela de Player também permite que o usuário cadastre novos colaboradores, inserindo suas informações pessoais, profissionais e de acesso ao sistema. Essa funcionalidade é essencial para manter o cadastro de colaboradores sempre atualizado e garantir a segurança das informações da empresa. Além da opção de cadastrar manualmente um novo player, o Ex.it também permite que o cadastro seja realizado de forma automática por meio de integrações com outros sistemas que armazenam dados das pessoas da empresa. Dessa forma, o processo de inclusão de novos colaboradores no sistema é simplificado e os dados ficam mais precisos e atualizados. A integração também evita o retrabalho e possíveis erros de digitação, tornando a gestão de pessoas mais eficiente. A tela de Player é, portanto, uma interface completa e indispensável para a gestão de colaboradores de qualquer empresa.

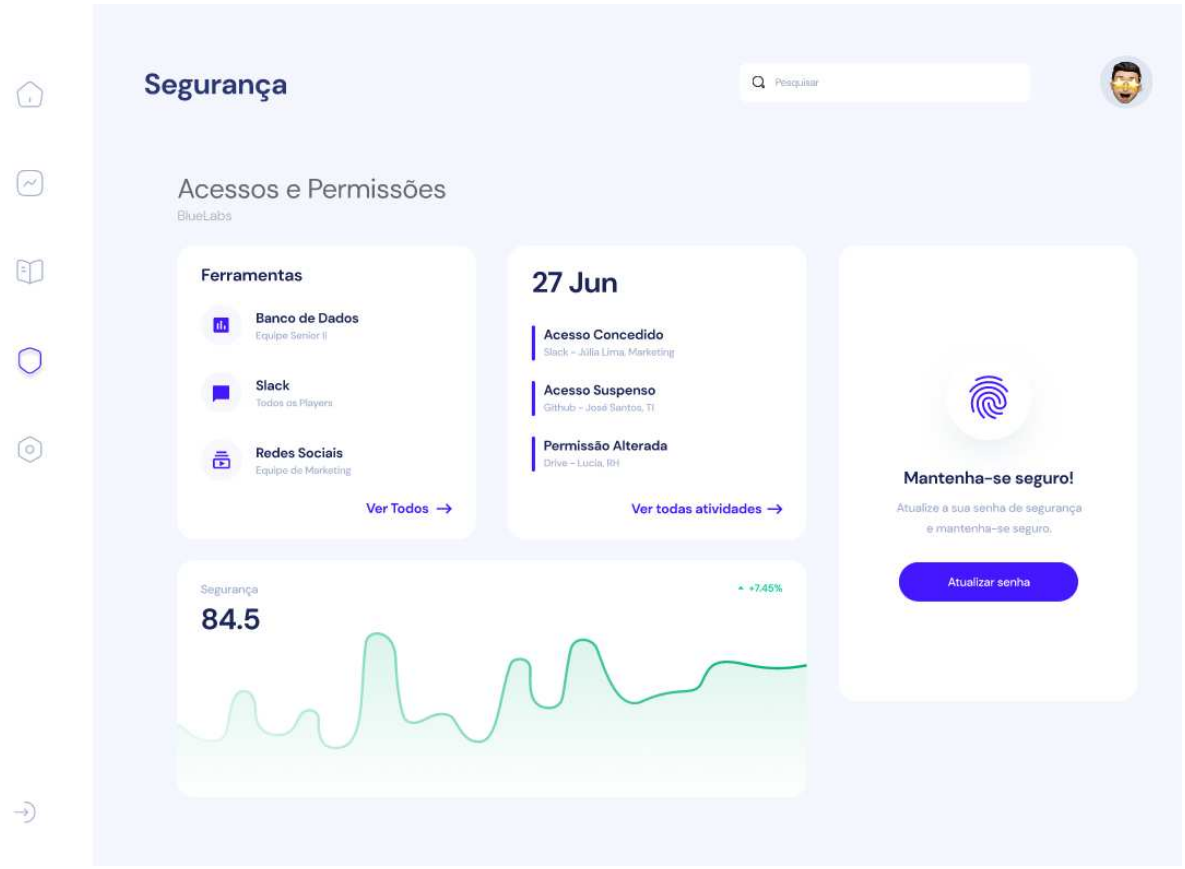


Figura 6 – Tela de Segurança do Ex.it

Fonte: dados da pesquisa.

A tela de Segurança do Ex.it, mostrada na Figura 6, é uma das mais importantes, pois permite a gestão de acessos e permissões das ferramentas utilizadas pelas equipes. Nela, os gestores de equipes, RH ou diretores podem visualizar as permissões concedidas a cada colaborador, bem como conceder ou revogar acessos e permissões. Além disso, a tela de Segurança do Ex.it conta com um histórico de acessos concedidos, acessos suspensos, permissões alteradas e outras atividades relevantes relacionadas à segurança. Dessa forma, é possível monitorar as ações realizadas e identificar eventuais falhas ou tentativas de acessos indevidos.

A tela também possui a funcionalidade de atualização de senha de ferramentas utilizadas pelas equipes, garantindo que as senhas sejam trocadas periodicamente e a segurança das informações seja preservada. Por fim, a tela de Segurança conta com um indicador visual de nível de segurança em relação às permissões e acessos concedidos, permitindo que os gestores monitorem e garantam a segurança dos dados da empresa.

5. CONCLUSÃO

Este trabalho, mostrou a relevância do controle de acessos às ferramentas digitais em empresas e a necessidade de soluções eficazes, como o software Ex.it, projetado a partir da experiência com a empresa Alfa. Através da pesquisa e entrevistas com gestores, além de uma revisão nos conceitos sobre segurança de dados, consegue-se demonstrar que o software Ex.it é uma ferramenta robusta e eficiente para unificação de acessos digitais, garantindo um grau maior de segurança de dados e informações.

A contribuição do trabalho não se limita apenas à apresentação de uma solução, este estudo também intensificou a compreensão da problemática da segurança de dados nas empresas. Neste sentido, auxiliou na promoção da conscientização acerca da importância de investir em soluções de segurança de dados e informações. Evidenciando que a segurança de dados não se constitui mais em uma escolha, mas sim uma necessidade imprescindível em um ambiente de negócios que está se tornando cada vez mais digital e interconectado.

A solução proposta não apenas atende à situação apresentada, mas também abre portas para futuras pesquisas e aprimoramentos tanto na gestão de recursos humanos como na segurança de dados. Algumas dessas perspectivas é fazer com que o Ex.it funcione junto com outros programas que auxiliam a gerenciar informações sobre recursos de empresas. Essa possibilidade representa um avanço substancial, reduzindo consideravelmente o trabalho manual de cadastro de informações relacionadas às pessoas levando à otimização de tempo e redução de erros comuns associados a entradas manuais, garantindo a precisão e a integridade dos dados. Além disso, é importante considerar a questão de existirem sistemas em que não é possível fazer a configuração de acesso direta no Ex.it. Uma alternativa seria enviar uma notificação ou e-mail automático de alerta ao gestor caso tente desativar ou configurar um determinado acesso, o que pode auxiliar na segurança do sistema.

Outro aspecto que pode ser estudado é a coleta de dados suficientes para alimentar os painéis de controle com informações relevantes. Esse enfoque terá um impacto direto na capacidade dos gestores de tomar decisões. É fundamental que eles tenham à disposição indicadores confiáveis e alinhados para avaliar o desempenho tanto dos funcionários quanto da organização como um todo. Implicando na possibilidade de coletar, analisar e utilizar métricas como a taxa de rotatividade, retenção de pessoal e o Net Promoter Score (NPS) para realizar uma avaliação precisa do desempenho das empresas.

Para tornar a integração com outros sistemas mais rápida, é necessário realizar uma etapa de análise para entender como o Ex.it pode ser utilizado de forma mais eficiente. É

importante mapear todos os processos que envolvem a gestão de pessoas e identificar onde o Ex.it pode ser inserido de forma mais estratégica, evitando duplicidade de informações e fortalecendo o desempenho do sistema.

Quanto às limitações, podemos destacar que o estudo se limitou a apresentar uma solução para a problemática proposta, sem aprofundar-se em outras questões relacionadas à segurança de dados, como a privacidade e a proteção contra-ataques cibernéticos. Além disso, o estudo foi baseado em uma pesquisa com número limitado de empresas, com entrevistas realizadas apenas com gestores, o que pode ter limitado a abrangência dos resultados.

REFERÊNCIAS

BLANK, S.; DORF, B. **The Startup owner's manual:** The step-by-step guide for building a great company. K & S Ranch, 2012.

CHIAVENATO, I. **Gestão de Pessoas**. 3Ed. Rio de Janeiro: Elsevier, 2010.

FEINBERG, R.A; JEPPESON, N. **Validity of exit interviews in retailing**. Journal of Retailing and Consumer Services, Philadelphia, v. 7, n. 3, p. 123-127, jul. 2000

FEW, S. **Information Dashboard Design** - The Effective Visual Communication of Data. Sebastopol: O'Really Media, 2006.

FONTES, E. **Políticas e Normas para a Segurança da Informação:** Como desenvolver, implementar e manter regulamentos para a proteção da informação nas organizações. Brasport, 2012.

HINTZBERGEN, J.; HINTZBERGEN, K.; SMULDERS, A.; BAARS, H. **Fundamentos de Segurança da Informação:** com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport Livros e Multimídia Lda, 2018.

LIMA, I., **A Segurança da Informação no Contexto das Sociedades de Revisores Oficiais de Contas Portuguesas**. ISCAC, 2019. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/31887/1/Isadora_Lima.pdf. Acesso em: 28 jul. 2023.

MARCONDES, R. C., MIGUEL, L. A. P., FRANKLIN, M. A., PEREZ, G. **Metodologia para elaboração de trabalhos práticos e aplicados**: administração e contabilidade. São Paulo: Editora Mackenzie, 2017.

MASCARENHAS NETO, P. T.; ARAÚJO, W. J. **Segurança da informação:** Uma visão sistêmica para implantação em organizações. João Pessoa: Editora UFPB, 2019.

MIRO. Página inicial do Miro. Disponível em: https://miro.com/pt/. Acesso em: 27 jul. 2023

PIPKIN, D. L. **Information security:** protecting the global enterprise. New Jersey, USA: Prentice Hall PTR, 2000.

REICHHELD, F. F. **Harvard Business Review**. The one Number you Need to

RUIZ, P. B. DE O.; PERROCA, M. G.; JERICÓ, M. DE C. Cost of nursing turnover in a Teaching Hospital. **Revista da Escola de Enfermagem da U S P**, v. 50, n. 1, p. 104–111, 2016.

SILVA NETTO, A.; SILVEIRA, M. A. P. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. **Journal of Information Systems and Technology Management**, v. 4, n. 3, p. 375–397, 2007.

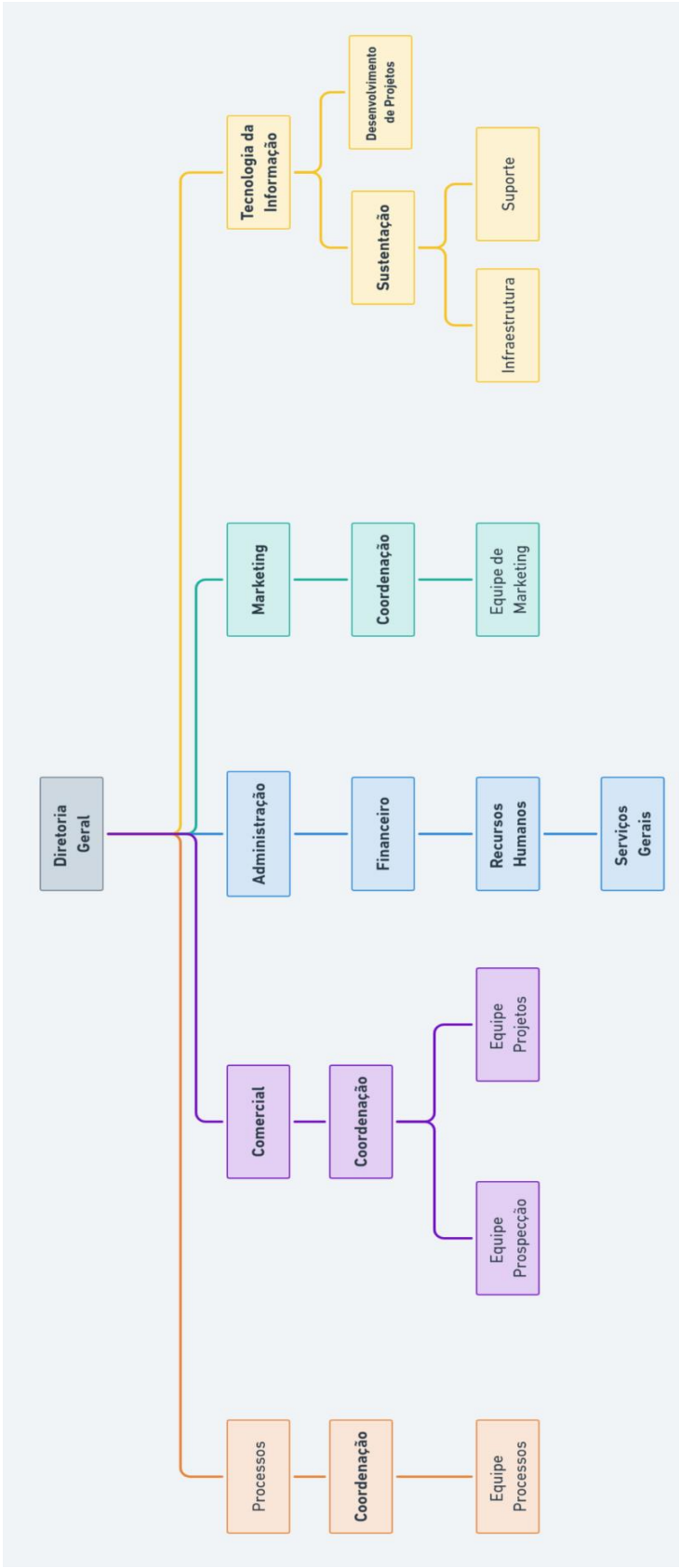
TRELLO. Página inicial. Disponível em: https://trello.com/pt-BR/tour. Acesso em: 27 jul. 2023.

WAINER, J. O Paradoxo da Produtividade. **Informática, Organizações e Sociedade no Brasil**. São Paulo: Cortez, 2002

WHITMAN, M.; MATTORD, H. **Principles of information security**. 6. ed. Mason, OH, USA: CENGAGE Learning Custom Publishing, 2017.

APÊNDICES

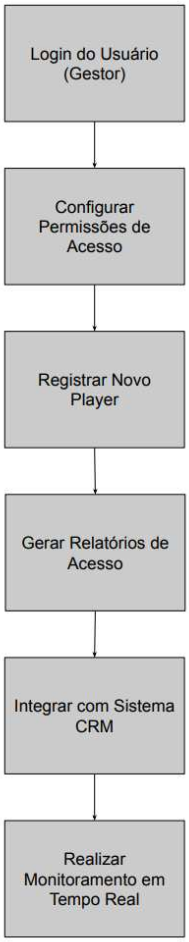
Apêndice 1- Organograma da empresa Alfa



Apêndice 2 - Lista de requisitos do sistema

Tipo de Requisito	Prioridade	Nome	Observação
Requisito Funcional	Essencial	Autenticação de Usuário	Necessário para garantir a segurança do sistema.
Requisito Funcional	Importante	Cadastro de Novos Usuários	Permite a inclusão de novos usuários no sistema.
Requisito Funcional	Importante	Configuração de Permissões de Acesso	Essencial para o controle de segurança.
Requisito Funcional	Importante	Geração de Relatórios de Acesso	Importante para auditorias de segurança.
Requisito Funcional	Desejável	Integração com Sistema CRM	Pode melhorar a eficiência na gestão de dados.
Requisito Funcional	Essencial	Monitoramento em Tempo Real	Importante para a segurança em tempo real.
Requisito Funcional	Desejável	Notificações por E-mail	Pode melhorar a comunicação com os usuários.
Requisito Funcional	Importante	Registro de Atividades do Sistema	Importante para rastreamento de eventos.
Requisito Funcional	Desejável	Integração com ERP	Pode facilitar a gestão de recursos.
Requisito Funcional	Importante	Personalização de Permissões	Importante para se adequar às necessidades específicas.
Requisito Não Funcional	Essencial	Segurança de Dados	Crítico para proteção de informações confidenciais.
Requisito Não Funcional	Importante	Desempenho do Sistema	Importante para garantir a eficiência do sistema.
Requisito Não Funcional	Importante	Confiabilidade	Importante para garantir a disponibilidade do sistema.
Requisito Não Funcional	Desejável	Usabilidade	Pode melhorar a experiência do usuário.
Requisito Não Funcional	Desejável	Compatibilidade	Pode ser desejável para suportar diferentes plataformas.
Requisito Não Funcional	Essencial	Escalabilidade	Importante para atender ao crescimento futuro.
Requisito Não Funcional	Desejável	Facilidade de Manutenção	Pode reduzir custos de manutenção a longo prazo.
Requisito Não Funcional	Importante	Tolerância a Falhas	Importante para a continuidade do serviço.
Requisito Não Funcional	Importante	Segurança contra Ataques Cibernéticos	Importante para a proteção contra ameaças.

Apêndice 3 - Fluxo de Atividades



Login do Usuário:

- O Gestor inicia o sistema Ex.it e insere suas credenciais (nome de usuário e senha).
- O sistema verifica as credenciais e autentica o usuário.
- O usuário acessa o sistema após a autenticação bem-sucedida.

Configurar Permissões de Acesso:

- Os administradores acessam o módulo de configuração de permissões.
- Eles selecionam os usuários ou grupos de usuários para os quais desejam definir ou modificar permissões de acesso.
- Os administradores especificam quais recursos, pastas, arquivos ou áreas do sistema cada usuário ou grupo pode acessar.
- As configurações de permissão são salvas no sistema e aplicadas aos usuários correspondentes.

Registrar Novo Player:

- Os administradores ou gerentes de recursos humanos acessam o módulo de gerenciamento de players.
- Eles preenchem as informações do novo usuário, incluindo nome, e-mail, cargo, departamento e outras informações relevantes.
- Um nome de player e senha temporária são gerados.
- O novo player recebe as credenciais temporárias e é notificado para fazer login e alterar a senha.

Gerar Relatórios de Acesso:

- Os administradores ou gerentes de segurança acessam o módulo de relatórios.
- Eles selecionam o tipo de relatório desejado.
- Os critérios de pesquisa são especificados.
- O sistema gera o relatório com base nos critérios selecionados e exibe ou exporta os resultados.

Integrar com Sistema CRM:

- Os administradores configuram a integração com o sistema CRM.
- Eles especificam como os dados devem ser compartilhados entre o Ex.it e o sistema CRM.
- A integração é ativada, permitindo o compartilhamento de informações em tempo real entre os sistemas.

Realizar Monitoramento em Tempo Real:

- Os administradores ou equipes de segurança acessam o módulo de monitoramento em tempo real.
- Eles visualizam informações sobre atividades e acessos em andamento.
- Alertas automáticos são gerados em caso de atividades suspeitas ou violações de segurança.

Apêndice 4 - Diagrama de sequência