17/11/2025

RELATÓRIO DE AUDITORIA 2025

Agência Brasileira de Desenvolvimento Industrial

TECNOLOGIA DA INFORMAÇÃO

Sumário

ABDI – AGÊNCIA BRASILEIRA DE DESENVOLVIMENTO INDUSTRIAL

Brasília – DF

RELATÓRIO CIRCUNSTANCIADO DE AUDITORIA EXTERNA
REFERENTE AO ANO DE 2025

(Com vistas em Outubro e Novembro / 2025)

1 INTRODUÇÃO

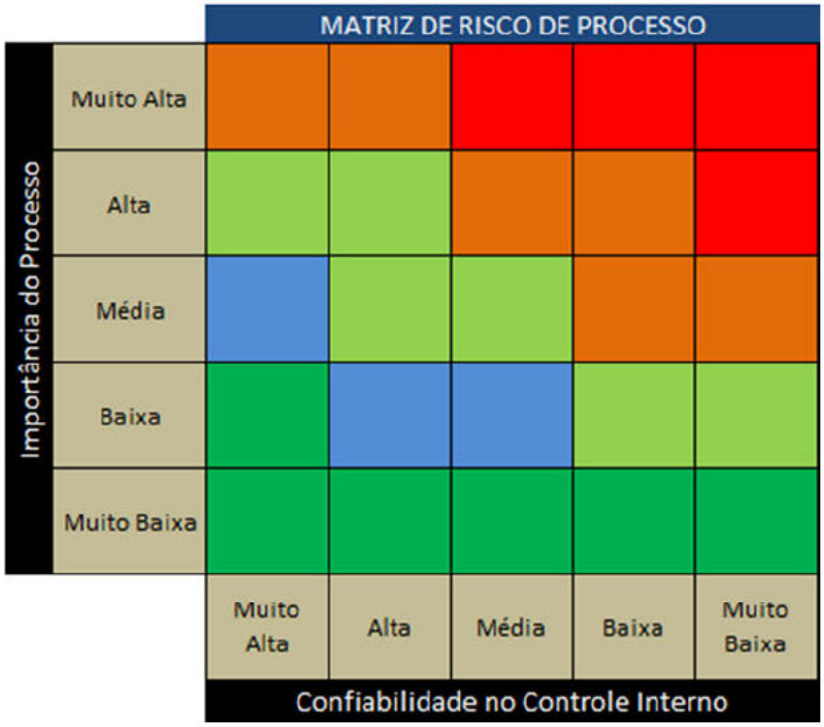
Com vistas à execução dos trabalhos de auditoria no ambiente de Tecnologia da Informação do ABDI, procedemos às análises da segurança da informação e seus controles (Governança de TI e Segurança da Informação), com base na competência atual.

Os trabalhos foram realizados seguindo padrões usuais de auditoria aplicáveis no Brasil, em conformidade com as normas de governança de TI, de acordo com as metodologias internacionais Isaca, Cobit 5, em consonância com as Normas NBR ISO/IEC 12.119 (Tecnologia de Informação – Pacotes de *Software* – Testes e Requisitos de Qualidade) e NBR ISO/IEC 14.598 e NBR ISO 27.001 e 27.002. Objetivamos atender ao disposto na Resolução CFC nº 1.029/05**,** que aprova a NBC T 11.12 – Processamento Eletrônico de Dados, que trata da revisão dos Controles Internos e NBC P 1 (Normas Profissionais dos Auditores Independentes).

Foram executados exames documentais e evidências, utilizando critérios fundamentados em uma base seletiva, na extensão e profundidade julgadas necessárias nas circunstâncias, coletando informações e evidências.

Para cada apontamento do presente relatório está estabelecido o nível do risco da não conformidade, onde é utilizada a matriz Importância do Processo versus Confiabilidade no Controle Interno.

MATRIZ IMPORTÂNCIA DO PROCESSO x CONFIABILIDADE NO CONTROLE INTERNO



2 ESCOPO

O objetivo do presente trabalho de auditoria foi avaliar o ambiente, a conformidade e os controles dos processos de Tecnologia da Informação, considerando os seguintes eixos de analise:

GOVERNANÇA DE TI
Estrutura Organizacional de TI
Organograma TI
Estrutura de TI
Políticas
Procedimentos
Boas Práticas
Arquitetura de TI
Dimensionamento
Recursos Humanos

Análise Recursos Humanos Capacitados na Gestão de TI
Contingência de TI
Plano de Contingência e Continuidade dos Negócios
Mecanismos e Ferramentas - Backup e Redundância
Processos Documentados
Conformidade da execução dos processos de negócio de TI
Gestão de Riscos de TI
Processos Documentados
Matriz de Riscos
PDTI - Plano Diretor de TI
Plano Estratégico
Aquisições de TI
Parque Tecnológico
Metas e Diretrizes

SEGURANÇA DA INFORMAÇÃO
Gestão de Controle de Acesso Lógico
Active Directory
Sistemas Corporativos
Banco de Dados
Administração de acesso
Usuários
Perfis de revogação
Gestão de Controle de Acesso Físico
Instalações e Ambientes
Data Centers
Sistemas de Segurança e acessos
Software de Segurança de Acesso
Instalação, Parametrização e Configuração.
Antivírus, antispyware, firewall.
Atualização de pacotes e os servidores de Proxy

- ✓ Avaliação do ambiente organizacional relacionado aos processos mencionados acima, vinculados ao Macroprocesso Gestão de TI, sob o foco de gerenciamento dos riscos e controles;

- ✓ Avaliação da efetividade e a eficiência da estrutura de TI as atividades de disponibilidade interna a manter e direcionamento da eficácia a continuidade dos negócios.

3 PROCEDIMENTOS DE AUDITORIA

O trabalho foi conduzido por meio de análises documentais e da avaliação de evidências relacionadas à Governança de TI e Segurança da Informação. No decorrer da auditoria, foram aplicados testes de observância com o objetivo de obter segurança razoável de que os procedimentos de controle interno estabelecidos pela gestão estão em funcionamento efetivo e em conformidade com as normas e diretrizes aplicáveis.

3.1 RESULTADOS DAS ANÁLISES E AVALIAÇÕES DOS EIXOS

3.1.1 GOVERNANÇA DE TI

GOVERNANÇA DE TI	Auditoria	Resultado da auditoria	Parecer da auditoria
Estrutura Organizacional de TI			
Organograma TI	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em Conformidade
Estrutura de TI	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em Conformidade
Políticas	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em Conformidade
Procedimentos	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em Conformidade
Boas Práticas	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em Conformidade
Arquitetura de TI	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em Conformidade
Dimensionamento	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em Conformidade
Recursos Humanos			

Recursos Humanos - Análise Recursos Humanos Capacitados na Gestão de TI	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em Conformidade
Contingência de TI			
Plano de Contingência e Continuidade dos Negócios	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em Conformidade
Mecanismos e Ferramentas - Backup e Redundância	Análise documental, evidências e amostragem.	Sugestão de melhorias na política	Não Conformidade Menor
Processos Documentados			
Conformidade da execução dos processos de negócio de TI	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em Conformidade
Gestão de Riscos de TI			
Processos Documentados	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em Conformidade
Matriz de Riscos	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em Conformidade
PDTI - Plano Diretor de TI			
Plano Estratégico	Análise documental, evidências e amostragem.	PDTI está em processo de atualização conforme registros no documento PETIC_PDTIC_ABDI_leia-me	Em conformidade
Aquisições de TI	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Parque Tecnológico	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Metas e Diretrizes	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade

3.1.2 SEGURANÇA DA INFORMAÇÃO

SEGURANÇA DA INFORMAÇÃO	Auditoria	Resultado da auditoria	Parecer da auditoria
Gestão de Controle de Acesso Lógico			
Active Directory	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Sistemas Corporativos	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Banco de Dados			
Administração de acesso	Análise documental, evidências e amostragem.	Correções de melhorias logs e trilhas de auditoria	Não conforme
Usuários	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Perfis de revogação	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Gestão de Controle de Acesso Físico			
Instalações e Ambientes	Análise documental, evidências e amostragem.	Recomendações apontadas	Em conformidade
Data Centers	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Sistemas de Segurança e acessos	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Software de Segurança de Acesso			
Instalação, Parametrização e Configuração.	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Antivírus, antispyware, firewall	Análise documental, evidências e amostragem.	Recomendações apontadas	Em conformidade
Atualização de pacotes e os servidores de Proxy	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade

4 PRINCIPAIS RESULTADOS APONTADOS

Com base nas avaliações realizadas em conformidade com os objetivos e o escopo do trabalho, destacamos a seguir os principais resultados obtidos, que visam contribuir para a melhoria contínua dos controles internos.

4.1 MECANISMOS E FERRAMENTAS – BACKUP E REDUNDÂNCIA

SITUAÇÃO IDENTIFICADA

Durante a análise, foi evidenciado que a empresa possui um processo de backup operacional e funcional, abrangendo diferentes ambientes, com elevado índice de sucesso.

Entretanto, tanto o relatório de execução quanto a política vigente carecem de informações sobre os locais de armazenamento das cópias. A adoção do complemento proposto reforçará a governança, a rastreabilidade e a conformidade com os requisitos de auditoria e segurança da informação.

EVIDÊNCIAS

- 01_Politica_de_Backup&Restore;
- Evidência de Execução - Julho2025;
- Evidência_de_Execução_RestoreMar2025;
- ScheduleReport_Backups
- Controle_de_Backups

RISCO

CLASSIFICAÇÃO RISCO	Muito baixo

Apesar disso, a política não especifica os locais de armazenamento dos backups (on-premises, data center externo ou cloud), o que gera uma lacuna de controle e rastreabilidade.

RECOMENDAÇÕES

Sugerimos que para aprimorar a rastreabilidade e conformidade, incluir na Política de Backup a localização das copias dos backups, como virtualizados, disco de servidores e em mídias.

COMENTÁRIOS ABDI

A sugestão será acatada pela UTEC e atualizaremos a versão da política incluindo a informação sobre a localização das cópias dos backups, de acordo com os tipos de serviços contratados e existentes na ABDI, como Nuvem e On premises. Este item será incorporado no plano de ação.

COMENTÁRIOS UTEC (REGISTRO NO DOCUMENTO CONTRARRAZÕES)**:**

Esta Unidade apresentou todas as evidências necessárias para demonstrar a execução do processo de cópia de segurança, incluindo sua periodicidade, procedimentos de restauração e demais controles correlatos. Considerando que a recomendação da auditoria foi emitida como boa prática, acolhemos a sugestão de aprimorar a política apenas para explicitar, de forma mais clara, o local de armazenamento das cópias. Assim, entendemos que não se trata de fragilidade nos mecanismos e ferramentas de backup, mas sim de um aperfeiçoamento pontual voltado ao fortalecimento das práticas já adotadas pela Unidade.

COMENTÁRIOS AUDITORIA

A auditoria reconhece que a ABDI /UTEC manifestou concordância com a recomendação e informou que irá atualizar Política de Backup para incluir a localização das cópias de segurança, contemplando os ambientes em Nuvem e On-premises, conforme os serviços atualmente contratados. Trata-se de medida positiva e alinhada às boas práticas de Governança de TI.

4.2 BANCOS DE DADOS – LOGS DE AUDITORIA

4.2.1 LOGS - POSTGRESQL

SITUAÇÃO IDENTIFICADA

Foram analisados os registros de log do servidor PostgreSQL referentes ao dia 25 de agosto de 2025, armazenados no arquivo 'SABDIJBS03_postgresql-Mon-Ago-2025.log'. O objetivo foi identificar possíveis falhas, erros recorrentes e mensagens de advertência que possam indicar problemas de configuração, compatibilidade ou desempenho.

1- Erro: column "waiting" does not exist
O log apresenta repetidas ocorrências do erro:

ERROR: column "waiting" does not exist at character 154
STATEMENT: SELECT COUNT(*) FROM pg_stat_activity WHERE pid != pg_backend_pid() AND waiting.
Esse erro ocorre porque a coluna 'waiting' foi removida das versões mais recentes do PostgreSQL (a partir da versão 9.6). Scripts ou ferramentas de monitoramento que ainda utilizam essa coluna precisam ser atualizados.

2- Log: incomplete startup packet
Também foram identificadas mensagens do tipo:

LOG: incomplete startup packet

Essas mensagens indicam tentativas de conexão TCP que não foram completadas. Podem ocorrer devido a ferramentas de monitoramento, testes de conectividade de rede ou encerramento abrupto de conexões por parte dos clientes.

EVIDÊNCIAS

Documento: SABDIJBS03_postgresql-Mon-Ago-2025.log

RISCO

CLASSIFICAÇÃO RISCO	Baixo

1- Esse erro não interrompe o funcionamento do banco de dados, mas gera ruído nos logs e pode causar lentidão em ferramentas de monitoramento que executam essa consulta em loop contínuo.

2- Normalmente inofensivo, mas se recorrente pode indicar varreduras de rede, falhas de configuração de monitoramento ou problemas de conexão de clientes intermediários.

RECOMENDAÇÕES

1- A análise indica que o principal problema é a utilização de scripts ou ferramentas desatualizadas que acessam a coluna 'waiting' inexistente. Recomenda-se atualizar todos os scripts de monitoramento para compatibilidade com a versão atual do PostgreSQL, substituindo o campo removido por 'wait_event'.

Correção recomendada:
Substituir o campo 'waiting' pela condição 'wait_event IS NOT NULL', conforme o exemplo abaixo:

SELECT COUNT(*) FROM pg_stat_activity WHERE pid != pg_backend_pid() AND wait_event IS NOT NULL;

2- As mensagens 'incomplete startup packet' não representam risco imediato, mas devem ser monitoradas para garantir que não estejam relacionadas a acessos indevidos ou falhas de rede.

Após a aplicação das correções sugeridas, recomenda-se revisar os logs novamente e validar se as mensagens de erro cessaram.

COMENTÁRIOS ABDI

Os times de infraestrutura e de aplicações\sistemas analisarão as recomendações apresentadas e, quando cabíveis, efetuarão os devidos ajustes a fim de reduzir possíveis riscos e degradações de desempenho aos sistemas que utilizam este Banco de Dados.

Ressalta-se que as eventuais sugestões de correções devem ser analisadas diante dos eventuais impactos no ambiente e aplicações. Portanto, esses times necessitam realizar levantamentos de descoberta da origem para as devidas de mitigação. Este item será incorporado no plano de ação.

COMENTÁRIOS UTEC (REGISTRO NO DOCUMENTO CONTRARRAZÕES)**:**

A UTEC reconhece os apontamentos realizados pela auditoria quanto aos registros de alertas nos bancos de dados PostgreSQL, SQL Server e MySQL. No entanto, é importante contextualizar que, por natureza, sistemas de banco de dados dinâmicos geram alertas rotineiros — tais como falhas de transação, warnings, deadlocks ocasionais e mensagens de conexão — sem que isso represente, obrigatoriamente, risco operacional, falhas de segurança ou impacto à experiência do usuário final.

Todos os sistemas que utilizam essas bases de dados são continuamente sustentados, com monitoramento ativo e tratamento preventivo, garantindo que eventuais registros de log não resultem em indisponibilidades, inconsistências ou incidentes relevantes. Assim, reforçamos que os alertas apontados não têm gerado impactos às aplicações, tampouco comprometido a integridade ou a segurança das operações.

Consideramos os achados como categoria “BAIXO”, portanto, entendemos que não se tratam de fragilidades estruturais, mas sim de ocorrências naturais do funcionamento dos sistemas.

Ainda assim, conforme boa prática, esta Unidade realizará a análise das plataformas que originam tais logs, envolvendo os times multidisciplinares responsáveis. Após essa avaliação, será verificado caso a caso se o alerta é pertinente para tratamento ou se se trata de comportamento normal das aplicações e dos bancos de dados.

COMENTÁRIOS AUDITORIA

A auditoria reconhece que a ABDI /UTEC manifestou concordância com a recomendação e informou que irão realizar analises e levantamentos de descoberta da origem para ações corretivas e mitigação de riscos, onde este procedimento será incluído no Plano de ação.

4.2.2 LOGS - SQL SERVER

SITUAÇÃO IDENTIFICADA

Foram analisados os registros de log do Microsoft SQL Server, armazenados no arquivo 'Logs_SQLSERVER_Out25_21102025.csv', com o objetivo de identificar falhas de autenticação, erros de conexão, deadlocks e outros alertas que possam indicar problemas de segurança, desempenho ou disponibilidade.

1- Falhas de Login (Login Failed)

Foram detectadas diversas tentativas de login malsucedidas, incluindo usuários 'sa' e 'NT AUTHORITY\ANONYMOUS LOGON'. Essas falhas ocorrem quando há tentativas de autenticação com credenciais incorretas ou sem privilégios.

Causas prováveis:

- Tentativas de acesso indevido ou ataques de força bruta.
- Agentes de monitoramento ou scripts com senhas desatualizadas.

2- Timeouts e Falhas de Conexão

Foram registradas mensagens de 'Timeout expired' e 'Connection timeout exceeded', indicando falhas nas conexões ou lentidão nas execuções de consultas.

Causas prováveis:

- Consultas longas ou bloqueios (locks) no banco de dados.
- Problemas de rede entre a aplicação e o servidor SQL.
- Parâmetros de tempo limite (timeout) mal configurados.

3- Deadlocks

Os logs indicam ocorrências de deadlock, onde duas ou mais transações competem pelos mesmos recursos simultaneamente, fazendo com que o SQL Server encerre uma das transações para liberar o bloqueio.

Causas prováveis:

- Execução concorrente de transações sobre os mesmos registros.
- Falta de índices adequados.

4 Warnings (Avisos)

Foram encontrados avisos do tipo 'Null value eliminated in aggregate function', que ocorrem quando funções agregadas como SUM ou AVG ignoram valores nulos, podendo afetar a precisão dos relatórios.

EVIDÊNCIAS

Documento: Logs_SQLSERVER_Out25_21102025.csv

RISCO

CLASSIFICAÇÃO RISCO	Baixo

1- Risco de Segurança da Informação, indicando acesso não autorizado ao banco de dados, podendo ser causado por ataques de força bruta, Scripts desatualizados ou falha na conta de serviços, onde ocorre:

- Comprometimento de credenciais administrativas;
- Acesso indevido de dados sensíveis;
- Violação de requisitos de segurança e conformidade (LGPD e ISSO 27001).

2- Risco de Indisponibilidade de Serviços

O banco de dados apresentou falhas de conexão e lentidão, possivelmente relacionadas a consultas pesadas, locks ou problemas na rede e isso afeta o seguinte:

- Interrupção de aplicações do SQL Server;
- Perda de produtividade e impacto operacional

3- Riscos de inconsistências e Perda de Transações

Deadlocks indicam conflito de concorrência, em que duas transações tentam acessar os mesmos recursos simuntaneamente, levando o SQL Server a cancelar uma delas, onde tende a afetar:

- Perda de transações críticas ou falhas em gravações de dados;
- Inconsistências em relatórios e sistemas transacionais.

4- Riscos de Erros em Relatórios e Indicadores

Consultas com funções agregadas estão ignorando valores nulos sem tratamento adequado, onde pode causar:

- Dados incorretos ou incompletos em relatórios gerenciais;
- Decisão de negócios baseadas em informações inconsistentes.

RECOMENDAÇÕES

Os principais problemas identificados envolvem falhas de login, timeouts e deadlocks, indicando a necessidade de melhorias em segurança, desempenho e controle de concorrência.

1- Recomendações:

• Desabilitar o login 'sa' ou utilizar senha forte e complexa.

• Monitorar logs de segurança para identificar a origem dos acessos.

• Utilizar autenticação integrada do Windows sempre que possível.

2- Recomendações:

• Monitorar o desempenho utilizando DMV's como sys.dm_exec_requests e sys.dm_tran_locks.

• Ajustar o parâmetro de tempo limite conforme a complexidade das consultas.

• Avaliar índices e otimizar queries críticas.

3- Recomendações:

• Revisar a ordem de acesso às tabelas nas transações.

• Implementar retry logic na aplicação para reexecutar transações interrompidas.

• Ativar a trace flag 1222 para identificar a causa detalhada dos deadlocks.

4- Recomendações:

• Tratar valores nulos utilizando ISNULL() ou COALESCE() nas consultas SQL.

Recomendamos as seguintes ações prioritárias:

• Revisar políticas de autenticação e fortalecer o controle de acessos.

• Ajustar parâmetros de timeout e otimizar consultas que apresentem lentidão.

• Implementar mecanismos de retry e revisão de índices para evitar deadlocks.

• Manter monitoramento contínuo dos logs para identificar anomalias futuras.

Essas medidas contribuem para aumentar a segurança, estabilidade e desempenho do ambiente SQL Server.

COMENTÁRIOS ABDI

Para todos os itens apontados (1 a 4), a UTEC irá realizar um plano de ação para revisar e ajustar, quando cabível, os pontos sugeridos ao ambiente SQL Server, com o objetivo de mitigar os riscos apontados e evitar possíveis degradações de desempenho.

Os times de infraestrutura/segurança e de aplicações\sistemas analisarão os pontos destacados e as recomendações apresentadas e, quando cabíveis, efetuarão os devidos ajustes a fim de reduzir possíveis riscos de segurança e degradações de desempenho aos sistemas que utilizam este Banco de Dados.

Ressalta-se que as eventuais sugestões de correções devem ser analisadas diante dos eventuais impactos no ambiente e aplicações. Portanto, esses times necessitam realizar levantamentos de descoberta da origem para as devidas de mitigação. Este item será incorporado no plano de ação.

COMENTÁRIOS UTEC (REGISTRO NO DOCUMENTO CONTRARRAZÕES):

A UTEC reconhece os apontamentos realizados pela auditoria quanto aos registros de alertas nos bancos de dados PostgreSQL, SQL Server e MySQL. No entanto, é importante contextualizar que, por natureza, sistemas de banco de dados dinâmicos geram alertas rotineiros — tais como falhas de transação, warnings, deadlocks ocasionais e mensagens de conexão — sem que isso represente, obrigatoriamente, risco operacional, falhas de segurança ou impacto à experiência do usuário final.

Todos os sistemas que utilizam essas bases de dados são continuamente sustentados, com monitoramento ativo e tratamento preventivo, garantindo que eventuais registros de log não resultem em indisponibilidades, inconsistências ou incidentes relevantes. Assim, reforçamos que os alertas apontados não têm gerado

impactos às aplicações, tampouco comprometido a integridade ou a segurança das operações.

Consideramos os achados como categoria “BAIXO”, portanto, entendemos que não se tratam de fragilidades estruturais, mas sim de ocorrências naturais do funcionamento dos sistemas.

Ainda assim, conforme boa prática, esta Unidade realizará a análise das plataformas que originam tais logs, envolvendo os times multidisciplinares responsáveis. Após essa avaliação, será verificado caso a caso se o alerta é pertinente para tratamento ou se se trata de comportamento normal das aplicações e dos bancos de dados.

COMENTÁRIOS AUDITORIA

A auditoria reconhece que a ABDI /UTEC manifestou concordância com a recomendação e informou que irão realizar analises e levantamentos de descoberta da origem para ações corretivas e mitigação de riscos, onde este procedimento será incluído no Plano de ação.

4.2.3 LOGS - MYSQL

SITUAÇÃO IDENTIFICADA

Na análise dos registros dos Log do MYSQL, o servidor MySQL (versão 8.0.36) foi inicializado corretamente, sem falhas críticas de inicialização ou corrupção do InnoDB.

Entretanto, foram identificados diversos avisos ('Warnings') que indicam necessidade de ajustes de configuração e uso de parâmetros obsoletos.

1. Plugin de autenticação obsoleto

[Warning] [MY-013360] Plugin mysql_native_password reported: "mysql_native_password' is deprecated...

2. Parâmetro de configuração obsoleto

[Warning] [MY-010918] 'default_authentication_plugin' is deprecated...

O parâmetro 'default_authentication_plugin' não deve mais ser utilizado.

3. Certificado CA autoassinado

[Warning] [MY-010068] CA certificate ca.pem is self signed.

O servidor utiliza um certificado SSL/TLS autoassinado.

4. IPs não resolvidos (problema de DNS local)

[Warning] [MY-010055] IP address '192.168.x.x' could not be resolved: Name or service not known

O servidor tentou resolver nomes de hosts de IPs locais e falhou.

5. Aviso sobre log de redo (InnoDB)

[Warning] [MY-013865] [InnoDB] Redo log writer is waiting for a new redo log file...

O InnoDB atingiu o limite de capacidade de redo log (innodb_redo_log_capacity).

EVIDÊNCIAS

Documento: SABDIMYSQLPRD02_MYSQL_PRD.log

RISCO

CLASSIFICAÇÃO RISCO	Baixo

1. Plugin de autenticação obsoleto (mysql_native_password)

Risco: O método de autenticação 'mysql_native_password' é considerado obsoleto e será removido em versões futuras. Este método utiliza algoritmos menos seguros, suscetíveis a ataques de força bruta ou interceptação de hashes.

Impacto: Pode causar falhas de login após atualização do MySQL, comprometer a segurança das credenciais e gerar não conformidade com normas de segurança (ISO 27001, SOC 2, LGPD).

2. Parâmetro de configuração obsoleto (default_authentication_plugin)
Risco: Parâmetro descontinuado que pode deixar de funcionar em versões futuras, impedindo a aplicação de políticas de autenticação seguras.

Impacto: Falhas de inicialização do serviço e inconsistências de segurança entre ambientes.

3. Certificado CA autoassinado
Risco: O uso de certificado autoassinado compromete a validação da identidade do servidor e aumenta o risco de ataques do tipo 'Man-in-the-Middle' (MITM).

Impacto: Interceptação de dados em trânsito, falhas de conexão segura e rejeição de conexões por sistemas que exigem certificados confiáveis.

4. IPs não resolvidos / Falhas de DNS
Risco: O servidor não conseguiu resolver nomes de hosts de alguns IPs internos. Isso pode indicar falhas no DNS ou ausência de registros no arquivo '/etc/hosts'.

Impacto: Lentidão em conexões, falhas intermitentes entre aplicações e logs incompletos, dificultando auditorias.

5. Capacidade insuficiente de redo log (innodb_redo_log_capacity)

Risco: O InnoDB aguardou a criação de novos arquivos de redo log, indicando limitação de capacidade. Esse gargalo afeta a gravação de transações em momentos de pico.

Impacto: Lentidão em operações críticas, possíveis travamentos e degradação de desempenho dos sistemas de produção.

RECOMENDAÇÕES

O servidor MySQL está operacional, mas requer ajustes preventivos para garantir conformidade e desempenho ideal:

1. Migrar usuários para 'caching_sha2_password'.
2. Atualizar parâmetros obsoletos no arquivo 'my.cnf'.
3. Corrigir falhas de resolução DNS.
4. Substituir certificados autoassinados se houver conexões externas.
5. Aumentar 'innodb_redo_log_capacity'.

1- Alterar os usuários para o método 'caching_sha2_password', que é o padrão desde o MySQL 8.0.

2- Substituí-lo por 'authentication_policy' no arquivo de configuração 'my.cnf'.

3- Caso o banco seja acessado externamente, recomenda-se o uso de certificados assinados por uma autoridade certificadora confiável.

4- Adicionar os IPs e respectivos nomes no arquivo '/etc/hosts' ou revisar o DNS interno.

5- Aumentar o valor deste parâmetro no arquivo 'my.cnf', por exemplo: innodb_redo_log_capacity=4G, para evitar lentidão em momentos de pico de escrita.

COMENTÁRIOS ABDI

1 e 2 - Plugin de autenticação obsoleto (mysql_native_password) e Parâmetro de configuração obsoleto (default_authentication_plugin)

A sugestão será acatada e o time de infraestrutura/segurança juntamente com o time de aplicações\sistemas criarão um plano para realizar a modificação do método de autenticação e o ajuste de configuração no *default_authentication_plugin*. Este item será incorporado no plano de ação.

3 - Certificado CA autoassinado

O uso de certificados autoassinados são estritamente utilizadas para comunicações internas na ABDI. Para o uso em comunicações externas a ABDI utiliza certificados adequados, com chave SHA de 256 bits, como o exemplo do certificado do tipo WildCard, imagem abaixo:

4. Adicionar os IPs e respectivos nomes no arquivo '/etc/hosts' ou revisar o DNS interno.

A sugestão será acatada e o time de infraestrutura efetuará a análise dos destinos não encontrados no DNS. Este item será incorporado no plano de ação.

5. Aumentar 'innodb_redo_log_capacity'.

A sugestão será acatada e o time de infraestrutura/segurança efetuará a análise de capacidade do repositório e posterior ajuste no tamanho do referido log. Este item será incorporado no plano de ação.

COMENTÁRIOS UTEC (REGISTRO NO DOCUMENTO CONTRARRAZÕES)**:**

A UTEC reconhece os apontamentos realizados pela auditoria quanto aos registros de alertas nos bancos de dados PostgreSQL, SQL Server e MySQL. No entanto, é importante contextualizar que, por natureza, sistemas de banco de dados dinâmicos geram alertas rotineiros — tais como falhas de transação, warnings, deadlocks ocasionais e mensagens de conexão — sem que isso represente, obrigatoriamente, risco operacional, falhas de segurança ou impacto à experiência do usuário final.

Todos os sistemas que utilizam essas bases de dados são continuamente sustentados, com monitoramento ativo e tratamento preventivo, garantindo que eventuais registros de log não resultem em indisponibilidades, inconsistências ou incidentes relevantes. Assim, reforçamos que os alertas apontados não têm gerado impactos às aplicações, tampouco comprometido a integridade ou a segurança das operações.

Consideramos os achados como categoria “BAIXO”, portanto, entendemos que não se tratam de fragilidades estruturais, mas sim de ocorrências naturais do funcionamento dos sistemas.

Ainda assim, conforme boa prática, esta Unidade realizará a análise das plataformas que originam tais logs, envolvendo os times multidisciplinares responsáveis. Após essa avaliação, será verificado caso a caso se o alerta é pertinente para tratamento ou se se trata de comportamento normal das aplicações e dos bancos de dados.

COMENTÁRIOS AUDITORIA

A auditoria reconhece que a ABDI /UTEC manifestou concordância com a recomendação e informou que irão realizar analises e levantamentos de

descoberta da origem para ações corretivas e mitigação de riscos, onde este procedimento será incluído no Plano de ação referente aos itens: 1, 2, 4 e 5, e quanto ao item 3 a UTEC apresentou que utilizam certificados com chave SHA de 256 bits onde fortalece o controle sobre a segurança da situação.

4.3 SEGURANÇA DE ACESSO – LOGS DO FIREWALL

SITUAÇÃO IDENTIFICADA

Durante a análise dos registros de log do firewall, foram identificadas diversas ocorrências de bloqueio realizadas pelo sistema de segurança. Entre elas, destacam-se duas situações que requerem investigação mais aprofundada devido ao seu potencial risco à segurança do ambiente:

1- Tentativa de ataques por injeção de comando HTTP – Foi detectado o evento "Command injection detected in URL: "kill", o que indica uma possível tentativa de exploração de vulnerabilidade em serviço web interno ou externo".

2- Tráfego UDP nas portas 1250-1252 – Observou-se comunicação em portas não padronizadas, o que pode estar relacionado a aplicações customizadas, mal configuradas ou potencialmente suspeitas, sendo necessário verificar a origem e legitimidade desse tráfego.

EVIDÊNCIAS

Logs_Oct_21__2025_18_04_27_291_PM_Logs_Table_final.csv

RISCO

CLASSIFICAÇÃO RISCO	Baixo

1- Comprometimento de sistemas internos, execução remota de comandos, infiltração de dados ou indisponibilidade de serviços.

2- Possível uso de aplicações não homologadas, mau funcionamento de sistemas internos ou tentativas de evasão de política de segurança.

RECOMENDAÇÃO

1- Tentativa de ataques por injeção de comando HTTP

- Investigar imediatamente a origem e o IP de ataque;
- Revisar regras de inspeção do firewall e do WAF;
- Reforçar validações de entrada em aplicações Web e atualizar assinaturas de segurança.

2- Tráfegos UDP nas portas 1250-1252

- Verificar se existem aplicações utilizando essas portas e alterar para portão padrão;
- Avaliar se irão utilizar para outros meios essas portas, senão fazer bloqueio definitivo para não mais utilizar;
- Implementar monitoramento proativo para detecção de portas anômalas.

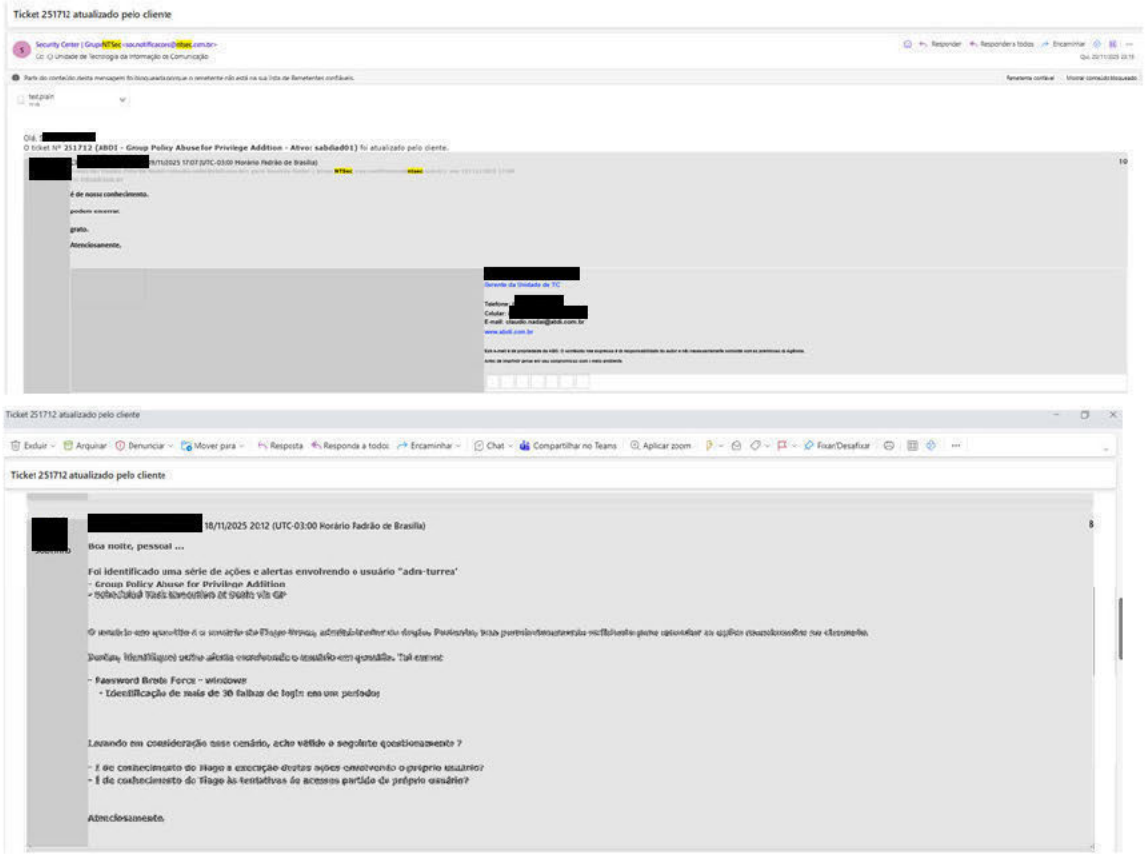
COMENTÁRIOS ABDI

Tentativa de ataques por injeção de comando HTTP
Quanto a evidência apontada, cabe esclarecer o seguinte:

A mensagem do log é acompanhada ao final pelo termo kill (“Command injection detected in URL: “kill”). Este é um tipo de mensagem usualmente apresentada pelo nosso atual sistema de gestão do Firewall e indica que houve uma tentativa de injeção de comando, porém ela foi derrubada ou morta (na tradução literal). Entendemos a preocupação deste time de auditoria, contudo, tentativas como estas ocorrem repetidamente durante o dia e, por este motivo, fica inviável rastrear caso a caso. Portanto, fica a cargo do sistema de inteligência da nossa solução de

Firewall identificar comportamentos anormais como este e realizar o trabalho de derrubar a conexão e demais ações necessárias.

Além disso, a UTEC possui um serviço contratado de SNOC com uma empresa especializada em segurança da informação, que atua preventivamente com foco em evitar exploração de vulnerabilidades, sempre nos acionando quando há comportamentos anormais. Vide exemplo de e-mails abaixo que evidenciam ações do nosso SNOC:



2 - Tráfegos UDP nas portas 1250-1252

Os tráfegos nas portas indicadas serão alvo de avaliação junto ao nosso time de infraestrutura/segurança, via abertura de ticket e, havendo a falta de identificação\informação sobre o motivo do uso e a constatada a representação de risco de comunicação externa será feita a análise de troca para outra porta. Este item será incorporado no plano de ação.

COMENTÁRIOS UTEC (REGISTRO NO DOCUMENTO CONTRARRAZÕES**):**

A Segurança da Informação é um dos pilares prioritários da UTEC. Atualmente, contamos com um serviço contratado de SNOC, operado por empresa especializada, que atua preventivamente na identificação e mitigação de vulnerabilidades, acionando a equipe interna sempre que são detectados comportamentos anormais.

Além disso, mantemos um conjunto abrangente de mecanismos de proteção, incluindo:

- segurança perimetral;
- serviços de Anti-DDoS;
- proteção de endpoints;
- soluções IDS/IPS;
- segurança na camada de aplicação (cloudfare);
- segmentação de rede;
- bloqueios automáticos de eventos suspeitos;
- entre outras camadas técnicas de defesa.

No relatório de auditoria foram identificados dois achados relacionados à segurança. O primeiro foi respondido de forma detalhada e consistente. Quanto ao segundo, esclarecemos que as portas UDP 1250–1252 correspondem aos protocolos utilizados pelas câmeras Intelbras responsáveis pelo monitoramento físico das dependências da Agência. Como evidenciado nas imagens abaixo, tais portas encontram-se devidamente bloqueadas na console do firewall, demonstrando controle efetivo sobre esse tráfego específico.

Por fim, destacamos que as regras e políticas de segurança são continuamente monitoradas e ajustadas conforme a necessidade, tanto pela UTEC quanto pela empresa contratada. Diante dos achados e das respostas já apresentadas, não identificamos a necessidade de análises adicionais referentes às ocorrências registradas pelo firewall, tampouco revisão extraordinária de regras, segmentação, políticas ou implantação de novos mecanismos. As práticas atuais já contemplam processos contínuos de vigilância, adequação e melhoria, garantindo a proteção e a resiliência do ambiente tecnológico da Agência.

COMENTÁRIOS AUDITORIA

O objetivo da auditoria é identificar situações que demandem atenção e avaliação, de forma a minimizar possíveis riscos ao ambiente tecnológico. Constatamos que o firewall está ativo, operante e configurado com mecanismos de proteção adequados à segurança da informação, contribuindo para a continuidade dos negócios da organização.

O ponto identificado foi registrado como sinal de alerta, reforçando a necessidade de monitoramento contínuo para garantir que eventuais anomalias sejam detectadas e tratadas tempestivamente.

Com relação à situação observada referente às portas UDP 1250–1252, após os esclarecimentos apresentados nos comentários da UTEC, verificamos que o controle está implementado de forma adequada. Conforme informado:

“Encontram-se devidamente bloqueadas na console do firewall, demonstrando controle efetivo sobre esse tráfego específico.”

Diante disso, entendemos que o risco inicialmente identificado foi devidamente esclarecido e que os controles existentes atendem aos requisitos de segurança esperados.

Quanto aos mecanismos de proteção a UTEC registrou e apresentou em seus comentários os mecanismos implantados para a segurança e a auditoria entende que o risco identificado esta esclarecido.

4.4 CONTROLES DE ACESSO FÍSICO CPD

SITUAÇÃO IDENTIFICADA

Nas avaliações dos registros de acesso ao CPD com base nos dados fornecidos, identificando anomalias, riscos e situações que requerem atenção em uma auditoria de TI.

1. Aberturas por Botoeira (Sem Identificação)

Foram identificados diversos registros apenas como 'Botoeira', sem nome, matrícula ou autenticação. Este tipo de abertura representa uma falha grave no controle de acesso, pois permite a entrada ou saída sem identificação.

Nesta situação o que achamos mais provável que esteja acontecendo é que a Entrada no CPD é feita e registrada através do equipamento eletrônica e a saída é feita através da Botoeira, pois não estão utilizando o equipamento eletrônico registrando a saída do ambiente.

0	16/10/2025 18:50:26				Botoeira			UTEC	UTEC
0	16/10/2025 18:48:56				Botoeira			UTEC	UTEC
0	16/10/2025 18:45:06				Botoeira			UTEC	UTEC
0	16/10/2025 18:44:35				Botoeira			UTEC	UTEC
0	16/10/2025 18:44:17				Botoeira			UTEC	UTEC
0	16/10/2025 18:43:36				Botoeira			UTEC	UTEC
0	16/10/2025 18:41:50				Botoeira			UTEC	UTEC

2. Registros de Tentativas com Usuário 'Não Identificado'

Alguns registros indicam que o sistema não conseguiu identificar a credencial utilizada, classificando-a como 'Não identificado'. Isso pode representar tentativas de uso indevido ou falhas no equipamento.

0	17/10/2025 13:14:31				Não identificado			UTEC	UTEC

3. Volume Elevado de Acessos ao CPD

Alguns usuários acessaram o CPD repetidas vezes ao longo do dia. O CPD é uma área crítica e normalmente não deve ter trânsito frequente, exceto por manutenção ou atividades específicas.

1300542	17/10/2025 08:19:59	[redacted]			Autorizado			UTEC	UTEC
1247638	17/10/2025 07:58:04				Autorizado			UTEC	UTEC
1247643	17/10/2025 07:00:24				Autorizado			UTEC	UTEC
1247643	17/10/2025 07:00:23				Autorizado			UTEC	UTEC
0	17/10/2025 06:44:06				Botoeira			UTEC	UTEC
1247648	17/10/2025 06:43:42				Autorizado			UTEC	UTEC
0	16/10/2025 20:08:23				Botoeira			UTEC	UTEC
1247631	16/10/2025 20:07:41				Autorizado			UTEC	UTEC
0	16/10/2025 19:37:04				Botoeira			UTEC	UTEC
1317621	16/10/2025 19:32:26				Autorizado			UTEC	UTEC

4. Acessos Fora do Horário Comercial

Foram identificados acessos ao CPD em horários como 19h, 20h e outros fora do expediente. Acessos nesses períodos normalmente requerem aprovação formal e supervisão.

0	14/10/2025 05:38:04				Botoeira			UTEC	UTEC
1247645	14/10/2025 05:37:31	[redacted]			Autorizado			CPD	CPD
1247645	14/10/2025 05:37:13				Autorizado			UTEC	UTEC
1079243	13/10/2025 22:52:26				Autorizado			UTEC	UTEC
0	13/10/2025 22:47:03				Botoeira			UTEC	UTEC
1079243	13/10/2025 22:46:22				Autorizado			UTEC	UTEC
0	13/10/2025 22:35:05				Botoeira			UTEC	UTEC
1079243	13/10/2025 22:33:36				Autorizado			UTEC	UTEC
0	13/10/2025 22:30:19				Botoeira			UTEC	UTEC
1247645	13/10/2025 22:29:05				Autorizado			CPD	CPD
1247645	13/10/2025 22:28:38				Autorizado			UTEC	UTEC
0	13/10/2025 21:30:52				Botoeira			UTEC	UTEC

5. Registros Duplicados no Mesmo Segundo

Houve casos de entradas registradas no mesmo segundo, indicando possível redundância na leitura ou falha do dispositivo.

1300542	16/10/2025 11:53:47	[redacted]			Autorizado			UTEC	UTEC
0	16/10/2025 11:53:47				Botoeira			UTEC	UTEC

6. Acesso de Pessoas que não consta na estrutura de TI

Foram identificados alguns usuários que acessaram o CPD, seus nomes não constam a relação da estrutura de TI, onde relacionamos alguns:

- [redacted];
- [redacted];
- [redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- Outros.

EVIDÊNCIAS

Relatório_AcessoFísico_ControlID_UTEC&CPD_2025.pdf

Pilar Governança de TI.pdf

Estrutura de TI

Nome	Cargo	Função	Situação	Quantitativo
[redacted]	Analista de Produtividade e Inovação	Gerente	Efetivo	1
[redacted]	Analista de Produtividade e Inovação	Lider da torre de Sistemas e Produtos Digitais	Efetivo	1
[redacted]	Analista de Produtividade e Inovação	Lider da torre de Infraestrutura de TIC	Efetivo	1
[redacted]	Analista de Produtividade e Inovação	Lider da torre de Dados	Efetivo	1
[redacted]	Prestadores de Serviços	Gerente de projetos de TIC	Terceirizado	3
[redacted]	Prestadores de Serviços	Analista de Governança de TIC	Terceirizado	1
[redacted]	Prestadores de Serviços	Analista de ERP	Terceirizado	2
[redacted]	Prestadores de Serviços	Analista de projetos de sistemas	Terceirizado	1
[redacted]	Prestadores de Serviços	Assitente Administrativo	Terceirizado	1
[redacted]	Prestadores de Serviços	Analista de infraestrutura de TIC	Terceirizado	1
[redacted]	Prestadores de Serviços	Suporte ao usuário de TIC	Terceirizado	2
[redacted]	Prestador de Serviços	Analista de desenvolvimento de TIC	Terceirizado	1
Total de colaboradores				**16**

RISCO

CLASSIFICAÇÃO RISCO	Médio

A análise demonstra falhas significativas no controle de acesso físico ao CPD, especialmente relacionadas à ausência de autenticação, permissões inadequadas e acessos fora do horário.

1- Possibilidade real de acesso não autorizado ao CPD e quebra da trilha de auditoria.
2- Possível tentativa de acesso não autorizado.
3- Indício de falta de controle restritivo ou ausência de justificativas formais.
4- Intervenções não supervisionadas em ambiente crítico.
5- Pode comprometer a precisão da trilha de auditoria.
6- Acesso de pessoas que não fazem parte da TI e se forem suporte externo não houve acompanhamento por um usuário da equipe interna.

RECOMENDAÇÕES

É recomendado revisar as políticas de controle de acesso, restringir perfis, eliminar o uso indiscriminado da botoeira e reforçar a supervisão dos acessos ao ambiente.

COMENTÁRIOS ABDI

1- Sobre as Aberturas por Botoeira (Sem Identificação)

O modelo de dispositivo contratado e implementado pela Unidade Administrativa/ABDI, responsável pela infraestrutura predial, em suas dependências (ControlD) possui um mecanismo físico composto de um dispositivo de identificação por biometria facial para liberar ou bloquear uma porta e, outro dispositivo, chamado de “botoeira” posicionado do lado interno\contrário de uma sala ou unidade, para permitir a saída ou liberação da porta. Vale destacar que a “botoeira” ou “biometria facial” não impede a entrada de outra pessoa que porventura se aproveite da abertura da porta. Ressalta-se que é o modelo padrão adotada em todas as suas dependências.

Considerando o aspecto crítico dos equipamentos e operações realizadas em um DataCenter, cabe ressaltar que, além do controle de acesso detalhado acima, a referida sala possui também monitoramento por câmeras, vide arquivo de evidência “Câmera DataCenter(CPD).jpg”, que possibilita averiguar as saídas do DataCenter, assim como a saída da UTEC, como pode ser checado na evidência “Câmera UTEC.jpg”.

2- Dos Registros de Tentativas com Usuário 'Não Identificado' (item 2), Registros Duplicados no Mesmo Segundo (item 5) e Do Acesso de Pessoas que não constam na estrutura da TI (item 6).

Inicialmente, ratificamos que o relatório presente no arquivo “Relatório_AcessoFísico_ControlID_UTEC&CPD_2025.pdf”, apresenta dois pontos cruciais:

a) A coluna “Dispositivo” diferencia o local dos registros de acesso entre UTEC (sala dos colaboradores da unidade e CPD (Sala do Dacenter- Ambiente Restrito);

b) O sistema do ControlID retorna a mensagem de “Usuário não identificado” quando determinado colaborador tenta se autenticar via biometria facial e este não está liberado para acessar aquele ambiente\dispositivo. Isso não quer dizer que a pessoa adentrou ao recinto.

c) Ademais, cabe ratificar que dentro da estrutura de pastas “Gestão de Controle de Acesso Físico – Acesso Físico - ControlID - UTEC e DATACENTER (CPD) – (5 documentos)”, há um arquivo de evidência com o nome “Relatório_AcessoFísico_ControlID_UTEC&CPD_2025.pdf” e duas imagens “Control_ID_EntradaUTEC” e “Control_ID_DataCenter(CPD)”.

As duas imagens demonstram a entrada de duas salas distintas. A imagem “Control_ID_EntradaUTEC” demonstra o equipamento que faz o controle de acesso (entrada) à Unidade de Tecnologia da Informação e Comunicação (UTEC). Já a imagem “Control_ID_DataCenter(CPD)” demonstra o equipamento que faz o controle de acesso (entrada) ao DataCenter (CPD), cuja localização está dentro da UTEC.

d) Já o arquivo“Relatório_AcessoFísico_ControlID_UTEC&CPD_2025.pdf” trata-se de um relatório obtido pelo sistema de controle do ControlID, no qual foram filtrados apenas 2 dispositivos de controle de acesso de toda a ABDI e que podem ser constatados na coluna de nome “Dispositivo” no referido relatório. Nesta coluna, é possível distinguir quais acessos foram relacionados à UTEC e quais foram relacionados ao DataCenter (CPD).

e) Outrossim, cabe elucidar que qualquer colaborador ou funcionário ativo da ABDI cadastrado no ControlID possui permissão para entrar na UTEC, pois a regra é de livre acesso à nossa unidade. Isso responde ao item 6 quando se menciona usuários que não fazem parte da TI. Entretanto, o acesso ao DataCenter é restrito a pessoal específico, que possui a responsabilidade de realizar operações, manutenções ou monitoramento em equipamentos dentro do referido local.

Como exemplo prático, é possível destacar as visitas noturnas realizadas pelos agentes de piso da ABDI ao DataCenter, fora do horário de expediente, para checar se o sistema de ar-condicionado está em pleno funcionamento ou funcionamento do sistema de Nobreak. Esta medida em questão foi adotada pela ABDI para monitoramento e proporcionar maior agilidade na comunicação de eventual incidente.

f) A respeito da evidência de registro duplicado no mesmo segundo, entendemos que isto pode ter ocorrido quando, em momento paralelo, um colaborador fez a autenticação biométrica e ao mesmo tempo outro colaborador apertou a botoeira. Cabe ratificar novamente que há o sistema de monitoramento por câmeras caso haja alguma demanda para averiguar o evento.

g) A respeito do excesso de acessos ao Datacenter, este comportamento não é rotineiro. Tais situações ocorrem quando há demandas que requerem acessos, tais como:

- Remanejamento de áreas: Requerem ajustes em pontos de rede e testes de conectividade até a finalização da troca e validação de acesso à rede pelas estações de trabalho;
- Demandas Operacionais: Apesar da maioria das atividades realizadas por meio dos recursos do Datacenter, algumas demandas somente podem ser realizadas de dentro do

DataCenter. Exemplos: Gerencia dos HyperVisors, ajustes de hardware em Servidores, Storages, Switches.

- Quedas de energia: Em eventuais casos de quedas de energia, a equipe costuma acessar com mais frequência o DataCenter para acompanhar a temperatura do ambiente e realizar as operações cabíveis para o este cenário.
- Acesso ao equipamento CFTV: Em eventuais casos específicos de necessidade de acesso direto ao equipamento.
- Acesso para manutenção ou checagem de links de internet, telefonia, entre outros.

Vale destacar que os acessos são dinâmicos de acordo com a necessidade, podendo ter em algum momento maior número de acesso e em outros menor ou nenhum acesso ao CPD.

COMENTÁRIOS UTEC (REGISTRO NO DOCUMENTO CONTRARRAZÕES)**:**

Todos os achados relacionados ao controle de acesso físico ao CPD foram analisados minuciosamente por esta Unidade e devidamente esclarecidos, contemplando informações sobre os mecanismos de autenticação, controles de acesso, permissões vigentes, registros de entradas e saídas, monitoramento por câmeras, acessos fora do horário comercial, restrições implementadas, entre outros elementos pertinentes.

Diante das explicações apresentadas, entendemos que os pontos levantados pela auditoria foram respondidos de forma abrangente e robusta, evidenciando a efetividade dos controles atualmente adotados. Assim, não identificamos a necessidade de novas ações adicionais, considerando que os mecanismos existentes já mitigam adequadamente o risco classificado como alto no relatório.

COMENTÁRIOS AUDITORIA

A UTEC apresentou esclarecimentos detalhados sobre os achados relacionados ao controle de acesso físico ao CPD, informando a existência de mecanismos de autenticação, controles de acesso, permissões vigentes, registros de entradas e

saídas, monitoramento por câmeras, análise de acessos fora do horário comercial e demais restrições implementadas.

As justificativas apresentadas demonstram a existência de controles relevantes e alinhados às boas práticas de segurança física. Contudo, a conclusão da auditoria baseia-se não apenas nas declarações da área gestora, mas também na evidência documental disponível no momento da avaliação.

Após análise das informações encaminhadas, entendemos que as explicações apresentadas contribuem para mitigar o risco apontado, porém recomendamos manter o acompanhamento periódico dos controles de acesso físico, considerando que se trata de um risco classificado como alto e que requer monitoramento contínuo para garantir sua efetividade.

** NOTA: REGISTRO NA CONTRARRAZÕES ABDI / UTEC

Controles e Evidências de Governança de TI

- Ausência de evidências de controles relativos a:
  - Inventário de software.
  - Aderência das aplicações ao negócio.
  - Usabilidade.
  - Compatibilidade tecnológica.
  - Qualidade dos serviços de TI.

Recomendação:

Verificou-se ausência de evidências em controles relacionados a inventário de software, aderência das aplicações ao negócio, usabilidade, compatibilidade tecnológica e qualidade de serviços de TI, o que limita a plena validação da conformidade nesses aspectos.

GOVERNANÇA DE TI	Auditoria	Resultado da auditoria	Parecer da auditoria
Estrutura Organizacional de TI			
Organograma TI	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em Conformidade
Estrutura de TI	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em Conformidade
Políticas	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em Conformidade
Procedimentos	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em Conformidade
Boas Práticas	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em Conformidade
Arquitetura de TI	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em Conformidade
Dimensionamento	Análise documental, evidências e amostragem.	Nenhuma exceção observada	Em Conformidade
Recursos Humanos			

COMENTÁRIOS UTEC (REGISTRO NO DOCUMENTO CONTRARRAZÕES):

Todas as evidências relacionadas à Governança de TI, especialmente aquelas vinculadas aos pontos recomendados, foram apresentadas de forma completa por esta Unidade.

O relatório encaminhado demonstra que todos os itens avaliados se encontram “em conformidade”, atendendo aos requisitos verificados pela auditoria.
Dessa forma, não compreendemos tais aspectos como recomendações adicionais, uma vez que já foram integralmente atendidos e evidenciados no material submetido.

COMENTÁRIOS AUDITORIA

A Unidade Técnica apresentou os documentos solicitados referentes aos controles de Governança de TI, incluindo informações relacionadas ao inventário de software, aderência das aplicações ao negócio, usabilidade, compatibilidade tecnológica e qualidade dos serviços. A auditoria reconhece o envio dos materiais e os esclarecimentos prestados.

PARECER:

A auditoria definiu o parecer como em conformidade dos itens abaixo analisados, conforme relação encaminhada a ABDI com as solicitações documentais e evidências.

Estrutura Organizacional de TI	
Organograma TI	Organograma institucional atualizado, descrição de cargos e responsabilidades
Estrutura de TI	Regimento interno ou documento que descreva as funções, fluxograma funcional, quadro de alocação de pessoal
Políticas	Políticas formais de TI (Governança, Segurança da Informação, Acesso , backup, contratações, serviços, etc.)
Procedimentos	Procedimentos operacionais padrão (POPs), manuais de operação e instrução normativas
Boas Práticas	Evidências de adoção de frameworks (COBIT, ITIL, ISO 27001 etc.), Atas do Cômite de governança
Arquitetura de TI	Documentos de arquitetura corporativa, mapa de sistemas e integrações Padrões tecnologico, diagrama de rede
Dimensionamento	Relatórios de dimensionamento de infraestrutura (servidores, storange, rede, licenças, equipe, inventário técnico)

CONCLUSÃO SOBRE A NOTA

Diante da analise realizada e considerando o material encaminhado, a auditoria entende que os pontos levantados foram devidamente esclarecidos pela UTEC, sendo possível concluir que os controles avaliados encontram-se em conformidade para o período examinado.

5 DOCUMENTOS E EVIDÊNCIAS APRESENTADAS

PILAR GOVERNAÇA
Boas Práticas – (11 documentos)
Certificados Cursos UTEC – (19 documentos)
Diagrama e topologia de rede – (6 documentos)
PDTIC – (6 pastas e 7 documentos)
PDTIC - Aquisições de TI – (1 documento)
PDTIC - Compatibilidade com o parque tecnológico – (7 documentos)
PDTIC - Depreciação de Ativos de TI – (1 documento)
PDTIC - Inventário de ativos de TI – (2 documentos)
PDTIC - Observar a existência de inventário de software – (4 documentos)
PDTIC - Processo de Contratação de TI – (6 documentos)
Plano de Contingência
Politica de acordo de confidencialidade – (5 documentos)
Politica de backup – (1 pastas e 5 documentos)
Politica de backup – Controle de Backups – (1 documento)

Politica_de_Backup&Restore
Política de Comunicação
Política de Gerenciamento de Crises
POLÍTICA DE GERENCIAMENTO DE CRISES E PROBLEMAS UTEC
Política de Gerenciamento de Riscos – (9 documentos)
Política de Incidentes – (4 documentos)
Política de Privacidade e Proteção de Dados - INA-14-e-resolucao
Política de Segurança da Informação - INA 12 - Segurança da Informação_16022023_ultimaversão
Procedimentos de trabalhos de TI – (67 documentos)
Processos Documentados – (11 pastas)
Processos Documentados - Conformidade da execução dos processos de negócio de TI
Processos Documentados - Devolução de ativos – (3 documentos)
Processos Documentados - Processo de Atendimento às Requisições de Titulares de Dados Pessoais - Processo para tratamento das solicitações dos titulares de dados pessoais_rev
Processos Documentados - Processo de avaliação e acompanhamentos dos serviços contratados por TI – (pasta vazia)
Processos Documentados - Processo de empréstimo e devolução de ativos – (3 documentos)
Processos Documentados - Processo de Gestão de Incidentes e Violação de Dados Pessoais - Processo de Gestão de Incidentes e Violação de Dados Pessoais - entrega
Processos Documentados - Processo de Mudanças nos Sistemas – (3 documentos)
Processos Documentados - PROCESSO DE NOTIFICAÇÃO AOS FORNECEDORES CONTRATADOS QUANTO AO FECHAMENTO DO CICLO MENSAL DE EXECUÇÃO – (2 documentos)
Processos Documentados - Processo de Suporte Técnico (gestão de incidentes) - PROCESSO DE SUPORTE TÉCNICO
Processos Documentados - Processo de Violação de Dados Pessoais – (pasta vazia)
PROCESSOS DE GOVERNANÇA DE ACESSOS E IDENTIDADE DE USUÁRIOS – (2 documentos)
Pilar Governança de TI

PILAR SEGURANÇA DA INFORMAÇÃO
Banco de Dados – (4 pastas)
Banco de Dados - Estrutura de SGBD - Estrutura de SGBDs da ABDI_0425
Banco de Dados - Evidencias de registro de bloqueios de acessos - Registro de Bloqueios de Acessos
Banco de Dados - Logs de acesso ao banco de dados – (7 documentos)
Banco de Dados - Procedimento de Acesso aos SGBDs - Acessos aos SGBDs_2025
Gestão de Controle de Acesso Físico – (6 pastas)
Gestão de Controle de Acesso Físico – Acesso Físico - ControlID - UTEC e DATACENTER (CPD) – (5 documentos)
Gestão de Controle de Acesso Físico – Evidências - Câmeras de Monitoramento – (3 documentos)
Gestão de Controle de Acesso Físico – Fotos - DataCenter_Nobreak – Datacenter – (5 documentos)
Gestão de Controle de Acesso Físico – Fotos - DataCenter_Nobreak – Nobreak – (5 documentos)
Gestão de Controle de Acesso Físico – Fotos - DataCenter_Nobreak – Rack Distribuição

Terreo – (4 documentos)
Gestão de Controle de Acesso Físico – Politica de controle de acesso - Política de Seg. da Informação-INA-12-e-resolucao
Gestão de Controle de Acesso Físico – Política de Segurança da Informação - INA 12 - Segurança da Informação_16022023_ultimaversão
Gestão de Controle de Acesso Físico – Processo de Acesso Físico e Lógico de TI - Política de Segurança da Informação - PSI
Gestão de Controle de Acesso Lógicos – (6 pastas)
Gestão de Controle de Acesso Lógicos – Controle de Acesso (Privilegiado) - Controle_de_Acesso_(Privilegiado)
Gestão de Controle de Acesso Lógicos – Evidencias de registro de bloqueios de acessos - Registro de Bloqueios de Acessos
Gestão de Controle de Acesso Lógicos – Perfil de acesso usuarios - apresentar todos tipos de perfis - Detalhamento_Perfis_Acesso_2025
Gestão de Controle de Acesso Lógicos – Politica de controle de acesso - Política de Seg. da Informação-INA-12-e-resolucao
Gestão de Controle de Acesso Lógicos – Política de Segurança da Informação - INA 12 - Segurança da Informação_16022023_ultimaversão
Gestão de Controle de Acesso Lógicos – Processo de Acesso Físico e Lógico de TI - Política de Seg. da Informação-INA-12-e-resolucao
Software de Segurança de Acesso – (7 pastas)
Software de Segurança de Acesso – Anti virus - logs - Nivel de Endpoint – Relatório – (4 documentos)
Software de Segurança de Acesso – Inventário Licenças e Softwares – SystemCenter - SystemCenter_Export_Inventário_Licenças&Softwares_211025
Software de Segurança de Acesso – Logs de trafego de rede - Logs_Firewall_Oct_21__2025_18_04_27_291_PM_Logs_Table_final
Software de Segurança de Acesso – Logs do firewall - Logs_Oct_21__2025_18_04_27_291_PM_Logs_Table_final
Software de Segurança de Acesso – Monitoramento_Servidores&AtivosdeRede_Zabbix_Stefanini – (2 documentos)
Software de Segurança de Acesso – Política de Segurança da Informação - INA 12 - Segurança da Informação_16022023_ultimaversão
Software de Segurança de Acesso – Proxy_Evidências_AtualizaçõesSegurança_AuditLogs_ErrorLogs – (5 documentos)
Pilar Segurança da Informação

6 CONSIDERAÇÕES FINAIS

O presente trabalho teve como finalidade avaliar a Governança de TI, os controles de Segurança da informação e os mecanismos operacionais adotados pela ABDI /

UTEC, considerando documentos, evidências e registros apresentados ao longo da auditoria. Observou-se que a área de Tecnologia da Informação mantém processos estruturados, políticas formalizadas, mecanismos de controle implantados e aderência geral às boas práticas aplicáveis, alinhadas às normas de referência (COBIT 5, ISO/IEC 27001 / 27002, ISO/IEC 12.119, entre outras).

De maneira geral, os controles avaliados demonstram conformidade com os requisitos previstos no escopo desta auditoria, tendo sido evidenciada a efetividade de governança, das políticas estabelecidas, dos procedimentos operacionais e das práticas de monitoramento aplicadas pela UTEC. Os documentos encaminhados contemplam, de forma consistente, os elementos necessários à validação de processos críticos, como gestão de acessos, políticas de segurança, inventário de ativos, diretrizes de PDTI, monitoramento de ambientes, continuidade dos serviços e demais componentes de suporte à Governança de TI.

No decorrer das analises foram identificados apontamentos classificados como risco de Baixo e Alto impacto, todos devidamente esclarecidos pela UTEC. Destacam-se:

- Backup e Redundância: Recomendação e aprimoramento documental quanto à especificação dos locais de armazenamento das cópias. A UTEC reconheceu e incorporou a atualização no Plano de Ação.

- Logs de Bancos de Dados (PostreSQL, SQL Server e MySQL): Os alertas identificados refletem comportamentos típicos de sistemas dinâmicos e não apontaram impacto operacional. A UTEC esclareceu a natureza dos registros e apresentou plano de análise pontual e tratamento preventivo.

- Firewall e Segurança Perimetral: A auditoria registrou ocorrências que requerem acompanhamento. Porém a UTEC demonstrou, por meio de evidências e controle contratados (SNOC, IDS / IPS, Anti-DDos e monitoramento continuo), que os mecanismos existentes são robustos e mitigam adequadamente os riscos apresentados.

- Acesso Físico ao CPD: Embora inicialmente classificado como risco Alto, as explicações apresentadas pela UTEC – contemplando mecanismos de autenticação, restrições vigentes, monitoramento por câmeras, diferenciação entre acessos UTEC x CPD, registros de tentativas não autorizadas e justificativas operacionais – demonstram que há controles eficazes em operação. A auditoria reforça, ainda assim, a importância de monitoramento periódico, considerando a criticidade do ambiente.

Além disso, na etapa de contrarrazões, a UTEC apresentou todos os documentos referente a Governança de TI, evidenciando conformidade integral dos itens avaliados.

Diante do conjunto de informações recebidas, dos controles verificados e das justificativas apresentadas, conclui-se que os processos de Tecnologia da Informação da ABDI encontram-se, de forma geral, em conformidade, com maturidade adequada, aderências às normas aplicáveis e mecanismos de controle consistentes. Os pontos registrados ao longo da auditoria não configuram falhas estruturais, mas oportunidades de aprimoramento contínuo – já acolhidas pela UTEC e incorporadas a seus respectivos plano de ação.

Recomenda-se a continuidade das ações de melhoria, especialmente no acompanhamento dos logs críticos, na atualização de políticas e no monitoramento periódico dos controles dos acessos físico e lógicos, assegurando a evolução constante do ambiente tecnológico da ABDI e a manutenção da confiabilidade necessária aos serviços prestados.

17 de novembro de 2025.

Audilink & Cia Auditores

ROBERTO CALDAS BIANCHESSI [redacted]
Assinado de forma digital por ROBERTO CALDAS BIANCHESSI [redacted]
Dados: 2025.12.02 15:38:44 -03'00'

Roberto Bianchessi

26/9/2025

RELATÓRIO DE AUDITORIA 2025

Agência Brasileira de Desenvolvimento Industrial

TECNOLOGIA DA INFORMAÇÃO

Sumário

ABDI – AGÊNCIA BRASILEIRA DE DESENVOLVIMENTO INDUSTRIAL

Brasília – DF

RELATÓRIO CIRCUNSTANCIADO DE AUDITORIA EXTERNA

REFERENTE AO ANO DE 2025

(Com vistas em Setembro / 2025)

1 INTRODUÇÃO

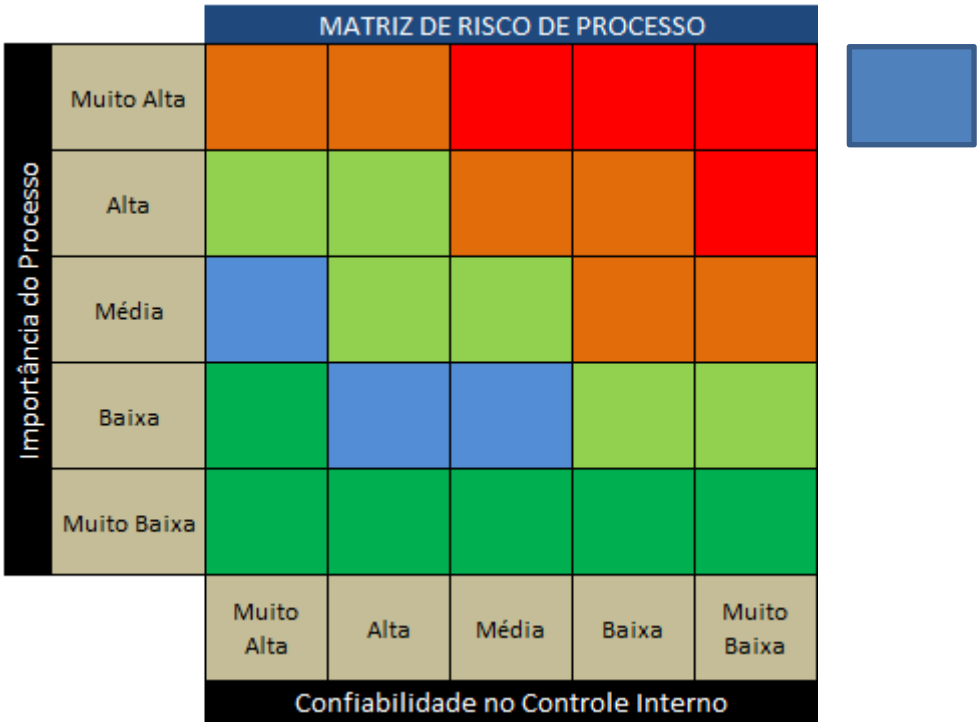
Com vistas à execução dos trabalhos de auditoria no ambiente de Tecnologia da Informação do ABDI, procedemos às análises da segurança da informação e seus controles (Sistemas, Contratos e Dados), com base na competência atual.

Os trabalhos foram realizados seguindo padrões usuais de auditoria aplicáveis no Brasil, em conformidade com as normas de governança de TI, de acordo com as metodologias internacionais Isaca, Cobit 5, em consonância com as Normas NBR ISO/IEC 12.119 (Tecnologia de Informação – Pacotes de *Software* – Testes e Requisitos de Qualidade) e NBR ISO/IEC 14.598 e NBR ISO 27.001 e 27.002. Objetivamos atender ao disposto na Resolução CFC nº 1.029/05**,** que aprova a NBC T 11.12 – Processamento Eletrônico de Dados, que trata da revisão dos Controles Internos e NBC P 1 (Normas Profissionais dos Auditores Independentes).

Foram executados exames documentais e evidências, utilizando critérios fundamentados em uma base seletiva, na extensão e profundidade julgadas necessárias nas circunstâncias, coletando informações e evidências.

Para cada apontamento do presente relatório está estabelecido o nível do risco da não conformidade, onde é utilizada a matriz Importância do Processo versus Confiabilidade no Controle Interno.

MATRIZ IMPORTÂNCIA DO PROCESSO x CONFIABILIDADE NO CONTROLE INTERNO



2 ESCOPO

O objetivo do presente trabalho de auditoria foi avaliar o ambiente, a conformidade e os controles dos processos de Tecnologia da Informação, considerando os seguintes eixos de analise:

SISTEMAS
Metodologia de Desenvolvimento de Sistemas
Ciclo de vida de softwares corporativos
Plano de gestão de mudanças - GMUD - Melhorias e Atualizações
Conformidade da documentação dos sistemas

CONTRATOS
Processo de contratações de TI
Planejamento da contratação
Planejamento da TI
Parcelamento de serviços
Análise da viabilidade da contratação
Plano de sustentação
Termos contratuais
Análise de riscos
Projeto básico ou termo de referência
Modalidades e tipos de licitação
Aferição de exequibilidade de propostas
Contratação direta
Registro de preços
Manutenção do equilíbrio econômico financeiro do contrato
Transição contratual
Analise de Aderência
Observar a existência de inventário de software
Aderência das aplicações ao negócio da Agência
Usabilidade
Compatibilidade com o parque tecnológico
Conformidade da Execução dos Contratos
Objetos contratados
Pagamentos
Qualidade do serviço e produto
Controle efetivo sobre execução

DADOS
Integridade
Confiabilidade
Sigilo
Disponibilidade dos dados
Relacionados ao negócio suportado pelos sistemas de informação

- ✓ Avaliação do ambiente organizacional relacionado aos processos mencionados acima, vinculados ao Macroprocesso Gestão de TI, sob o foco de gerenciamento dos riscos e controle;
- ✓ Avaliação da efetividade e a eficiência da estrutura de TI as atividades de disponibilidade interna a manter e direcionamento da eficácia a continuidade dos negócios.

3 PROCEDIMENTOS DE AUDITORIA

O trabalho foi conduzido por meio de analises documentais e da avaliação de evidências relacionadas à Sistemas, Contratos e Dados. No decorrer da auditoria, foram aplicados testes de observância com o objetivo de obter segurança razoável de que os procedimentos de controle interno estabelecidos pela gestão estão em funcionamento efetivo e em conformidade com as normas e diretrizes aplicáveis.

3.1 RESULTADOS DAS ANALISES E AVALIAÇÕES DOS EIXOS

CONTRATOS	Auditoria	Resultado da auditoria	Parecer da auditoria
Planejamento da contratação	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Planejamento da TI	Analise documental, evidências e amostragem.	Sugestão de melhoria	Em conformidade
Parcelamento de serviços	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Análise da viabilidade da contratação	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade

Plano de sustentação	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Termos contratuais	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Análise de riscos	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Modalidades e tipos de licitação	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Aferição de exequibilidade de propostas	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Contratação direta	Analise documental, evidências e amostragem.	Sugestão de melhoria	Em conformidade
Registro de preços	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Manutenção do equilíbrio econômico financeiro do contrato	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Transição contratual	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Observar a existência de inventário de software	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Aderência das aplicações ao negócio da Agência	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Usabilidade	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Compatibilidade com o parque tecnológico	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Objetos contratados	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Pagamentos	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Qualidade do serviço e produto	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Controle efetivo sobre execução	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade

SISTEMAS	Auditoria	Resultado da auditoria	Parecer da auditoria

Metodologia de Desenvolvimento de Sistemas	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Ciclo de vida de softwares corporativos	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Plano de gestão de mudanças - GMUD - Melhorias e Atualizações	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Conformidade da documentação dos sistemas	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade

DADOS	Auditoria	Resultado da auditoria	Parecer da auditoria
Integridade	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Confiabilidade	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Sigilo	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Disponibilidade dos dados	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade
Relacionados ao negócio suportado pelos sistemas de informação	Analise documental, evidências e amostragem.	Nenhuma exceção observada	Em conformidade

4 PRINCIPAIS RESULTADOS APONTADOS

Com base nas avaliações realizadas em conformidade com os objetivos e o escopo do trabalho, destacamos a seguir os principais resultados obtidos, que visam contribuir para a melhoria contínua dos controles internos.

4.1 PROCESSOS DE CONTRATOS – CONTRATAÇÃO DIRETA – SEM JUSTIFICATIVA

SITUAÇÃO IDENTIFICADA

Fluxo de Contratação Direta – Motivo de Dispensa

Durante a análise dos processos no fluxo de contratação direta de serviços, verificamos a inexistência do processo (etapa) e documentação que apresente a motivação legal para a dispensa de licitação, conforme exigido pela Lei nº 14.133/2021 e regulamentos internos da empresa pública.

O fluxo contempla a base legal para a dispensa de licitação, conforme o art. 9º do regulamento com limitações de valores.

EVIDÊNCIAS

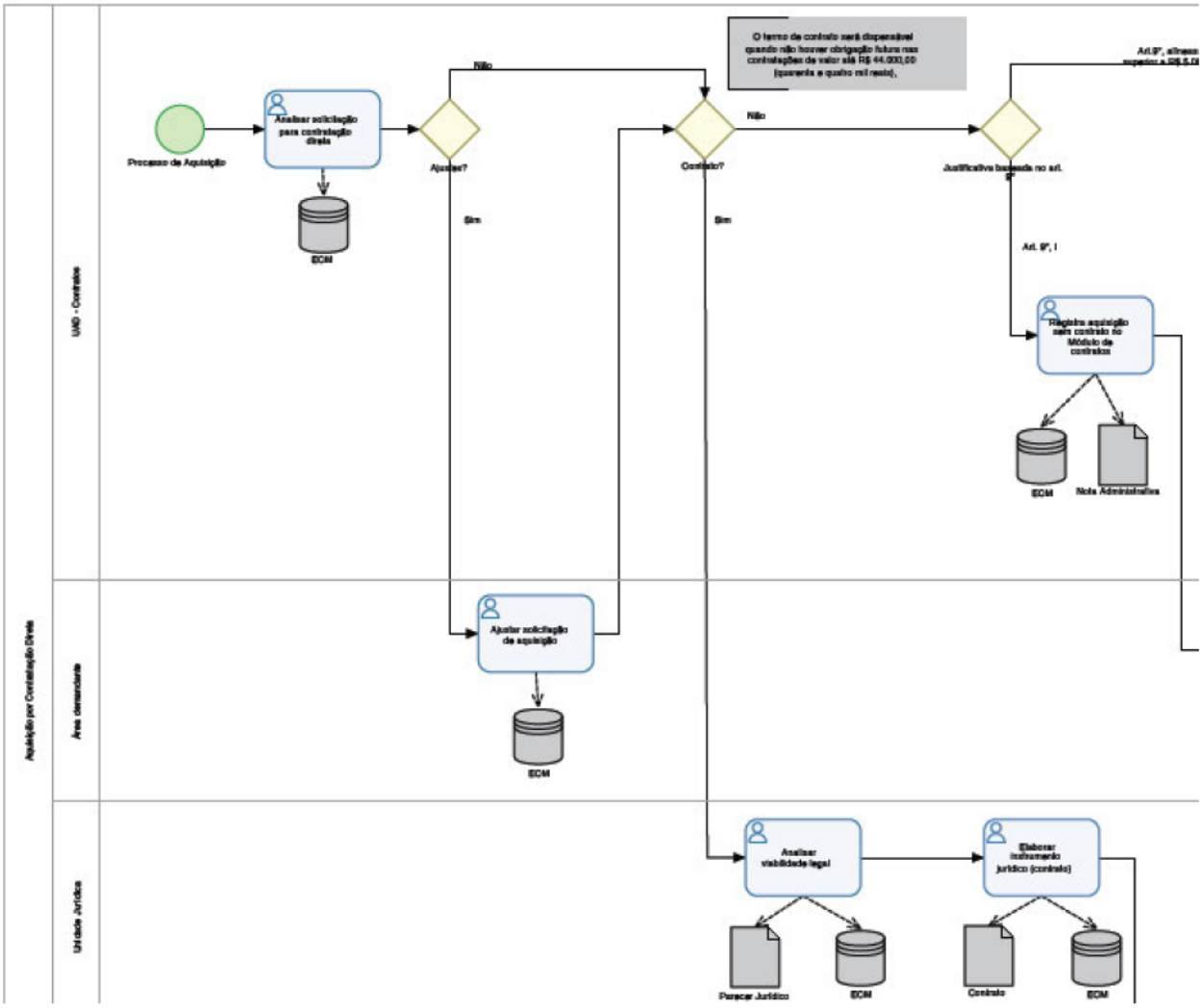
3. DEFINIÇÕES

3.1. Solicitação de aquisição: formulário emitido pela área demandante, ratificado pelo respectivo gerente, no qual será contextualizado o pedido, contendo:

3.1.1 Contratação direta: descrição do objeto a ser contratado; justificativa da necessidade/interesse da ABDI; base legal da dispensa e/ou inexigibilidade, com a devida justificativa; escolha da pessoa (física ou

a) Ter como fundamento a dispensa de licitação em razão do valor (artigo 7º, II, a, do RLC/ABDI), salvo se existir obrigação futura; ou

b) Quaisquer outros casos de enquadramento de dispensa.



RISCO

CLASSIFICAÇÃO RISCO	Alto

Nesta situação identificamos alguns riscos significativos e que devem serem levados em consideração:

• Descumprimento legal e regulatório: ausência de justificativa formal pode caracterizar violação da legislação de licitações e contratos, sujeitando a empresa a questionamentos por órgãos de controle externo.

• Responsabilização de gestores: sem respaldo documental, os responsáveis pela contratação podem ser responsabilizados por ato de improbidade administrativa ou irregularidade na gestão.

• Ineficiência na gestão: contratações sem justificativa podem não estar alinhadas ao planejamento estratégico ou às necessidades reais da organização.

RECOMENDAÇÕES

Sugerimos que a gestão adote procedimentos formais para assegurar que todos os processos de contratação direta contenham:

1. Fundamentação legal clara que justifique a dispensa de licitação;

2. Justificativa da escolha do fornecedor;

3. Demonstração da compatibilidade dos preços contratados com os praticados no mercado.

A adoção dessas medidas contribuirá para maior conformidade legal, transparência, economicidade e eficiência na gestão das contratações públicas.

COMENTÁRIOS ABDI

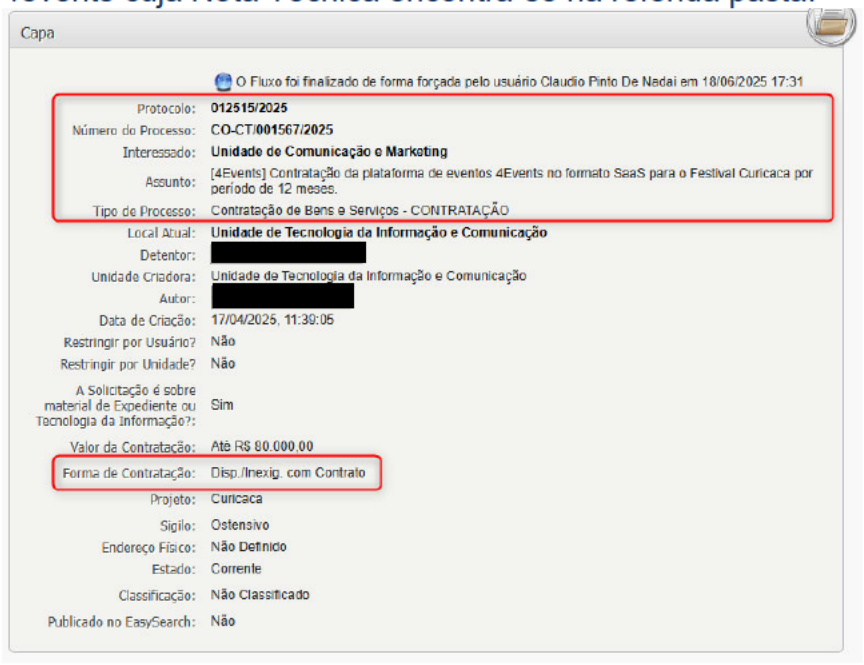
As contratações diretas, seja por dispensa ou inexigibilidade de licitação, são sempre fundamentadas e justificadas nas instruções processuais da Unidade de Tecnologia da Informação e Comunicação, por meio de Notas Técnicas. Tais documentos apresentam, de forma estruturada, os elementos necessários, tais como: a demonstração da necessidade da contratação, a justificativa da demanda, os estudos técnicos preliminares, as cotações de valores e a fundamentação para escolha da modalidade de contratação direta, em conformidade com os regulamentos desta Agência.

Adicionalmente, conforme estabelece a Instrução Normativa nº 07, compete à Unidade de Licitações, Contratos e Convênios (ULCC) a análise das solicitações de contratação direta, cabendo-lhe indicar a necessidade ou não de contrato formal, realizar ajustes eventualmente necessários junto à unidade demandante e elaborar a minuta contratual e seus anexos, quando aplicável.

Dessa forma, todas as contratações originadas desta Unidade são submetidas à apreciação da ULCC e da Unidade Jurídica, que realizam a devida verificação de conformidade, assegurando o cumprimento integral das obrigações legais e regulamentares.

Seguem, abaixo, o link para acesso à referida pasta com as evidências:
Contratação Direta

Capa do processo de contratação direta por dispensa – Contratação da plataforma 4events cuja Nota Técnica encontra-se na referida pasta.

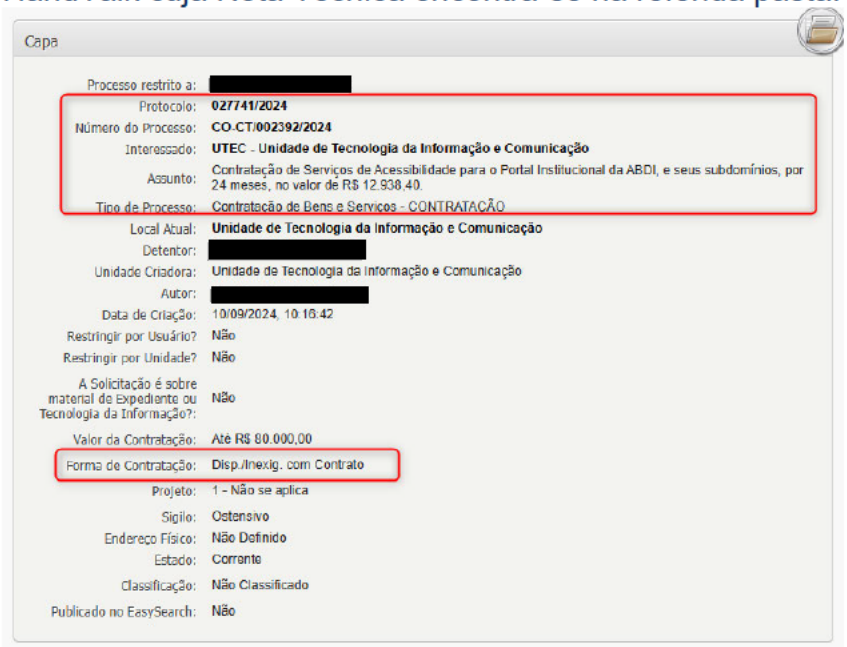


Capa

O Fluxo foi finalizado de forma forçada pelo usuário Claudio Pinto De Nadai em 18/06/2025 17:31

Protocolo:	012515/2025
Número do Processo:	CO-CT/001567/2025
Interessado:	Unidade de Comunicação e Marketing
Assunto:	[4Events] Contratação da plataforma de eventos 4Events no formato SaaS para o Festival Curicaca por período de 12 meses.
Tipo de Processo:	Contratação de Bens e Serviços - CONTRATAÇÃO
Local Atual:	Unidade de Tecnologia da Informação e Comunicação
Detentor:	[redacted]
Unidade Criadora:	Unidade de Tecnologia da Informação e Comunicação
Autor:	[redacted]
Data de Criação:	17/04/2025, 11:39:05
Restringir por Usuário?	Não
Restringir por Unidade?	Não
A Solicitação é sobre material de Expediente ou Tecnologia da Informação?:	Sim
Valor da Contratação:	Até R$ 80.000,00
Forma de Contratação:	Disp./Inexig. com Contrato
Projeto:	Curicaca
Sigilo:	Ostensivo
Endereço Físico:	Não Definido
Estado:	Corrente
Classificação:	Não Classificado
Publicado no EasySearch:	Não

Capa do processo de contratação direta por dispensa – Contratação da plataforma HandTalk cuja Nota Técnica encontra-se na referida pasta.



Capa

Processo restrito a:	[redacted]
Protocolo:	027741/2024
Número do Processo:	CO-CT/002392/2024
Interessado:	UTEC - Unidade de Tecnologia da Informação e Comunicação
Assunto:	Contratação de Serviços de Acessibilidade para o Portal Institucional da ABDI, e seus subdomínios, por 24 meses, no valor de R$ 12.938,40.
Tipo de Processo:	Contratação de Bens e Serviços - CONTRATAÇÃO
Local Atual:	Unidade de Tecnologia da Informação e Comunicação
Detentor:	[redacted]
Unidade Criadora:	Unidade de Tecnologia da Informação e Comunicação
Autor:	[redacted]
Data de Criação:	10/09/2024, 10:16:42
Restringir por Usuário?	Não
Restringir por Unidade?	Não
A Solicitação é sobre material de Expediente ou Tecnologia da Informação?:	Não
Valor da Contratação:	Até R$ 80.000,00
Forma de Contratação:	Disp./Inexig. com Contrato
Projeto:	1 - Não se aplica
Sigilo:	Ostensivo
Endereço Físico:	Não Definido
Estado:	Corrente
Classificação:	Não Classificado
Publicado no EasySearch:	Não

COMENTÁRIOS AUDITORIA

Conforme informado e evidenciado nos comentário da ABDI, todas as contratações são instruídas com Notas Técnicas que contêm justificativas, estudos, cotações e escolha do

fornecedor, com análise da ULCC e da Unidade Jurídica. Demonstra existência de procedimento formal e aderência normativa.

Sugerimos que no documento do fluxo seja incluída a etapa da documentação que comprove o motivo da contratação direta, assim apresenta mais clareza em todo o processo.

COMENTÁRIOS ABDI

A Unidade de Gestão Estratégica (UGE), responsável pela gestão dos processos da Agência, e a Unidade de Licitações, Contratos e Convênios (ULCC), unidade proprietária do processo, serão acionadas para orientação quanto à inclusão, na documentação do fluxo processual, de uma etapa específica destinada à apresentação de justificativa formal para contratações diretas, de modo a assegurar maior transparência e clareza em todo o processo.

4.2 PROCESSOS DE CONTRATOS – CONTRATAÇÃO DIRETA - VALORES

SITUAÇÃO IDENTIFICADA

Fluxo de Contratação Direta – Valores Desatualizados no Fluxo

Durante a análise dos processos no fluxo de contratação direta de serviços, verificamos que os valores estão diferentes do que consta no documento "Regulamento de Licitações e Contratos".

EVIDÊNCIAS

Fluxo de Contratação Direta
O termo de contrato será dispensável quando não houver obrigação futura nas contratações de valor até R$ 44.000,00 (quarenta e quatro mil reais),

__Art 9º, I do RLC __
Art. 9º A licitação poderá ser dispensada: I - nas contratações até os valores previstos nos incisos I, alínea "a",
e II, alínea "a", do art. 6º;
Art. 6º São limites para as dispensas e para as modalidades de licitação;
I - para obras e serviços de engenharia:
a)Dispensa - até R$ 79.000,00 (setenta e nove mil reais);
II - para compras e demais serviços:
a) Dispensa - até R$ 44.000,00 (quarenta e quatro mil reais);

Regulamento de Licitações e Contratos

Art. 7º. São limites para as dispensas e para as modalidades de licitação:

I - para obras e serviços de engenharia:

a) dispensa: até R$ 150.000,00 (cento e cinquenta mil reais);

b) convite: até R$ 2.200.000,00 (dois milhões e duzentos mil reais);

c) concorrência: acima de R$ 2.200.000,00 (dois milhões e duzentos mil reais).

II - para compras e demais serviços:

a) dispensa: até R$ 80.000,00 (oitenta mil reais);

RISCO

CLASSIFICAÇÃO RISCO	Baixo

Nesta situação identificamos alguns riscos significativos e que devem serem levados em consideração:

• Inconsistência normativa e divergência entre fluxo interno e regulamentação oficial gera insegurança jurídica fragilizando a governança e o controle das contratações.

• Descumprimento normativo interno do processo segue parâmetros distintos do regulamento oficial, gerando inconsistências normativas.

• Retrabalho e Burocracia ao adotar limites menores, a empresa pode estar exigindo mais processos de contratação do que a lei e o regulamento determinam, aumentando o custo administrativo, tempo de dedicação e prazos de contratação.

RECOMENDAÇÕES

Sugerimos que seja realizado avaliação e ajustes no fluxo de contratação direta ao regulamento de licitação e contratos vigente, de forma que os valores limites estejam atualizados e consistentes, garantindo a uniformidade normativa, simplificação do processo, redução de burocracias e segurança jurídica.

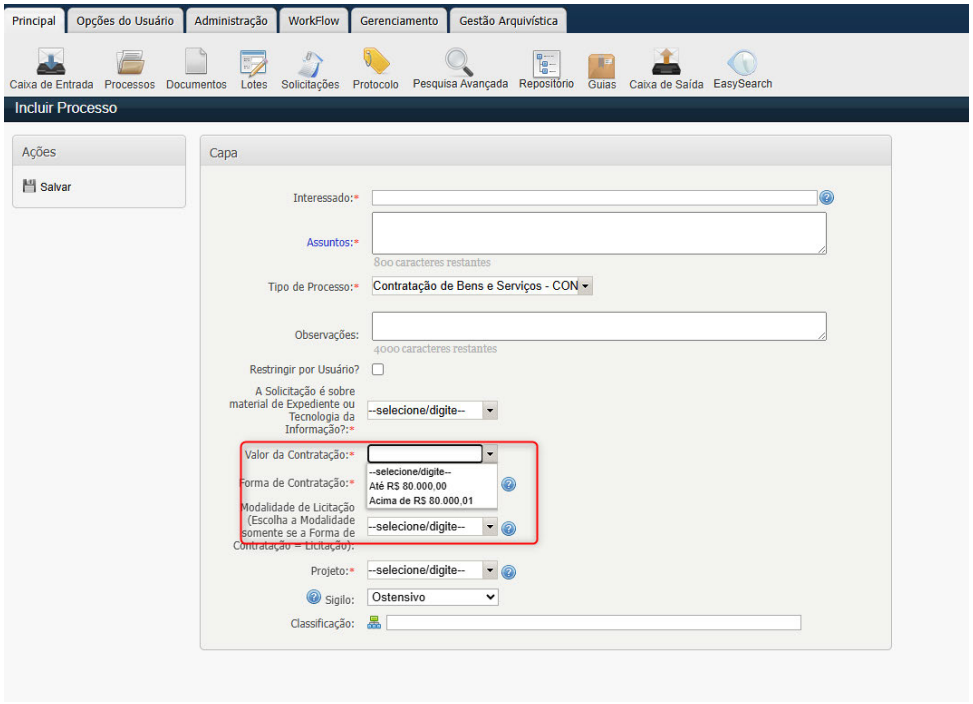
COMENTÁRIOS ABDI

O fluxo de contratação apresentado com valor divergente para a hipótese de dispensa de licitação refere-se a um mapeamento em BPMN cadastrado no sistema SA Interact, cuja responsabilidade de atualização é da Unidade de Gestão Estratégica (UGE).

Ressaltamos que a Instrução Normativa nº 07, que regulamenta os valores de contratação, teve sua última atualização em 16/09/2024.

Embora o fluxo no SA Interact ainda não tenha refletido essa atualização, destacamos que o Sistema ECM (Abertura de Contratações) já se encontra devidamente parametrizado com os valores atualizados, conforme demonstrado na imagem em anexo.

Dessa forma, não há impacto na instrução processual das contratações de TI, tampouco desconformidade nos processos conduzidos, uma vez que o sistema utilizado efetivamente para abertura e tramitação das contratações adota os valores corretos e vigentes.



COMENTÁRIOS AUDITORIA

Nos comentários da ABDI, esta esclarecendo que o fluxo BPMN é responsabilidade da UGE e ainda não foi atualizado, mas o sistema ECM já está parametrizado com os valores corretos desde a atualização da IN nº 07/2024.

Para uma efetividade melhor e também maior clareza, sugerimos que os valores também sejam atualizados no fluxo de contratação direta.

COMENTÁRIOS ABDI

A Unidade de Gestão Estratégica (UGE), responsável pela gestão dos processos da Agência, e a Unidade de Licitações, Contratos e Convênios (ULCC), unidade proprietária do processo, serão acionadas para orientação quanto à atualização do fluxo de contratação direta a fim de dar conformidade à IN nº 07/2024 e ao sistema ECM.

4.3 PROCESSOS DE CONTRATOS – PLANEJAMENTO DE AQUISIÇÕES

SITUAÇÃO IDENTIFICADA

Durante a análise do documento Planejamento Aquisições de TI 2025, identificamos um item que não é propriamente ligado ao planejamento de TI, pois trata de despesas administrativas gerais.
Podendo gerar confusão ao integrar custos não tecnológicos dentro do planejamento de TI.

EVIDÊNCIAS

Documento: PLANEJAMENTO_AQUISIÇÕES DE TI_2025

16	Contrato 039/2023 - Quatto Tecnologia	Serviços Especializados de TI	DESPESAS C/ SERVIÇOS DE SOFTWARE - PJ	Despesas c/ Serviços de TI - PJ	R$ 1.090.800,00
17	Despesas Gerais Administrativas	Despesas Gerais Administrativas	DESPESAS ADMINISTRATIVAS GERAIS	DESPESAS ADMINISTRATIVAS GERAIS	R$ 20.000,00
18	ARP Aquisição de computadores tipo Desktop, Notebook, Monitores e Acessórios	Equipamentos e Material Permanente		INV - Equipamentos e Material Permanente	R$ 247.900,00
				TOTAL	R$ 8.626.431,42

RISCO

CLASSIFICAÇÃO RISCO	Baixo

Nesta situação identificamos podemos apontar que esta havendo um desvio de finalidade do orçamento de TI, pois gera interpretações equivocadas sobre o recurso efetivamente destinado a TI, comprometendo o planejamento com o plano estratégico institucional.

RECOMENDAÇÕES

Sugerimos retirar ou reposicionar o item 'Despesas Gerais Administrativas' em outro planejamento (administrativo geral) e complementares o documento com objetivos estratégicos, indicadores e cronograma de execução.

COMENTÁRIOS ABDI

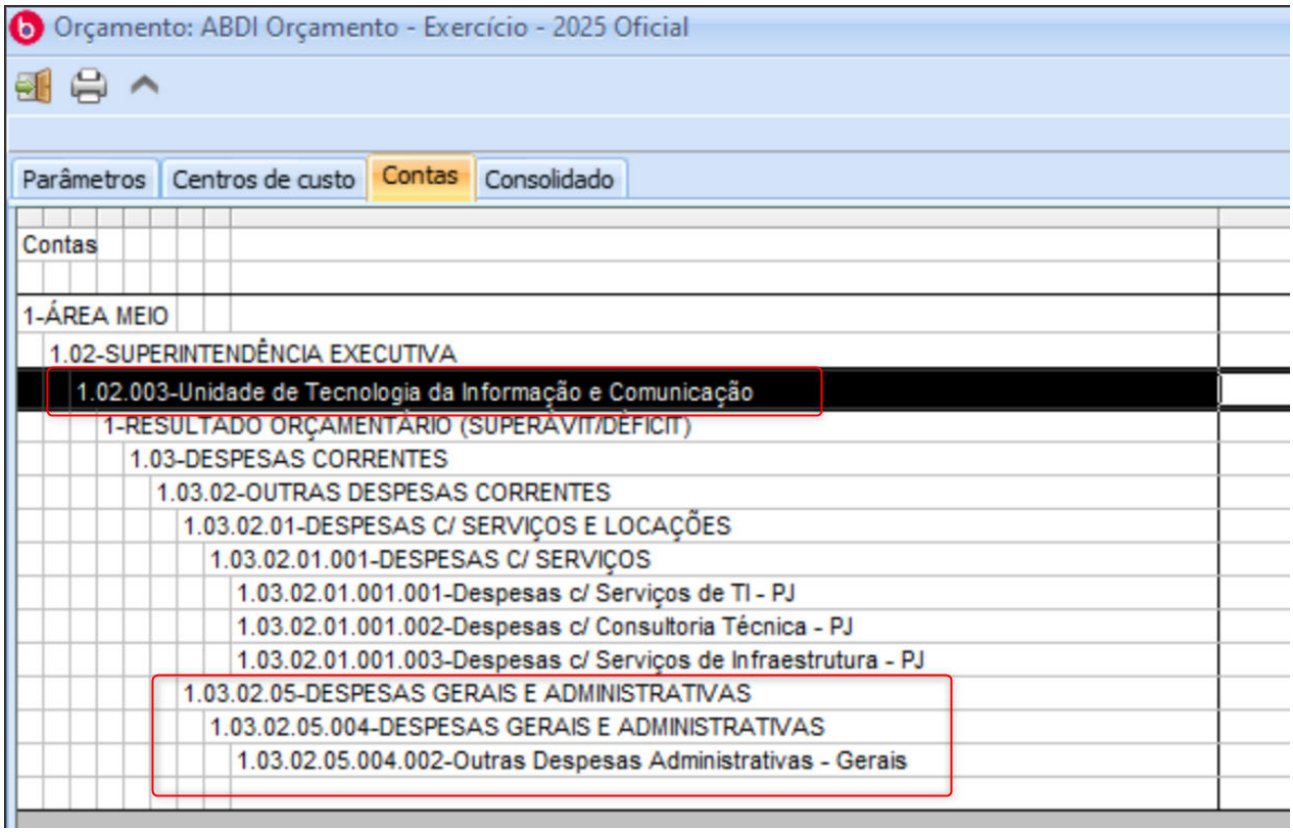
As rubricas orçamentárias são previamente definidas pela Unidade Administrativa competente e preenchidas pelas unidades demandantes, compondo de forma integrada a árvore orçamentária da Agência. Ressalta-se que a rubrica em questão está vinculada exclusivamente à Unidade de Tecnologia da Informação e Comunicação, o que garante a correta classificação e destinação dos recursos.

Dessa forma, não há margem para interpretações divergentes quanto à sua aplicação, tampouco para eventuais desvios de finalidade.

Tabela padrão disponibilizada para o planejamento orçamentário.

Unidade de Tecnologia da Infoaudio)			TOTAL	R$
PROJETOS DA ÁREA				
Unidade / Assessoria	Projeto	Tipo de Despesa – Conta Gerencial	Objeto do Instrumento	
Unidade de Tecnologia da Informação e Comunicação (UTEC)	Custeio e Serviços Adm - PAA	Despesas c/ Serviços de TI - PJ	Contrato 03/2025 - VSData e Contrato 036/2020 - Engesoftware e Contrato 036/2021 - Stefanini e Contrato 037/2020 - NTSEC - Segurança Perimetral (TI) e Contrato 038/2023 - Telefônica e Contrato 039/2023 - Quatto Tecnologia e Contrato 086/2022 - G4F e Contrato 24/2023 - Nexdata e Contrato 66/2024 - Benner	R$
Unidade de Tecnologia da Informação e Comunicação (UTEC)	Custeio e Serviços Adm - PDP Rateio	Despesas c/ Serviços de TI - PJ	Contrato 03/2025 - VSData;Contrato 036/2020 - Engesoftware;Contrato 036/2021 - Stefanini; Contrato 037/2020 - NTSEC;Contrato 038/2023 - Telefônica; Contrato 039/2023 - Quatto Tecnologia; Contrato 086/2022 - G4F;Contrato 24/2023 - Nexdata;Contrato 66/2024 - Benner	R$
Unidade de Tecnologia da Informação e Comunicação (UTEC)	Custeio e Serviços Adm - PAA	Despesas c/ Serviços de Consultoria Técnica - PJ	Contrato 017/2022 - EveryTI	R$
Unidade de Tecnologia da Informação e Comunicação (UTEC)	Custeio e Serviços Adm - PDP Rateio	Despesas c/ Serviços de Consultoria Técnica - PJ	Contrato 017/2022 - EveryTI	R$
Unidade de Tecnologia da Informação e Comunicação (UTEC)	Custeio e Serviços Adm - PAA	Despesas c/ Serviços de Infraestrutura - PJ	Contrato 08/2021 - Leistung - No Break;Contrato 09/2021 - Método - Telefonia VOIP e Contrato 55/2024 - Algar;Contrato 16/2024 - Telefônica Contrato 27/2023 - Technocopy;Contrato 57/2024 - NWI e Contrato 56/2024 - MCD;NIC.BR	R$
Unidade de Tecnologia da Informação e Comunicação (UTEC)	Custeio e Serviços Adm - PDP Rateio	Despesas c/ Serviços de Infraestrutura - PJ	Contrato 08/2021 - Leistung - No Break;Contrato 09/2021 - Método - Telefonia VOIP e Contrato 55/2024 - Algar;Contrato 16/2024 - Telefônica Contrato 27/2023 - Technocopy;Contrato 57/2024 - NWI e Contrato 56/2024 - MCD;NIC.BR	R$
Unidade de Tecnologia da Informação e Comunicação (UTEC)	Custeio e Serviços Adm - PAA	Outras Despesas Administrativas - Gerais	-	R$
Unidade de Tecnologia da Informação e Comunicação (UTEC)	Custeio e Serviços Adm - PDP Rateio	Outras Despesas Administrativas - Gerais	-	R$
Unidade de Tecnologia da Informação e Comunicação (UTEC)	Inv - Equipamentos e Material Permanente PAA	Equipamentos de Material Permanente	ARP 02/2025 - Insight	R$

Estrutura orçamentária da Unidade UTEC no sistema ERP.



COMENTÁRIOS AUDITORIA

Conforme os comentários da ABDI foi apresentado e justificado a forma que é realizada a classificação orçamentária e consideramos válida, mas na interpretação das informações para analises pode gerar dúvidas.

Sendo assim, sugerimos revisar o documento de planejamento para segregar despesas administrativas, incluindo objetivos e direcionamento, facilitando a interpretação de futuras analises.

COMENTÁRIOS ABDI

Com o objetivo de mitigar eventuais dúvidas e aprimorar os processos futuros, a Unidade de Tecnologia da Informação e Comunicação (UTEC) adotará as sugestões apresentadas a partir do ciclo orçamentário de 2026 e também aos exercícios subsequentes.

4.4 PROCESSOS DE CONTRATOS – CONTROLE DOS PROCESSOS

SITUAÇÃO IDENTIFICADA

Durante a execução dos trabalhos, não foram apresentadas evidências e documentos que comprovem controles relacionados aos contratos de TI, referente aos seguintes itens avaliados:

- Observar a existência de inventário de software;
- Aderência das aplicações ao negócio da Agência;
- Usabilidade;
- Compatibilidade com o parque tecnológico;
- Qualidade do serviço e produto;
- Transição contratual.

EVIDÊNCIAS

Não apresentadas

RISCO

CLASSIFICAÇÃO RISCO	Baixo

A ausência de documentação e evidências limita a capacidade da auditoria em confirmar:

- A efetividade da gestão de softwares e aplicações utilizadas;
- O alinhamento das aplicações ao negócio institucional;
- A qualidade e confiabilidade dos serviços de TI prestados;
- A compatibilidade tecnológica necessária para a continuidade dos serviços.

CONCLUSÃO

Na ausência de evidencias e documentos, não foi possível validar a conformidade dos controles sobre os contratos de TI nos itens apontados.

COMENTÁRIOS ABDI

Ressalta-se que os controles inicialmente apontados como “não possível validar a conformidade por ausência de evidências” não foram plenamente submetidos em virtude da ausência de clareza e objetividade nas solicitações encaminhadas, as quais demandavam um conjunto amplo de documentações sem detalhar especificamente quais controles deveriam ser apresentados. Diante disso, alguns controles não foram evidenciados pela Unidade de Tecnologia da Informação e Comunicação no momento oportuno.

Cabe destacar, contudo, que parte desses controles já estava contemplada em documentos previamente enviados, como termos de referência e contratos. Para mitigar eventuais lacunas e assegurar a devida rastreabilidade, esta Unidade organizou pastas específicas contendo as evidências correspondentes a cada um dos controles questionados.

Seguem, abaixo, os links para acesso às referidas pastas:
Observar a existência de inventário de software
Qualidade do serviço e produto
Compatibilidade com o parque tecnológico
Aderência das aplicações ao negócio da Agência
Usabilidade
Transição Contratual

COMENTÁRIOS AUDITORIA

Após analises das evidências enviadas, comprova que os controles estão formalizados e vigentes aos processos.

Desta forma consideramos este item em conformidade.

4.4 DADOS – FALHAS DE ACESSO COM USUÁRIO “SA”

SITUAÇÃO IDENTIFICADA

Durante as analises dos registros no relatório dos Logs, identificamos muitas falhas de acesso utilizando o usuário “Owner” – “SA” (Administrador do Banco do Dados) do SQL Server.

Este situação ocorre desde as 00h00min horas até 24h00min horas de cada dia, ou melhor, todos os dias conforme registros, com intervalos de 30 segundos a 1 minuto.

EVIDÊNCIAS

A quantidade de registros e bem grande e abaixo apresentamos uma pequena quantidade por amostragem:

```
Information,31/07/2025 21:59:28,MSSQL$SSIS_SSRS,18456,Logon,Login failed for user 'sa'. Reason:
Password did not match that for the login provided. [CLIENT: <local machine>]
Information,31/07/2025 21:59:19,MSSQL$SSIS_SSRS,18456,Logon,Login failed for user 'sa'. Reason:
Password did not match that for the login provided. [CLIENT: <local machine>]
Information,31/07/2025 21:58:28,MSSQL$SSIS_SSRS,18456,Logon,Login failed for user 'sa'. Reason:
Password did not match that for the login provided. [CLIENT: <local machine>]
Information,31/07/2025 21:58:19,MSSQL$SSIS_SSRS,18456,Logon,Login failed for user 'sa'. Reason:
Password did not match that for the login provided. [CLIENT: <local machine>]
Information,31/07/2025 21:57:28,MSSQL$SSIS_SSRS,18456,Logon,Login failed for user 'sa'. Reason:
Password did not match that for the login provided. [CLIENT: <local machine>]
Information,31/07/2025 21:57:19,MSSQL$SSIS_SSRS,18456,Logon,Login failed for user 'sa'. Reason:
Password did not match that for the login provided. [CLIENT: <local machine>]

Information,31/07/2025 21:52:18,MSSQL$SSIS_SSRS,18456,Logon,Login failed for user 'sa'. Reason:
Password did not match that for the login provided. [CLIENT: <local machine>]
Information,31/07/2025 21:51:27,MSSQL$SSIS_SSRS,18456,Logon,Login failed for user 'sa'. Reason:
Password did not match that for the login provided. [CLIENT: <local machine>]
Information,31/07/2025 21:51:18,MSSQL$SSIS_SSRS,18456,Logon,Login failed for user 'sa'. Reason:
Password did not match that for the login provided. [CLIENT: <local machine>]
Information,31/07/2025 21:50:27,MSSQL$SSIS_SSRS,18456,Logon,Login failed for user 'sa'. Reason:
Password did not match that for the login provided. [CLIENT: <local machine>]
Information,31/07/2025 21:50:18,MSSQL$SSIS_SSRS,18456,Logon,Login failed for user 'sa'. Reason:
Password did not match that for the login provided. [CLIENT: <local machine>]
Information,31/07/2025 21:49:27,MSSQL$SSIS_SSRS,18456,Logon,Login failed for user 'sa'. Reason:
Password did not match that for the login provided. [CLIENT: <local machine>]
```

RISCO

CLASSIFICAÇÃO RISCO	Muito alto

Esta é uma situação muito crítica e merece uma verificação o mais breve possível, podendo, pois transparece uma ação de ataque de força bruta, podendo ser:

- Tentativas de descobrir a senha do administrador do banco de dados;
- Tentativas de ataque por Vírus ou Malware;
- Serviço ou aplicação configurada com credenciais antigas;
- Script ou Jobs rodando em loop;
- Falhar de segurança do Firewall;
- Backup automático ou software legado que perdeu sincronismo de credenciais;
- Entre outras situações.

RECOMENDAÇÕES

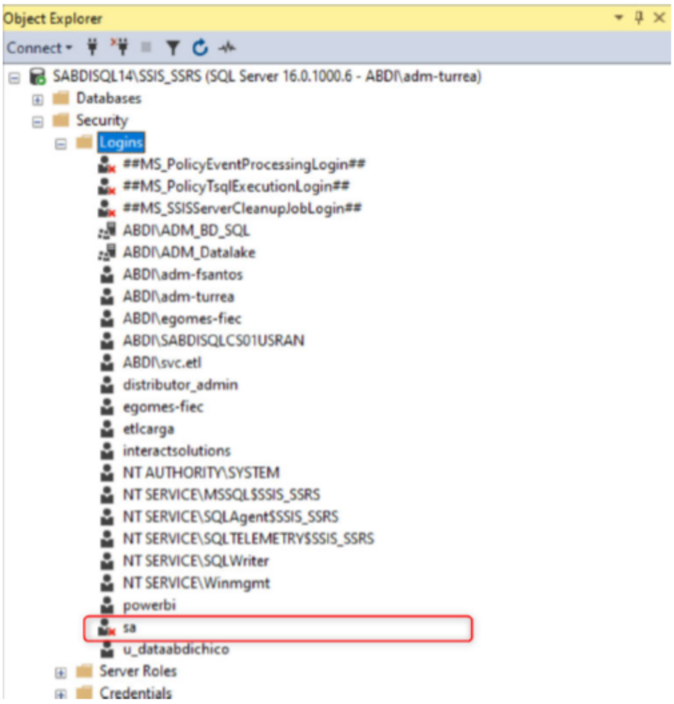
Sugerimos que sejam revisados todos os serviços, aplicações e Jobs que utilizam a conta "SA" e corrigir as credenciais configuradas ou até mesmo criar um usuário específico para cada serviço, deixando o "Owner" exclusivo para utilização apenas pelo administrador do banco de dados.
Reforçar controles de segurança: Antivírus se está emitindo alertas, Registros de auditoria, entre outros.

COMENTÁRIOS ABDI

Identificamos que as ocorrências registradas nos logs estavam relacionadas a uma rotina configurada com o usuário **"sa"**, cuja senha encontrava-se expirada, ocasionando falhas recorrentes de autenticação e, consequentemente, a geração de registros classificados como falsos positivos.

Para sanar a situação, a rotina foi reconfigurada com um usuário específico e mais adequado ao seu propósito. Além disso, o usuário **"sa"** foi devidamente desabilitado,

mitigando o risco de novas tentativas de acesso indevido e reforçando a segurança do ambiente de banco de dados, conforme evidenciado abaixo.



COMENTÁRIOS AUDITORIA

Conforme comentários da ABDI informaram que a situação foi normalizada e resolvida após a ação de reconfiguração do usuário de uma rotina interna do banco de dados.

Desta forma consideramos o problema foi resolvido e este ponto esta em conformidade.

5 DOCUMENTOS E EVIDÊNCIAS APRESENTADAS

PILAR CONTRATOS
Amostra Atas e SR (3 documentos)
OS6_DPO_1C - Relatório de Atendimento 1.0
Status Report (2 documentos)
Amostra Contratos de Fornecedores de TI (13 pastas)
Contratos_de_Fornecedores_de_TI
Relação dos Processos de Contratação de TI
PLANEJAMENTO_AQUISIÇÕES DE TI_2025
Notas de Pagamentos Fornecedores (4 pastas)
Minuta_Atualização_PETIC.PDTIC_2025-2026
PETIC.PDTIC_ABDI2020_2023

RESOLUÇÃO DIREX N UJ 00035-2025, DE 06 DE AGOSTO DE 2025 - Aprova proposta de Orçamento Programa, de acordo com o Primeiro Termo Aditivo ao Contrato de Gestão.
RESOLUÇÃO DIREX N UJ 00036-2025, DE 06 DE AGOSTO DE 2025 - Aprovacao Portfolio de Projetos
RESOLUÇÃO DIREX N UJ 00037-2025, DE 06 DE AGOSTO DE 2025 - Aprova proposta de reformulação.
Contratação de Bens e Serviços - CONTRATAÇÃO2508131135
Fluxo_Contratação_Direta
Fluxo_de_contratação
Fluxo_Solicitação_de_Aquisição
INA-07-Aquisicao-de-bens-e-servicos-consolidade-publicar
Regulamento-de-Licitacoes-e-Contratos-2021_compressed
Acompanhamento de Contratos - UTEC_ERPBENNER_vigentes
Controle de pagamentos 2024-2025
Controle de processos de fornecedores
EVIDÊNCIAS CONTROLE DE FORNECEDORES PELO SISTEMA ECMv2
GESTÃO DE FORNECEDORES PELO PORTAL MAISBI
Processo de avaliação e acompanhamentos dos serviços contratados por TIv2
Processos de Pagamento UTEC (5 pastas)
Aviso de final do clico de faturamento dos fornecedores
Fluxo do Processo de Pagamento da ABDI
Fluxo_de_contratação
Fluxo_de_pagamento_de_fornecedores_de_TI
Relação dos Processos Adm. de Contratação de TI / Processos por unidade2508131159
Aviso de final do clico de faturamento dos fornecedores
Contratações de TI_Leiame
Fluxo do Processo de Pagamento da ABDI
Fluxo_de_pagamento_de_fornecedores_de_TI

PILAR DADOS
Controle_de_Acesso_(Privilegiado)
Controle de Backups
Estrutura de SGBDs da ABDI_0425
Registro de Bloqueios de Acessos
Processo de Gestão de Incidentes e Violação de Dados Pessoais – entrega
Fluxo de Gestão de Incidente
Logs de acesso ao banco de dados (3 documentos)
Politica de backup
Evidência de Execução - Julho2025
Evidência_Backup_Nuvem_Microsoft
Evidência_de_Execução_RestoreMar2025
ScheduleReport_Backups
Política de Seg. da Informação-INA-12-e-resolucao
Política de governança de dados_VF
Produto 1.5 - Metodologia de Governança de Dados ABDI_v2
Política de Privacidade e Proteção de Dados
Relatório de bloqueio de acesso a internet
[2025-07_ABDI] Relatório Mensal de segurança
31._Relatorio_ABDI_Julho_2025_assinado
Regulamento-de-Licitacoes-e-Contratos-2021_compressed-1 (1)

PILAR SISTEMAS
PORTAL DA ABDI (7 pastas)
PROREG (6 pastas)
ABDI_MGP3_Metodologia-1
ESTRUTURA DE DOCUMENTAÇÃO DE SISTEMAS
MDS_ABDI_V1.1
PLANO_DE_GESTÃO_DE_MUDANÇA_-_GMUD
POLÍTICA_DE_CICLO_DE_VIDA_DE_SISTEMAS_E_PORTAIS
POLÍTICA_DE_DESENVOLVIMENTO_DE_SISTEMAS

6 CONSIDERAÇÕES FINAIS

O presente trabalho teve como objetivo avaliar os processos de Tecnologia da Informação no âmbito da ABDI. Constatou-se que, em termos gerais, a área apresenta processos estruturados e definidos, com aderência a práticas de governança e controles internos.

Entretanto, foram identificadas fragilidades relevantes no processo de contratação direta, notadamente: (i) ausência de justificativa legal formal para a dispensa de licitação, configurando risco ALTO de descumprimento normativo; (ii) divergências de valores no fluxo de contratação direta em relação ao regulamento oficial, configurando risco BAIXO, mas que pode impactar a uniformidade e eficiência dos procedimentos; e (iii) falhas de acesso pelo usuário, configurado risco MUITO ALTO, que pode impactar na segurança do banco de dados e até a continuidade dos negócios da organização.

Adicionalmente, verificou-se ausência de evidências em controles relacionados a inventário de software, aderência das aplicações ao negócio, usabilidade, compatibilidade tecnológica e qualidade de serviços de TI, o que limita a plena validação da conformidade nesses aspectos.

Recomenda-se que a gestão adote medidas corretivas, priorizando a formalização das contratações diretas, a atualização do fluxo de contratação de acordo com a regulamentação vigente e o fortalecimento dos planos e políticas de controle,

assegurando maior clareza nos processos internos, transparência, conformidade legal e eficiência na gestão de TI.

26 de setembro de 2025.

AudiLink & Cia Auditores

ROBERTO CALDAS BIANCHESSI: [redacted]

Assinado de forma digital por ROBERTO CALDAS BIANCHESSI: [redacted]
Dados: 2025.10.14 11:17:48 -03'00'

[redacted]

Roberto Bianchessi

Protocolo de Assinatura(s)

O documento acima foi proposto para assinatura digital. Para verificar as assinaturas acesse o endereço http://ecm.abdi.com.br/docflow/digitalSignChecker.jsf e utilize o código abaixo para verificar se este documento é válido.

Código de verificação: ZYLI-SEJW-VUHL-A9ZI

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 04/12/2025 é(são) :

Legenda: Aprovada Indeterminada Pendente

- ROBERTO CALDAS BIANCHESSI - 14/10/2025 11:17:48 (Certificado Digital)