INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA GOIANO – CAMPUS MORRINHOS

GIOVANI GAZZI PAGANINI

RELATÓRIO DE ATIVIDADES PROFISSIONAIS REALIZADAS NA ÁREA DE SEGURANÇA DA INFORMAÇÃO

MORRINHOS

2024

GIOVANI GAZZI PAGANINI

RELATÓRIO DE ATIVIDADES PROFISSIONAIS REALIZADAS NA ÁREA DE SEGURANÇA DA INFORMAÇÃO

Trabalho de Conclusão apresentado ao Curso Superior de Tecnologia em Sistemas para Internet do Instituto Federal Goiano – Campus Morrinhos, como parte dos requisitos necessários à obtenção do título de Tecnólogo em Sistemas para Internet.

Orientador: Prof. Dr. Antônio Neco de Oliveira

MORRINHOS

2024

Sistema desenvolvido pelo ICMC/USP
Dados Internacionais de Catalogação na Publicação (CIP)
Sistema Integrado de Bibliotecas - Instituto Federal Goiano

Paganini, Giovani Gazzi
P129r Relatório de Atividades Profissionais Realizadas na Área de Segurança da Informação / Giovani Gazzi Paganini; orientador Antonio Neco de Oliveira. -- Morrinhos, 2024.
41 p.

TCC (Graduação em Tecnologia em Sistemas para Internet) -- Instituto Federal Goiano, Campus Morrinhos, 2024.

1. Segurança da informação. 2. Infraestrutura. 3. Backup. 4. Recuperação. I. Oliveira, Antonio Neco de, orient. II. Título.

Responsável: Johnathan Pereira Alves Diniz - Bibliotecário-Documentalista CRB-1 n°2376

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA GOIANO

Ata nº 1/2024 - CCSTSI-MO/DE-MO/CMPMHOS/IFGOIANO

ATA DE DEFESA DE TRABALHO DE CURSO

Aos quatro dias do mês de abril de 2024, às 19 horas e 30 minutos, reuniu-se a banca examinadora composta pelos docentes: Dr. Antônio Neco de Oliveira (orientador), Ma. Ana Maria Martins Carvalho (membro), Dr. Fernando Barbosa Matos (membro), para examinar o Trabalho de Curso intitulado "RELATÓRIO DE ATIVIDADES PROFISSIONAIS REALIZADAS NA ÁREA DE SEGURANÇA DA INFORMÇÃO" do estudante GIOVANI GAZZI PAGANINI, Matrícula nº 2016104211710034, do Curso de Tecnologia em Sistemas para Internet, do IF Goiano – Campus Morrinhos. A palavra foi concedida ao estudante para a apresentação oral do TC, seguida de arguição pelos membros da banca examinadora. Após essa etapa, a banca examinadora decidiu pela APROVAÇÃO do estudante. Ao final da sessão pública de defesa, foi lavrada a presente ata, a qual segue assinada pelos membros da banca examinadora.

(Assinado Eletronicamente)

Dr. Antônio Neco de Oliveira
Orientador

(Assinado Eletronicamente)

Ma. Ana Maria Martins Carvalho
Membro

(Assinado Eletronicamente)

Dr. Fernando Barbosa Matos
Membro

Documento assinado eletronicamente por:

- Ana Maria Martins Carvalho, PROFESSOR ENS BASICO TECN TECNOLOGICO, em 05/04/2024 16:10:32.
- Fernando Barbosa Matos, PROFESSOR ENS BASICO TECN TECNOLOGICO, em 05/04/2024 14:11:35.
- Antonio Neco de Oliveira, PROFESSOR ENS BASICO TECN TECNOLOGICO, em 05/04/2024 13:28:19.

Este documento foi emitido pelo SUAP em 04/04/2024. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifgoiano.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 590127
Código de Autenticação: e44930ff7b

INSTITUTO FEDERAL GOIANO
Campus Morrinhos
Rodovia BR-153, Km 633, Zona Rural, SN, Zona Rural, MORRINHOS / GO, CEP 75650-000
(64) 3413-7900

Dedico este trabalho a todos os profissionais de tecnologia e segurança da informação, cujo trabalho é o alicerce do mundo digital em que vivemos.

AGRADECIMENTOS

A minha família, que me incentivou e me apoiou desde pequeno em minha busca por conhecimento. Em especial a minha esposa e meus cachorros, que sempre estiveram ao meu lado enquanto me dedicava a este trabalho.

Aos meus professores, que não mediram esforços em transferir a sabedoria necessária para minha formação acadêmica.

Ao meu coordenador de infraestrutura, que me ensinou que conhecimento é o único bem que ninguém pode nos tomar e sempre incentivou meu aprendizado.

Por fim, a todos os eternos aprendizes.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira das Normas Técnicas
AWS	*Amazon Web Services*
CID	Confidencialidade, Integridade e Disponibilidade
CSF	*Cybersecurity Framework*
EIMM	Estabelecer, Implementar, Manter e Melhorar
IEC	*International Electrotechnical Commission*
ISO	*International Organization for Standardization*
LGPD	Lei Geral de Proteção de Dados
NBR	Norma Brasileira
NIST	*National Institute of Standards and Technology*
PDCA	*Plan, Do, Check, Act*
RPO	*Recovery Point Objective*
RTO	*Recovery Time Objective*
S3	*Simple Storage Service*
SGSI	Sistema de Gestão de Segurança da Informação
TI	Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO

Relatório de atividades profissionais realizadas na empresa Aviva Parques & Resorts pelo Analista de Infraestrutura de TI Giovani Gazzi Paganini.

A sede da empresa Aviva Parques & Resorts está localizada no município de Rio Quente – GO sob o nome de Rio Quente Resorts, onde é popularmente conhecida por Pousada do Rio Quente. A Aviva também administra as marcas Hot Park e Costa do Sauípe Resorts, que são alguns dos pontos turísticos mais visitados do Brasil.

Dentre as principais atividades de atuação da Aviva, destaca-se a venda de seus produtos de viagens turísticas aos resorts, seus pacotes de hospedagem no formato de *time sharing* e seus clubes de férias. A Aviva também possui uma operadora de viagens própria, oferecendo aos seus clientes soluções de turismo e logística integradas, proporcionando condições competitivas em relação aos seus concorrentes.

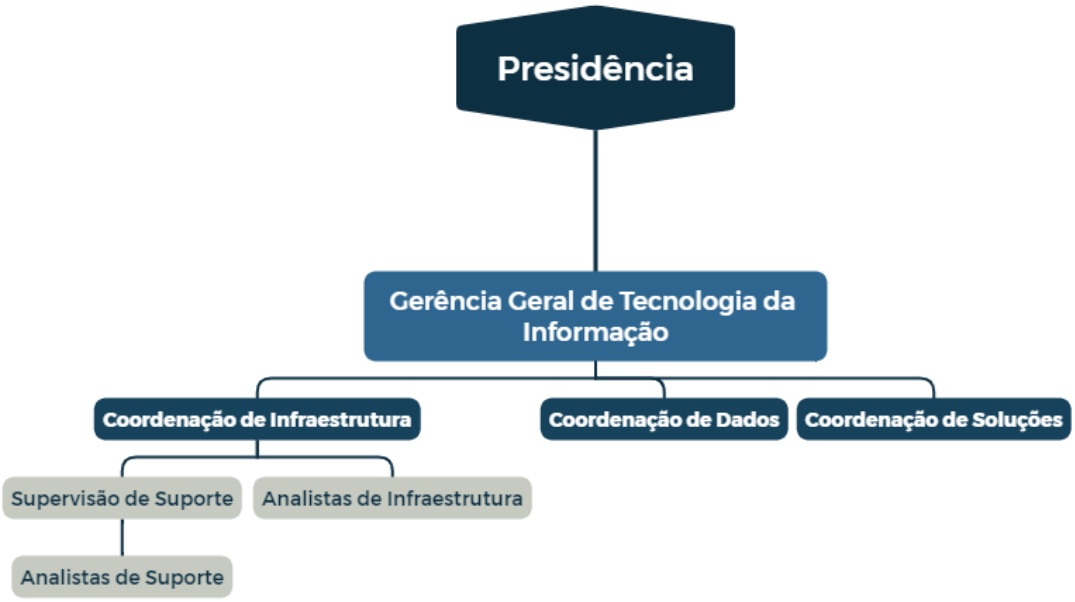
Por se tratar de uma empresa de entretenimento e turismo, seu foco é a experiência do cliente acerca da natureza de águas naturalmente quentes da região de Rio Quente, utilizando a tecnologia a seu favor para maximizar o conforto e prover serviços de qualidade para seus hóspedes e visitantes. Proporcionar aos hóspedes na Costa do Sauípe a possibilidade de compartilhar seus momentos em família direto da orla da praia, através de uma rede gerenciada de *access points* de alta velocidade, é a forma da Aviva de utilizar a tecnologia para fazer famílias felizes.

Apesar do ramo de atuação, a companhia possui um *data center* próprio e investe em tecnologias de ponta para garantir a conectividade e segurança dos dados de seus clientes. Tais tecnologias requerem dedicação diária e, sua execução utilizando metodologias e normas asseguram que os dados da empresa e de seus clientes estejam protegidos e sempre disponíveis.

A equipe de analistas de infraestrutura de TI da Aviva é composta por 5 profissionais dedicados ao ambiente de servidores e de telecomunicações. Esta equipe é responsável por implementar e manter cerca de 1500 computadores, 250 servidores virtuais, 10 *hosts* físicos de virtualização e 4 unidades de armazenamento de alta capacidade. Tal infraestrutura é conectada por uma rede de cerca de 200 *switches* de rede e 960 *access points,* provendo a conexão de banda larga necessária para o alto tráfego de dados. A Aviva possui cerca de 4 *petabytes* de dados armazenados em seus 3 *data centers*.

A Figura 1 exibe onde o departamento de Tecnologia da Informação da Aviva está localizado dentro da estrutura organizacional da empresa.

Figura 1. Estrutura organizacional do departamento de TI na Aviva.



Fonte: o autor (2024).

Para manter uma infraestrutura complexa como a da Aviva segura, é necessário ter uma equipe capacitada para implementar e operar as ferramentas de proteção de forma eficaz, respeitando as recomendações dos fabricantes de tais ferramentas e as melhores práticas de segurança da informação.

Este relatório tem como objetivo correlacionar as normas e boas práticas de segurança da informação, focando em como elas podem ser implementadas em uma organização, visando elevar a sua postura de segurança cibernética estabelecendo processos que busquem sua resistência perante as ameaças virtuais.

Também faz parte do escopo deste trabalho demonstrar como as atividades profissionais desenvolvidas pelo discente Giovani Gazzi Paganini na área segurança da informação, contribuíram para a configuração de um ambiente de infraestrutura resiliente e seguro dentro da Aviva, focado na arquitetura de ambientes com alta disponibilidade e capacidade de recuperação rápida, utilizando ferramentas modernas de gestão de vulnerabilidades, proteção de *endpoints* com antivírus, gestão de *backups* e replicação de dados.

1.1 Atividades Profissionais Desenvolvidas

As principais atividades desenvolvidas tiveram início em maio de 2021, por meio da implementação da ferramenta de gestão de *backups* Veeam Backup & Replication, tanto para criação e gestão de *backups*, quanto para a replicação do ambiente de produção para um ambiente de recuperação de desastres.

Não se limitando apenas a proteção do ambiente, foram implementadas soluções de gestão de ativos usando a ferramenta LanSweeper, gestão de vulnerabilidades utilizando o Nessus Pro da fabricante Tenable Security e gestão de segurança de *endpoints* utilizando o CrowdStrike Falcon. As atividades desenvolvidas foram alinhadas com as boas práticas e recomendações dos fabricantes bem como com as normas ABNT NBR ISO/IEC 27001 e o NIST CSF.

Foram implementados, utilizando orientações das normas e guias de segurança citadas neste trabalho, processos como: gestão de acessos e identidades, gestão de riscos, gestão de atualizações de segurança, gestão de mudanças, gestão de chaves criptográficas, planos de resposta à incidentes e planos de recuperação de desastre.

O discente também participou de treinamentos oficiais dos fabricantes que contribuíram com o conhecimento necessário para executar suas atividades e operar as soluções implementadas com maior acurácia.

2 DESENVOLVIMENTO

2.1 A Segurança da Informação

Organizações de todos os tipos e tamanhos armazenam, processam e transmitem informações a todo o tempo. Sabendo que as informações, seus processos, sistemas, redes e pessoas são importantes para atingir sua missão de negócio, estas perpassam uma variedade de riscos que podem afetar suas operações, sendo necessário, assim, implementar controles de segurança para garantir que sua exposição ao risco seja a menor possível (ISO, 2018).

Toda informação gerada e processada por uma organização está sujeita a diversos tipos de ataques e vulnerabilidades. Normalmente, as informações de uma organização podem ser consideradas como um ativo, dado o valor que está atrelado e, portanto, requer que sejam apropriadamente protegidas contra a perda da disponibilidade, confidencialidade e integridade (ISO, 2018).

Assim, a segurança da informação é o conjunto de práticas e medidas que devem ser adotadas para proteger contra ameaças a confidencialidade, integridade e disponibilidade das informações de uma organização, buscando mitigar sua exposição a riscos. Desse modo, surge a necessidade de um Sistema de Gestão de Segurança da Informação (SGSI). O SGSI consiste em políticas, procedimentos, guias, recursos e atividades gerenciadas por uma corporação com o intuito de proteger seus ativos de informação de ameaças (ISO, 2018).

2.1.2 Os Princípios da Segurança da Informação

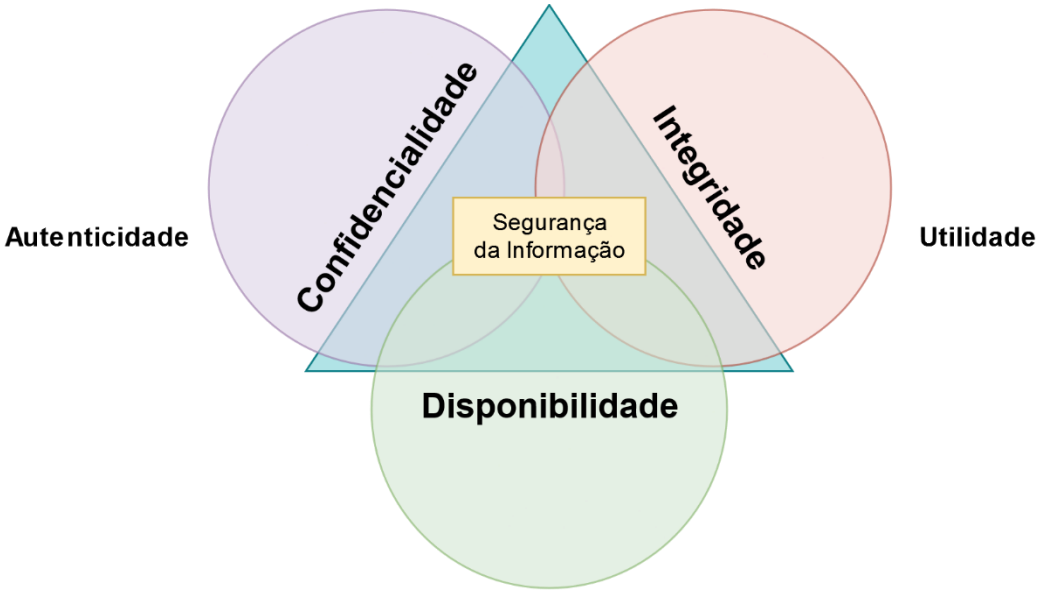
A segurança da informação visa garantir e proteger a confidencialidade, integridade e disponibilidade da informação. Esses três princípios normalmente também são acompanhados dos aspectos da autenticidade e da utilidade (BEAL, 2005).

A Figura 2 exibe os principais pilares da segurança da informação, onde são definidos os conceitos de que:

- A informação deve estar acessível somente para pessoas que possuírem autorização, mantendo sua confidencialidade;
- Ao acessá-la, a informação deve ser confiável e estar íntegra, livre de alterações de seu estado original e mantendo sua utilidade preservada;
- A informação deve estar disponível para ser acessada por pessoas autorizadas sempre que necessário;

- Sua autoria deve ser autêntica, mantendo a veracidade sobre quem é seu autor.

Figura 2. Diagrama CID dos pilares da segurança da informação.



Fonte: o autor (2024).

2.1.3 Normas Regulatórias

No Brasil, a implementação das regras de caráter regulatório da segurança da informação é regida pela ABNT, sob a NBR ISO/IEC 27001:2013. A NBR ISO/IEC 27001:2013, referência em gestão da segurança da informação, é um dos itens do grupo de normas ISO/IEC 27000, onde são tratados os itens regulatórios necessários para a implementação e conformidade de um SGSI.

Nela, são especificados os requisitos necessários para estabelecer, implementar, manter e melhorar continuamente (EIMM) o Sistema de Gestão de Segurança da Informação, incluindo os requisitos para avaliação e tratamento dos riscos de segurança da informação voltados para as necessidades da organização a qual está sendo prestada. Esses requisitos são genéricos, de tal forma que possam ser aplicados em qualquer entidade, independente do ramo de atuação ou tamanho (ABNT, 2013).

A norma é dividida em 11 seções e Anexo A[1], das quais 4 são apenas de cunho informativo e 7 são de caráter obrigatório em que todos seus requisitos são necessários para

[1] O Anexo A é um conjunto de controles de segurança e objetivos de controles, apresentados na forma de tabelas, presente na própria norma ABNT NBR ISO 27001, não se confundido com os anexos do presente trabalho.

atingir a conformidade com o regulamento e garantir a elegibilidade à sua certificação. O Anexo A traz um catálogo com 114 controles de segurança, distribuídos em 14 seções.

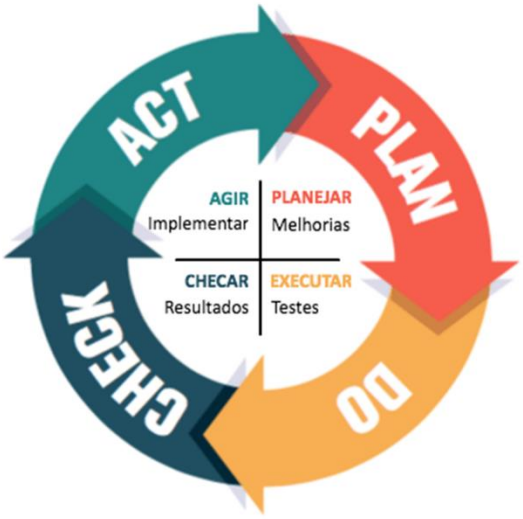
As seções de 0 a 3 introduzem o propósito da ISO 27001, elucidando sua importância de como ela visa proteger os fundamentos da segurança da informação por meio da implementação de processos e diretivas que compõem um SGSI. Além disso, também destaca sua compatibilidade com outras normas de sistemas de gestão e como ela está intrinsecamente vinculada à ISO/IEC 27000, onde estão registrados outros termos e definições indispensáveis para a aplicação da ISO 27001.

Em contrapartida, as seções numeradas de 4 a 10 estabelecem processos e requisitos, que além de imprescindíveis para propósitos regulatórios, também constroem as etapas do ciclo PDCA.

O PDCA, também conhecido como *Ciclo de Deming*, é um ciclo de melhoria contínua composto por quatro etapas, que busca propor mudanças, implementá-las, avaliá-las coletando dados e tomar decisões baseadas nos dados coletados, retornando ao início do ciclo sempre que necessário, a fim de elevar a qualidade de um produto ou processo de forma perpétua (LEAN, 2024).

A Figura 3 demonstra os quatro estágios do PDCA: planejamento, execução, checagem e atuação.

Figura 3. Ciclo de estágios do PDCA.



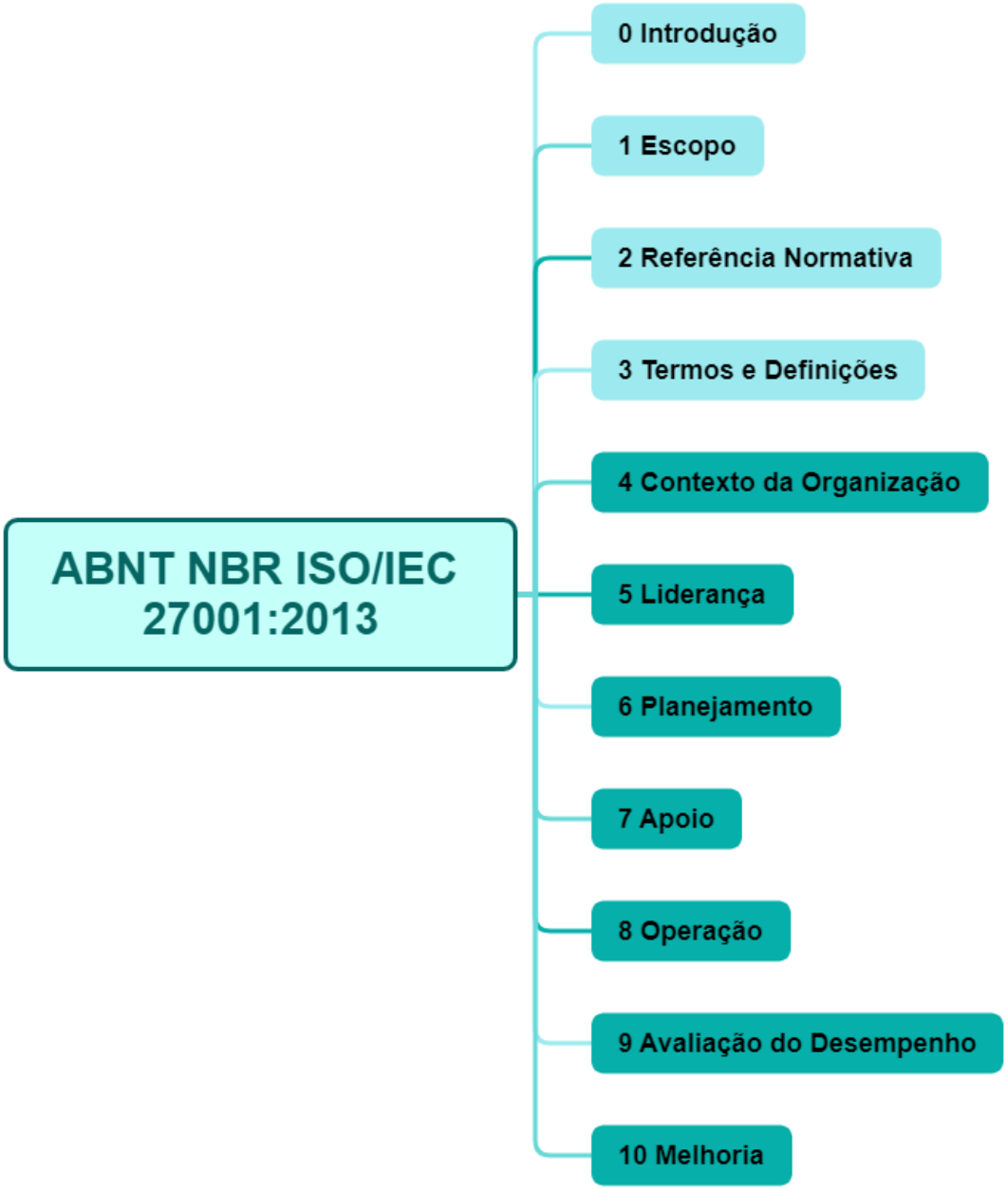
Fonte: Ávila (2014).

Tendo em vista que a ISO 27001 está profundamente conectada com o PDCA, as seções de 4 a 10 descrevem de forma sucinta como planejar, executar, checar e agir, quanto ao SGSI proposto pela norma.

As seções (4) contexto da organização, (5) liderança, (6) planejamento e (7) apoio, por exemplo, tratam da etapa de planejamento do PDCA, restando para a execução, checagem e atuação as seções (8) operação, (9) avaliação do desempenho e (10) melhoria, respectivamente.

A Figura 4 mostra a estrutura base da NBR ISO/IEC 27001:2013, destacando em verde escuro as etapas obrigatórias para obtenção da certificação da norma.

Figura 4. Estrutura geral da norma NBR ISO/IEC 27001:2013.



Fonte: o autor (2024).

No segmento de contexto da organização, são determinados os quesitos para o entendimento de assuntos internos e externos pertinentes à instituição, quais são as partes interessadas e o escopo do sistema de gestão da segurança da informação. Já em liderança, são estabelecidas as responsabilidades da alta direção, definindo seus papéis e o conteúdo da política de segurança da informação de nível executivo (ABNT, 2013).

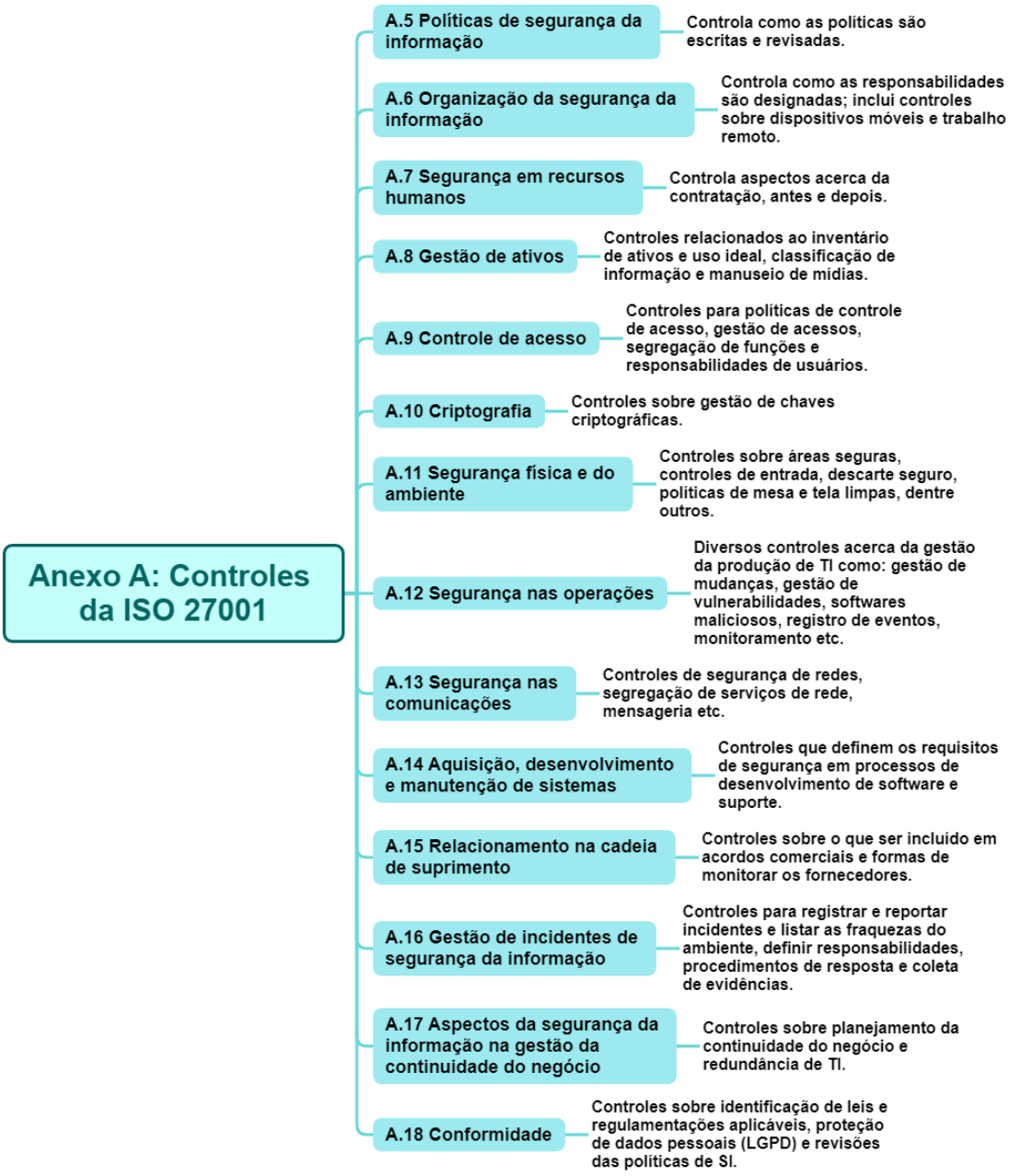
No planejamento do SGSI, a corporação deve elencar os riscos e oportunidades que devem ser consideradas para assegurar que seja possível alcançar os resultados a ela propostos, precaver quanto aos efeitos indesejados e alcançar a melhoria contínua, nomeada como definida pelo EIMM: estabelecer, implementar, manter e melhorar (ABNT, 2013).

A companhia também deve, como forma de apoio e como parte da etapa de planejamento do PDCA, determinar e prover os recursos necessários para estabelecer e implementar a manutenção do sistema de gestão da segurança da informação (ABNT, 2013).

A camada de operação da norma é onde todas as etapas anteriores entram em execução, colocando em prática os controles definidos no Anexo A da NBR ISO/IEC 27001:2013. Esta seção dita como devem ser planejados e implementados os processos necessários para atender os requisitos de segurança da informação, bem como implementar as ações determinadas na seção de planejamento (ABNT, 2013).

A Figura 5 descreve de forma resumida os 14 grupos de controles do Anexo A da NBR ISO/IEC 27001:2013 e como cada grupo de controle auxilia na implementação da SGSI.

Figura 5. Estrutura dos controles de segurança do Anexo A da ISO 27001.



Fonte: o autor (2024).

Além do planejamento operacional e controle, também devem ser realizadas avaliações de riscos periódicas, respeitando mudanças significativas e mantendo a documentação dos resultados das avaliações de risco realizadas. Por fim, deve ser colocado em prática o tratamento dos riscos de segurança da informação identificados (ABNT, 2013).

Concluindo a implementação do SGSI, é executada a etapa de melhoria onde as não conformidades encontradas durante a execução da norma devem ser corrigidas. Nessa fase, a organização deverá traçar um plano e tomar ações para reagir aos problemas encontrados e/ou implementar meios de prevenir que tais problemas ocorram de forma proativa. Também é aberto o espaço para que a organização realize ajustes no SGSI, visando manter o sistema atualizado pertinente às evidências encontradas. Essa etapa visa fundamentalmente implementar a melhoria contínua do SGSI (ABNT, 2013).

2.2 Cibersegurança

A cibersegurança ou segurança cibernética é um conjunto de práticas e/ou processos que visam proteger computadores, telefones celulares, redes de Internet, dispositivos móveis, dentre outros ativos de tecnologia, de ameaças ou ataques que possam comprometer a confidencialidade, integridade e disponibilidade de informações (CISA, 2021).

Apesar de ser fundamentalmente semelhante à segurança da informação, a cibersegurança busca implementar de forma prática processos e métodos que visam não só proteger ativos de tecnologia de ataques, como também aplicar formas de responder a esses ataques de forma defensiva e recuperar a operabilidade de uma organização após um incidente de segurança. Um dos principais guias de implementação de cibersegurança em uma organização é o NIST CSF (IBM, 2024).

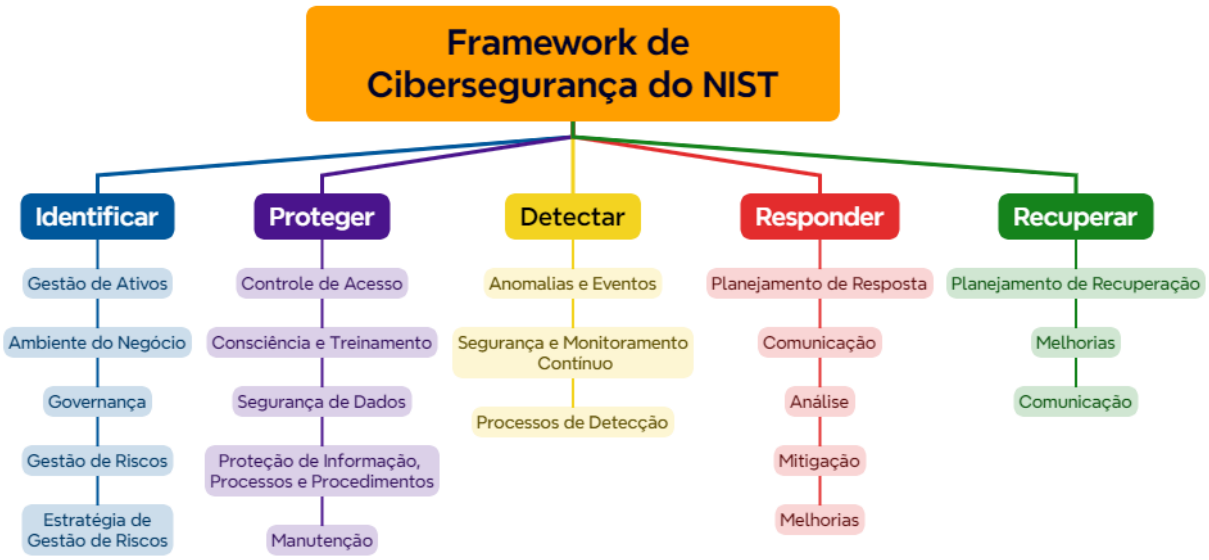
2.2.1 Framework de Cibersegurança do NIST

Criado pelo NIST, o *framework* de cibersegurança é tido como um guia que ajuda empresas e organizações a desenvolver ou melhorar seus processos de segurança de informação, podendo através dele melhorar sua postura de segurança digital (IBM, 2024).

O CSF está segregado em 5 funções principais: identificar, proteger, detectar, responder e recuperar. Cada função determina categorias de atividades que devem ser desenvolvidas ou implementadas que em conjunto, oferecem valor agregado perante a gestão de riscos relacionada à segurança de uma empresa ou organização. De forma geral, cada tópico pode ser tratado de forma individual, no entanto, em conjunto os tópicos formam um ciclo de atividades (IBM, 2024).

A Figura 6 demonstra as funções do CSF e seus principais tópicos.

Figura 6. Estrutura das funções do *Framework* de Cibersegurança do NIST.



Fonte: o autor (2024).

Para ajudar as organizações a medir o progresso durante a implementação do NIST CSF, o *framework* elucida quatro níveis de implementação:

- Nível 1 - Parcial: a organização possui alguma familiaridade com o *framework* e implementou alguns controles de forma reativa;
- Nível 2 - Risco informado: a organização está mais consciente dos riscos de segurança cibernética, porém ainda não possui um processo de gestão de riscos implementado de forma geral na empresa;
- Nível 3 - Repetido: a organização e seus executivos estão completamente cientes dos riscos de segurança cibernética e foi implementado um plano de gestão de riscos em toda a organização, contendo planos de ação para monitorar e responder a ameaças;
- Nível 4 - Adaptativo: a resiliência cibernética foi atingida e a organização já usa indicadores preditivos de modo a evitar ataques cibernéticos. Existe uma equipe de segurança agindo de forma proativa melhorando continuamente as práticas de segurança e se adaptando às mudanças no cenário global de cibersegurança em tempo real. Organizações deste nível possuem a gestão de riscos incorporada em sua estrutura.

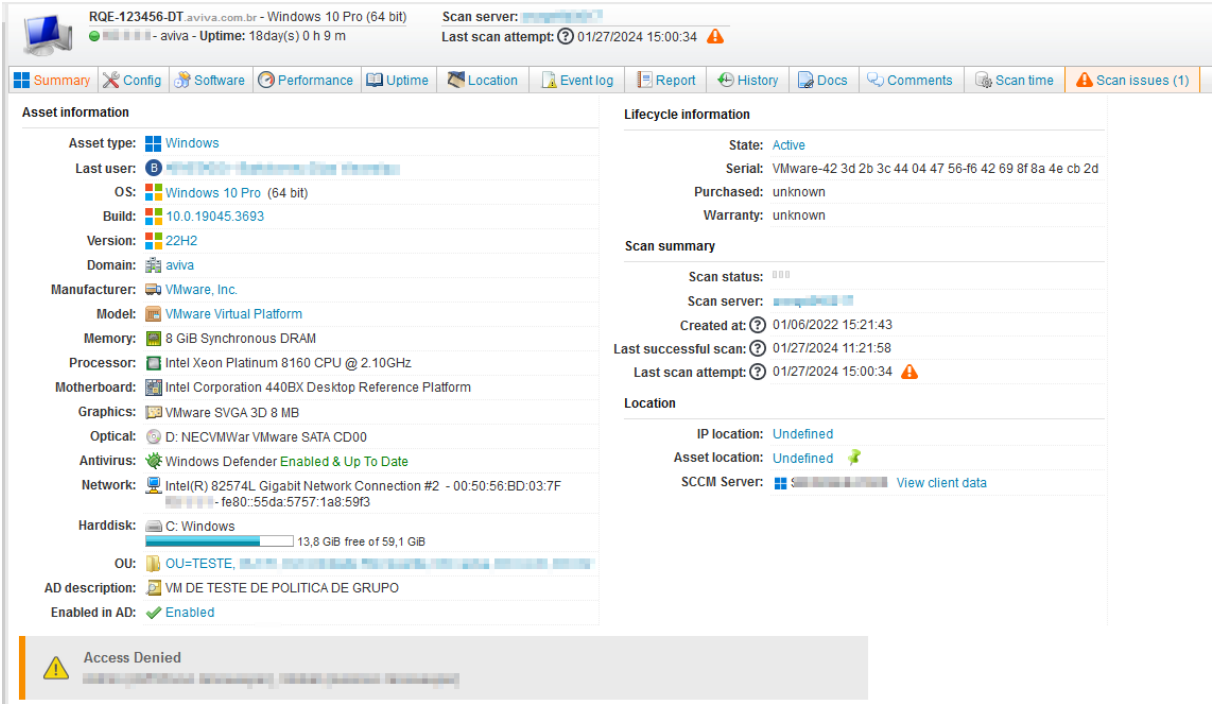
2.2.2 Identificar (Identify)

A principal premissa da função de identificação do NIST CSF é prover um entendimento organizacional de gerir riscos de segurança de sistemas, ativos de TI ou dados. Identificar os processos críticos, ativos envolvidos e seus riscos de segurança relacionados é crucial para elencar as atividades que são imprescindíveis para a continuidade do negócio. Deste modo a empresa pode ser capaz de priorizar sua estratégia de gestão de riscos e atividades que devem ter sua atenção redobrada (NIST, 2018).

Como parte da identificação de ativos, manter um bom inventário de *hardware* e *software* é extremamente importante para ter uma compreensão adequada do parque de computadores da organização, principalmente devido a serem frequentemente as portas de entrada para ataques maliciosos (NIST, 2018).

Na Figura 7 é demonstrado um exemplo de *software* de gestão e inventário de ativos, a ferramenta LanSweeper implementada na Aviva. Na figura, informações classificadas como sensíveis foram ocultadas por questões de privacidade e adequação à Lei Geral de Proteção de Dados (LGPD).

Figura 7. Captura de tela da ferramenta LanSweeper.



Fonte: o autor (2024).

Além disso, também devem ser identificadas as ameaças, vulnerabilidades existentes e riscos aos ativos. Um bom plano de gestão de riscos deve existir de modo a manter as vulnerabilidades e ameaças bem documentadas, buscando identificá-las e priorizar suas correções (NIST, 2018).

A Figura 8 demonstra a identificação de vulnerabilidades da ferramenta de gestão de vulnerabilidades Nessus Pro na Aviva.

Figura 8. Captura de tela da ferramenta Nessus Pro.

Fonte: o autor (2024).

2.2.3 Proteger (Protect)

A fase de proteção do ciclo visa implementar meios seguros de entregar os serviços, de forma a garantir que os dados estejam protegidos. Semelhante ao conceito de confidencialidade da segurança da informação, essa etapa define que contas de usuário, por exemplo, sejam únicas

a cada funcionário e que suas credenciais de acesso se restrinjam somente a informações ou ativos que lhes foram concedidos (NIST, 2018).

Nesta etapa também são abordados conceitos de sensibilidade dos dados, guiando as empresas em como garantir que tais informações estejam seguras, tanto no trânsito quanto em repouso, como por exemplo utilizando criptografia. Se tratando de dados em repouso, realizar *backups* frequentes dos dados também é considerada uma estratégia de proteção, já que manter uma cópia segura dos dados de produção é uma excelente tática para prevenir desastres e ataques de *ransomware* (NIST, 2018).

Além de cópias de segurança, também é fundamental proteger os dispositivos utilizando ferramentas de proteção ativa, como *firewalls* e produtos de segurança, como os antivírus. Manter as configurações padronizadas, desativar funções que não sejam utilizadas e documentar mudanças no ambiente também fazem parte da estratégia de proteção. Além disso, manter os funcionários treinados e conscientes dos riscos de segurança, auxilia a garantir um bom nível de maturidade de segurança da informação (NIST, 2018).

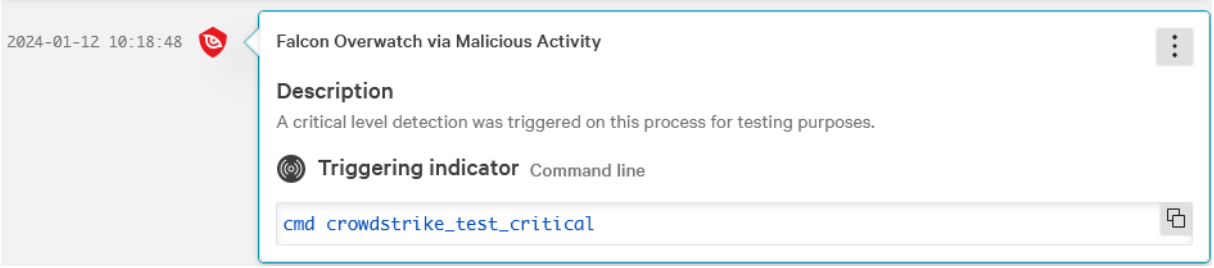
2.2.4 Detectar (Detect)

Para detectar atividades suspeitas ou possíveis ameaças devem ser implementadas soluções que permitam identificar ocorrências não autorizadas. Nesse aspecto pode ser extremamente útil ter em mãos ferramentas que registrem todas as atividades em *logs* centralizados, por exemplo, para facilitar a identificação de tentativas de acesso não autorizadas.

Para que isso seja possível, é necessário conhecer a fundo o fluxo de informações da empresa. Ter esse tipo de informação bem documentada facilita o rastreio de um incidente e ajuda na remediação. Incidentes de cibersegurança são de importância crítica, portanto, possuir meios que encurtem o tempo entre detecção e resposta é de extrema importância para impedir um desastre de segurança (NIST, 2018).

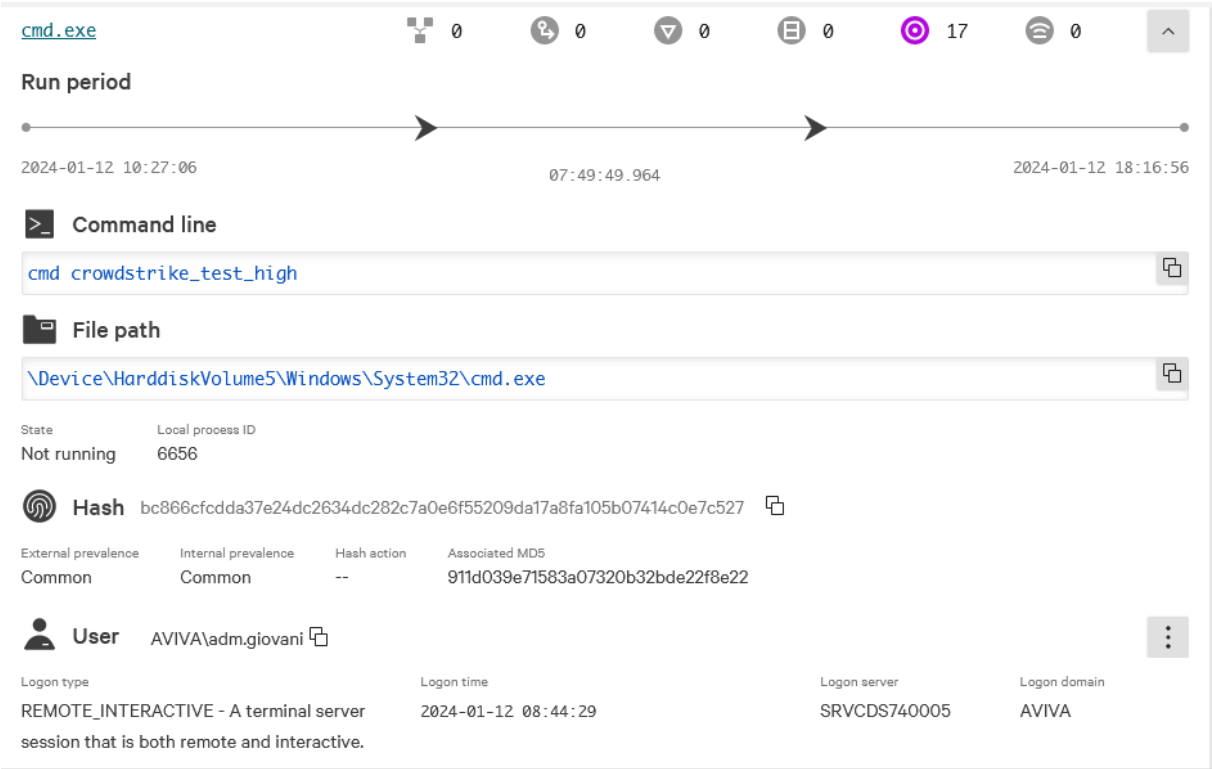
As Figuras 9 e 10 exibem um exemplo de detecção de uma atividade maliciosa utilizando o antivírus CrowdStrike Falcon na Aviva, onde é exibido em detalhes todos os ativos e envolvidos de um incidente, como por exemplo, comandos executados, criticidade da detecção, tempos de execução, ações tomadas e atores envolvidos.

Figura 9. Detecção de atividade maliciosa na ferramenta CrowdStrike Falcon.



Fonte: o autor (2024).

Figura 10. Detecção de atividade maliciosa detalhada no CrowdStrike Falcon.



Fonte: o autor (2024).

2.2.5 Responder (Respond)

Tão importante quanto detectar uma ameaça, respondê-la de forma eficiente e organizada garante que o impacto de um incidente de cibersegurança seja minimizado. Planos de resposta a incidentes devem ser criados e atualizados para garantir que a sequência de atividades necessárias seja executada para conter as ameaças identificadas (NIST, 2018).

Um plano de resposta a incidentes pode ter, por exemplo, itens como:

- Lista de pessoas envolvidas, seus papéis e suas responsabilidades;

- Ordem de execução das etapas de acordo com sua necessidade;
- Envolvimento com forças da lei, caso necessário;
- Categorização e comunicação clara dos incidentes;
- Documentação do impacto causado;
- Atividades realizadas com o fim de mitigar o impacto causado e resolver o incidente.

2.2.6 Recuperar (Recover)

As categorias da função de recuperação implementam planos resilientes e robustos, visando garantir a continuidade do negócio em caso de ataque cibernético e restaurar rapidamente a operação ou serviços impactados durante um incidente de cibersegurança (NIST, 2018).

Parte da função de recuperação é planejar e criar processos de recuperação, garantindo que sejam sempre atualizados e que estejam disponíveis para utilização. Durante um incidente de segurança, os planos de recuperação deverão ser utilizados para recuperar a operabilidade do ambiente. Após normalizado, os planos de recuperação deverão ser atualizados com as lições aprendidas e com as estratégias de recuperação melhoradas (NIST, 2018).

Atividades de recuperação devem ser realizadas envolvendo todos os interessados, internos ou externos, incluindo: autoridades, sistemas, vítimas, provedores de Internet ou outros que se fizer necessário. Manter e gerenciar uma estratégia de relações públicas e reputação da organização garante que a informação esteja completa e precisa ao ser compartilhada, evitando que a reputação seja manchada (NIST, 2018).

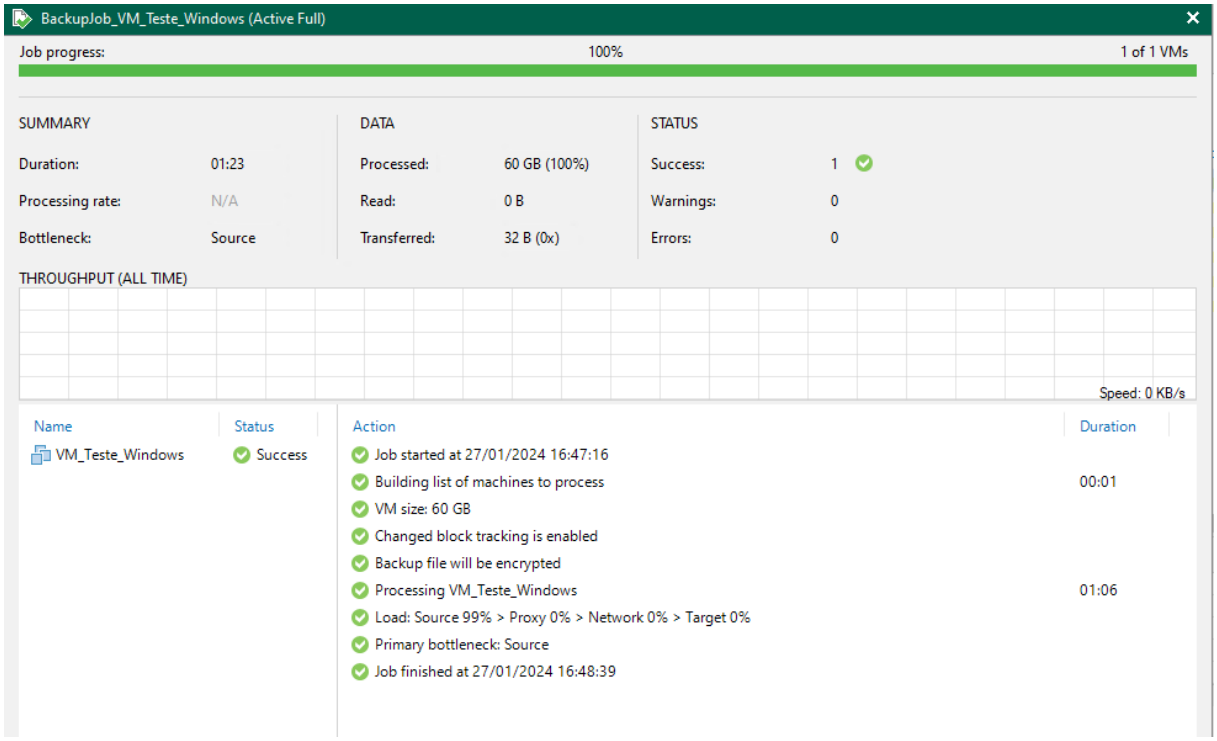
2.3 Implantação de Ambiente de *Backup*

Atualmente, os dados de uma empresa podem ser considerados seus ativos de maior valor, onde em uma eventual perda poderia significar um prejuízo de milhões, senão a própria falência. De acordo com a Sophos (2021), em 2021 a média do custo de recuperação após um desastre de *ransomware* é de cerca de US$2.000.000,00. A tamanha importância desses dados requer que uma postura de segurança robusta seja adotada dentro de uma organização, a fim de proteger os dados existentes a qualquer custo, com o mínimo de perda o possível.

Dentre as medidas de segurança que podem ser adotadas, o *backup* dos dados é fundamental para assegurar que as informações da empresa sejam armazenadas de forma segura e eficiente. Apesar de um *backup* ser essencialmente uma cópia de segurança dos dados originais, existem maneiras mais eficientes de lidar com as rotinas de cópia dos arquivos, o que normalmente demanda o uso de uma solução mais robusta. Na Aviva, visando atingir conformidade com o controle A.17.2 da norma ABNT ISO/IEC 27001, bem como garantir a aplicabilidade da função de "recuperar" do CSF do NIST, foi implementado uma infraestrutura de *backup* utilizando o Veeam Backup & Replication como solução de gestão de *backups* da empresa.

A Figura 11 demonstra o funcionamento da ferramenta de *backup* Veeam em uma rotina de *backup* criada para um determinado ativo.

Figura 11. Rotina de *backup* em execução na ferramenta Veeam Backup.



Fonte: o autor (2024).

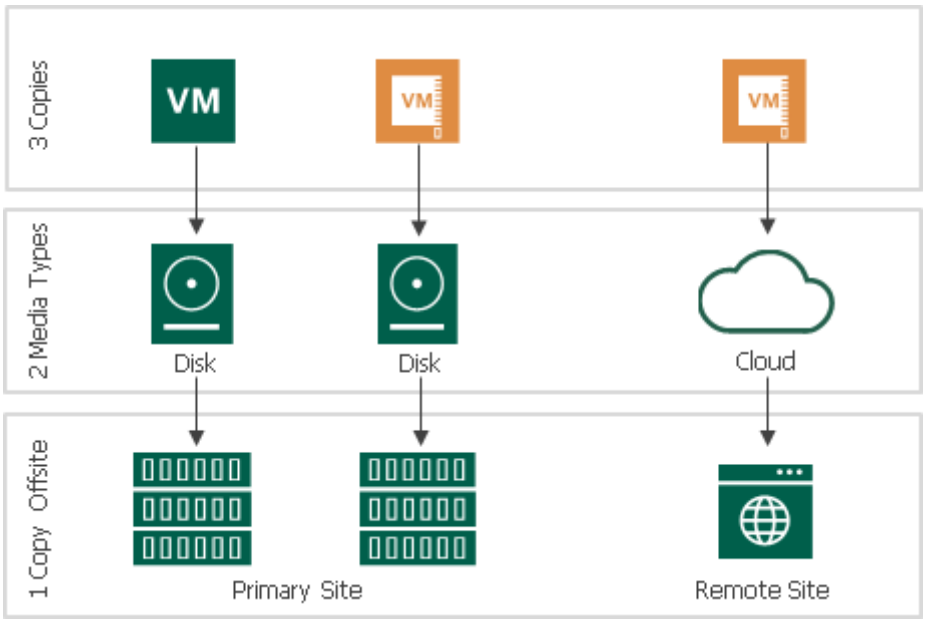
Para que uma cópia de segurança possa ser considerada segura, efetivamente, existem boas práticas que devem ser seguidas de acordo com o manual do fabricante do *software* de *backup*. Segundo a Veeam, a regra de ouro dos *backups* é a regra "3-2-1", onde devem existir 3 cópias, sendo uma original, um *backup* e uma cópia do *backup*. Dessas, 2 devem ser

armazenadas em tipos de mídias diferentes, como disco, nuvem ou fita, e pelo menos 1 delas deve estar armazenada de forma totalmente *offline* ou imutável.

Além disso, a regra "3-2-1" de *backups*, apesar de não ser explícita na norma ABNT ISO/IEC 27001, está alinhada com a busca constante de conformidade da norma (VEEAM, 2023b).

A Figura 12 elucida a cadeia de cópias de *backup* para garantir a aplicação da regra "3-2-1".

Figura 12. Cópias de *backup* segundo o tipo de mídia de armazenamento.

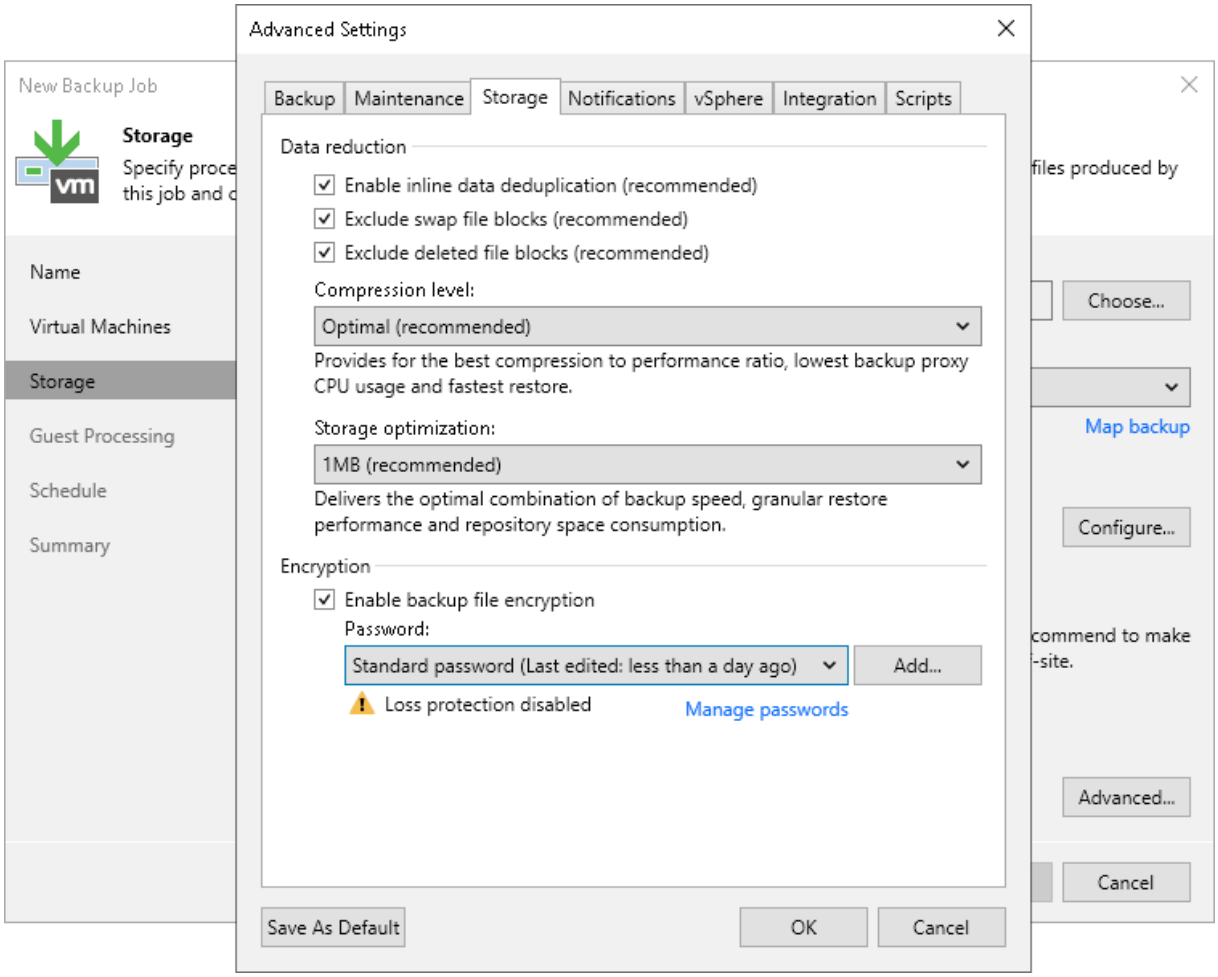


Fonte: Veeam (2024a).

Do mesmo modo, existem outras recomendações de segurança para o armazenamento dos *backups*, como por exemplo a criptografia dos *backups* gerados, onde fica impossibilitada a leitura dos dados em caso de um vazamento do *backup*. A criptografia de dados também foi aplicada no ambiente, buscando compatibilidade com o controle A.10.1 da ABNT ISO 27001 e com as funções de proteger e recuperar do CSF (VEEAM, 2023a).

Na Figura 13 é demonstrado como é ativada a criptografia de *backups* no Veeam Backup.

Figura 13. Captura de tela da configuração de criptografia no Veeam Backup.

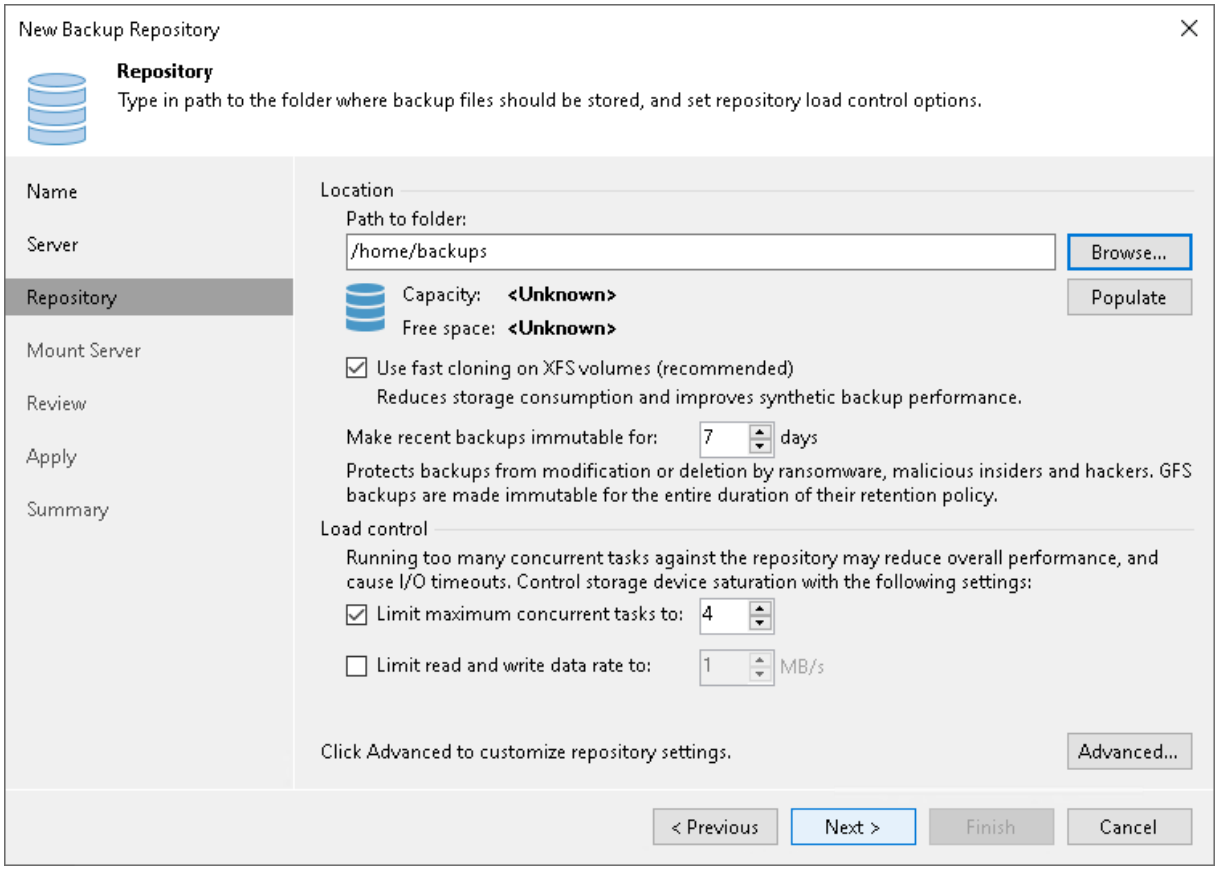


Fonte: Veeam (2024b).

Outra recomendação de segurança é a própria separação do ambiente de *backup* de um ambiente produtivo, mantendo os dois ambientes em comunicação paralela e limitada a fim de evitar ataques laterais pela infraestrutura lógica por trás dos serviços. A segregação de funções e de redes faz parte dos controles A.6.1.2 e A.13.1.3 da ISO 27001 (ABNT, 2013).

O Veeam ainda oferece um recurso adicional para a proteção de *backups* contra *ransomware*: a imutabilidade de objetos. Utilizando este recurso, é possível configurar um repositório de *backup* com imutabilidade ativada. Neste cenário, os *backups* criados ficarão imutáveis, ou seja, impedidos de sofrer quaisquer alterações, por um determinado período. A imutabilidade pode facilmente ser configurada no Veeam Backup através da configuração de um repositório de *backup*, conforme demonstra a Figura 14.

Figura 14. Captura de tela da configuração de imutabilidade do Veeam Backup.



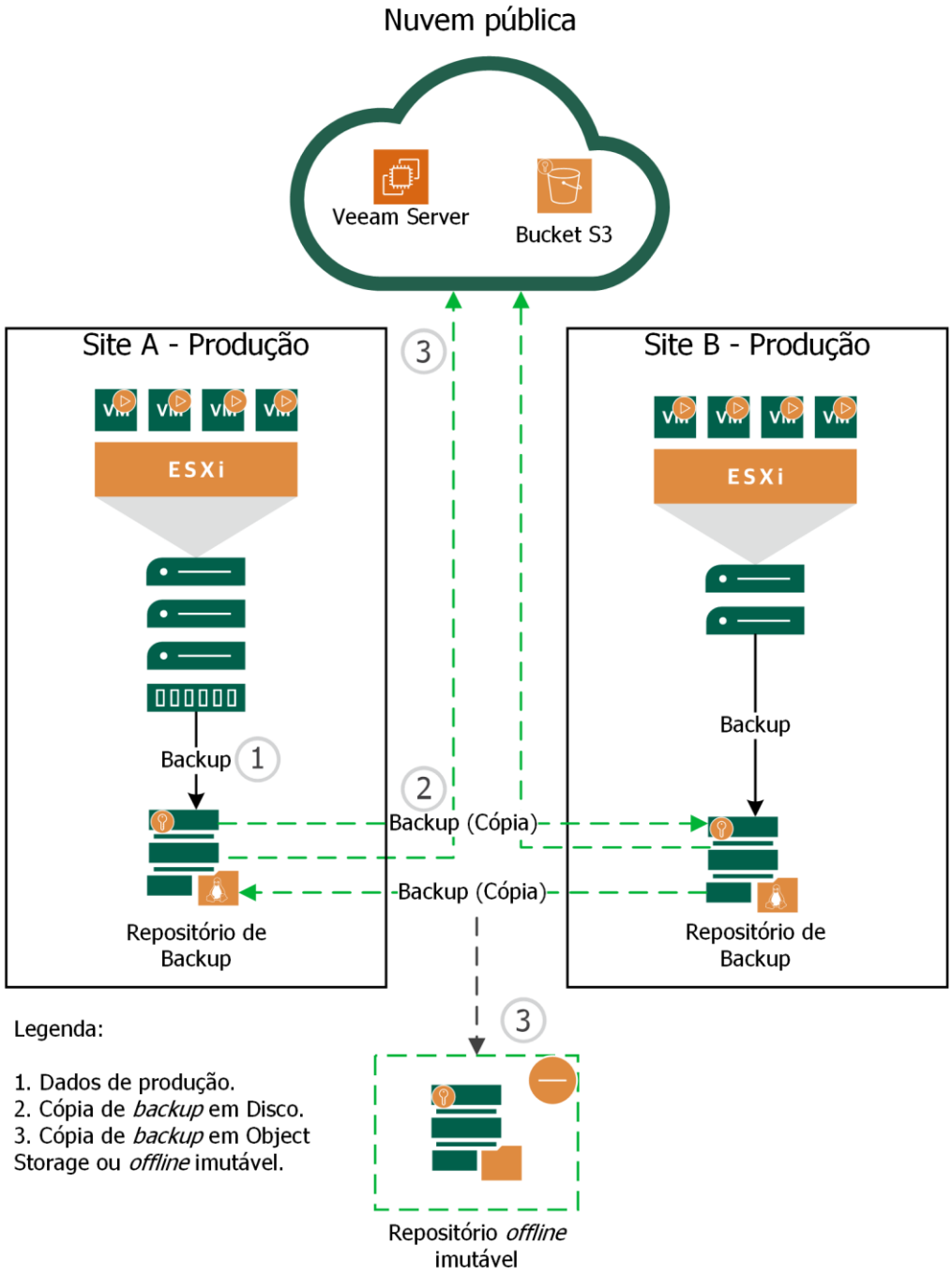
Fonte: Veeam (2024c).

Deste modo, foi possível arquitetar um ambiente robusto e seguro de *backup* dentro da Aviva, possibilitando não só a proteção eficiente dos dados armazenados, mas também a garantia de que tais dados estarão disponíveis de forma rápida em um cenário de desastre envolvendo perda de dados.

Além disso, usando como guia as normas da ABNT e o NIST CSF durante a implantação do ambiente de *backup*, foi possível elevar a maturidade e posicionamento de segurança da Aviva de forma considerável, fazendo com que os processos utilizados para armazenar cópias dos dados estejam congruentes com o que as normas recomendam no que tangem a disponibilidade, integridade e recuperabilidade dos dados.

A Figura 15 exibe um exemplo de arquitetura de *backup* desenhado para atender tais critérios, focando em recuperabilidade e redundância dos dados armazenados. A figura também demonstra a utilização de repositórios *offline* com imutabilidade ativa bem como um repositório de armazenamento de objetos, chamado de *bucket*, utilizando o serviço de armazenamento S3 da AWS.

Figura 15. Exemplo de arquitetura de *backup* resiliente utilizando Veeam Backup.



Fonte: o autor (2024).

2.4 Implantação de Ambiente de Recuperação de Desastres

De acordo com o NIST (2018), o plano de recuperação de desastres pode ser considerado uma série de procedimentos ou processos documentados que de forma organizada, determinam a ordem na qual as ações devem ser tomadas diante de um desastre de tecnologia a fim de restabelecer as operações.

Ainda segundo o NIST (2018), tal plano deve conter etapas que visam a identificação ou classificação de ameaças, tipos de respostas a ações, comunicação do incidente, testes de laboratório e relatórios executivos, desta forma alinhando-se à fase "Identificar" do CSF. Diante disso, uma organização deve desenvolver e manter atualizado, um plano para recuperação de desastres de seu ambiente, visando prevenir ou minimizar os impactos causados por um incidente grave de tecnologia, seja este desastre natural ou de ocorrência criminosa.

Como parte da estratégia de recuperação de desastres da Aviva, foi projetado um ambiente de *data center* secundário, onde utilizando ativos de *hardware* e *software* foi possível orquestrar um ambiente robusto pronto para agir em caso de um desastre em seu *data center* primário. Este ambiente visa garantir a compatibilidade com as normas ABNT ISO/IEC 27001 bem como o NIST CSF.

O *data center* secundário possui a mesma capacidade de processamento e armazenamento do *data center* principal, tendo como única diferença o estado de operação que os dados se encontram. Enquanto nos servidores principais ocorre toda a carga de processamento, os servidores secundários apenas recebem cópias periódicas dos dados originais, possibilitando uma menor perda de dados em caso de uma falha.

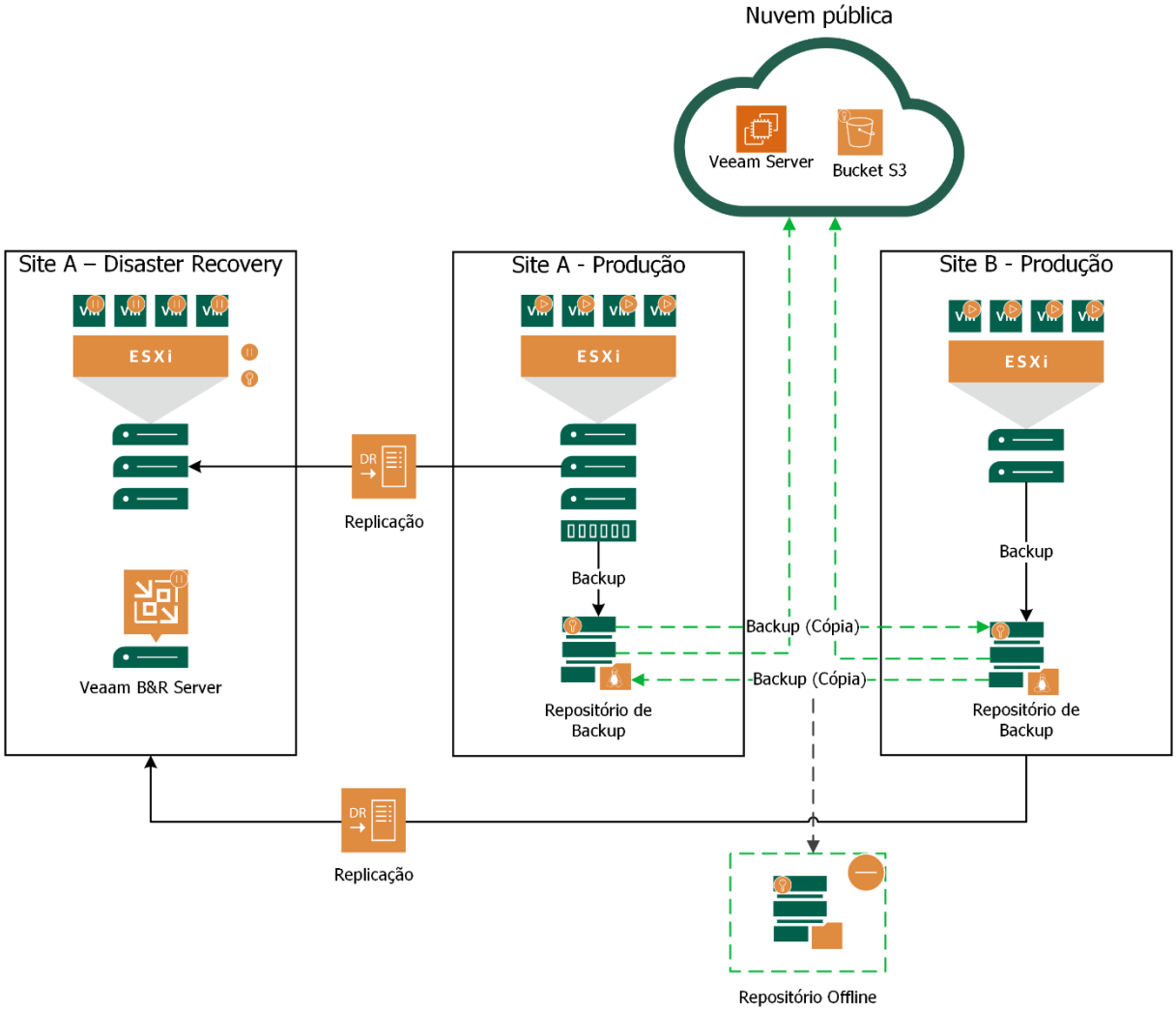
A replicação de dados foi implementada na Aviva utilizando a funcionalidade de replicação de máquinas virtuais do Veeam Backup, visando atingir a conformidade com o controle A.17.2.1 da ISO 27001 e das fases "Proteger" e "Recuperar" do NIST CSF.

A frequência entre as réplicas executadas entre o ambiente produtivo e o ambiente secundário, é definida em suma pela determinação dos indicadores de Objetivo de Ponto de Recuperação (da sigla em inglês RPO) e Objetivo de Tempo de Recuperação (da sigla em inglês RTO), onde se estipula a tolerância à perda de dados. Tal tolerância deve ser analisada e determinada levando em consideração o impacto ao negócio de uma organização causado por um desastre.

Utilizando as orientações do CSF do NIST e da ISO 27001, é possível desenhar um ambiente de recuperação de desastres seguro e eficiente, garantindo que a confiabilidade,

integridade e disponibilidade dos dados de uma empresa não seja comprometida, como é demonstrado na arquitetura de exemplo da Figura 16.

Figura 16. Exemplo de arquitetura de ambiente de recuperação de desastres com Veeam.



Fonte: o autor (2024).

Utilizando tecnologias robustas de infraestrutura de virtualização, como o VMware vSphere, e de replicação de máquinas virtuais, como o Veeam Backup & Replication, foi possível arquitetar um ambiente de recuperação de desastres robusto dentro da Aviva. A Figura 17 demonstra a frequência de réplicas executadas no ambiente da Aviva, mantendo um RPO constante dos dados replicados.

Figura 17. *Log* de frequência de réplicas executadas.

Job Name	Status	Start Time	End Time	Session Type
RQE-DR SLA 0H (Incremental)	61% completed	27/01/2024 17:01		Replication
RQE-DR SLA 4H (Incremental)	Success	27/01/2024 16:10	27/01/2024 16:28	Replication
RQE-DR SLA 2H (Incremental)	Success	27/01/2024 16:01	27/01/2024 16:37	Replication
RQE-DR SLA 0H (Incremental)	Success	27/01/2024 16:01	27/01/2024 16:27	Replication
RQE-DR SLA 4H - Fileserver (...	Success	27/01/2024 16:00	27/01/2024 16:18	Replication
RQE-DR SLA 2H (Incremental)	Success	27/01/2024 14:01	27/01/2024 14:14	Replication
RQE-DR SLA 0H (Incremental)	Success	27/01/2024 14:01	27/01/2024 15:49	Replication
RQE-DR SLA 0H (Incremental)	Success	27/01/2024 13:01	27/01/2024 13:31	Replication
RQE-DR SLA 4H (Incremental)	Success	27/01/2024 12:10	27/01/2024 12:37	Replication
RQE-DR SLA 2H (Incremental)	Success	27/01/2024 12:01	27/01/2024 12:19	Replication
RQE-DR SLA 0H (Incremental)	Success	27/01/2024 12:01	27/01/2024 12:24	Replication
RQE-DR SLA 4H - Fileserver (...	Success	27/01/2024 12:00	27/01/2024 12:29	Replication
RQE-DR SLA 0H (Incremental)	Success	27/01/2024 11:01	27/01/2024 11:41	Replication
RQE-DR SLA 2H (Incremental)	Success	27/01/2024 10:01	27/01/2024 10:15	Replication
RQE-DR SLA 0H (Incremental)	Success	27/01/2024 10:01	27/01/2024 10:36	Replication
RQE-DR SLA 0H (Incremental)	Success	27/01/2024 09:01	27/01/2024 09:22	Replication
RQE-DR SLA 4H (Incremental)	Success	27/01/2024 08:10	27/01/2024 08:27	Replication
RQE-DR SLA 2H (Incremental)	Success	27/01/2024 08:01	27/01/2024 08:19	Replication
RQE-DR SLA 0H (Incremental)	Success	27/01/2024 08:01	27/01/2024 08:26	Replication
RQE-DR SLA 4H - Fileserver (...	Success	27/01/2024 08:00	27/01/2024 08:25	Replication
RQE-DR SLA 4H (Incremental)	Success	27/01/2024 06:10	27/01/2024 06:54	Replication
RQE-DR SLA 2H (Incremental)	Success	27/01/2024 06:01	27/01/2024 06:48	Replication
RQE-DR SLA 0H (Incremental)	Success	27/01/2024 06:01	27/01/2024 07:25	Replication
RQE-DR SLA 4H - Fileserver (...	Success	27/01/2024 06:00	27/01/2024 06:56	Replication
RQE-DR SLA 24H (Increment...	Success	27/01/2024 02:40	27/01/2024 05:10	Replication
Moving RQE-CDS (Increment...	Success	27/01/2024 01:12	27/01/2024 01:46	Replication
Moving RQE-CDS_FileServer...	Success	27/01/2024 01:12	27/01/2024 01:39	Replication
Moving RQE-CDS_CM (Incre...	Success	27/01/2024 00:01	27/01/2024 05:17	Replication
RQE-DR SLA 0H (Incremental)	Success	26/01/2024 20:01	26/01/2024 21:06	Replication
RQE-DR SLA 0H (Incremental)	Success	26/01/2024 19:01	26/01/2024 19:20	Replication
RQE-DR SLA 0H (Incremental)	Success	26/01/2024 18:01	26/01/2024 18:30	Replication
RQE-DR SLA 4H (Incremental)	Success	26/01/2024 16:10	26/01/2024 16:35	Replication

Fonte: o autor (2024).

Tendo como objetivo cópias automáticas dos dados produtivos sendo executadas constantemente para um ambiente secundário, foi possível minimizar o possível impacto que pode ser causado por um desastre, uma vez que os dados replicados em baixa periodicidade possibilita a recuperação a um clique, reduzindo o esforço necessário para reestabelecer o ambiente e contendo o impacto nos processos operacionais e financeiros.

Ademais, tal ambiente de recuperação de desastres foi desenvolvido de forma a alinhar-se com as boas práticas e recomendações da ABNT ISO/IEC 27001 e do CSF do NIST, elevando o nível da postura de segurança da informação da Aviva, bem como adotando uma abordagem de gestão de riscos, objetivando a garantia da disponibilidade e integridade dos dados da empresa.

3 CONCLUSÃO

A infraestrutura por trás das aplicações que usamos diariamente está intrinsicamente conectada com a segurança da informação. Por meio do uso de normas, regulamentações e conjuntos de boas práticas, é possível elevar consideravelmente o nível de maturidade de segurança de uma empresa, transformando sua consciência e atitude perante os riscos, tornando-a capaz de responder às ameaças de forma proativa.

Normas como a ABNT NBR ISO/IEC 27001:2013 e práticas como o CSF do NIST, demonstram que a segurança da informação não envolve somente os processos e a cultura de uma empresa, sendo capazes de implementar práticas de segurança de alto nível desde a camada de infraestrutura de um *data center* até a simples conscientização de que um funcionário não deve compartilhar sua senha com outras pessoas. Se implementadas, essas normas possibilitam a arquitetura de ambientes robustos de infraestrutura que trazem não só a segurança administrativa e financeira de uma organização, mas também garantem que seu ativo mais precioso, os seus dados, estejam seguros e protegidos contra as ameaças de cibersegurança.

Deste modo, a grade curricular do curso de Tecnologia em Sistemas para Internet contribuiu majoritariamente para minha formação como profissional, proporcionando o sólido conhecimento necessário para meu crescimento. Em destaque, as disciplinas de Segurança da Informação e Redes de Computadores foram fundamentais em minha evolução de carreira, dando condições propícias para aprender e implementar as melhores práticas de segurança da informação existentes no mercado de tecnologia em meu local de trabalho.

Apesar das diferenças técnicas de minha carreira profissional em relação as matérias vistas em sala de aula, seu embasamento teórico foi o que me tornou capaz de me aprofundar em tópicos que não são vistos no dia a dia de um analista de infraestrutura. Conteúdos como gestão e padronização de projetos, redes, sistemas operacionais e segurança da informação, trouxeram fundamentos sólidos, que imprescindivelmente elevaram minha capacidade de elencar e elaborar soluções práticas em um ambiente profissional de trabalho.

Buscar metodologias, normas ou práticas de segurança da informação, deve ser parte do escopo de trabalho de todo analista de infraestrutura de tecnologia. É importante conhecer formas de criar arquiteturas e ambientes que estejam protegidos desde seu alicerce. Isso não só contribui para soluções robustas em uma empresa, como também para o crescimento do profissional de tecnologia.

REFERÊNCIAS

ABNT. **NBR ISO/IEC 27001:2013**: tecnologia da informação - técnicas de segurança - sistemas de gestão da segurança da informação - requisitos. Rio de Janeiro: [*s. n.*], 2013.

ÁVILA, Rafael. **[Ciclo PDCA**: o que é e como usar para ganhar performance? - Blog LUZ]. 2 jun. 2014. Imagem. Disponível em: https://blog.luz.vc/o-que-e/ciclo-pdca/. Acesso em: 9 dez. 2023.

BEAL, Adriana. **Segurança da informação. princípios e melhores práticas para a proteção dos ativos de informação nas organizações**. São Paulo: Atlas, 2005. 176 p.

CISA. **What is cybersecurity?** 2024. Disponível em: https://www.cisa.gov/news-events/news/what-cybersecurity. Acesso em: 18 fev. 2024.

IBM. **O que é o NIST cybersecurity framework?** 2024. Disponível em: https://www.ibm.com/br-pt/topics/nist. Acesso em: 18 fev. 2024.

ISO. **ISO/IEC 27000:2018**: information tecnology - security techniques - information security management systems - overview and vocabulary. Genebra, Suíça: [*s. n.*], 2018.

LEAN ENTERPRISE INSTITUTE. **Plan, do, check, act (PDCA) — A resource guide**. 2024. Disponível em: https://www.lean.org/lexicon-terms/pdca/. Acesso em: 18 fev. 2024.

NIST. **NIST CSF**: framework for improving critical infrastructure cybersecurity. Gaithersburg, Estados Unidos: [*s. n.*], 2018. Disponível em: https://doi.org/10.6028/NIST.CSWP.04162018. Acesso em: 15 dez. 2023.

SOPHOS. **Ransomware recovery cost reaches nearly $2 million, more than doubling in a year, sophos survey shows**. 2021. Disponível em: https://www.sophos.com/en-us/press/press-releases/2021/04/ransomware-recovery-cost-reaches-nearly-dollar-2-million-more-than-doubling-in-a-year. Acesso em: 13 out. 2023.

VEEAM. **[Backup copy - user guide for vmware vsphere]**. 2024a. Imagem. Disponível em: https://helpcenter.veeam.com/docs/backup/vsphere/backup_copy.html?ver=120. Acesso em: 10 jan. 2024.

VEEAM. **[Backup job encryption - user guide for vmware vsphere]**. 2024b. Imagem. Disponível em: https://helpcenter.veeam.com/docs/backup/vsphere/encryption_backup_job.html?ver=120. Acesso em: 17 jan. 2024.

VEEAM. **Encryption**. 2023a. Disponível em: https://bp.veeam.com/security/Design-and-implementation/Encryption.html. Acesso em: 22 set. 2023.

VEEAM. **Protect**. 2023b. Disponível em: https://bp.veeam.com/security/Design-and-implementation/Protect.html. Acesso em: 22 set. 2023.

VEEAM. **[Step 4. configure hardened repository settings - user guide for vmware vsphere]**. 2024c. Imagem. Disponível em: https://helpcenter.veeam.com/docs/backup/vsphere/hardened_repo_configure_settings.html. Acesso em: 18 jan. 2024.

ANEXOS

D E C L A R A Ç Ã O

Declaramos para os devidos fins que se fizerem necessários que o(a) Sr(a). **GIOVANI GAZZI PAGANINI**, portador(a) da carteira de identidade sob o nº **7374116/PC-GO** e CPF sob o nº **091.543.219-64**, é nosso(a) associado(a) na empresa **COMPANHIA THERMAS DO RIO QUENTE**, inscrita sob o CNPJ **01.540.533/0001-29**, admitido(a) em **15/01/2018**, exercendo atualmente a função de **ANALISTA DE INFRAESTRUTURA PL**.

Tendo como principais atividades vinculadas a sua função:

Responsável pela implantação, manutenção, monitoramento e segurança de TI em todos os ativos de hardware e software como computadores, servidores, switches, access points, sistemas, entre outros de toda a companhia, garantindo a disponibilidade, confidencialidade e integridade destes ativos para que os demais colaboradores atinjam e otimizem os objetivos da empresa.

Por ser verdade, firmamos a presente.

COMPANHIA THERMAS DO RIO QUENTE

Rio Quente – GO, 21 de março de 2024.

Carteira de Trabalho Digital

Dados Pessoais

Data de emissão: **10/05/2020**

Nome Civil: **GIOVANI GAZZI PAGANINI**
CPF: [redacted]
Data de Nascimento: [redacted]

Contratos de Trabalho

- 15/01/2018 - Aberto

COMPANHIA THERMAS DO RIO QUENTE
CNPJ RAIZ: 01.540.533
Endereço: **R PA COMPLEXO TURISTICO RIO QUENTE RESORTS SN**
Ocupação **212405 - ANALISTA DE DESENVOLVIMENTO DE SISTEMAS**
Tipo de contrato: **Prazo indeterminado**
Tipo de admissão: **Admissão**
Salário contratual: [redacted]
Remuneração inicial: [redacted]
Última remuneração informada: [redacted] (03/2024)
Relação de trabalho: **Empregado**
Fonte da informação: **ESOCIAL**
Anotações:

26/01/2024 - Salário definido para [redacted]
08/03/2023 - Salário definido para [redacted]
08/03/2023 - Ocupação alterada para ANALISTA DE DESENVOLVIMENTO DE SISTEMAS
07/03/2023 - Salário definido para [redacted]
07/03/2023 - Ocupação alterada para ANALISTA DE SUPORTE COMPUTACIONAL
01/08/2022 - Férias de 30 dia(s) com previsão de encerramento em 30/08/2022
01/01/2022 - Salário definido para [redacted]
01/01/2022 - Ocupação alterada para ANALISTA DE DESENVOLVIMENTO DE SISTEMAS
01/07/2021 - Salário definido para [redacted]
03/05/2021 - Férias de 30 dia(s) com previsão de encerramento em 01/06/2021
01/05/2021 - Salário definido para [redacted]
01/03/2021 - Salário definido para [redacted]
01/12/2020 - Férias de 30 dia(s) com previsão de encerramento em 30/12/2020
01/10/2020 - Salário definido para [redacted]
01/07/2020 - Salário definido para [redacted]