1/11/2022

RELATÓRIO DE AUDITORIA 2022

Agência Brasileira de Desenvolvimento Industrial

TECNOLOGIA DA INFORMAÇÃO

Sumário

ABDI – AGÊNCIA BRASILEIRA DE DESENVOLVIMENTO INDUSTRIAL

São Paulo – SP

RELATÓRIO CIRCUNSTANCIADO DE AUDITORIA EXTERNA
REFERENTE AO ANO DE 2022

(Com vistas em Novembro/22)

1 INTRODUÇÃO

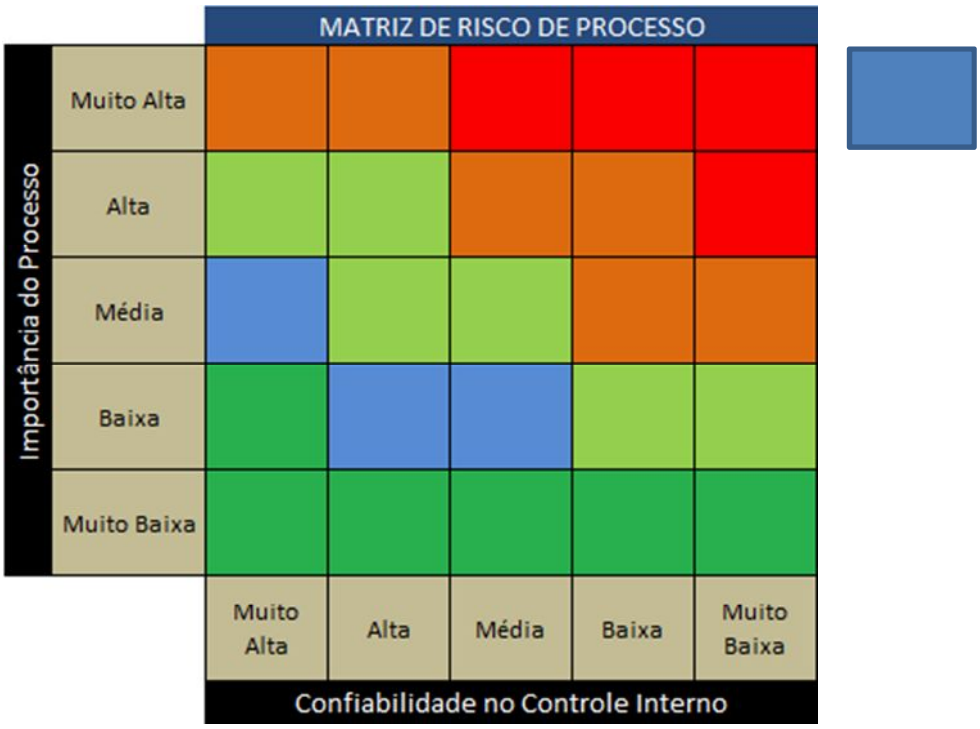
Com vistas à execução dos trabalhos de auditoria no ambiente de Tecnologia da Informação do ABDI, procedemos às análises da segurança física e lógica da informação (rede, sistemas, controles e gestão), com base na competência atual.

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 trabalho foi realizar avaliação do ambiente, conformidade e controles dos processos:

SEGURANÇA DA INFORMAÇÃO
➢ GESTÃO DE CONTROLE DE ACESSOS LÓGICOS ▪ ACTIVE DIRECTORY; ▪ SISTEMAS CORPORATIVOS. ➢ BANCO DE DADOS ▪ ADMINISTRAÇÃO DE ACESSO (ADMINISTRADOR); ▪ USUÁRIOS; ▪ PERFIL E REVOGAÇÃO. ➢ GESTÃO DE CONTROLE DE ACESSO FÍSICO ▪ INSTALAÇÕES E AMBIENTES; ▪ DATA CENTERS; ▪ SISTEMAS DE SEGURANÇA E ACESSOS. ➢ SOFTWARE DE SEGURANÇA DE ACESSO ▪ ANTIVÍRUS; ▪ ANTI-SPYWARE; ▪ ANTI-MALWARE; ▪ FIREWALL. ▪ PROCEDIMENTOS (Instalação, Parametrização e Configuração).

SISTEMAS
➢ METODOLOGIA DE DESENVOLVIMENTO DE SISTEMAS; ➢ CICLO DE VIDA DE SOFTWARE CORPORATIVO; ➢ PLANO DE GESTÃO DE MUDANÇAS – GMUD: ▪ MELHORIAS; ▪ ATUALIZAÇÕES. ➢ CONFORMIDADE DA DOCUMENTAÇÃO DOS SISTEMAS.

DADOS
➢ INTEGRIDADE; ➢ CONFIABILIDADE; ➢ SIGILO; ➢ DISPONIBILIDADE DOS DADOS; ➢ RELACIONAMENTO 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 realizado através de analises e procedimentos de avaliação de documental e evidências referente à **Segurança da Informação, Sistemas em Produção e Dados.**

Nas analises foram aplicados testes de observância para à obtenção da razoável segurança de que os procedimentos de controle interno estabelecidos pela gestão estão em efetivo funcionamento e cumprimento.

4 PRINCIPAIS RESULTADOS APONTADOS

Com base nas avaliações procedidas de acordo com os objetivos do escopo do trabalho, destacamos a seguir os principais resultados obtidos para a melhoria continua dos controles internos:

4.1 SEGURANÇA DA INFORMAÇÃO

4.1.1 PLANO DE CONTINGÊNCIA DISASTER RECOVERY- AMBIENTE E SISTEMA

SITUAÇÃO IDENTIFICADA

O plano de recuperação de ambiente do Data Center, sistemas e aplicações por recuperação de desastres e continuidade dos negócios a fim de garantir com segurança e tecnologia nas áreas de maior risco, fazendo parte do planejamento de contingência.

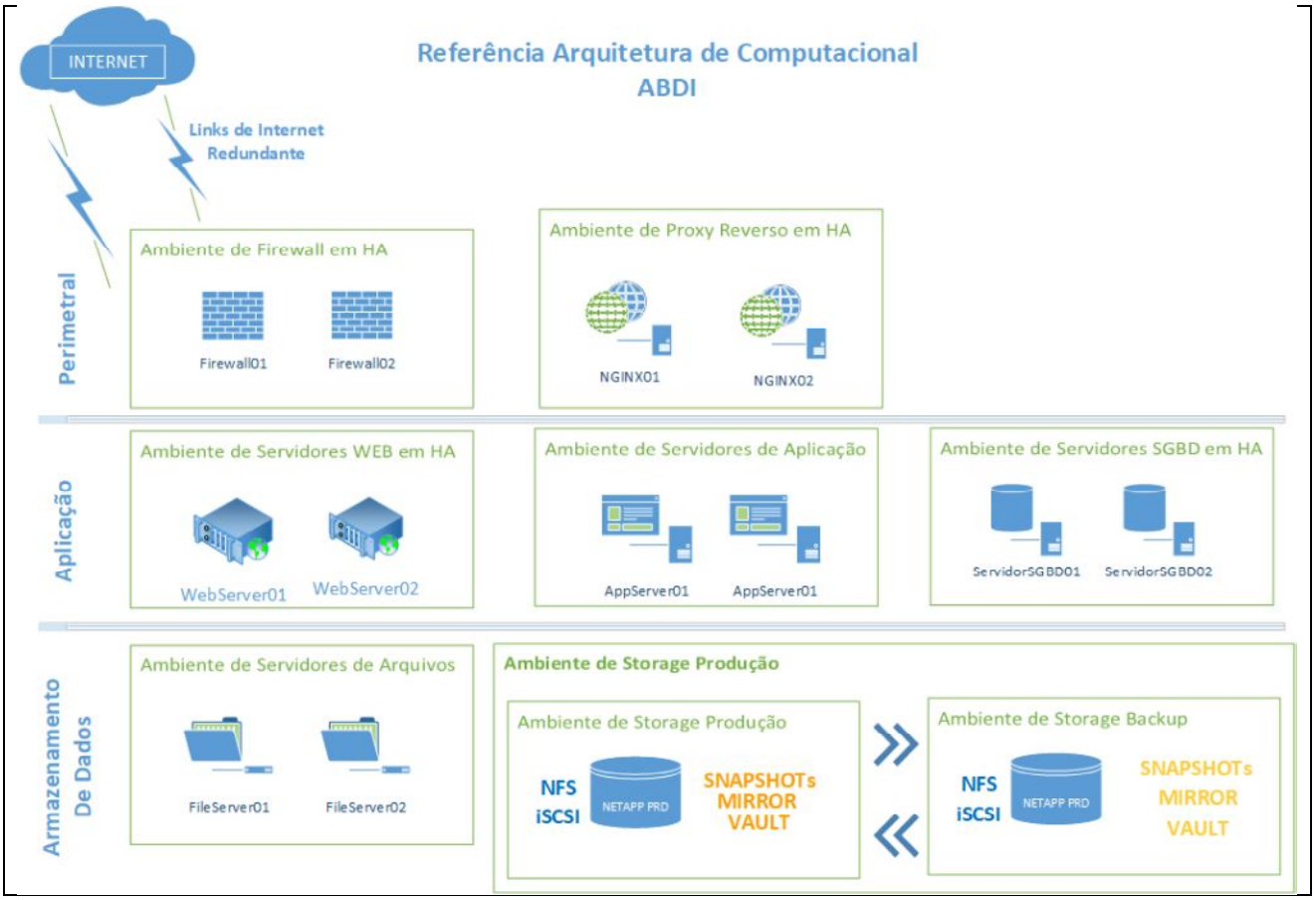
Avaliando os documentos evidenciais documentais, identificamos que atualmente não existe um ambiente totalmente replicável e plano de contingência para atingir toda a necessidade dos negócios da ABDI, sendo replicado ou até mesmo com espelhamento para recuperação de todo o ambiente de Tecnologia caso ocorra um desastre e deixe inoperante todo o processamento de dados e informações da organização.

O documento apresentado informa que existem configurações do ambiente quanto a espelhamento e replica de dados dentro do ambiente da ABDI todos os sistemas são configurados utilizando-se de soluções de HÁ, Cluster e/ou espelhamento de dados.

Mas não foi apresentado registros do plano de testes já executados, ou seja, onde desliga o ambiente atual e aciona (coloca em produção) o ambiente espelhado.

EVIDÊNCIAS APRESENTADAS

Documento: Diagrama de espelhamento ou replica de ambiente.pdf



RISCO

CLASSIFICAÇÃO RISCO	Médio

Uma eventual falha é questão primordial para evitar paradas indesejáveis com graves consequências de perdas financeiras, processamentos ou de imagem.

Deixando de possuir informações para manter a continuidade dos negócios com controles, processos e apoio aos órgãos que prestam serviços e precisam estar no ar ininterruptamente.

A disponibilidade das informações é fundamental para todas as áreas administrativas, financeira, produção e as que dependem interruptamente de sistemas para a atuação de seus trabalhos.

Interrupção significante a todo trabalhos e armazenamento de informações do ABDI gerando grande impacto a continuidade dos negócios e prejuízos financeiros.

Embora o impacto seja alto, a probabilidade de acontecimento é muito baixa, pois possuem outros servidores externos nas próprias unidades da empresa que armazenam dados e informações de certos processos.

RECOMENDAÇÕES

Recomendamos elaborar um plano de contingência visando reduzir custos e atendendo apenas o suficiente para manter os serviços vitais da empresa. A partir de uma análise é possível mensurar o que é realmente importante para a empresa, comparando os custos para se criar a contingência de um determinado item e o eventual prejuízo gerado pela falta da contingência.

Garantir o sucesso da empresa para ter alta disponibilidade em seus serviços considerando suas características e limitações.

O principal é ter a visão de que diante de uma situação de desastre, o risco de indisponibilidade será mitigado ou evitado, preservando as suas operações.

COMENTÁRIOS ABDI

Foram apresentados documentos e evidências que demonstram a preocupação quanto a alta disponibilidade e contingenciamento dentro do contexto técnico/financeiro da ABDI.

A análise desta auditoria ao mencionar que não há um ambiente totalmente replicado apresentou uma visão voltada a *Disaster Recovery*, na qual se aborda a réplica de ambiente de forma que todos os dados e serviços sejam replicados em ambiente (espaço físico) apartado do atual, ou seja, mantendo sites primário e secundário síncronos ou assíncronos visando a continuidade dos negócios.

Vale destacar que o custo de se manter um ambiente de réplica total dos dados e serviços de forma online é extremamente oneroso e quando o colocado no contexto da ABDI, esta opção pode não ser a mais viável, com isso a UTEC já está em fase de projeto com migração gradual dos serviços críticos para ambientes de cloud pública o que mitigará esta questão. Esse projeto se iniciará em 2023 com planejamento de execução em três ondas consecutivas.

Vale também lembrar que possuímos vários níveis possíveis de desastres e que estes vão, por exemplo, desde o corrompimento de um arquivo de sistema operacional até o colapso da estrutura de um prédio.

Hoje, o ambiente computacional da ABDI possui vários mecanismos que mitigam os riscos de desastres com maior probabilidade de ocorrer, exemplificando: o já citado corrompimento de um arquivo, a falha de um equipamento, a falha de um sistema operacional, a falha de um link de comunicação, dentre inúmeros outros. Os mecanismos que mitigam estes riscos foram apresentados nos documentos encaminhados à auditoria, que demonstram a preocupação e a visão de manter um ambiente contingenciado de alta disponibilidade.

Exemplificando, todos os dados da ABDI são armazenados em sistemas de storage redundantes que possuem múltiplos discos em Sistemas RAID de TRPLA Paridade com discos de hot-spare.

Traduzindo, para que o dado que está armazenado em uma unidade RAID do storage venha a ser perdido por falha de discos, será necessário a falha de 3 discos de forma simultânea, situação que tem probabilidade muito pequena de acontecer, mas mesmo que venha acontecer, existe a cópia de segurança dos dados em um segundo sistema de storage.

Esta filosofia de proteção é estendida para todas as esferas do ambiente computacional da ABDI, conforme apresentamos na imagem de referência de Arquitetura Computacional da ABDI.
Em que pese, entendermos que o plano formal de contingência ser parte integrante da 2ª etapa de auditoria, por se tratar de norma e decisões a serem tomadas para minimizar impactos negativos gerados por cenários que atinjam a agência, e por fazer parte de um *framework* de governança de TI, entendemos a importância de um plano de contingência homologado conforme a realidade da agência, seguindo critérios de prioridades, fragilidades, custos, etc., e será colocado como atividade a ser realizada com a devida prioridade.

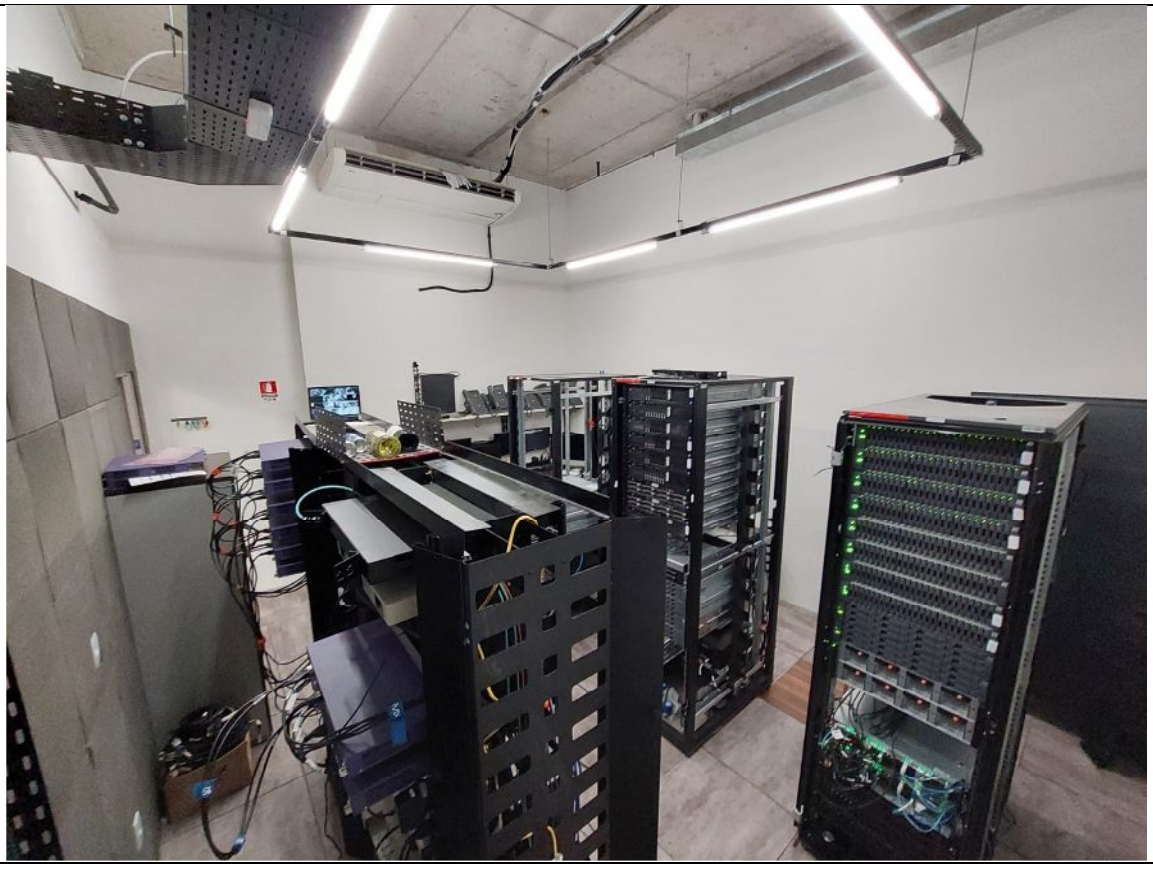
4.1.2 AMBIENTE FÍSICO CPD / DATA CENTER

SITUAÇÃO IDENTIFICADA

Identificamos após analises visuais de evidências fotográficas que a estrutura (edificação) do ambiente do CPD / Data Center não é totalmente de alvenaria, sendo uma construção mista: Alvenaria e Drywall Rosa.

O Drywall Rose é composto por fibra de vidro e gesso e resiste por pouco tempo a chamas causadas por incêndio e desta forma não é muito eficaz para a segurança do CPD, sendo que a estrutura de alvenaria possui muito mais resistência e proteção aos equipamentos e servidores.

EVIDÊNCIAS FOTOGRÁFICAS



RISCO

CLASSIFICAÇÃO RISCO	Alto

A estrutura da sala do Data Center apresenta alto riscos dos servidores serem danificados e até mesmo destruídos caso ocorra algum incêndio, podendo ser externo ou interno trazendo grandes prejuízos para a empresa de forma financeira, perda do ambiente do Data Center, também de perda de informações e paralisando a produção das fábricas.

RECOMENDAÇÕES

As paredes podem ser de alvenaria ou concreto, precisam ser altamente resistentes a impactos físicos e desastres naturais. Além disso, os componentes da alvenaria não podem ser inflamáveis. A infraestrutura física do Data Center de alvenaria deve suportar pelo menos uma hora de fogo a 1260°C.

Sugerimos que a sala do Data Center tenha reforma substituindo as paredes de Drywall por alvenaria, ou até mesmo mudança do local físico para sala estruturada, ou então que o Data Center seja totalmente virtualizado e hospedado em nuvem proporcionando toda segurança possível com as informações da empresa.

COMENTÁRIOS ABDI

A estrutura das salas que compõem o ambiente de DATACENTER da ABDI fora construída durante a reforma efetuada, em 2017, para a ocupação da agência. À época, a UTEC orientou que todo o ambiente fosse construído se utilizando de:

- Paredes feitas de Cimento Celular;
- Portas corta fogo;
- Controle de acesso integrado com sistema de incêndio;
- Não utilização de acabamentos que pudessem gerar focos de incêndio (ex: forro);
- Retirada de toda e qualquer tubulação de hidráulica;
- Instalação de sistema de combate a incêndio adequado a ambientes com equipamentos eletrônicos; e;
- Sistema de exaustão de gases nocivos (no caso da sala do nobreak).

Porem, de todas as recomendações, estas foram atendidas:

- Paredes foram feitas em Drywall Rosa;
- Portas corta fogo;
- Controle de acesso sem a integração com sistema de incêndio;
- Não utilização de acabamentos que pudessem gerar focos de incêndio (ex: forro)
- Retirada de toda e qualquer tubulação de hidráulica.

E recentemente com a instalação do sistema de troca de ar fora instalado o exaustor de gases nocivos junto aos bancos de baterias da sala de nobreak.

Ressaltamos está em fase de projeto a migração gradual dos serviços críticos para ambientes de cloud pública o que mitigará esta questão, conforme recomendação. Esse projeto se iniciará em 2023 com planejamento de execução em três ondas consecutivas.

Entendemos que as recomendações citadas elevam a segurança do local e, que as adequações sugeridas das salas, deverão ser analisadas e discutidas pelas unidades envolvidas, a exemplo, setor de serviços de infraestrutura predial, unidade de tecnologia e alta direção.

4.1.3 EQUIPAMENTOS DE COMBATE A INCÊNDIO NO CPD / DATA CENTER

SITUAÇÃO IDENTIFICADA

Identificamos após analises visuais de evidências fotográficas que a sala do CPD / Data Center não possui equipamentos / sistemas de combate à incêndio adequados ocorra algum incidente no local.

Existe apenas um extintor de combate a incêndio posicionado ao solo, próximo à porta- corta fogo.

EVIDÊNCIAS FOTOGRÁFICAS


n00b
PORTA CORTA - FOGO
mantenha fechada

RISCO

CLASSIFICAÇÃO RISCO	Alto

Para as empresas, proteger seus servidores contra incêndio é uma segurança obrigatória, pois hoje, com todos os dados e operações da empresa passando pelos servidores e neles armazenados, um incêndio resultará em uma paralisação total das atividades da empresa. Por essa razão, existem normas internacionais para os sistemas de incêndio para Data Center.

O sistema fixo para CPD é um sistema de combate e prevenção contra incêndios.

Ele pode ser composto por procedimentos de brigadas de incêndio, de gases inibidores e extintores e sistemas de detecção de fumaça.

RECOMENDAÇÕES

Sugerimos que a área de Tecnologia (TI) acione a área da brigada de incêndio e a segurança do trabalho para avaliarem a situação e tomar medidas corretivas para aprimorar os equipamentos de segurança a combate a incêndio e desastre naturais e operacionais na sala do CPD / Data Center.

O sistema incêndio para CPD é um sistema de combate e prevenção contra incêndios. Pode ser monitorada por procedimentos de brigadas de incêndio, através de gases inibidores e extintores e sistemas de detecção de fumaça.

Os equipamentos mais utilizados e mais adequados para serem implantados em ambientes de processamento de dados são os de gases limpos, que não conduzem eletricidade, não causam danos ao ser humano, não agridem o meio ambiente e não são nocivos aos dispositivos elétricos e eletrônicos. Estes gases são: NOVEC, FM200, Fe227 e alguns outros menos populares.

COMENTÁRIOS ABDI

A estrutura das salas que compõem o ambiente de DATACENTER da ABDI fora construída durante a reforma efetuada, em 2017, para a ocupação da agência. À época, a UTEC orientou que todo o ambiente fosse construído se utilizando de:

- Paredes feitas de Cimento Celular;
- Portas corta fogo;
- Controle de acesso integrado com sistema de incêndio;
- Não utilização de acabamentos que pudessem gerar focos de incêndio (ex: forro);
- Retirada de toda e qualquer tubulação de hidráulica;
- Instalação de sistema de combate a incêndio adequado a ambientes com equipamentos eletrônicos; e;
- Sistema de exaustão de gases nocivos (no caso da sala do nobreak).

Porem, de todas as recomendações, estas foram atendidas:

- Paredes foram feitas em Drywall Rosa;
- Portas corta fogo;
- Controle de acesso sem a integração com sistema de incêndio;
- Não utilização de acabamentos que pudessem gerar focos de incêndio (ex: forro)

- Retirada de toda e qualquer tubulação de hidráulica.

E recentemente com a instalação do sistema de troca de ar fora instalado o exaustor de gases nocivos junto aos bancos de baterias da sala de nobreak.

Entendemos que as recomendações citadas elevam a segurança do local e, que as adequações sugeridas das salas, deverão ser analisadas e discutidas pelas unidades envolvidas, a exemplo, setor de serviços de infraestrutura predial, unidade de tecnologia e alta direção.

4.2 GERENCIAMENTO DE DADOS

4.2.1 SIGILO – LOG BANCO MYSQL - SENHA

SITUAÇÃO IDENTIFICADA

Verificando os registros gerados por "*Log*" do banco de dados MySql, identificamos uma situação que nos parece que a informação da senha não está sendo criptografada nos registros, estando transparente para leitura, mesmo que seja uma senha temporária.

Como não temos acesso ao banco de dados e estamos realizando as analises através de evidências documental, **não podemos afirmar que a situação acontece**, pois não temos como executar testes, porém, **estamos registrando o fato para que a equipe de TI possa avaliar e analisar**.

EVIDÊNCIAS APRESENTADAS

Documento: mysqld.log

A temporary password is generated for root@localhost: bap1hqkFne

RISCO

CLASSIFICAÇÃO RISCO	Muito alto

Caso a situação identificada seja verdadeira, estamos temos que considerar como risco muito alto para devidas providências, mas só teremos esta certeza após análise da equipe técnica do ABDI.

RECOMENDAÇÕES

Sabemos que a ABDI possui um sistema para gerenciamento de senha (cofre) segura, mas registramos a situação para possíveis analises.

Todas as senhas de acesso a todas as aplicações, sistemas, servidores, entre outros, devem estar totalmente seguras para evitar qualquer tipo de acesso não autorizados.

COMENTÁRIOS ABDI

Vale destacar que, nas evidências, fora enviado log completo desde a instalação do banco de dados. Ao analisar, esta UTEC constatou que o log em questão é de 2021, quando estávamos instalando e validando a instalação. Entretanto, este achado já foi corrigido e atualmente esta situação não mais acontece.

2021-02-02T12:11:45.057184Z 6 [Note] [MY-010454] [Server] A temporary password is generated for root@localhost: bap1hqkFne-?

5 DOCUMENTOS E EVIDÊNCIAS APRESENTADAS

Antivírus - logs - Nível de Endpoint – Relatório
Contratos de fornecedores de TI
Controle de Acesso (Privilegiado)
Controle de Aquisição de Equipamentos
Controle de Backups
Controle de Licença de Softwares
Controle de Ocorrências de TI
Dashboards de sistemas
Diagrama e topologia de rede
Documentação de projetos e tecnicos referente a manutenção ou desenvolvimentos de sistemas
Documentação operacional (manual de orientação) completa de um sistema em produção principal

Evidências Conduta
Evidências de Admitidos-Demitidos-Afastados-Terceiros – DP
Evidências de Gestão de Fornecedores
Evidencias de registro de bloqueios de acessos
Fotos do Data Center (CPD) de todos os ângulos
Fotos dos servidores e equipamentos dentro do Data Center (CPD)
Inventario
Listas Ativos e Inativos
Logs de trafego de rede
Perfil de acesso usuários - apresentar todos tipos de perfis
Processo de Controle de Contratos
Relação de todos os sistemas em produção
Relatório de bloqueio de acesso a internet
Relatório de Pentest
Controle - relação dos documentos dos principais sistemas de operação
Diagrama de espelhamento ou replica de ambiente
Documento referente a gestão de projetos de desenvolvimento e manutenção de sistemas internos
Documento técnico e funcional do principal sistema ERP
Logs registros de atualização dos servidores proxy_
Logs de acesso ao banco de dados
Logs do firewall
PLANO DE CONTINUIDADE DE NEGÓCIOS
Manual de conduta
Politica de gestão de serviços
Politica de acordo de confidencialidade
ABDI - Book Mensal Backup Junho.pptx
_01_01_ABDI_REL_PROCESSOS-AJUSTES-COMMVAULT.pdf
Política de Segurança da Informação - PSI.pdf
Politica de gerenciamento de riscos
Política de Privacidade e tratamento de dados pessoais e cookies.pdf

6 CONSIDERAÇÕES FINAIS

O presente trabalho teve por foco a avaliação das atividades compreendidas nos processos correspondentes à área de Tecnologia da Informação.

Como resultado da avaliação procedida conclui-se que, em linhas gerais, conforme está manifestado nos comentários contidos nos itens do presente relatório, sob o aspecto formal as atividades do Processo de Tecnologia da Informação, dentre as prováveis causas que contribuem para aprimorar processos mencionadas.

Em resumo geral os processos referentes à tecnologia da informação estão bem estruturados e definidos, mas cabe a melhoria constante aos itens mencionados e aprimoramento dos planos e políticas de controle, trazendo clareza aos processos internos e definições ao direcionamento das execuções.

ROBERTO CALDAS BIANCHESSI:38051745000

Assinado de forma digital por ROBERTO CALDAS BIANCHESSI:38051745000
Dados: 2022.12.07 14:56:00 -03'00'

30 de novembro de 2022.

Audilink & Cia Auditores

Roberto Bianchessi