RELATÓRIO PRELIMINAR DE AUDITORIA EXTRAPLANO

1. ORDEM DE SERVIÇO

OS nº 2019.06464.

2. IDENTIFICAÇÃO

2.1. Objeto

Data Center - SF.

2.2. Objetivo

Avaliar a eficácia e a efetividade dos controles de segurança física e lógica da estrutura de *Data Center* da Secretaria Municipal da Fazenda (SF).

2.3. Metodologia

As principais técnicas utilizadas nos trabalhos de auditoria foram: entrevistas, questionários, análise documental e inspeção física.

2.4. Critérios de Avaliação

- Norma ABNT NBR 15.247:2004 – Unidades de armazenagem segura – Salas-cofre e cofres para *hardware* - Classificação e método de ensaio de resistência ao fogo;
- Norma ABNT ISO/IEC 27.001:2013 – Sistema de Gestão de Segurança da Informação;

- Norma ABNT ISO/IEC 27.002:2013 – Boas práticas para Gestão de Segurança da Informação;

- Norma ABNT NBR IEC 60.529:2017 – Graus de proteção para invólucros de equipamentos elétricos (Código IP).

2.5. Área auditada

Secretaria da Fazenda (SF).

2.6. Período da realização

21.10.19 a 21.03.20.

2.7. Período de abrangência

Não aplicável.

2.8. Siglas

ABNT	Associação Brasileira de Normas Técnicas
CFTV	Circuito Fechado de Televisão
Cotec	Coordenação de Tecnologia da Informação e Comunicação
ECB	*European Certification Body*
GSI	Gestão de Segurança da Informação
IEC	*International Electrotechnical Commission*
IN	Instrução Normativa
ISO	*International Organization for Standardization*
NBR	Norma Brasileira
PMSP	Prefeitura do Município de São Paulo
PSI	Política de Segurança da Informação
SF	Secretaria da Fazenda
Smit	Secretaria Municipal de Inovação e Tecnologia
TI	Tecnologia da Informação
UPS	*Uninterruptible Power Supply*

2.9. Equipe técnica

Carlos Albuquerque Lemos	RF nº 20.289
Helio Ricardo Guimarães Murci de Azevedo	RF nº 20.302
Maurício Kazuhiro Sato	RF nº 20.117

2.10. Procedimentos

- Avaliar a aderência da relação de ativos e utilidades aos requisitos de segurança para *Data Centers*;
- Avaliar a validade e autenticidade das certificações de segurança obtidas;
- Avaliar a existência de *Data Centers* de Contingência (Sítio *Backup*);
- Avaliar adequação da política de controle de acesso físico implementada.

3. RESULTADO

3.1. Introdução

A presente auditoria tem por finalidade inspecionar e avaliar a efetividade dos controles da Política de Segurança da Informação (PSI) implementados no intuito de proteger a infraestrutura física e lógica do *Data Center* da Secretaria Municipal da Fazenda (SF).

O objetivo do trabalho é destacar as possíveis fragilidades encontradas na infraestrutura do *Data Center* SF em comparação às boas práticas do mercado, às normas ABNT ISO/IEC, ANSI/TIA, ECB-S, assim como, às Orientações Técnicas elaboradas pela Secretaria Municipal de Inovação e Tecnologia (Smit).

3.2. Conceito de *Data Centers*

Com o avanço tecnológico e com o grande fluxo de dados e crescimento vertiginoso das solicitações de serviços digitais, as entidades estão investindo cada vez mais na área de Tecnologia da Informação (TI). Em busca de garantir a proteção dos dados e maior disponibilidade de recursos, houve a necessidade de criação de áreas para concentração de equipamentos de TI. Como exemplo, temos os *Data Centers*, que passaram a ser ativos de fundamental importância para as operações das organizações.

Denomina-se como *Data Center* um ambiente tecnológico protegido, sala ou edifício, projetado para concentrar os equipamentos dedicados ao processamento e armazenamento de dados, incluindo os equipamentos de infraestrutura e suporte a redes, ativos de telecomunicações e outros.

A infraestrutura do *Data Center* tem por objetivo hospedar os equipamentos de processamento e armazenamento de dados, no intuito de preservar os requisitos de segurança necessários para garantir a eficiência e a disponibilidade dos equipamentos e sistemas suportados pela infraestrutura.

3.3. *Data Center* SF

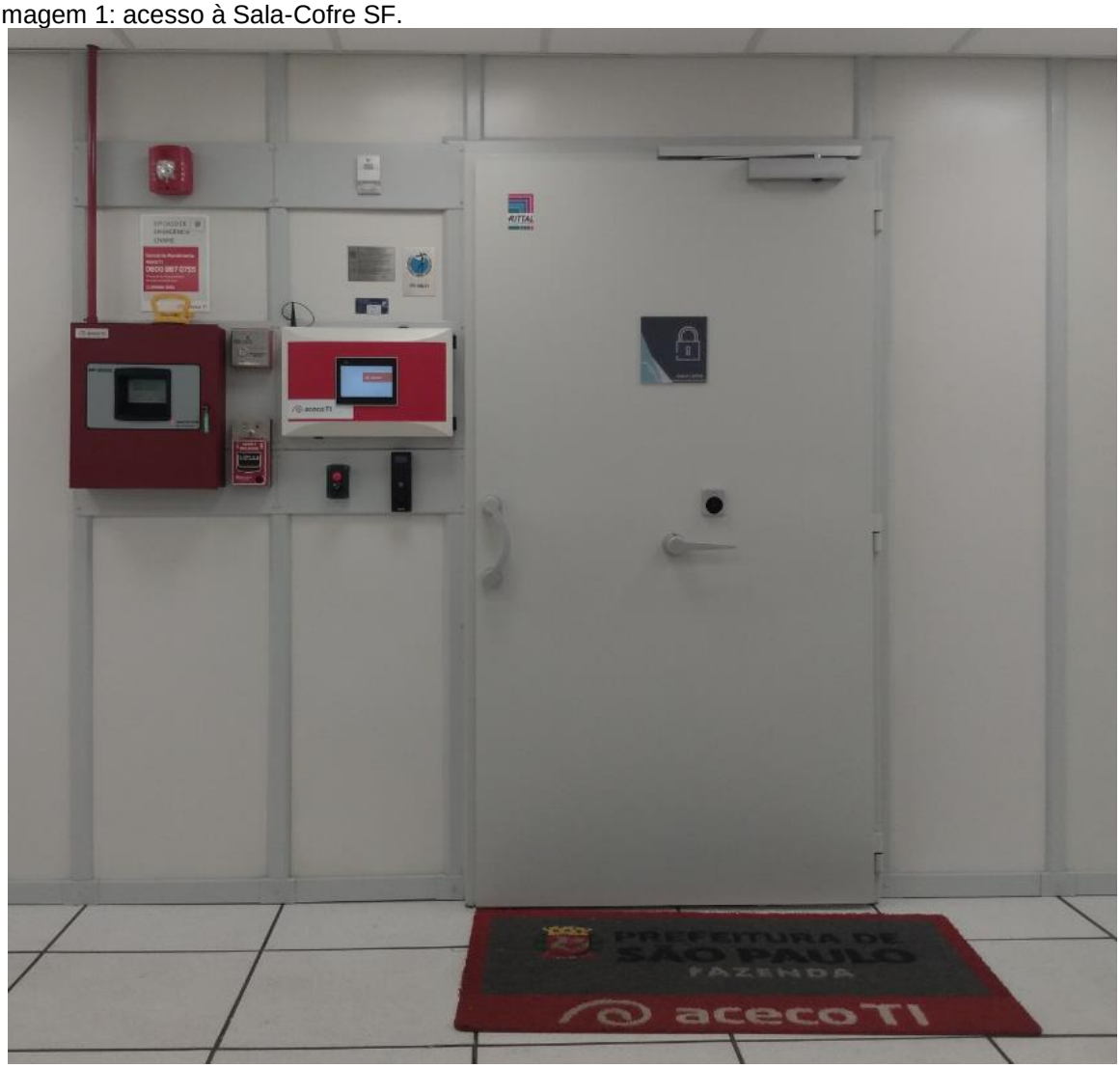
A SF possui uma unidade de armazenagem segura (sala cofre) abrigado em um Data Center, localizado nas dependências da sede da SF.

Uma sala cofre é um sistema modular composto por painéis para proteção física de equipamentos de hardware, formando uma “sala” dentro de sala e independente da estrutura existente de qualquer edifício.

A sala cofre contempla sistemas de infraestrutura de elétrica, climatização e dados, compondo uma solução integrada, e tem como função garantir a disponibilidade de funcionamento de um Data Center.

A imagem 1 demonstra o acesso à Sala-Cofre do *Data Center* SF

Imagem 1: acesso à Sala-Cofre SF.



Fonte: própria.

Resultado do termo contratual nº 57/2015 (peça 5, fls. 1/37) e seus respectivos termos aditivos (peça 6, fls. 1/2; peça 7, fls. 1/2; peça 8, fls. 1/2; e peça 9, fls. 1/6), o *Data Center* SF foi construído e certificado pela empresa Aceco TI S.A. no ano de 2017 e abriga os servidores de processamento e armazenamento de dados, equipamentos de telecomunicações e todos os sistemas e ativos de proteção nele instalados.

A Sala Cofre Blindada foi certificada por organismo certificador independente acreditado pelo INMETRO, conforme normas ABNT NBR 15.247[1], ABNT NBR IEC 60.529[2] e ECB-S EN 1047-2[3], provendo suporte aos principais processos de negócios utilizados pela SF e seus departamentos.

O projeto do *Data Center* SF é composto pelos seguintes ambientes:

- **Sala-Cofre -** certificada pela ABNT NBR 15.247, ABNT NBR IEC 60.529 e ECB-S EN 1047-2, com aproximadamente 31 m², destinado a hospedar servidores, sistemas de armazenamentos de dados e equipamentos de redes de dados da SF;

- **Sala UPS - *Uninterruptible Power Supply*** área com aproximadamente 16 m² utilizada para armazenar módulos de UPS/*No-breaks*, módulos de baterias e quadros de energia;

- **Sala de Telecom -** área com aproximadamente 11 m² para armazenamento de equipamentos de redes de telecomunicações da SF;

- **Sala de Desembalagem -** área com aproximadamente 8 m² para armazenamento temporário e desembalagem de equipamentos que estão instalados na Sala-Cofre, na Sala Telecom ou na Sala UPS;

- **Sala de Laboratório -** área de aproximadamente 8 m² para trabalhos técnicos de instalação e testes de equipamentos antes da instalação definitiva na Sala-Cofre, na Sala Telecom ou na Sala UPS;

---

[1] ABNT NBR 15247:2004 - Objetivo: Esta Norma especifica os requisitos para salas-cofre e cofres para hardware resistentes a incêndios. Ela inclui um método de ensaio para a determinação da capacidade de salas-cofre e cofres para hardware para proteger conteúdos sensíveis a temperatura e umidade, e os respectivos sistemas de hardware, contra os efeitos de um incêndio. Esta Norma também especifica um método de ensaio para medir a resistência mecânica a impactos (ensaio de impacto) para salas-cofre do tipo B e cofres para hardware.

[2] ABNT NBR IEC 60529:2017 - Objetivo: Esta norma é aplicada para a classificação dos graus de proteção providos aos invólucros dos equipamentos elétricos com tensão nominal não superior a 72,5 kV.

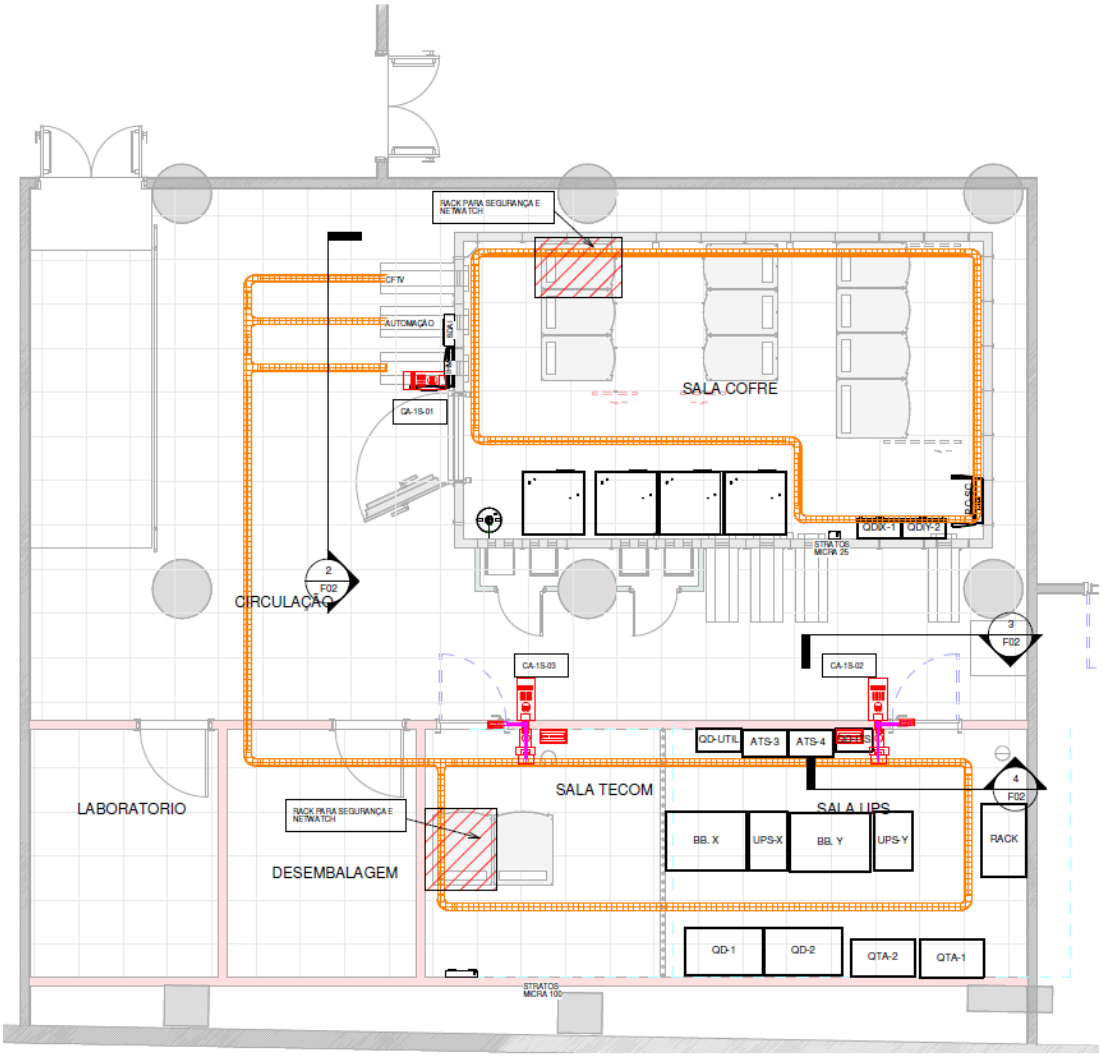
3 ECB-S EN 1047-2 - Objetivo: A norma *European Certification Body* - ECB-S European Norm - EN 1047-2 especifica requisitos para salas de dados e recipientes de dados, o que inclui um método de teste para a determinação da capacidade de *Data Centers* e de Contêiner de Dados em protegerem dados sensíveis à temperatura, à umidade e aos efeitos do fogo.

- **Sala de Condensadoras -** área externa com aproximadamente 21,58 m² onde estão instaladas as condensadoras que se integram aos sistemas de ar condicionado/evaporadoras da Sala-Cofre;

- **Sala de Geradores -** área entre 25 m² e 35 m² para instalação dos grupos geradores que estão utilizados para fornecimento de energia para o *Data Center* em caso de indisponibilidade da rede pública de energia.

A SF disponibilizou uma série de croquis das áreas seguras que compõem o *Data Center* (peça 14, fls. 1/11). A figura 1 ilustra o croqui simplificado da área:

Figura 1: croqui do *Data Center* – SF



Fonte: Cotec-SF.

As imagens 2 a 5 ilustram alguns exemplos dos ativos contidos no *Data Center* SF:

Imagens 2 a 5: Equipamentos de *Rack*, Armazenamentos de *Backup*, Servidores de Aplicação e Banco de Dados

Fonte: própria.

Considerando os documentos apresentados e as inspeções realizadas durante os trabalhos de auditoria, conclui-se que a infraestrutura física do *Data Center* SF, assim como seus ambientes seguros e segregados estão alinhadas às

orientações das normas de segurança ABNT NBR 15.247:2004, ABNT NBR IEC 60.529:2017 e ECB-S EN 1047-2.

3.3.1. Redundâncias e soluções de contingência

A norma ISO/IEC 27.002:2013 orienta que, onde aplicável, os principais recursos de processamento da informação sejam implementados com redundância suficiente para atender aos requisitos de disponibilidade, integridade e continuidade.

Adicionalmente, a norma orienta que os sistemas de informação redundantes sejam testados no intuito de assegurar que a transferência de um componente para outro componente funcione conforme esperado, quando da ocorrência de uma falha no componente principal.

Durante os trabalhos de auditoria, foi constatada a inexistência de uma solução para redundância e contingência para dados, sistemas e demais serviços providos pelo *Data Center* SF.

Esta constatação demonstra uma vulnerabilidade para a continuidade dos serviços providos pela infraestrutura de *Data Center*, pois caso eventos de indisponibilidade ocorram, poderá haver a perda da disponibilidade dos dados pela interrupção dos sistemas e serviços instalados no *Data Center* SF, assim como, poderão haver perdas totais ou parciais da integridade dos dados hospedados no centro de dados.

No intuito de atender à necessidade de redundância e contingência para as operações e serviços disponíveis em um *Data Center*, podemos citar os seguintes exemplos:

- a utilização de infraestrutura de *Data Center* espelho, isto é, instalada em localidade diversa e com a mesma capacidade de processamento do ambiente principal, que assumiria o provimento dos sistemas, serviços e

dados nas eventuais indisponibilidades ocorridas no *Data Center* principal;

- a utilização de serviços de computação em nuvem, sejam eles, providas por nuvens públicas ou privadas, ou até mesmo, providas por uma solução de nuvem híbrida.

Ressalta-se que a adoção de uma solução para contingência é um ponto fundamental para se alcançar alinhamento às boas práticas de Governança Corporativa e de Governança de TI.

A situação encontrada constitui uma fragilidade na salvaguarda da segurança das informações, sistemas e da continuidade dos serviços providos por meio do ambiente computacional, indo de encontro às orientações da norma ISO/IEC 27.002:2013.

3.4. Normas Técnicas e Certificações de *Data Centers*

3.4.1. Norma ABNT NBR 15.247:2004

A norma ABNT NBR 15.247:2004 (peça 17, fls. 1/26) especifica os requisitos para salas-cofre e cofres para *hardware* resistentes a incêndios. Ela inclui um método de ensaio para proteger os equipamentos de processamento e armazenamento de dados contra os efeitos de um incêndio, conteúdos sensíveis à temperatura e à umidade, bem como os respectivos sistemas. A norma também especifica um método de ensaio para medir a resistência mecânica à impactos de salas-cofres e cofres para *hardware*.

O *Data Center* SF foi certificado conforme a ABNT NBR 15.247:2004, sendo classificado como S 60 D, Tipo B (peça 19, fl. 1), isto é, o Data Center da SF possui certificação de resistência ao fogo por 60 minutos e adequação para equipamentos sensíveis ao calor e umidade, com limites de exposição de até 70° C e umidade relativa do ar abaixo de 85%.

3.4.2. Norma ABNT NBR IEC 60.529:2017

Essa norma é aplicada para a classificação dos graus de proteção providos aos invólucros dos equipamentos elétricos (quadros e centrais de energia) com tensão nominal não superior a 72,5 kV (*kiloVolt*).

O *Data Center* também foi certificado pela SF de acordo com a norma ABNT NBR IEC 60.529:2017 (peça 18, fls. 1/57), alcançando o grau de proteção IP67 (peça 19, fl. 1), ou seja, o ambiente possui proteção contra penetração de objetos sólidos estranhos, inclusive poeira, assim como contra imersão temporária em água (até 1 metro) por 30 minutos.

3.4.3. Norma ECB-S EN 1047-2

A norma *European Certification Body* - ECB-S *European Norm* - EN 1047-2 especifica requisitos para salas de dados e recipientes de dados, o que inclui um método de teste para a determinação da capacidade de *Data Centers* e de Contêiner de Dados em protegerem dados sensíveis à temperatura, à umidade e aos efeitos do fogo.

O *Data Center* SF foi certificado conforme a ECB-S EN 1047-2, sendo classificado como R 60 D (peça 19, fl. 2), isto é, o ambiente da SF possui certificação de resistência ao fogo por 60 minutos e adequação para equipamentos sensíveis ao calor e à umidade, com limites de exposição de até 70° C e 85% de umidade relativa do ar.

Por fim, considerando as certificações apresentadas pela equipe técnica da SF (itens 3.4.1, 3.4.2 e 3.4.3), evidencia-se que o Data Center SF atende às normas de segurança ABNT NBR 15.247:2004, ABNT NBR IEC 60.529:2017 e ECB-S EN 1047-2.

3.5. Política de Segurança da Informação (PSI)

A Gestão da Segurança da Informação (GSI) engloba processos voltados ao monitoramento da integridade das informações e à prevenção de ataques e ao furto de dados, assegurando o pronto restabelecimento dos sistemas e o acesso seguro às informações da organização, caso incidentes de segurança ocorram, sejam eles provocados por agentes externos, falhas em equipamentos ou pela ação de indivíduos autorizados ou mal-intencionados.

A família de normas ABNT NBR ISO/IEC 27.000 constitui-se de um rol de normas com foco especial em GSI. Dentre elas, destacam-se as normas ISO IEC 27.001:2013 e ISO IEC 27.002:2013 (peça 10, fls. 1/42 e peça 11, fls. 1/111, respectivamente), que apesar destas normas não terem um caráter cogente, são utilizadas como as principais referências para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um sistema de GSI com base em uma abordagem de riscos de negócio.

Segundo a norma ISO/IEC 27.002:2013, a PSI tem por objetivo prover apoio e orientação da Direção para a segurança da informação de acordo com os requisitos do negócio e leis e regulamentações relevantes.

A norma orienta que, no seu mais alto nível, uma organização defina uma PSI aprovada pela alta Direção, e que esta estabeleça a forma de abordagem adotada pela organização para gerenciar os objetivos e os riscos de segurança da informação.

Adicionalmente, no intuito de assegurar sua contínua pertinência, adequação e eficácia, o normativo ISO sugere que uma PSI vigente seja analisada criticamente a intervalos planejados ou quando mudanças significativas no escopo de segurança da informação ocorrer.

No intuito de atender às orientações da norma e estabelecer uma PSI, a SF sintetizou normas e diretrizes gerais sobre segurança da informação no

documento de Procedimentos Mínimos de Segurança da Informação (peça 4, fls. 1/10), adotado pelas unidades organizacionais da SF e também pelos terceiros que utilizem os recursos de Tecnologia da Informação e Comunicação (TIC) da SF.

Analisando a Política de Segurança da Informação e seus documentos auxiliares, foi constado que a versão atual do documento está estruturada de acordo com as orientações e temas de segurança abordados na norma ISO/IEC 27.002:2013 (peça 11, fls. 1/111).

Por outro lado, devido à inexistência de um controle de versões no documento apresentado, não foi possível confirmar se o conteúdo da PSI vigente passa por trabalhos de análises críticas e revisões periódicas. Cabe destacar que, de acordo com a norma ISO 27.002/2013, uma PSI deve analisada e revisada periodicamente, desta forma, a falta da comprovação desses trabalhos, demonstra um desalinhamento em relação às orientações da norma.

3.6. Sistemas de Segurança do *Data Center* SF

Os ambientes seguros que compreendem o *Data Center* SF são monitorados por um sistema de segurança que adotam um conjunto de soluções específicas e integradas em uma única rede exclusiva e dedicada para essa função.

O sistema de segurança implantado no *Data Center* SF é constituído pelos seguintes itens:

- **Sistema de controle de acesso -** composto por sistemas de leitura biométrica, botoeiras de saída, botoeiras de emergência, travas magnéticas, servidores de informações (compartilhado com sistema de CFTV) e demais interfaces;

- **Sistema de CFTV -** para monitoramento e gravação de imagens de áreas previamente definidas, incluindo câmeras, *switch*, *patch panel*, servidor de

informações (compartilhado com o sistema de Controle de Acesso) e demais interfaces;

- **Sistema de Combate a Incêndios -** para monitoramento, detecção, alarme e supressão de incêndio em *Data Centers*.

3.6.1. Política de Controle de Acesso Físico ao *Data Center* SF

O controle de acesso físico busca gerenciar o fluxo de pessoas que acessam um Ambiente de Segurança com o auxílio de dispositivos como fechaduras, catracas, chaves e outros. É um sistema fortemente indicado para edifícios residenciais e comerciais, bem como para áreas de segurança, tais como exemplo *Data Centers* e salas-cofre.

Segundo a norma ABNT ISO/IEC 27.002:2013 (peça 11, fls. 1/111), os procedimentos utilizados para controlar o acesso físico às dependências do *Data Center* devem ser institucionalizados através da elaboração de políticas de controle de acesso que sejam monitoradas e revisadas periodicamente pela equipe técnica da organização e aprovadas por sua alta direção.

Analisando o documento de Procedimentos Mínimos de Segurança da Informação (peça 4, fls. 1/10), documento similar à PSI, verifica-se que os procedimentos operacionais utilizados para Gestão da Política de Controle de Acesso Físico ao *Data Center* SF foram formalmente registrados em um documento elaborado e aprovado pela direção do órgão, estando este alinhado à PSI vigente para o órgão.

A existência de uma Política de Controle de Acesso Físico e de uma PSI, demonstra o alinhamento das práticas de segurança do órgão em relação às orientações da norma ABNT ISO/IEC 27.002:2013 (peça 11, fls. 50/52) e à Orientação Técnica 013 - Das Diretrizes Básicas de Segurança da Informação, emitida pela Smit (peça 12, fls. 1/21).

3.6.2. Acesso *Data Center* SF

Segundo a norma ABNT ISO/IEC 27.002:2013, o termo “Área Segura” remete à prevenção do acesso físico não autorizado e à prevenção contra danos e interferências aos recursos de armazenamento e processamento das informações.

A norma indica que é conveniente a criação de Perímetros de Segurança Física. Ademais, convém que eles sejam claramente definidos de acordo com os requisitos de segurança exigidos pelos ativos hospedados nesses perímetros.

Data Centers são ambientes considerados como perímetros de segurança, que além de seguir suas respectivas normas técnicas e certificações, devem ser equipados com controles de acesso apropriados aos riscos e aos requisitos de segurança identificados, de forma a garantir que somente o pessoal autorizado tenha acesso liberado.

A norma ABNT ISO/IEC 27.002:2013 (peça 11, fls. 50/52) orienta que o acesso às áreas em que são processadas ou armazenadas informações sensíveis da organização seja restrito apenas ao pessoal autorizado.

O *Data Center* SF possui um sistema de controle de acesso com regras baseadas na Política de Controle de Acesso e na Política de Segurança da Informação, ambas elaboradas pela equipe técnica da SF e aprovadas pela alta direção da secretaria. O Sistema de Controle de Acesso, assim como, seus respectivos componentes serão abordados nos itens subsequentes do relatório.

3.6.3. Sistema de Controle de Acesso *Data Center* SF

Durante as visitas realizadas na SF, constatou-se que a liberação de acesso aos ambientes seguros é baseada na identificação biométrica por meio de leitores instalados junto às portas de cada perímetro de segurança (Sala-Cofre, Sala Telecom e Sala UPS), controlando as respectivas trancas eletrônicas.

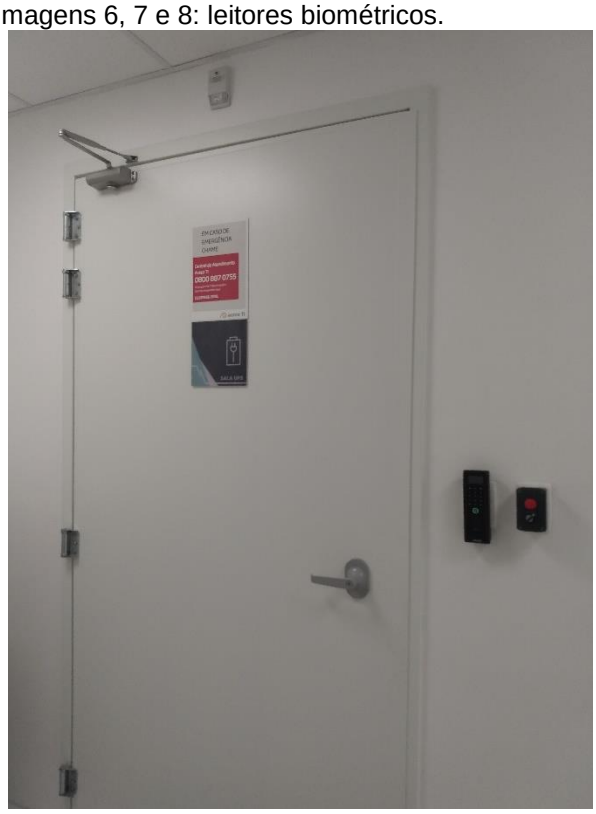
A identificação biométrica permite o monitoramento e controle do acesso aos ambientes seguros do *Data Center* SF de acordo com o nível de autorização pré-definido para cada indivíduo.

Entre os itens que constituem o sistema de controle de acesso implementado no *Data Center* SF, destacam-se os seguintes:

Leitores Biométricos: o *Data Center* da SF é munido de leitores biométricos de identificação que estão presentes ao lado das portas de acesso aos ambientes da Sala-Cofre, Sala UPS - *Uninterruptible Power Supply* e Sala de Monitoramento.

As imagens 6, 7 e 8 mostram os leitores biométricos utilizados nesses locais:

Imagens 6, 7 e 8: leitores biométricos.



Fonte: própria.

Os leitores biométricos controlam a abertura e fechamento das portas dos ambientes seguros, tendo ainda a função de receber e armazenar de forma

contínua as informações biométricas, enviando-as para na Estação Central de Segurança para registro e armazenamento dos acessos realizados em cada ambiente controlado.

Fechaduras Eletromagnéticas: as fechaduras eletromagnéticas controlam a abertura e o fechamento das portas monitoradas pela Central de Controle e Acesso. Esses equipamentos estão interligados aos respectivos leitores de identificação biométrica, de forma a possibilitar a sinalização à Central sobre o *status* da porta monitorada (aberta ou fechada).

Caso a porta em questão permaneça aberta além de um período pré-determinado, a Central será sinalizada e um alarme de porta aberta ou destravada será acionado.

Botões de saída: os botões de saída são equipamentos utilizados pelos usuários para requisitar a abertura da porta monitorada, permitindo a saída do indivíduo do ambiente controlado. Da mesma forma que as fechaduras eletromagnéticas, os botões de saída estão interligados aos respectivos leitores de identificação biométrica, possibilitando o envio da sinalização das requisições de saída efetuadas à Central.

Considerando os documentos apresentados, a solução de controle de acesso por meio biométrico adotada no Data Center SF está alinhada às especificações contidas no termo de referência do contrato nº 57/2015 e seus respectivos termos aditivos, assim como, possui alinhamento às orientações das normas ABNT ISO/IEC 27.002:2013, ABNT NBR 15.247:2004, ABNT NBR IEC 60.529:2017 e ECB-S EN 1047-2.

3.6.3.1. Registros Eletrônicos de Entradas e Saídas.

A norma ABNT ISO/IEC 27.002:2013 (peça 11, fls. 1/111) orienta que a data e hora da entrada e saída de usuários autorizados e de visitantes sejam devidamente registradas e que o sistema de controle de acesso utilizado permita

uma trilha de auditoria, de forma a possibilitar a formação, manutenção e a salvaguarda segura do histórico de acessos físicos realizados ao ambiente, para fins de verificação e auditoria.

Conforme informações fornecidas pela Cotec-SF, o *software* utilizado pela SF, responsável pelo gerenciamento das atividades de Controle de Acesso ao Data Center, está configurado para realizar o registro e a posterior salvaguarda dos eventos de acesso físico realizados ao *Data Center*.

Como evidência do efetivo gerenciamento do controle de acesso físico, a SF apresentou em planilha os registros dos eventos de biometria efetuada nos últimos 120 dias (peça 13, fls. 1/16), sendo demonstradas as entradas e saídas no ambiente seguro, possibilitando futura averiguação ou para fins de auditoria.

Por outro lado, ressalta-se que os acessos realizados por visitantes não são registrados, seja eletronicamente, seja fisicamente em livro de visitantes específico, o que demonstra um desalinhamento em relação às orientações da Norma. Dessa forma, o procedimento de controle de acesso adotado para o *Data Center* SF não está aderente a recomendação, item 11.1.2.c (peça 11, fl. 51), da norma ABNT ISO/IEC 27.002:2013.

3.6.4. Circuito Fechado de Televisão (CFTV)

Um Circuito Fechado de Televisão (CFTV) é uma solução de monitoramento que consiste na colocação de câmeras de monitoramento, analógicas ou digitais, em pontos estratégicos do ambiente a ser monitorado. As imagens capturadas são transmitidas para um ou mais pontos de visualização, contribuindo assim para a prevenção contra intrusões nesses locais.

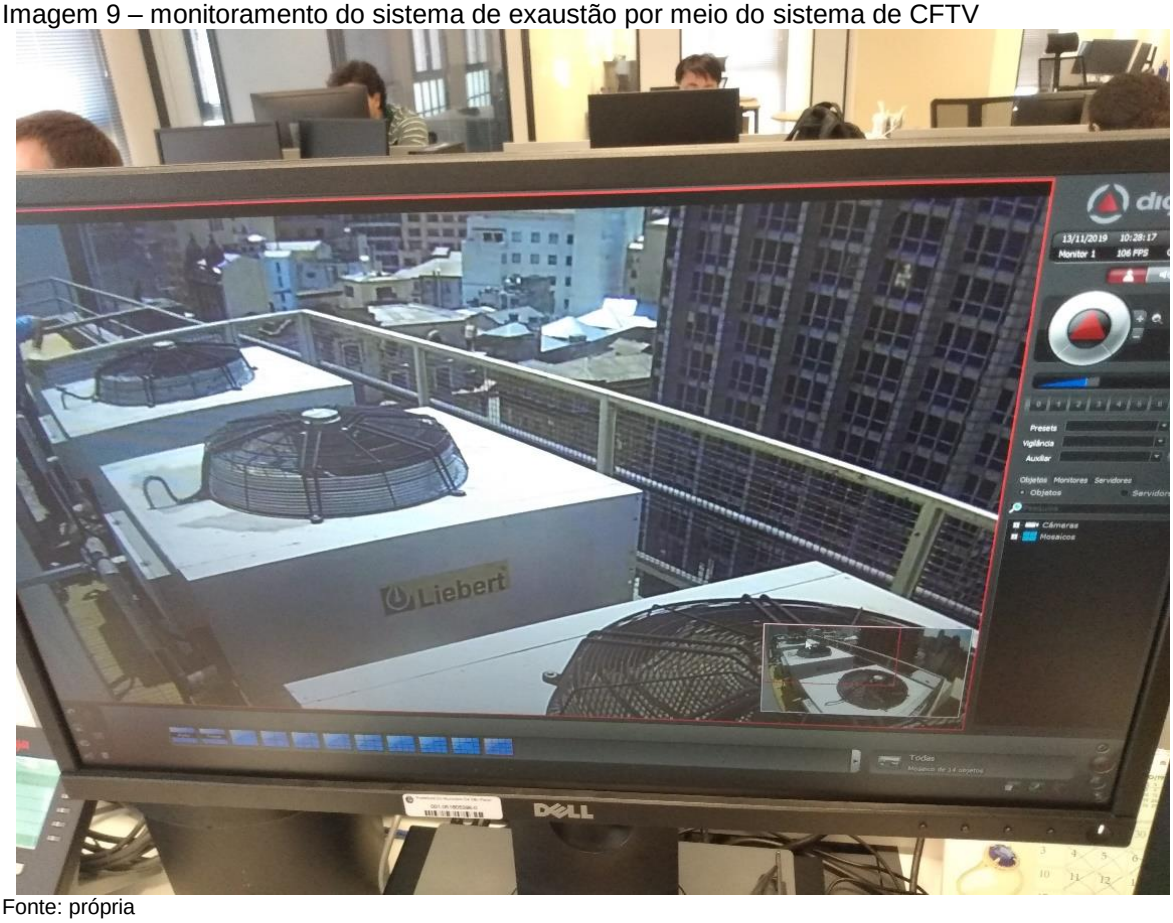
Durante a inspeção, foi constatado que os pontos de acesso aos ambientes seguros do *Data Center* SF, assim como seus interiores, são monitorados por câmeras interligadas a um sistema de CFTV.

A captura de imagens dos ambientes monitorados é iniciada automaticamente por meio de sensores de movimento, tornando o armazenamento das gravações em mídia digital mais efetivo. O armazenamento dos arquivos de gravação possibilita um rápido acesso e resgate das imagens para futura averiguação ou para fins de auditoria.

Como evidência do efetivo gerenciamento do sistema de CFTV, a SF apresentou em planilha os registros de armazenamento de imagens efetuados de março/2019 a setembro/2019 (peça 13, fls. 1/3).

As imagens 9 e 10 demonstram exemplos de imagens capturadas pelo Sistema de CFTV:

Imagem 9 – monitoramento do sistema de exaustão por meio do sistema de CFTV



Fonte: própria

Imagem 10 – monitoramento por meio de múltiplas câmeras administradas pelo sistema de CFTV

Fonte: própria

Por fim, considerando os documentos apresentados e as vistorias realizadas ao *Data Center* SF, a solução de CFTV adotada está alinhada às especificações contidas no termo de referência do contrato nº 57/2015 e seus respectivos termos aditivos, assim como, possui alinhamento às orientações das normas ABNT ISO/IEC 27.002:2013, ABNT NBR 15.247:2004, ABNT NBR IEC 60.529:2017 e ECB-S EN 1047-2.

3.6.5. Sistema de Prevenção, Detecção, Alarme e Combate a Incêndios

Um sistema de prevenção, detecção, alarme e combate a incêndios, por padrão, é composto por uma Central de Detecção que gerencia uma infraestrutura especialista de combate a incêndios que compreende equipamentos, tais como:

sensores, sistemas de monitoramento, agentes extintores, sistemas de tubulação e distribuição, assim como, outros equipamentos auxiliares correlatos.

A especificação técnica dos itens dessa infraestrutura deve estar alinhada às normas de combate a incêndios vigentes na localidade, de forma a garantir que a atuação do sistema em ambientes de *Data Centers* não cause danos aos equipamentos de processamento de dados, bem como à própria infraestrutura do local.

Ressalta-se que, por padrão, esse tipo de sistema funciona de forma automática, cujo acionamento é realizado por meio de sinalização de equipamentos de detecção de gases, fumaça ou calor.

3.6.6. Agentes extintores

Os agentes extintores são elementos que atuam sobre a combustão com o objetivo de debelar focos de incêndio evitando perdas materiais, humanas, assim como degradação ao meio ambiente. Dessa forma, a escolha e a aplicação de um agente extintor adequado são de suma importância para uma maior eficácia de sua ação. Assim, devem ser consideradas as normas de segurança vigentes, bem como deve ser levado em conta o tipo dos equipamentos envolvidos e as suas respectivas classes de incêndio.

A dispersão do agente extintor no ambiente seguro é realizada por meio de sistemas fixos de tubulações suspensas, que direcionam a emissão do elemento extintor até o local de risco. O principal propósito do sistema é a rápida detecção e supressão de focos de incêndios, evitando assim que atinjam grandes proporções e causem maiores danos.

Na prevenção e combate de incêndios em *Data Centers*, os principais agentes extintores utilizados são gases, dentre os quais:

- **Gás Químico FM-200 -** é um agente extintor limpo e inerte, mundialmente utilizado em sistemas de supressão de incêndios por inundação total. Esse tipo de gás não deixa resíduo, sendo uma das melhores soluções de combate a incêndios para as salas de equipamentos de TI. O agente extintor age em até 10 segundos após seu acionamento, impedindo os impactos devastadores causados por um incêndio.

- **Gás Inerte IG-55 -** é um agente extintor natural, sem cor e inodoro. Por ser um gás inerte não ataca a camada de ozônio e não faz aumentar o efeito estufa. Seu objetivo é reduzir o oxigênio do ambiente até que o incêndio se extinga;

- **Gás Dióxido de Carbono (CO2) -** é um agente extintor natural, que não conduz corrente elétrica e atua na inibição da combustão efetuando a troca de oxigênio. Sua ação não gera resíduo, sendo muito eficiente na proteção de equipamentos eletrônicos.

No caso do *Data Center* SF, devido às características técnicas e à forma de atuação, optou-se pela a utilização do gás químico FM200 como agente extintor de incêndios, tal opção consiste em uma escolha usual de mercado para uso em ambientes computacionais.

Imagens 11 e 12 ilustram a infraestrutura e o cilindro de gás FM-200 utilizados no sistema de combate a incêndios no Data Center SF:

Imagens 11 e 12 – cilindro de gás FM-200.

Fonte: própria.

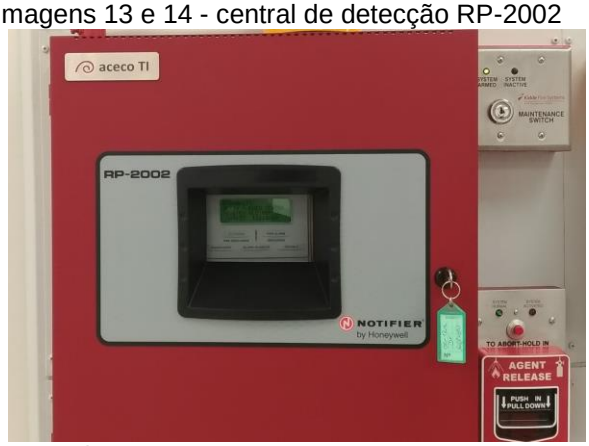
3.6.7. Sistema de Prevenção, Detecção, Alarme e Combate a Incêndios *Data Center* SF

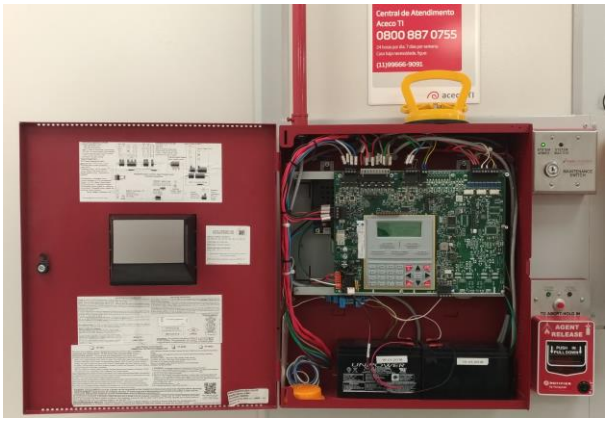
A Central de Detecção RP-2002 vinculada ao *Data Center* SF é equipada por dois laços de detecção, um desses laços vinculado exclusivamente à Sala-Cofre e o outro vinculado aos ambientes de Circulação, Sala Telecom, Sala UPS, Desembalagem e Laboratório. Esses laços de detecção controlam o acionamento do gás FM-200 nos seus respectivos ambientes.

Por último, após o acionamento do sistema, o agente extintor FM-200 é espalhado pelo ambiente seguro, não deixando resíduos que danifiquem os equipamentos eletrônicos mais sensíveis e não requerendo a limpeza dos equipamentos e do ambiente.

As imagens 13 e 14 ilustram a Central de Detecção RP-2002 instalada no *Data Center* SF:

Imagens 13 e 14 - central de detecção RP-2002





Fonte: própria

3.6.8. Equipamentos de Detecção de Incêndios

Os detectores de fumaça, calor e incêndio são os dispositivos encarregados de fazer a vigilância permanente de um local e constituem uma parte sensível da instalação de detecção automática de incêndio.

Esses dispositivos são usualmente constituídos por células fotoelétricas que emitem uma corrente variável segundo o fluxo luminoso que recebem. Dessa forma, caso o ambiente monitorado apresente sinais de fumaça, fato este que normalmente precede e acompanha um incêndio, esse evento fará o fluxo luminoso reduzir, fazendo com que o dispositivo envie uma sinalização à Central de Detecção que, após o devido tratamento, acionará o disparo do agente extintor no local afetado.

As imagens 15, 16, 17 e 18 ilustram os equipamentos sensores de detecção de incêndios:

Imagens 15, 16, 17 e 18 – sensores de detecção a incêndios.

Fonte: própria.

3.6.9. Acionadores Manuais e Chaves de Bloqueio

O funcionamento do sistema de dispersão do agente extintor FM-200 poderá ser acionado manualmente por meio da alavanca de dupla ação (são necessários dois movimentos para atuação do sistema), de forma a simular o funcionamento da dispersão do agente extintor.

Chave de bloqueio é um equipamento utilizado na ação de bloqueio do sistema de dispersão de agente de extintor. O bloqueio do sistema propicia o acionamento do sistema de combate a incêndio, com o intuito de simular o seu funcionamento, sem haver a liberação efetiva do gás FM-200.

As imagens 19, 20 e 21 ilustram os equipamentos de acionamento manual e chave de bloqueio do sistema de combate a incêndios:

Imagens 19, 20 e 21 – acionadores manuais e chave de bloqueio do sistema de combate a incêndios

Fonte: própria.

3.6.10. Extintores Manuais

Adicionalmente ao sistema automatizado de Detecção e Combate a Incêndios, o *Data Center* SF também possui extintores de incêndio do tipo manual, instalados em locais apropriados e devidamente identificados por placas sinalizadoras de piso.

Extintores manuais são cilindros abastecidos com agentes extintores a base de água, pó químico seco e gás carbônico, destinados a combater princípios de incêndio.

Constitui-se unidade extintora um aparelho contendo o mínimo de capacidade de substância ou agente especificado, certificados por selos de conformidade emitidos pelas entidades competentes do setor.

O quadro 1 demonstra os tipos de extintores manuais de combate a incêndio disponíveis no ambiente de *Data Center* SF:

Quadro 1: tipos de extintores manuais disponíveis no *Data Center* SF

Elemento extintor	**Capacidade em Kg** **Tipo de aplicação: (A – Sólidos; B - Líquidos e gases inflamáveis; C - Equipamentos elétricos)**
Gás Carbônico	5 kg – BC
Pó Químico	20 kg – BC
Água Pressurizada	10 kg – A

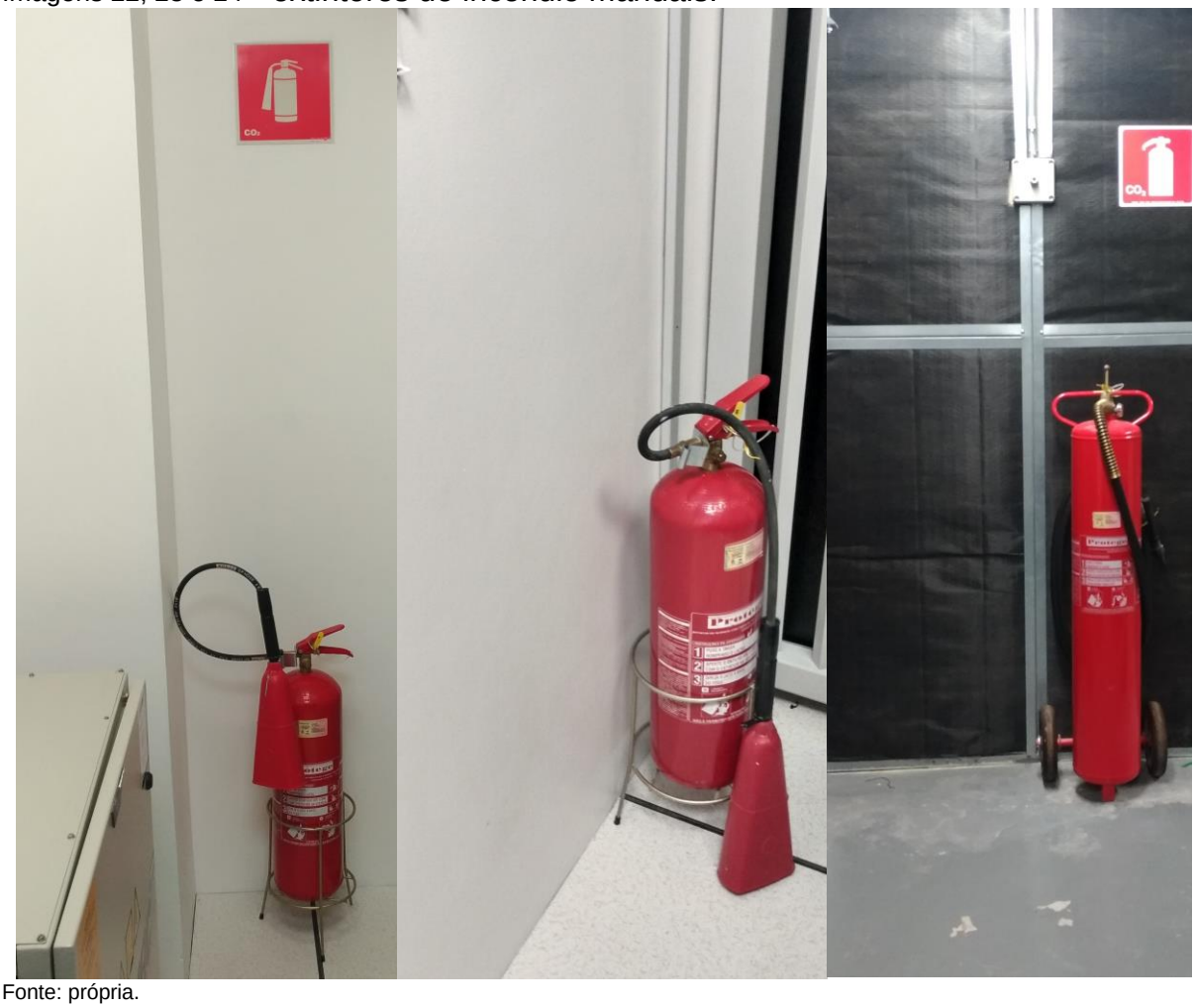
Pó Triclasse (ABC)	3 kg - A; 20 kg – BC

Fonte: própria.

Durante inspeção, foi constatada a existência de extintores manuais com carga de monóxido de carbono na Sala dos Geradores, na Sala TELECOM e na Sala UPS.

As imagens 22, 23 e 24 ilustram os equipamentos manuais de extinção de incêndio:

Imagens 22, 23 e 24 – extintores de incêndio manuais.



Fonte: própria.

Concluindo, considerando os documentos apresentados e as vistorias realizadas ao Data Center SF, o Sistema de Prevenção, Detecção, Alarme e Combate a

Incêndios e em seus respectivos equipamentos auxiliares adotado está alinhado às especificações contidas no termo de referência do contrato nº 57/2015 e seus respectivos termos aditivos, assim como, possui alinhamento em relação às orientações das normas ABNT NBR 15.247:2004, ABNT NBR IEC 60.529:2017 e ECB-S EN 1047-2.

3.7. Projeto Elétrico Data Center SF

Um *Data Center* possui um fluxo elevado e contínuo de informações, que são processadas 24 horas por dia e sete por semana. Dessa forma, existe a dependência de um fornecimento de energia elétrica constante e que obedeça a certos padrões de qualidade, a fim de manter seus serviços e operações sempre disponíveis.

O conceito de instalações elétricas em um *Data Center* consiste em componentes redundantes de alimentação a partir dos quadros de distribuição de energia elétrica (QD-1 e QD-2). O objetivo a ser atendido é garantir o recurso mínimo necessário para que as cargas críticas sofram o menor impacto possível numa eventual falha ou manutenção da instalação elétrica.

O projeto elétrico do *Data Center* SF foi implementado de forma que todos os equipamentos contidos no ambiente seguro recebam um fornecimento de energia elétrica oriundo de fontes de alimentação distintas e redundantes, a fim de que, caso uma das fontes de alimentação falhe, a fonte redundante assumirá o fornecimento de energia elétrica do *Data Center*.

O fornecimento de energia elétrica ao *Data Center* SF é constituída por três fontes distintas:

- Fontes externas e redundantes (Fontes X e Y), providas pela concessionária de energia elétrica;

- Fontes internas e redundantes, providas pelos sistemas de *No-breaks*, também conhecido como *Uninterruptible Power Supply* (UPS) (UPS-X e UPS-Y);

- Fontes internas e redundantes, providas pelos Geradores de Energia Elétrica à combustão instalados na edificação.

As características técnicas das fontes de fornecimento elétrico serão abordadas no decorrer do relatório.

3.7.1. Fornecimento de Energia via Concessionária Local

A fonte principal de energia do *Data Center* SF é constituída por dois circuitos redundantes e independentes a partir dos Quadros de Distribuição Geral (QD-1 e QD-2) com transferência automática de carga, ambas as fontes providas pela concessionária de energia elétrica local, perfazendo uma capacidade total de 260 *kiloVoltAmperes (*kVA) em 220*Volts (V*) trifásico.

As imagens 25 e 26 ilustram as instalações da infraestrutura principal de energia elétrica e seus respectivos cabeamentos.

Imagens 25 e 26: painel de controle de energia elétrica

Fonte: própria.

Segundo a SF, todos os componentes dos sistemas elétricos a partir dos Quadros de Distribuição Geral (QD-1 e QD-2) trabalham em um limite de

aproximadamente 50% de sua capacidade nominal, de forma que, caso haja alguma falha em um dos sistemas redundantes, há a transferência automática de 100% do consumo nominal do *Data Center* para o outro sistema.

3.7.2. *Uninterruptible Power Supply* (UPS)

O *Data Center* SF está equipado com dois UPS (*No-breaks*) de 80kVA cada, tensão de 220V trifásico, identificados respectivamente como UPS-X e UPS-Y. Cada um desses sistemas está equipado com banco de baterias integrado ao UPS que possui baterias estacionárias com capacidade de sete minutos de fornecimento de energia. Assim, caso ocorra falha no sistema de fornecimento elétrico externo, os UPS-X e UPS-Y irão manter a carga até o final de suas baterias, mantendo o fornecimento de energia para os equipamentos do *Data Center* SF.

Dessa forma, no intuito de minimizar possíveis interrupções no fornecimento de energia elétrica, o *Data Center* SF adota soluções de contingência que utilizam fontes de alimentação ininterruptas como UPS.

O UPS é um sistema de alimentação secundário, que entra em ação imediatamente após uma interrupção no fornecimento primário de energia. A alimentação é provida por um conjunto de baterias que possuem uma autonomia geralmente não muito grande, mas que garante tempo suficiente para que sejam iniciados os procedimentos de acionamento de geradores auxiliares ou ações para salvaguarda dos dados e desligamento dos sistemas.

Ressalta-se que um gerador auxiliar não substitui um UPS, pois, caso uma interrupção de energia ocorra, sempre haverá um hiato entre a falha de alimentação e o arranque do gerador do seu estado de "*standby*". Essa interrupção no fornecimento de energia poderá resultar em perdas financeiras irreparáveis ao órgão e, por isso, esse hiato de fornecimento é suportado pelo acionamento automático do sistema UPS.

3.7.3. Gerador de Energia Elétrica

Complementando o sistema de redundância no suprimento de energia elétrica, o *Data Center* SF ainda conta com Geradores de Energia Elétrica a combustão (diesel). Os geradores atuam como uma contingência à alimentação elétrica oriunda da rede local, assim como em relação aos equipamentos de *No-breaks*.

Juntamente com o fornecimento externo de energia elétrica e do sistema de *No-breaks*, há um sistema moto-gerador para garantir o fornecimento de energia visando atender o suprimento de energia elétrica do *Data Center*. Dessa forma, caso uma eventual falta de energia externa ocorra, os geradores entrarão em operação e o Quadro de Transferência Automática (QTA) se encarregará de transferir a carga entre os sistemas de alimentação elétrica.

A sede da SF conta com dois geradores com uma capacidade total de 260kVA, que fornecem, exclusivamente, energia elétrica ao *Data Center* para o caso de ocorrem falhas nas outras fontes de energia. Cada um dos geradores possui um tanque de combustível com capacidade para 250 litros de óleo diesel. Cada tanque é equipado com seus respectivos boxes de contenção de combustível, o que permite uma autonomia média de oito horas de operação, podendo chegar a 18 horas de fornecimento dependendo da carga demandada.

As imagens 27, 28 e 29 apresentam os geradores de energia elétrica responsáveis pela alimentação de contingência do *Data Center* SF e seus respectivos equipamentos auxiliares:

Imagens 27, 28 e 29: geradores de energia elétrica a diesel – SF

Fonte: própria.

De acordo com o exposto, as soluções redundantes de fornecimento de energia elétrica vinculadas ao *Data Center* SF estão alinhadas às especificações contidas no termo de referência do contrato nº 57/2015 e seus respectivos termos aditivos, assim como, possui alinhamento às orientações das normas ABNT ISO/IEC 27.002:2013.

3.8. *Links* de Telecomunicações

As telecomunicações no *Data Center* SF são providas por *links* 2 de internet de 1 Gbps (*Gigabit* por segundo) cada, redundantes e independentes, ambos contratados junto à empresa Wireless Comm Services Ltda., por meio do Contrato nº 66/SF/2016. Os *links* de internet permitem a interconexão do *Data Center* à rede da SF, a fim de oferecer acesso aos sistemas nele hospedados.

A redundância implementada na infraestrutura de telecomunicações vinculada ao *Data Center* SF está alinhada às especificações contidas no termo de referência do contrato nº 57/2015 e seus respectivos termos aditivos.

Por outro lado, a situação encontrada está parcialmente alinhada à ABNT ISO/IEC 27.002:2013, pois, a norma ISO orienta ser conveniente que, no intuito de aumentar o nível de contingenciamento, disponibilidade e segurança dos dados, sistemas e serviços providos pelo *Data Center,* os *links* de conectividade redundantes devem ser contratados com provedores de telecomunicação distintos.

3.9. Manutenções Preventivas do *Data Center* SF

De acordo com o item 13 do Anexo do Termo Contratual nº 57/2015 (peça 5, fls. 1/37) e seus respectivos termos aditivos (peça 6, fls. 1/2; peça 7, fls. 1/2 peça 8, fls. 1/2; e peça 9, fls. 1/6), a contratada obriga-se a efetuar Serviços de Manutenção nas dependências do *Data Center* da SF. A execução dos serviços segue um Roteiro de Manutenção que prevê a verificação, manutenção e/ou substituição de peças e reposição dos itens que se fizerem necessárias.

Os serviços periódicos de manutenção realizados na sala cofre têm como objetivo:

- Manter a continuidade operacional e preservar a vida útil dos equipamentos;
- Garantir que os sistemas de alarmes funcionem corretamente;
- Manter as evidências dos testes efetuados nos sistemas.

As verificações, ajustes e correções contemplam dos seguintes itens:

- **Porta da sala:** verificação de vedações, dobradiças, soleira, almofada, fechadura, molas e micro *switch*;

- **Blindagens:** verificação de blindagens, cunhas e caixas de passagens de cabos;

- **Luminárias:** verificação de lâmpadas, soquetes, reatores eletrônicos, iluminação de emergência e demais componentes do sistema de iluminação;

- **Paredes (painéis):** verificação de integridade das placas, perfis de acabamento, pintura e vedações externas;

- **Painéis elétricos:** verificação das réguas, botoeiras, fusíveis, interruptores de correntes de fuga, e disjuntores; checagem de temperatura das fontes e transformadores; verificação de tensão de saída, carga e baterias; verificação dos temporizadores, LEDS de sinalização e contadores; limpeza interna e externa dos painéis, verificação e lubrificação das fechaduras, verificação da pintura;

- **Testes:** testes de fechamento da porta; das luzes de emergência; da sinalização áudio visual após alarme; do tempo de atuação do *No-break*; testes de *reset* da sala e testes após *reset*, verificando se a sala se rearma automaticamente após *reset*.

Em atendimento à requisição de documentos (peça 20, fl. 1/1), a SF apresentou comprovantes de fornecimento mensal dos serviços de manutenção preventiva executados no *Data Center* SF (peça 15, fls. 1/461) referentes ao período de janeiro de 2018 a outubro de 2019, atestados pela SF.

Considerando os documentos apresentados, conclui-se que os serviços de teste e manutenção executados no *Data Center SF* e em seus respectivos equipamentos auxiliares estão sendo realizados de acordo com as disposições do contrato nº 57/2015 e as orientações das normas ISO/IEC 27.002:2013.

3.10. Responsável pela área auditada

Nome	Cargo
Luciano Felipe de Paula Capato	*Coordenador Geral de Tecnologia da Informação e Comunicação*

4. CONCLUSÕES

À vista dos exames documentais e das verificações realizadas *in loco,* a Auditoria chegou aos seguintes apontamentos:

4.1. A inexistência de uma solução de contingência de dados (Sítio *Backup*), serviços e processos de negócios constitui uma fragilidade para salvaguarda da segurança das informações, assim como demonstra desalinhamento às orientações da norma ISO/IEC 27.0002:2013. **(Item 3.3.1)**;

4.2. Não foram encontradas evidências de que o documento que representa a Política de Segurança da Informação (PSI) passou por análises e revisões regulares, demonstrando um desalinhamento às orientações da norma ISO/IEC 27.0002:2013. **(Item 3.5)**;

4.3. O processo de controle de acesso adotado para o *Data Center* SF, especificamente a inexistência de registro da entrada dos visitantes ao ambiente seguro, não está aderente às recomendações da norma ABNT ISO/IEC 27.002:2013. **(Item 3.6.3.1)**.

4.4. A infraestrutura de telecomunicações implantada no *Data Center* SF é parcialmente adequada, pois a solução de redundância existente (*links* redundantes) não está alinhada às orientações da norma ABNT ISO/IEC 27.002:2013. **(Item 3.8)**.

Grupo de Auditoria de Tecnologia da Informação – GATI

Em 30.04.20.

CARLOS ALBUQUERQUE LEMOS
Agente de Fiscalização

HÉLIO RICARDO G. M. DE AZEVEDO
Agente de Fiscalização

MAURICIO KAZUHIRO SATO
Agente de Fiscalização

RENATO SAMBRA SUYAMA
Supervisor de Equipes de Fiscalização e Controle 5

De acordo em 02.07.20.

MARCOS THULYO TAVARES
Coordenador-Chefe de Fiscalização e Controle I