The Enlighten Company

Relatório de Asseguração dos Auditores Independentes sobre a descrição e eficácia operacional de controles.
24 de março de 2023

ALF/TG/AA/TP
409/2023

Sumário

Seção I – Relatório de Asseguração dos Auditores Independentes sobre a descrição e eficácia operacional de controles

Rua Castilho, 392 - 3º Andar
Brooklin - São Paulo - SP
CEP 04568-010
São Paulo - Brasil
T: +5511 5102-2510

T: +55 (11)5102-2510

www.bakertillybr.com.br

Para
The Enlighten Company
São Paulo – SP

Alcance

Fomos contratados para emitir um relatório sobre a descrição elaborada pela The Enlighten Company (Companhia), (páginas 11 a 18) do seu Portal do BEN para processamento de transações de clientes durante o período de 01 de junho de 2022 a 31 de dezembro de 2022, e sobre o projeto de controles relacionados com os objetivos de controle especificados na descrição.

Os sistemas integrantes do Portal do BEN contidos neste escopo são:

- Asken;
- Cleaner;
- Closing;
- Budgeetfy;
- Pagben;
- URI; e
- EN-Space.

Responsabilidades da organização prestadora de serviços

A Companhia é responsável por: (i) elaborar a descrição e a correspondente afirmação (página 8), incluindo a integridade, a precisão e o método de apresentação da descrição e da afirmação; (ii) prestar os serviços incluídos na descrição; (iii) especificar os objetivos de controle; e (iv) projetar, implementar e operacionalizar os controles de maneira efetiva para alcançar os objetivos de controle especificados.

Responsabilidade dos auditores independentes

Nossa responsabilidade é a de expressar uma opinião sobre a descrição elaborada pela Companhia, bem como sobre o projeto e a operação de controles relacionados com os objetivos de controle especificados nessa descrição, com base em nossos procedimentos. Conduzimos nosso trabalho de acordo com a NBC TO 3402 – Relatórios de Asseguração de Controles em Organização Prestadora de Serviços, emitida pelo Conselho Federal de Contabilidade. Essa Norma requer o cumprimento de exigências éticas pelos auditores e que o trabalho seja planejado e executado para a obtenção de segurança razoável sobre se a descrição está apresentada adequadamente, em todos os aspectos relevantes, e se os controles foram apropriadamente projetados e estão operando efetivamente.

Responsabilidade dos auditores independentes--Continuação

Um trabalho de asseguração para emitir um relatório sobre a descrição, o projeto e a eficácia operacional dos controles de organização prestadora de serviços envolve a execução de procedimentos selecionados para obtenção de evidência sobre as divulgações na descrição do seu sistema, projeto e efetividade operacional dos controles. Os procedimentos selecionados dependem do julgamento do auditor, incluindo a avaliação dos riscos de que a descrição não esteja apresentada adequadamente e de que os controles não foram apropriadamente projetados ou não estão operando efetivamente. Nossos procedimentos incluíram testes da eficácia operacional dos controles que consideramos necessários para fornecer segurança razoável de que os objetivos de controle especificados na descrição foram alcançados. Um trabalho de asseguração desse tipo incluí, também, a avaliação da apresentação geral da descrição, da adequação dos objetivos nela especificados e da adequação dos critérios especificados pela organização prestadora de serviços e descritos na página (11).

Acreditamos que a evidência obtida é suficiente e apropriada para fundamentar nossa opinião.

Limitações de controles na organização prestadora de serviços

A descrição foi elaborada pela Companhia para atender as necessidades comuns de ampla gama de clientes e de seus auditores independentes e, portanto, pode não incluir todos os aspectos do sistema que cada cliente possa considerar importante em seu próprio ambiente específico. Além disso, devido à sua natureza, os controles da organização prestadora de serviços podem não prevenir ou detectar todos os erros ou omissões no processamento ou no relato das transações.

Opinião

Nossa opinião foi fundamentada nos assuntos descritos neste relatório. Os critérios utilizados na formação de nossa opinião são aqueles descritos na Seção IV - Teste do Desenho e Eficácia Operacional dos Controles. Em nossa opinião, em todos os aspectos relevantes:

(a) A descrição apresenta adequadamente o sistema Portal do BEM, conforme projetado e implementado durante o período de 01 de junho a 31 de dezembro de 2022;
(b) O projeto dos controles relacionados com os objetivos de controle especificados na descrição foi adequado durante o período de 01 de junho a 31 de dezembro de 2022 e;
(c) Os controles testados, necessários para fornecer segurança razoável de que os objetivos de controle especificados na descrição foram alcançados, operaram efetivamente durante o período 01 de junho a 31 de dezembro de 2022.

Usuários previstos e objetivo

Este relatório se destina exclusivamente aos clientes que utilizaram o sistema Portal do BEN da Companhia e seus auditores independentes que possuem entendimento suficiente para considerá-lo, em conjunto com outras informações, incluindo aquelas sobre controles operacionalizados pelos próprios clientes, na avaliação dos riscos de distorções relevantes nas suas demonstrações contábeis.

São Paulo, 24 de março de 2023.

Baker Tilly 4Partners Auditores Independentes S.S.
CRC 2SP-031.269/O-1

Alexandre De Labetta Filho
Contador CRC 1SP-182.396/O-2

Seção II – Declaração da Entidade Prestadora de Serviço

A descrição foi elaborada para clientes que usaram o sistema Portal do BEN e seus auditores que têm entendimento suficiente para considerar a descrição, juntamente com outras informações sobre controles operacionalizados pelos próprios clientes, na obtenção de entendimento dos sistemas de informações de clientes relevantes para relatórios financeiros. A Companhia confirma que:

(a) A descrição nas páginas [11-18] apresenta adequadamente o sistema Portal do BEN para processamento de transações de clientes no período de 01 de junho de 2022 a 31 de dezembro de 2022. Os critérios usados na elaboração dessa afirmação foram as seguintes:

(i) Apresenta como o sistema foi projetado e implementado, incluindo:

- Os tipos de serviços prestados, incluindo, conforme apropriado, as classes de transações processadas;
- Os procedimentos dos sistemas de tecnologia da informação (TI) e manuais usados para iniciar, registrar, processar, corrigir conforme necessário e transferir essas transações para os relatórios elaborados para clientes;
- Os respectivos registros contábeis, informações de suporte e contas específicas que foram usadas para iniciar, registrar, processar e comunicar as transações, incluindo a correção de informações incorretas e como as informações são transferidas para os relatórios elaborados para clientes;
- Como o sistema tratou de eventos e condições significativos que não eram transações;
- O processo usado para elaborar relatórios para clientes;
- Os objetivos de controle relevantes e os controles projetados para alcançar esses objetivos;
- Os controles que, no projeto do sistema, seriam implementados por entidades usuárias e que, se necessário para alcançar os objetivos de controle especificados na descrição, são identificados na descrição juntamente com os objetivos de controle específicos que não podem ser alcançados individualmente;
- Outros aspectos do ambiente de controle, do processo de avaliação de riscos, do sistema de informações (incluindo os respectivos processos de negócio) e da comunicação, das atividades de controle e dos controles de monitoramento que foram relevantes para o processamento e a comunicação de transações de clientes.

(ii) Inclui detalhes relevantes de mudanças realizadas nos sistemas da Companhia durante o período de 01 de junho de 2022 a 31 de dezembro de 2022;

(iii) Não omite ou distorce informações relevantes para o alcance do sistema que está sendo descrito, apesar de saber que a descrição foi elaborada para atender as necessidades comuns de ampla gama de clientes e seus auditores e, portanto, pode não incluir todos os aspectos do sistema que cada cliente individualmente possa considerar importante em seu próprio ambiente específico.

(b) Os controles relacionados com os objetivos de controle especificados na descrição foram adequadamente projetados. Os critérios usados na elaboração dessa afirmação foram que:

(i) Os riscos que ameaçaram o alcance dos objetivos de controle especificados na descrição foram identificados; e

(ii) Os controles identificados forneceriam, se estivessem operando conforme descrito, segurança razoável de que esses riscos não impediram que os objetivos de controle especificados fossem alcançados; e

(iii) Os controles foram aplicados de maneira uniforme conforme projetados, incluindo que foram aplicados controles manuais por pessoas com competência e autoridade adequadas, durante o período de 01 de junho de 2022 à 31 de dezembro de 2022.

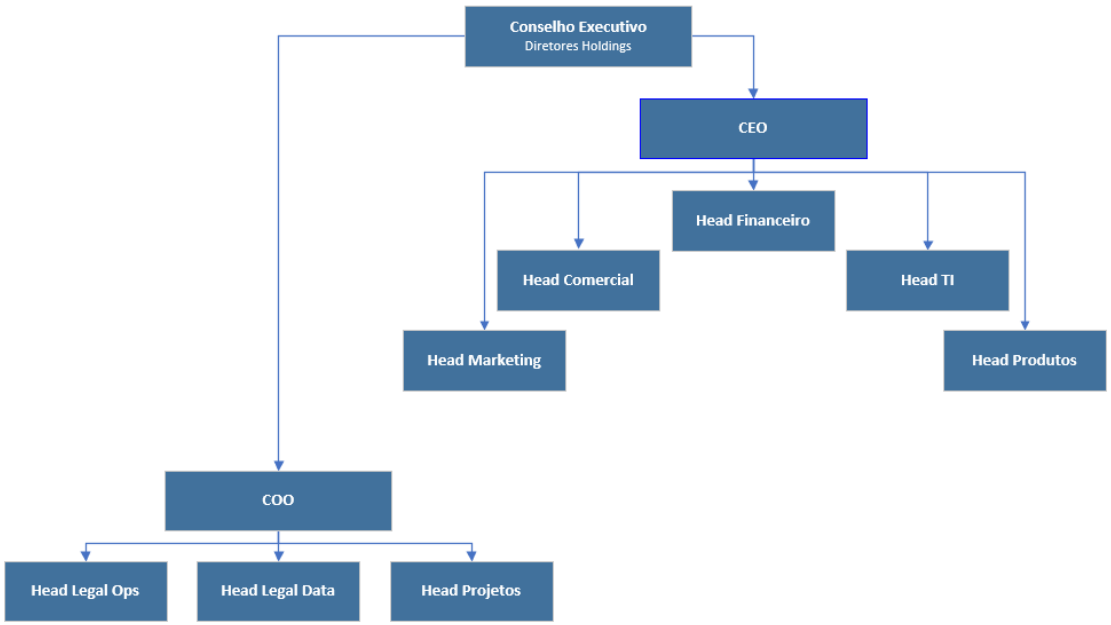
Seção III – Descrição dos Controles

1 Informações sobre a Companhia

A Companhia é uma empresa especializada em transformação digital, é um centro de excelência para operações de gerenciamento ao redor do mundo e considerada uma das mais respeitadas empresas de transformação digital.

Os serviços prestados pela empresa, aliam consultoria, serviços e produtos para que as organizações sejam cada vez mais eficientes.

2 Estrutura organizacional



3 Descrição dos produtos oferecidos

A) **Asken**: Software para gestão de consultas com inteligência artificial. Diminui repetição e controla a qualidade das respostas;

B) **Cleaner**: Software de captura de dados públicos e privados que realiza o tratamento das informações da base de dados desejada;

C) **Closing**: Software para fechamentos contábeis e circularização de informações entre auditoria, escritórios e departamentos jurídicos. Controle e monitoramento das alterações de Provisões e Contingências, tal como de atas automáticas;

D) **Budgeetfy**: Software que otimiza o planejamento financeiro das áreas de negócio. Adequado para monitorar recursos, aprovações, alçadas e planejamento financeiro;

E) **Pagben**: Software que otimiza a operação de pagamentos área, aprovações e lançamentos financeiros, com previsibilidade, transparência e auditoria para todos os envolvidos;

F) **URI**: Produto destinado ao controle de circularização de dados processuais entre departamentos jurídicos e seus fornecedores, capaz de comparar dados apresentados pelos fornecedores, para que haja a consolidação das informações controladas pelos departamentos jurídicos;

G) **ENSPACE**: Trata-se de um módulo localizado no mesmo software utilizado para o Closing, Pagben e Asken. Esse módulo é destinado para a gestão empresarial, auxiliando na organização de diversas áreas de uma empresa, através de componentes, como campos, fluxos, relatórios, e-mails integrados, entre outros.

4 Descrição dos controles internos de TI

Os objetivos de controle foram selecionados de acordo com os serviços prestados pela Companhia, as atividades de controles estão documentadas por meio de políticas e procedimentos a fim de fornecer razoável garantia para que os objetivos de controle sejam alcançados.

Acesso Lógico.

Objetivo de controle:	
A) Política de Segurança da Informação Assegurar que a Política de Segurança da Informação está devidamente implementada e que os usuários da empresa estão cientes do conteúdo do documento.	
AL.A01	A Companhia possui um documento denominado "Política de Gerenciamento de Incidentes de Segurança da Informação" que descreve as diretrizes e controles os controles relacionados ao gerenciamento e segurança da informação. Este documento é aplicável a todos os funcionários da organização. Durante o processo de admissão, os funcionários devem assinar o "Termo de Confidencialidade", este documento é utilizado como a evidência de que o funcionário possui ciência do conteúdo da política.

Objetivo de controle:	
B) Restrição de acesso Os controles fornecem uma garantia razoável de que o acesso lógico aos recursos de TI é restrito ao pessoal autorizado a fim de reduzir o risco de acesso não autorizado a sistemas e dados.	
AL.B01	Os sistemas de TI desenvolvidos pela Companhia são construídos em conformidade com as boas práticas de segurança da TI e possuem parâmetros para o gerenciamento de senhas a fim de mitigar o risco de acessos não autorizados.

Objetivo de controle:	
AL.B02	A Companhia possui um documento denominado “Política de Gestão de Acessos” que descreve a atividade de controle para a restrição de acessos privilegiados ou administradores aos sistemas e recursos de TI. O acesso às configurações do sistema é dado aos usuários administradores e deverá ser restrito a pessoal adequado que exerça atividade compatível com a administração dos sistemas. A libração dos acessos ocorre por meio do controle de concessão de acessos.

Objetivo de controle:	
C) Concessão, modificação e revogação de acessos dos usuários Os controles fornecem garantia razoável de que a concessão, modificação e revogação de contas de usuário são requisitadas e aprovadas por pessoal adequado, a fim de mitigar o risco de acesso não autorizado ou indevido a sistemas e dados.	
AL.C01	A Companhia possui um documento denominado “Política de Gestão de Acessos” que descreve a atividade de controle para a concessão de novos acessos aos sistemas e recursos de TI. Toda requisição de concessão de acesso aos sistemas e recursos de TI da Companhia deverá ser formalizada por meio da ferramenta de ITSM e aprovada por pessoa com nível hierárquico igual o superior à coordenação da área em que o colaborador beneficiário do acesso está alocado ou da área de recursos humanos. O formulário preenchido por meio da ferramenta Asken deve conter no mínimo, as seguintes informações: Nome do usuário; ID do Usuário; Motivo da Concessão; Perfil ou Grupo de acesso e a Data da Concessão. Todo usuário deverá possuir uma chave de identificação, controlada através de um Número Único de Identificação (ID), para garantia de rastreabilidade, o qual nunca poderá ser repetido. No momento da requisição do acesso, o solicitante poderá utilizar o documento denominado “Matriz de Acessos” para consultar todos os perfis disponíveis nos sistemas..
AL.C02	A Companhia possui um documento denominado “Política de Gestão de Acessos” que descreve a atividade de controle para a revogação de acessos aos sistemas e recursos de TI. Toda requisição de revogação de acesso a um colaborador da Companhia deverá ser realizada ou aprovada por uma pessoa em um nível hierárquico igual ou superior à coordenação, seja ela da área de Recursos Humanos, ou da área que o colaborador está alocado. Além disso, é imprescindível que a requisição ocorra de maneira formal, de forma tempestiva e através do preenchimento de um formulário, de acordo

Objetivo de controle:	
	com o término da vigência do contrato de trabalho. Neste formulário deverá conter, no mínimo, as seguintes informações: Nome do usuário; ID do Usuário; Motivo da Revogação; Data da Revogação. É dever da área de Recursos Humanos comunicar desligamentos de colaboradores da empresa às áreas de Desenvolvimento, Tecnologia da Informação e Projetos. O desligamento do colaborador deve ser informado com no máximo 24 horas após do término do seu contrato de trabalho, se este for o caso, para que a revogação do acesso ocorra no mesmo dia que o desligamento.

Objetivo de controle:	
D) Revisão de acessos Assegurar razoavelmente que há segregação de funções dos usuários dos sistemas e recursos de TI a fim de mitigar o risco de acesso não autorizado ou impróprio aos sistemas e dados.	
AL.D01	A Companhia possui um documento denominado “Política de Gestão de Acessos” que descreve a atividade de controle para a revisão periódica dos direitos de acessos dos usuários aos sistemas e recursos de TI. Anualmente, é dever dos departamentos de Projetos, Desenvolvimento e Tecnologia da Informação, realizar a revisão de acessos de todos os usuários internos da Companhia que estejam ativos, verificando com os gestores de cada área se os acessos deverão ser mantidos, inativados ou modificados. A resposta ou validação dos gestores para cada revisão deverá registrada de modo formal a fim de documentar todo o processo.

Gestão de Mudanças

Objetivo de controle:	
A) Autorização, testes, validação e aprovação das mudanças Assegurar de forma razoável que as modificações nos sistemas aplicativos foram devidamente autorizadas, testadas e aprovadas antes de serem implementadas no ambiente de produção.	
GM.A01	A Companhia possui um documento denominado “Política de Gerenciamento de Mudanças” que descreve as atividades de controle para a o processo de mudanças nos sistemas. Toda requisição de desenvolvimento / mudança nos sistemas deve ser realizada pelas áreas de negócio ou pela área de produtos da Companhia. Após a requisição da área solicitante, a área de produtos é responsável por

Objetivo de controle:	
	analisar a demanda e caso seja identificada a necessidade de um desenvolvimento. Após o alinhamento entre a área de produtos e a área de desenvolvimento, será estabelecido um prazo para conclusão da nova demanda, a qual deverá ser repassada ao solicitante, o "de acordo" do solicitante deverá ser obtido por meio do documento com o escopo de produção. Após aprovada a documentação, o escopo será incluído na próxima cerimônia de Sprint Planning, e assim colocado na esteira de desenvolvimento.
GM.A02	A homologação deverá ocorrer em ambiente de homologação separado da produção e devidamente registrado / documentado em formulário contendo as evidências dos testes realizados. Uma vez finalizada a homologação junto ao time de produtos, este enviará para validação do solicitante, que poderá pedir ajustes, os quais serão inseridos na próxima cerimônia de Sprint Planning, ou poderá ser enviado para produção, caso o solicitante esteja de acordo com o desenvolvimento realizado.
GM.A03	Toda alteração a ser realizada em ambiente produtivo, deverá ser acompanhada de documentação formal aprovada ou elaborada pelo *head* da equipe de produtos da Companhia.
GM.A04	As mudanças classificadas como emergenciais são decorrentes de incidentes ou problemas que resultem na indisponibilidade de produtos ou serviços impactando os clientes. Nestes casos não há necessidade da formalização do documento de escopo de produção, e a homologação é de responsabilidade do time de produtos.

Objetivo de controle:	
B) Restrição de acesso para migração das mudanças Assegurar que um número razoável de pessoas possua direito de acesso para realizar a migração de mudanças para o ambiente de produção dos sistemas aplicativos.	
GM.B01	Os Desenvolvedores devem realizar um *Commit* e enviar o código para o servidor de versionamento. Este, por sua vez, envia uma mensagem ao sistema de *Deploy* Automático – Build Works, o qual aguarda uma aprovação do responsável para executar a Pipeline que realiza o Build e os testes unitários. Em caso de obtenção de sucesso nos testes unitários, o *Deploy* é realizado no ambiente (aplicação online); caso localizada qualquer falha nos testes unitários, é enviada uma notificação aos *Developers*, que repetirão o processo até que seja obtido sucesso.

Objetivo de controle:	
	As permissões de acesso para aprovação na ferramenta Build Works devem estar restritas ao pessoal autorizado.

Gestão de Incidentes e Problemas.

Objetivo de controle:	
A) Registro, análise e resolução de incidentes e problemas Assegurar de forma razoável que os eventos ocorridos fora da normalidade (incidentes e problemas) são registrados, analisados e resolvidos.	
GIP.A01	A Companhia possui um documento denominado "Política de Gerenciamento de Incidentes de Segurança da Informação" que descreve as diretrizes e controles os controles relacionados ao gerenciamento de incidentes de segurança da informação. Os eventos / incidentes podem ser identificados por qualquer colaborador da empresa e devem ser registrados na ferramenta de ITSM como “Registro de Descobertas”, este registro será direcionado para análise da equipe de Segurança da Informação que é responsável por analisar e identificar a solução para o evento.
GIP.A02	Os incidentes registrados na ferramenta de ITSM devem ser analisados pelo time de segurança da informação e classificados de acordo com o “Risk Score” definido na política.
GIP.A03	O SLA para atendimento e solução dos incidentes registrados na ferramenta de ITSM está definido de acordo com a Política de Gerenciamento de Incidentes de Segurança da Informação, tal como é gerenciado pela ferramenta ITSM para que haja a devida resolução do evento.

Operações de TI.

Objetivo de controle:	
A) Monitoramento de servidores, sistemas e infraestrutura Assegurar de forma razoável que os servidores, sistemas e infraestrutura são monitorados e controlados a fim de detectar falhas ou indisponibilidade.	
OP.A01	Todos os sistemas e aplicações da Companhia associadas ao Portal do Ben, são disponibilizadas por meio da nuvem da empresa Digital Ocean que é responsável pelo monitoramento e sustentação do ambiente.
OP.A02	Os procedimentos de backup, monitoramento e restauração de ambientes estão documentados na "Política de Backup e Recuperação", com informações sobre periodicidade, conteúdo, retenção, etc. Os backups são agendados de acordo com as informações fornecidas na política.

Seção IV – Teste do Desenho e Eficácia Operacional dos Controles

Categoria do Controle: Acesso Lógico

A) Política de Segurança da Informação

Objetivo de Controle: Assegurar que a Política de Segurança da Informação está devidamente implementada e que os usuários da empresa estão cientes do conteúdo do documento.

#	Descrição do controle especificado pela Companhia	Procedimentos realizados pela Baker Tilly para o teste dos controles	Resultado
AL.A01	A Companhia possui um documento denominado "Política de Gerenciamento de Incidentes de Segurança da Informação" que descreve as diretrizes e controles relacionados ao gerenciamento e segurança da informação. Este documento é aplicável a todos os funcionários da organização. Durante o processo de admissão, os funcionários devem assinar o "Termo de Confidencialidade", este documento é utilizado como a evidência de que o funcionário possui ciência do conteúdo da política.	Consulta aos responsáveis para o entendimento dos processos e controles, inspeção de políticas e procedimento, tal como teste unitário para validação do desenho e testes amostrais para validação da eficácia operacional.	Não foram identificadas exceções.

Categoria do Controle: Acesso Lógico

B) Restrição de acesso

Objetivo de Controle: Os controles fornecem uma garantia razoável de que o acesso lógico aos recursos de TI é restrito ao pessoal autorizado a fim de reduzir o risco de acesso não autorizado a sistemas e dados.

#	Descrição do controle especificado pela Companhia	Procedimentos realizados pela Baker Tilly para o teste dos controles	Resultado
AL.B01	Os sistemas de TI desenvolvidos pela Companhia são construídos em conformidade com as boas práticas de segurança da TI e possuem parâmetros para o gerenciamento de senhas a fim de mitigar o risco de acessos não autorizados.	Consulta aos responsáveis para o entendimento dos processos e controles, inspeção de políticas e procedimento, tal como teste unitário para validação do desenho e testes amostrais para validação da eficácia operacional.	Não foram identificadas exceções.
AL.B02	A Companhia possui um documento denominado "Política de Gestão de Acessos" que descreve a atividade de controle para a restrição de acessos privilegiados ou administradores aos sistemas e recursos de TI. O acesso às configurações do sistema é dado aos usuários administradores e deverá ser restrito a pessoal adequado que exerça atividade compatível com a administração dos sistemas. A libração dos acessos ocorre por meio do controle de concessão de acessos.	Consulta aos responsáveis para o entendimento dos processos e controles, inspeção de políticas e procedimento, tal como teste unitário para validação do desenho e testes amostrais para validação da eficácia operacional.	Não foram identificadas exceções.

Categoria do Controle: Acesso Lógico

C) Concessão, modificação e revogação de acessos dos usuários de acesso

Objetivo de Controle: Os controles fornecem garantia razoável de que a concessão, modificação e revogação de contas de usuário são requisitadas e aprovadas por pessoal adequado, a fim de mitigar o risco de acesso não autorizado ou indevido a sistemas e dados.

#	Descrição do controle especificado Companhia	Procedimentos realizados pela Baker Tilly para o teste dos controles	Resultado
AL.C01	A Companhia possui um documento denominado "Política de Gestão de Acessos" que descreve a atividade de controle para a concessão de novos acessos aos sistemas e recursos de TI. Toda requisição de concessão de acesso aos sistemas e recursos de TI da Companhia deverá ser formalizada por meio da ferramenta Asken e aprovada por pessoa com nível hierárquico igual o superior à supervisão da área em que o colaborador beneficiário do acesso está alocado ou da área de recursos humanos. O formulário preenchido por meio da ferramenta Asken deve conter no mínimo, as seguintes informações: Nome do usuário; ID do Usuário; Motivo da Concessão; Perfil ou Grupo de acesso e a Data da Concessão. Todo usuário deverá possuir uma chave de identificação, controlada através de um Número Único de Identificação (ID), para garantia de rastreabilidade, o qual nunca poderá ser repetido. No momento da requisição do acesso, o solicitante poderá utilizar o documento denominado "Matriz de Acessos" para consultar todos os perfis disponíveis nos sistemas.	Consulta aos responsáveis para o entendimento dos processos e controles, inspeção de políticas e procedimento, tal como teste unitário para validação do desenho e testes amostrais para validação da eficácia operacional.	Não foram identificadas exceções.

#	Descrição do controle especificado Companhia	Procedimentos realizados pela Baker Tilly para o teste dos controles	Resultado
AL.C02	A Companhia possui um documento denominado "Política de Gestão de Acessos" que descreve a atividade de controle para a revogação de acessos aos sistemas e recursos de TI. Toda requisição de revogação de acesso a um colaborador da Companhia deverá ser realizada ou aprovada por uma pessoa em um nível hierárquico igual ou superior à coordenação, seja ela da área de Recursos Humanos, ou da área que o colaborador está alocado. Além disso, é imprescindível que a requisição ocorra de maneira formal, de forma tempestiva e através do preenchimento de um formulário, de acordo com o término da vigência do contrato de trabalho. Neste formulário deverá conter, no mínimo, as seguintes informações: Nome do usuário; ID do Usuário; Motivo da Revogação; Data da Revogação. É dever da área de Recursos Humanos comunicar desligamentos de colaboradores da empresa às áreas de Desenvolvimento, Tecnologia da Informação e Projetos. O desligamento do colaborador deve ser informado com no mínimo 24 horas antes do término do seu contrato de trabalho, se este for o caso, para que a revogação do acesso ocorra no mesmo dia que o desligamento.	Consulta aos responsáveis para o entendimento dos processos e controles, inspeção de políticas e procedimento, tal como teste unitário para validação do desenho e testes amostrais para validação da eficácia operacional.	Não foram identificadas exceções.

Categoria do Controle: Acesso Lógico

D) Revisão de acessos

Objetivo de Controle: Assegurar razoavelmente que há segregação de funções dos usuários dos sistemas e recursos de TI a fim de mitigar o risco de acesso não autorizado ou impróprio aos sistemas e dados.

#	Descrição do controle especificado pela Companhia	Procedimentos realizados pela Baker Tilly para o teste dos controles	Resultado
AL.D01	A Companhia possui um documento denominado "Política de Gestão de Acessos" que descreve a atividade de controle para a revisão periódica dos direitos de acessos dos usuários aos sistemas e recursos de TI. Anualmente, é dever dos departamentos de Projetos, Desenvolvimento e Tecnologia da Informação, realizar a revisão de acessos de todos os usuários internos da Companhia que estejam ativos, verificando com os gestores de cada área se os acessos deverão ser mantidos, inativados ou modificados. A resposta ou validação dos gestores para cada revisão deverá registrada de modo formal a fim de documentar todo o processo.	Consulta aos responsáveis para o entendimento dos processos e controles, inspeção de políticas e procedimento, tal como teste unitário para validação do desenho e testes amostrais para validação da eficácia operacional.	Não foram identificadas exceções.

Categoria do Controle: Gestão de mudanças

A) Autorização, testes, validação e aprovação das mudanças

Objetivo de Controle: Assegurar de forma razoável que as modificações nos sistemas aplicativos foram devidamente autorizadas, testadas e aprovadas antes de serem implementadas no ambiente de produção.

#	Descrição do controle especificado Companhia	Procedimentos realizados pela Baker Tilly para o teste dos controles	Resultado
GM.A01	A Companhia possui um documento denominado "Política de Gerenciamento de Mudanças" que descreve as atividades de controle para a o processo de mudanças nos sistemas. Toda requisição de desenvolvimento / mudança nos sistemas deve ser realizada pelas áreas de negócio ou pela área de produtos da Companhia. Após a requisição da área solicitante, a área de produtos é responsável por analisar a demanda e caso seja identificada a necessidade de um desenvolvimento. Após o alinhamento entre a área de produtos e a área de desenvolvimento, será estabelecido um prazo para conclusão da nova demanda, a qual deverá ser repassada ao solicitante, o "de acordo" do solicitante deverá ser obtido por meio do documento com o escopo de produção. Após aprovada a documentação, o escopo será incluído na próxima cerimônia de Sprint Planning, e assim colocado na esteira de desenvolvimento.	Consulta aos responsáveis para o entendimento dos processos e controles, inspeção de políticas e procedimento, tal como teste unitário para validação do desenho e testes amostrais para validação da eficácia operacional.	Não foram identificadas exceções.

#	Descrição do controle especificado Companhia	Procedimentos realizados pela Baker Tilly para o teste dos controles	Resultado
GM.A02	A homologação deverá ocorrer em ambiente de homologação separado da produção e devidamente registrado / documentado em formulário contendo as evidências dos testes realizados. Uma vez finalizada a homologação junto ao time de produtos, este enviará para validação do solicitante, que poderá pedir ajustes, os quais serão inseridos na próxima cerimônia de Sprint Planning, ou poderá ser enviado para produção, caso o solicitante esteja de acordo com o desenvolvimento realizado. Após aprovada a documentação, o escopo será incluído na próxima cerimônia de Sprint Planning, e assim colocado na esteira de desenvolvimento.	Consulta aos responsáveis para o entendimento dos processos e controles, inspeção de políticas e procedimento, tal como teste unitário para validação do desenho e testes amostrais para validação da eficácia operacional.	Não foram identificadas exceções.
GM.A03	Toda alteração a ser realizada em ambiente produtivo, deverá ser acompanhada de documentação formal aprovada ou elaborada pelo *head* da equipe de produtos da Companhia.	Consulta aos responsáveis para o entendimento dos processos e controles, inspeção de políticas e procedimento, tal como teste unitário para validação do desenho e testes amostrais para validação da eficácia operacional.	Não foram identificadas exceções.
GM.A04	As mudanças classificadas como emergenciais são decorrentes de incidentes ou problemas que resultem na indisponibilidade de produtos ou serviços impactando os clientes. Nestes casos não há necessidade da formalização do documento de escopo de produção, e a homologação é de responsabilidade do time de produtos.	Consulta aos responsáveis para o entendimento dos processos e controles, inspeção de políticas e procedimento, tal como teste unitário para validação do desenho e testes amostrais para validação da eficácia operacional.	Não foram identificadas exceções.

Categoria do Controle: Gestão de mudanças

B) Restrição de acesso para migração das mudanças

Objetivo de Controle: Assegurar que um número razoável de pessoas possua direito de acesso para realizar a migração de mudanças para o ambiente de produção dos sistemas aplicativos.

#	Descrição do controle especificado pela Companhia	Procedimentos realizados pela Baker Tilly para o teste dos controles	Resultado
GM.B01	Os Desenvolvedores devem realizar um *Commit* e enviar o código para o servidor de versionamento. Este, por sua vez, envia uma mensagem ao sistema de *Deploy* Automático – Build Works, o qual aguarda uma aprovação do responsável para executar a Pipeline que realiza o Build e os testes unitários. Em caso de obtenção de sucesso nos testes unitários, o *Deploy* é realizado no ambiente (aplicação online); caso localizada qualquer falha nos testes unitários, é enviada uma notificação aos *Developers*, que repetirão o processo até que seja obtido sucesso. As permissões de acesso para aprovação na ferramenta Build Works devem estar restritas ao pessoal autorizado.	Consulta aos responsáveis para o entendimento dos processos e controles, inspeção de políticas e procedimento, tal como teste unitário para validação do desenho e testes amostrais para validação da eficácia operacional.	Não foram identificadas exceções.

Categoria do Controle: Gestão de incidentes e problemas

A) Registro, análise e resolução de incidentes e problemas

Objetivo de Controle: Assegurar que um número razoável de pessoas possua direito de acesso para realizar a migração de mudanças para o ambiente de produção dos sistemas aplicativos.

#	Descrição do controle especificado pela Companhia	Procedimentos realizados pela Baker Tilly para o teste dos controles	Resultado
GIP.A01	A Companhia possui um documento denominado "Política de Gerenciamento de Incidentes de Segurança da Informação" que descreve as diretrizes e controles os controles relacionados ao gerenciamento de incidentes de segurança da informação. Os eventos / incidentes podem ser identificados por qualquer colaborador da empresa e devem ser registrados na ferramenta de ITSM como “Registro de Descobertas”, este registro será direcionado para análise da equipe de Segurança da Informação que é responsável por analisar e identificar a solução para o evento.	Consulta aos responsáveis para o entendimento dos processos e controles, inspeção de políticas e procedimento, tal como teste unitário para validação do desenho e testes amostrais para validação da eficácia operacional..	Não foram identificadas exceções.
GIP.A02	Os incidentes registrados na ferramenta de ITSM devem ser analisados pelo time de segurança da informação e classificados de acordo com o “Risk Score” definido na política.	Consulta aos responsáveis para o entendimento dos processos e controles, inspeção de políticas e procedimento, tal como teste unitário para validação do desenho e testes amostrais para validação da eficácia operacional.	Não foram identificadas exceções.
GIP.A03	O SLA para atendimento e solução dos incidentes registrados na ferramenta de ITSM está definido de acordo com a Política de Gerenciamento de Incidentes de Segurança da Informação, tal como é gerenciado pela ferramenta ITSM para que haja a devida resolução do evento.	Consulta aos responsáveis para o entendimento dos processos e controles, inspeção de políticas e procedimento, tal como teste unitário para validação do desenho e testes amostrais para validação da eficácia operacional.	Não foram identificadas exceções.

Categoria do Controle: Operações de TI

A) Monitoramento de servidores, sistemas e infraestrutura

Objetivo de Controle: Assegurar de forma razoável que os servidores, sistemas e infraestrutura são monitorados e controlados a fim de detectar falhas ou indisponibilidade.

#	Descrição do controle especificado pela Companhia	Procedimentos realizados pela Baker Tilly para o teste dos controles	Resultado
OP.A01	Todos os sistemas e aplicações da Companhia associadas ao Portal do Ben, são disponibilizadas por meio da nuvem da empresa Digital Ocean que é responsável pelo monitoramento e sustentação do ambiente.	Consulta aos responsáveis para o entendimento dos processos e controles, inspeção ao SOC 2 *Report* da empresa Digital Ocean para validação dos controles.	Não foram identificadas exceções.
OP.A02	Os procedimentos de backup, monitoramento e restauração de ambientes estão documentados na "Política de Backup e Recuperação", com informações sobre periodicidade, conteúdo, retenção, etc. Os backups são agendados de acordo com as informações fornecidas na política.	Consulta aos responsáveis para o entendimento dos processos e controles, inspeção ao SOC 2 *Report* da empresa Digital Ocean para validação dos controles.	Não foram identificadas exceções.