FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI

Curso Superior de Tecnologia em Segurança da Informação

Davi Rodrigues Galvão

Diagnóstico de maturidade de Segurança da Informação baseado nos controles do CIS Controls V8

Americana, SP

2023

FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI

Curso Superior de Tecnologia em Segurança da Informação

Davi Rodrigues Galvão

Diagnóstico de maturidade de Segurança da Informação baseado nos controles do CIS Controls V8

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Me. Edson Roberto Gaseta

Área de concentração: Segurança da Informação.

Americana, SP.

2023

Relatório Técnico

Diagnóstico de maturidade de Segurança da Informação baseado nos controles do CIS Controls V8

Elaborador:	Davi Rodrigues Galvão
Orientador:	Prof. Edson Roberto Gaseta

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana Ministro Ralph Biasi-CEETEPS Dados Internacionais de Catalogação-na-fonte

GALVÃO, Davi Rodrigues

Diagnóstico de maturidade de segurança da informação baseado nos controles do CIS Controls V8. / Davi Rodrigues Galvão – Americana, 2023.

40f.

Relatório técnico (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana Ministro Ralph Biasi – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Edson Roberto Gaseta

1. Segurança em sistemas de informação. I. GALVÃO, Davi Rodrigues II. GASETA, Edson Roberto III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 681.518.5

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

DAVI RODRIGUES GALVÃO

DIAGNÓSTICO DE MATURIDADE DE SEGURANÇA DA INFORMÇÃO BASEADO NOS CONTROLES DO CIS CONTROLS V8

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/Americana.

Área de concentração: Segurança da Informação.

Americana, 15 de junho de 2023.

Banca Examinadora:

Edson Roberto Gaseta (Presidente)
Mestre
Fatec Americana

Rodrigo Brito Battilana (Membro)
Mestre
Fatec Americana

Maxwel Vitorino da Silva (Membro)
Mestre
Fatec Americana

Abreviaturas e Siglas

(CIS) – *Center of Internet Security* (Centro de Segurança da Internet)

(CIS Controls V8) – Controles CIS Versão 8(do inglês, *Center Of Internet Security Controls Version 8)*

(DNS) – Sistema de nome de domínio (do inglês, *Domain Name System*)

(EUA) – Estados Unidos da América

(IoT) – Internet das Coisas (do inglês, *Internet of Things)*

(MFA) – Autenticação multifator (do inglês, *Multi-factor authentication*)

(SI) – Segurança da Informação

(SO) – Sistema Operacional

(TI) – Tecnologia da Informação

SUMÁRIO

1 Introdução

Este relatório tem o objetivo de apresentar como uma empresa pode avaliar seu nível de maturidade com os controles de Segurança da Informação (SI), buscando se posicionar bem no mercado demonstrando estar apta a lidar com a tratativa não só de proteção de dados, mas de incidentes que estão relacionados a SI, tendo em vista que na atualidade uma empresa que não está em conformidade com pelo menos um dos diversos *frameworks* de segurança cibernética dificilmente consegue suportar seus processos de negócios em um mercado cada vez mais exigente relativo em como seus dados serão tratados e assegurados.

Vivemos atualmente em um mundo totalmente conectado e tecnológico, onde um ecossistema de Tecnologia da Informação (TI) é altamente diversificado, manipulando diversos tipos de dados simultaneamente por vários indivíduos. Com a crescente utilização dos equipamentos de TI, aumenta-se a necessidade por políticas e controles para garantir a produtividade da organização e da saúde operacional dos ativos, mantendo os Pilares da Segurança da Informação que são: Integridade, Confidencialidade e Disponibilidade. Uma vez que um dos pilares não esteja protegido por controles, há possivelmente danos e perdas, tendo em vista que não é uma questão de “Se acontecer” e sim de “Quando acontecer” é necessário saber lidar com incidentes e crises, a fim de mitigar os prejuízos, para isso os controles de Segurança da Informação (SI) são vitais.

As áreas de conhecimento que contribuem para a confecção deste relatório são principalmente Gestão de Segurança da Informação, Políticas de Segurança da Informação e Auditoria de Segurança da Informação, conhecimento este assimilado na FATEC de Americana.

Uma vez que os controles são implementados, monitorá-los e mantê-los se torna imperativo, garantindo que os controles estejam em conformidade com as leis do país em que ativos de informação estão instalados, atualizados e de fato praticados por todos aqueles responsáveis em segui-los, tornando-se uma tarefa árdua, e caso não seja feito de forma periódica uma revisão dos processos e da maturidade da equipe responsável, isso ocasiona no aumento das brechas resultantes em incidentes.

2 Desenvolvimento

Para o desenvolvimento deste relatório foi realizado uma avaliação de maturidade de uma empresa de pequeno porte, que se enquadra no grupo de implementação um (IG1) do *framework CIS Controls V8* e seus respectivos controles, que tem por finalidade ser o ponto de partida da empresa na gestão de SI, entendendo melhor o quão em conformidade ela está com os parâmetros de Segurança da Informação básicos.

Foi realizada uma entrevista com a equipe de TI responsável pelos controles de segurança cibernética de uma pequena empresa da Região de Campinas conhecida como Center Tech, essa pequena empresa se enquadra no IG1 do CIS Controls V8 e atua no ramo de soluções Tecnológicas, sendo os colaboradores Israel da Mata e Roberto Junior, verificando os controles implementados e os não implementados, permitindo a análise da maturidade atual da empresa e então possibilitando uma proposta de melhoria (PM) na implementação dos controles.

2.1 Organização CIS

Conforme a (MICROSOFT**,** 2023) a CIS é uma entidade sem fins lucrativos, com a missão de identificar, desenvolver, validar, promover e manter soluções de boas práticas para a defesa cibernética. Recorrendo à experiência de profissionais de segurança cibernética e de TI de instituições governamentais, empresariais e acadêmicas de todo o mundo, buscando desenvolver padrões e práticas recomendadas, onde até as imagens protegidas, os controles e os parâmetros da CIS seguem um modelo de tomada de decisão por consenso.

Complementando, a CIS está presente no mercado desde os anos 2000, inicialmente composta por um pequeno grupo de empresas e líderes governamentais que se reuniam no Clube Cosmos (do inglês, "*Cosmos Club"*) em Washington. Com a evolução da internet e da tecnologia, a organização foi atraindo profissionais de TI e de segurança cibernética, aumentando sua capacidade e atividade, tornando-a reconhecida mundialmente por seus esforços em desenvolver padrões de boas práticas como o CIS Controls (CIS, 2021).

2.2 Controles CIS V8

Segundo (GAT, 2021) os Controles CIS V8 são um conjunto prioritário e prescritivo de práticas recomendadas de segurança cibernética e ações defensivas que podem ajudar a prevenir os ataques mais generalizados e perigosos, dando suporte à conformidade em uma era de múltiplas estruturas.

Atualmente na versão oito, trata-se de uma publicação de diretrizes e práticas recomendadas para segurança de computadores, que é constantemente atualizada e revisada, tendo início em 2008 em resposta a perdas extremas de dados ocorridas em organização na base industrial de defesa dos EUA.

A publicação foi inicialmente desenvolvida pelo *SANS Institute,* cuja publicação era conhecida como *SANS Top 20* e em 2013 a propriedade foi transferida para o Conselho de Segurança Cibernética (CCS) para finalmente ser transferido em 2015 para a CIS (OSTEC, 2022).

Os controles CIS V8 são compostos atualmente por 18 controles, distribuídos em 156 salvaguardas bem definidos. Segundo a (GAT, 2021) cada controle é amplo em escopo, mas se alinha com princípios sólidos, tais como garantir que os usuários certos tenham acesso aos ativos certos.

O princípio do *CIS Controls* é mapear os controles assim também mapeando requisitos de diversos frameworks que estão inseridos no mercado, tais como ISO27001, CSA ou PCI-DSS, NIST etc., não os substituindo, mas sim, preparando a empresa alvo para estes *frameworks* que visam controles específicos (FERREIRA, 2023)

Há três grupos de implementação sendo eles nomeados como IG1, IG2 e IG3, cada um abrange uma gama de salvaguardas e para compreender melhor cada grupo conforme (GAT, 2021) explica os três sendo, o IG1 sendo adequado para organizações com recursos limitados, o IG2 adequado a organizações que possuem uma recursos moderados e o IG3 é adequado às organizações que têm muitos recursos investidos em segurança cibernética.

O primeiro grupo de implementação, nomeado IG1, possui 56 salvaguardas que asseguram a defesa cibernética de qualquer empresa contra os ataques mais comuns, este grupo de implementação é definido pela CIS como como higiene cibernética básica representando um padrão mínimo emergente de segurança da informação para todas as empresas

A segunda categoria, nomeada IG2, aborda as 56 salvaguardas do IG1 mais 74 salvaguardas, totalizando 130 salvaguardas, sendo que uma empresa apta a

implementar o IG2 normalmente já possui diversos departamentos e possui uma equipe que suporta esses departamentos e já conseguem resistir a curtas interrupções de um serviço, tendo em seu foco de preocupação na perda de confiança do público caso ocorram violações.

A última categoria é a que aborda todos os salvaguardas do IG1, somando os do IG2 e adicionalmente tem mais 23 salvaguardas, totalizando 153 salvaguardas, a categoria IG3 é voltada para organizações maduras que possuem recursos dedicados à segurança cibernética e estão altamente expostos a riscos, lidando com ativos críticos e dados sigilosos em grande volume, os objetivos dos salvaguardas voltados para este grupo são diminuir ataques de um adversário interessado na organização e reduzir os impactos de ataques do tipo "***zero-day***".

Fica claro a importância dos controles CIS no mercado, seus controles são categorizados e podem se encaixar em qualquer empresa que deseja mapear seus controles e identificar sua maturidade e pontos de melhoria, considerando os esforços em utilizar esta ferramenta que abre portas para conseguir lidar com quaisquer que sejam os auditores, visto que é uma ferramenta mundialmente reconhecida, utilizada e sempre está em atualização.

2.3 Ambiente

O ambiente utilizado para o relatório foi uma empresa pequena que consiste em cinco colaboradores, com recursos limitados para realizar investimentos em defesa cibernética, todavia é uma empresa que está buscando amadurecer para conquistar mais espaço no mercado, entretanto a barreira é conhecer os controles que já possuem que podem estar em conformidade e quais precisam ser implementados.

A colaboração entre seus colaboradores é vital para que os controles sejam implementados efetivamente, será realizado uma entrevista com o colaborador responsável pela infraestrutura de TI interna que está buscando amadurecer seus conhecimentos e a empresa com estes controles.

2.4 Processo de diagnóstico

A entrevista realizada com o colaborador foi pautada nos dezoito controles do CIS V8 que visam a higiene cibernética básica, agindo não como uma verdade absoluta e garantindo a segurança cibernética da empresa e sua conformidade com as leis e o mercado, mas sim, ser o ponto de partida para que a empresa olhe com mais criticidade, buscando por outros frameworks para complementar esses controles e

gradativamente expandir sua segurança, agregando valor à empresa e trazendo confiança ao seu público.

O primeiro controle a ser abordado fala sobre inventário e controle de ativos da empresa, cujo objetivo é verificar e garantir que empresa está gerenciando ativamente todos os ativos corporativos (tais como dispositivos de usuário final, tanto os portáteis como os móveis, dispositivos de rede e aqueles não informáticos, *IoT* e servidores) conectados à infraestrutura fisicamente, virtualmente, remotamente e aqueles em ambiente de nuvem, para saber com precisão a totalidade de ativos que precisam ser monitorados e protegidos dentro da empresa. Isso apoiará também a identificação de ativos não autorizados e não gerenciados para remover ou corrigir.

As observações que sustentam a avaliação são que o inventário é realizado de forma manual com a utilização de controle de planilha, que pode causar falha no gerenciamento do inventário e não há mapeamento dos dispositivos para identificar os não autorizados e corrigi-los ou removê-los. A tabela 1 mostra as informações levantadas do controle

Tabela 1 – Informações do controle Inventário e controle de ativos da empresa

Inventário e controle de ativos da empresa	
Estabelecer e manter um inventário detalhado de ativos da empresa	O inventário de ativos é baseado em planilha, onde consta a informação de cada ativo, mas não é atualizado com a frequência determinada no controle.
Endereçar ativos não autorizados	Não há processo para identificação de ativos não autorizados e não há varredura interna para identificá-los.

O segundo controle a ser abordado fala sobre o Inventário e controle de ativos de software, com o objetivo de garantir que a empresa gerencie ativamente, inventariando, rastreando e corrigindo todos os softwares, tais como sistemas operacionais e aplicações, que estejam na rede, assegurando que apenas *softwares* autorizados sejam instalados e executados, quanto aos não autorizados e não gerenciados que sejam encontrados de forma a impedir sua instalação e execução.

As observações que sustentam o controle é que a empresa não possui uma relação que possa servir de inventário de *softwares,* podendo causar falhas no gerenciamento dos softwares e na identificação de aplicativos não autorizados. A tabela 2 mostra as informações levantadas do controle

Tabela 2 – Informações do controle Inventário e controle de ativos de software

Inventário e controle de ativos de software	
Estabelecer e manter um inventário de software	Não é realizado um inventário dos softwares licenciados e autorizados pela empresa.
Certificar-se de que o software autorizado seja atualmente suportado	Por não haver um controle rígido das atualizações, os softwares utilizados são sempre atualizados conforme é notificado pelo software.
Endereçar a software não autorizado	Quando identificado um software indevido este é removido, mas não há um mapeamento para identificar em cada ativo quais softwares estão instalados.

O terceiro controle aborda a proteção de dados com o objetivo de desenvolver processos e controles técnicos que visam identificar, classificar, manusear, reter e descartar dados com segurança, auxiliando na criação do mapa do ciclo de vida dos dados na organização.

As observações que sustentam a avaliação são que a empresa no momento não possui um processo para gerir os dados, o que pode causar prejuízos inestimáveis já que não há uma proteção dos dados ou categorização de sua sensibilidade dificultando a percepção dos dados que precisam de uma proteção adequada. As informações levantadas estão apresentadas na tabela 3 abaixo:

Tabela 3 – Informações do controle Proteção de dados

Proteção de dados	
Estabelecer e manter um processo de gerenciamento de dados	Não há um processo de gerenciamento de dados, ao ser discutido sobre o assunto, os integrantes não sabem como começar a desenhar o processo ou quem procurar para prover auxílio.
Estabelecer e manter um inventário de dados	Não há um inventário de dados, nem critério sobre a sensibilidade dos dados, dificultando o inventário deles.
Configurar listas de controle de acesso a dados	O acesso ao sistema que é onde se sabe que tem dados sensíveis é configurado de acordo com a necessidade do usuário, o privilégio de alteração nos equipamentos e sistemas operacionais só é concedido aos técnicos líderes.
Aplicar retenção de dados	Não há um período de retenção de dados definido, raramente um dado é excluído e não houve solicitações para exclusão de dados, durante o período de vida da empresa.
Descartar dados com segurança	O descarte feito pelo sistema em nuvem é feito através de um botão de exclusão, sem ciência de se o dado foi efetivamente excluído, o descarte de dados digitais nos equipamentos é feito através de formatação simples.
Criptografar dados em dispositivos de usuário final	A criptografia BitLocker® é desabilitada nos equipamentos dos usuários finais para não prejudicar a produtividade.

O quarto controle aborda a configuração segura de ativos corporativos e software, com o objetivo de encorajar a empresa a estabelecer e manter uma configuração segura dos ativos corporativos, tantos os dispositivos de usuário final, como dispositivos de rede, aqueles não informáticos/IoT e servidores como também softwares, sejam eles Sistemas Operacionais ou aplicativos.

As observações que sustentam a avaliação deste controle são que a configuração segura é feita parcialmente nos ativos corporativos possibilitando acessos não autorizados em momentos de desuso. A falta de um firewall implementado pode permitir tráfego de dados maliciosos, comprometendo a segurança da infraestrutura de rede, a falta de documentação dos processos dificulta identificar os pontos a serem fortalecidos, sendo necessário revisar completamente o assunto toda vez que este é discutido. A falta de gerenciamento dos protocolos possibilita a invasão visto que não há um conhecimento de todos os protocolos utilizados podendo estes serem usados

para extraviar dados por alguém mal-intencionado. A tabela 4 apresenta as informações levantadas:

Tabela 4 – Informações do controle Configuração segura de ativos corporativos e software

Configuração segura de ativos corporativos e software	
Estabelecer e manter um processo de configuração seguro	Não há documentação do processo, apenas a prática parcial, feita em desktops e notebooks corporativos, limitando os privilégios administrativos dos usuários utilizados nos Sistemas Operacionais.
Estabelecer e manter um processo de configuração seguro para infraestrutura de rede	Não há documentação do processo, a empresa por ser pequena ainda não utiliza firewall dedicado, utilizando apenas o firewall do próprio roteador do provedor de internet e neste é pouco confiado.
Configurar o bloqueio automático de sessão em ativos corporativos	O bloqueio automático não é configurado nos desktops e notebooks, e os usuários sem privilégio não possuem senhas configuradas. Nos dispositivos portáteis há um PIN configurado e bloqueio automático após 1 minuto.
Implementar e gerenciar um firewall em servidores	Nos servidores apenas o firewall nativo do Sistemas Operacional está ativo e minimamente configurado, de forma a não estar garantido a sua efetividade.
Implementar e gerenciar um firewall em dispositivos de usuário final	Não há bloqueio na navegação na empresa e não está implementado um firewall para filtragem de portas em usuários finais, há apenas uma filtragem de DNS no firewall do roteador do provedor de internet.
Gerenciar com segurança ativos corporativos e software	Não é gerenciado os serviços de portas, por regra do firewall nativo em todos os sistemas operacionais o uso de portas inseguras, como HTTP e Telnet, é bloqueado.
Gerenciar contas padrão em ativos corporativos e software	As contas padrões são desabilitadas sempre que possível e é alterado a senha para evitar o acesso não autorizado, todas as contas de software e usuário estão catalogadas em um aplicativo externo, onde somente duas pessoas possuem acesso, o fundador da empresa e o líder técnico.

O quinto controle aborda a Gestão de contas, com o objetivo de estabelecer processos e o uso de ferramentas para atribuir e gerenciar autorização para

credenciais em contas de usuário, incluindo contas de administrador e serviços, para ativos corporativos e software.

As observações que sustentam a avaliação deste controle são sobre a utilização de uma autenticação única com o uso de senhas não recomendadas, o que prejudica em via dupla a segurança, a falta de uma autenticação multifator facilita muito o acesso não autorizado visto que basta as credenciais de acesso para obter informações pessoais e sensíveis, não há restrições implementadas para eficientemente dificultar o acesso não autorizado aos dados ou navegação na internet. A tabela 5 apresenta as informações levantadas:

Tabela 5 – Informações do controle Gestão de Contas

Gestão de Contas	
Estabelecer e manter um inventário de contas	Por não utilizar domínio o inventário de contas é feito em aplicativo externo, onde se mantém contas de usuário, *e-mail* e contas de administrador.
Usar senhas exclusivas	Não há nenhum método MFA implementado e as senhas possuem no máximo 10 caracteres.
Desativar contas inativas	Equipe composta por poucos colaboradores sem alta rotatividade, os colaboradores desligados têm sua conta desativada e os *e-mail*s de uso geral tem sua senha alterada.
Restringir privilégios de administrador a contas de administrador dedicadas	Não há meios implementados para restrição de privilégios, as contas de AD, estão habilitadas e com senha segura, cada máquina possui uma senha de administrador local diferente. Para *e-mail* nenhum usuário possui privilégio, há um usuário administrador próprio para o painel de *e-mail*, não há autenticação para navegação na internet.

O sexto controle aborda o gerenciamento de controle de acesso, encorajando a empresa a fazer uso de processos e ferramentas para criação, atribuição, gerenciamento e revogação de credenciais de acessos e privilégios para contas de usuário comum, administrador e serviços para os ativos e softwares corporativos.

As observações que sustentam a avaliação deste controle são que o controle de acesso é feito manualmente, ocasionando falhas na atribuição e revogação das permissões, a não implementação do MFA nos demais controles apresentados que apesar de não conforme é porque os controles não se aplicam. A tabela 6 apresenta as informações levantadas sobre o controle:

Tabela 6 – Informações do controle gerenciamento de controle de acesso

Gerenciamento de controle de acesso	
Estabelecer um processo de concessão de acesso	Não há um processo ou documentação que mostre como é feito a concessão de acesso a novos colaboradores
Estabelecer um processo de revogação de acesso	Não há um processo para revogação dos acessos
Exigir MFA para aplicativos expostos externamente	Não há exigência de MFA implementada.
Exigir MFA para acesso remoto à rede	Não é feito acesso remoto à rede.
Exigir MFA para acesso administrativo	Não há exigência de MFA implementada.

O sétimo controle aborda o gerenciamento contínuo de vulnerabilidade, com o objetivo de encorajar a empresa a desenvolver um plano para avaliar e rastrear vulnerabilidades de forma contínua em todos seus ativos corporativos internos, visando remediar e minimizar as janelas de oportunidade para os invasores e constantemente monitorar as fontes da indústria tanto a pública quanto a privada para novas informações sobre ameaças e vulnerabilidades.

As observações que sustentam a avaliação deste controle são sobre a falta de uma documentação sobre os riscos aceitos acerca das vulnerabilidades não corrigidas, e a falta de uma ferramenta para automação da aplicação de patches de forma estável tanto para sistemas operacionais quanto para *softwares*. A tabela 7 apresenta as informações levantadas sobre o controle:

Tabela 7 – Informações do controle gerenciamento contínuo de vulnerabilidade

Gerenciamento contínuo de vulnerabilidade	
Estabelecer e manter um processo de gerenciamento de vulnerabilidade	Com a descoberta de uma vulnerabilidade, há ciência da equipe técnica, mas não é documentado a tratativa ou a ciência caso o risco seja aceito
Estabelecer e manter um processo de remediação	Há antivírus para proteção básica, *backup* em nuvem para recuperação de dados, mas não há uma estratégia para continuidade em casos de incidentes, apenas agindo corretivamente em casos de incidentes.
Executar um gerenciamento automatizado de patches do sistema operacional	As atualizações são feitas de forma automática pelo sistema apenas notificando a reinicialização do sistema para aplicação dos patches que é feita manualmente.
Executar o gerenciamento automatizado de patches de aplicativos	Os aplicativos utilizados são configurados para exibirem notificações assim que uma atualização é liberada a qual é aplicada o quanto antes.

O oitavo controle aborda o gerenciamento de registro de auditoria com o objetivo de coletar, alertar, analisar e reter logs de auditoria de eventos que podem ajudar a detectar, compreender ou recuperar-se de um ataque.

As observações que sustentam a avaliação deste controle são que a falta de centralização dos logs e de uma ferramenta especializada para análise deles há dificuldade da equipe técnica em compreender incidentes, dificultando a prevenção de ataques e limitando a visão da equipe em como assegurar a produtividade contínua da equipe. A tabela 8 apresenta as informações levantadas do controle:

Tabela 8 – Informações do controle de gerenciamento de registro de auditoria

Gerenciamento de registro de auditoria	
Estabelecer e manter um processo de gerenciamento de registro de auditoria	Não há um processo de gerenciamento de registro de auditoria estabelecido nem documentado, a ideia já foi discutida, mas não houve ação tomada.
Coletar registros de auditoria	Os logs são configurados por padrão e salvos no diretório padrão pelo Sistema Operacional de cada ativo corporativo, quando necessário é utilizado o Visualizador de eventos do SO para analisá-los.
Garantir o armazenamento adequado de registros de auditoria	Os logs, salvos no diretório padrão, não fazem parte da rotina de *backup* e ficam localmente em cada ativo, não havendo garantia de que estão seguros de acesso não autorizado.

O nono controle aborda as proteções de *e-mail* e navegador da *web* buscando auxiliar a empresa a melhorar as proteções e detecções de ameaças provindas de *e-mails* e da *web*, pois são os meios que os invasores mais obtêm oportunidades para manipularem o comportamento humano por meio do engajamento direto.

As observações que sustentam a avaliação do controle apresentam que a falta de um serviço dedicado e conhecido à filtragem de DNS podem comprometer a navegação segura. A tabela 9 apresenta as informações levantadas do controle:

Tabela 9 – Informações do controle proteções de *e-mail* e navegador da *web*

Proteções de *e-mail* e navegador da *web*	
Garantir o uso apenas de navegadores e clientes de *e-mail* com suporte total	O cliente de *e-mail* utilizado é o Outlook da Microsoft e navegadores usados são Edge, Firefox e Chrome que recebem atualizações com frequência.
Usar serviços de filtragem de DNS	A filtragem de DNS ocorre pelo provedor de internet, configurado de forma estática no roteador fornecido por ele.

O décimo controle aborda a defesa contra *malware*s, com o objetivo de impedir ou controlar a instalação, disseminação e execução de aplicativos, códigos ou scripts maliciosos em ativos corporativos.

As observações que sustentam a avaliação deste controle são que a utilização do *anti-malware* nativo do sistema operacional, não centraliza a análise de ações e coleta de dados, gerando um ecossistema diverso de *anti-malwares* dificultando a tomada de ação em caso de incidentes, visto que as informações podem ser divergentes. A tabela 10 apresenta as informações levantadas sobre o controle:

Tabela 10 – Informações do controle defesas contra *malware*

Defesas contra *malware*	
Implantar e manter um *software anti-malware*	É utilizado o *anti-malware* nativo do sistema operacional, sendo distinto para cada tipo de ativo, dispositivos com SO Android utilizam o nativo caso haja, equipamentos com Windows utilizam o Defender que é nativo do SO.
Configurar atualizações automáticas de assinatura *anti-malware*	Sempre que o *anti-malware* notifica atualizações disponíveis no mesmo dia é realizado e aplicado as atualizações, quando necessário a reinicialização do SO, este é realizado no período de descanso do colaborador de forma manual ou caso o sistema operacional esteja ligado após o expediente de forma automatizada.
Desativar a execução automática e reprodução automática para mídias removíveis	Por padrão é desabilitado manualmente a execução e reprodução de mídias removíveis em todos os ativos corporativos.

O décimo primeiro controle aborda a recuperação de dados, encorajando a empresa a estabelecer e manter as boas práticas de recuperação de dados que sejam suficientes para restaurar ativos dentro do escopo para um estado pré-incidente e confiável.

As observações que sustentam a avaliação do controle são que o processo está implementado, mas necessita estar documentado, para que este processo possa ser revisado a fim de identificar e definir com mais clareza a criticidade dos dados a serem recuperados e a segurança dos dados de *backup*. A tabela 11 apresenta as informações levantadas sobre o controle:

Tabela 11 – Informações do controle de recuperação de dados

Recuperação de dados	
Estabelecer e manter um processo de recuperação de dados	Há um processo implementado para recuperação de dados, mas não está documentado
Executar *backups* automatizados	Os *backups* são feitos através de um *software*, de forma automatizada, os arquivos no servidor são feitos diariamente e nos demais de forma semanal.
Proteger os dados de recuperação	Os dados de recuperação são encriptados pelo *software* de *backup.*

Estabelecer e manter uma instância isolada de dados de recuperação	Por ser na nuvem os dados de recuperação estão em uma instância isolada, sendo feita por versão, mantendo-se 5 instâncias de dados armazenados em cada ativo e 15 versões dos dados armazenados no servidor.

O décimo segundo controle aborda o gerenciamento de infraestrutura de rede encorajando a empresa a estabelecer, implementar e gerenciar ativamente os dispositivos de rede, objetivando evitar que invasores explorem serviços de rede e pontos de acesso vulneráveis.

A observação que sustenta a avaliação deste controle são o uso de equipamentos de rede obsoletos e/ou domésticos, que recebem poucas atualizações, comprometendo a segurança da infraestrutura de rede e seus serviços. A tabela 12 apresenta as informações levantadas sobre o controle:

Tabela 12 – Informações do controle gerenciamento da infraestrutura de rede

Gerenciamento da infraestrutura de rede	
Certificar-se de que a infraestrutura de rede esteja atualizada	É utilizado um *switch* não gerenciável de oito portas, um roteador doméstico para providenciar sinal de rede sem fio, atualização para este dispositivo não existe mais, é um roteador antigo.

O décimo terceiro controle não possui um controle aplicável ao grupo IG1 então será abordado apenas de forma descritiva. Este controle aborda o monitoramento e defesa de rede encorajando a empresa a operar processos e ferramentas para estabelecer e manter o monitoramento de rede abrangente e a defesa contra ameaças de segurança em toda a infraestrutura de rede e base de usuárias da empresa, controle este que demanda mais recursos e o IG1 não está maduro o suficiente para investir recursos neste controle.

O décimo quarto controle aborda a conscientização de segurança e treinamento de habilidades encorajando a empresa a estabelecer e manter programas de conscientização para influenciar o comportamento de toda a força de trabalho se qualificando adequadamente para reduzir os riscos de segurança cibernética para a empresa.

As observações que sustentam a avaliação deste controle são os poucos treinamentos existentes e tampouco disseminados entre os colaboradores, sendo o fator humano pouco incentivado a se manter consciente das ações a serem tomadas

em casos de suspeitas ou incidentes emergentes. A tabela 13 apresenta as informações levantadas sobre o controle:

Tabela 13 – Informações sobre o controle de conscientização de segurança e treinamento de habilidades

Conscientização de segurança e treinamento de habilidades	
Estabelecer e manter um programa de conscientização de segurança	Não é feito um treinamento com todos os colaboradores sobre o que é segurança cibernética.
Treinar membros da força de trabalho para reconhecer ataques de engenharia social	Não é feito um treinamento sobre o tema, apenas repassado casos que já ocorreram.
Treinar a força de trabalho em boas práticas para autenticação	Não há um treinamento sobre boas práticas de autenticação, apenas auxiliado na criação de uma primeira senha composta por 10 caracteres pelo menos.
Treinar a força de trabalho nas boas práticas para manuseio de dados	Não há treinamento sobre boas práticas no manuseio de dados.
Treinar membros da força de trabalho sobre as causas de exposição não intencional de dados	Não há treinamentos sobre exposição não intencional de dados.
Treinar membros na força de trabalho sobre como reconhecer e relatar incidentes de segurança	Há um treinamento básico sobre como identificar situação que podem se tornar um incidente e relatar à equipe técnica e o líder técnico para auxiliar na tratativa do caso.
Treinar a força de trabalho sobre como identificar e relatar se seus ativos corporativos estão falhando ao realizar atualizações de segurança	Não há um treinamento, apenas é encorajado a comunicação aberta sobre relatar a equipe técnica quando o usuário identificar falhas apresentadas pelas ferramentas de trabalho.
Treinar a força de trabalho sobre os perigos de se conectar e transmitir dados corporativos em redes inseguras	Não há um treinamento, apenas é comunicado a importância de não se conectar em sites suspeitos ou tentar baixar arquivos de sites não seguros ou desconhecidos e relatar a equipe técnica caso aconteça algo atípico na rotina do usuário.

O décimo quinto controle aborda a gestão de provedores de serviço, com o objetivo de desenvolver um processo para avaliar os provedores de serviços que mantêm dados confidenciais ou são responsáveis por plataformas ou processos de TI críticos de uma empresa, garantindo que esses provedores estejam protegendo essas plataformas e dados de uma forma adequada.

As observações que sustentam a avaliação desse controle são que o inventário é feito dentro do sistema de gestão da empresa, com informações que não são

atualizadas de forma periódica, ocasionando na imprecisão das informações. A tabela 14 apresenta as informações levantadas sobre o controle:

Tabela 14 – Informações do controle gestão de provedores de serviços

Gestão de provedores de serviços	
Estabelecer e manter um inventário de provedores de serviços	Há uma base com todos os fornecedores cadastrados, com contatos corporativos para uma comunicação direta, porém não é atualizado constantemente.

O décimo sexto controle aborda a segurança de software de aplicativo, encorajando a empresa a gerenciar o ciclo de vida da segurança de software desenvolvido, hospedado ou adquirido internamente para prevenção, detecção e correção dos pontos fracos de segurança antes que eles afetem a empresa, contudo este controle não é aplicável ao IG1.

O décimo sétimo controle aborda o gerenciamento de resposta a incidentes, visando estabelecer um programa para desenvolver e manter uma capacidade de resposta a incidentes para preparar detectar e responder rapidamente a um ataque.

A observação que sustenta a avaliação é a falta de contatos com setores e organizações de segurança cibernética podem prejudicar significativamente o tempo de resposta a incidentes, podendo parar toda a produção da empresa a falta de documentação de como proceder em casos de incidentes podem desorientar a força de trabalho de forma que seus esforços sejam desviados para buscar orientação ao invés de responder de forma assertiva ao incidente. A tabela 15 apresenta as informações levantadas sobre o controle:

Tabela 15 – Informações do controle gerenciamento de resposta a incidentes

Gerenciamento de resposta a incidentes	
Designar pessoal para gerenciar o tratamento de incidentes	Com a pouca quantidade de colaboradores, o dono da empresa é responsável pelo gerenciamento dos incidentes e o líder técnico é o suplente, porém não é documentado o processo de tratativa dos incidentes, não tendo histórico de como a empresa lida em ocorrências do tipo.
Estabelecer e manter informações de contato para relatar incidentes de segurança	Não há uma rede de contatos definida, havendo a necessidade de buscar contatos conhecidos que possam auxiliar na tratativa de um incidente, normalmente não obtendo sucesso nas primeiras tentativas.
Estabelecer e manter um processo empresarial para relatar incidentes	Não há um processo estabelecido e nem documentado de como a força de trabalho deve lidar em casos de incidentes.

O décimo oitavo controle aborda os testes de penetração, com o objetivo de testar a eficácia e a resiliência dos ativos corporativos por meio da identificação e exploração de fraquezas nos controles, tais como pessoas, processos e tecnologia, além da simulação dos objetivos e ações de um invasor, este controle não é aplicado ao IG1.

3 Proposta de Melhoria

As seguintes propostas de melhorias (PM) foram recomendadas e/ou aplicadas em cada controle, demonstrando como a empresa pode estar em conformidade com o *CIS Controls V8*, visando uma melhoria em todos os controles aplicáveis ao *IG1*.

Para o primeiro controle foi sugerido as seguintes PM visam implementar uma rotina automatizada para manter o inventário de ativos atualizado, conforme mostra a tabela 16:

Tabela 16 – Informações do controle e propostas de melhoria

Inventário e controle de ativos da empresa	
Estabelecer e manter um inventário detalhado de ativos da empresa	PM: Utilizar um *software* que permita sempre manter o inventário atualizado, como *Spiceworks* e *OCS Inventory* que são ferramentas gratuitas.
Endereçar ativos não autorizados	PM: Elaborar um processo simples que visualmente facilite a compreensão de como deve ser identificado um ativo não autorizado, coletar informações como nome, endereço físico e endereço IP, identificar sua localização física e sua tratativa.

Para o segundo controle a sugestão de melhoria visam a melhoria na gestão do inventário, listando os *softwares* autorizados e elaborando um processo para remoção de *softwares* não autorizados, tais propostas estão apresentadas na tabela 17:

Tabela 17 – Proposta de melhoria para o controle Inventário e controle de ativos de software

Inventário e controle de ativos de software	
Estabelecer e manter um inventário de *software*	PM: Utilizar um *software* para gestão, como *OCS Inventory, Ingite, Asset Tiger* que possuem um custo total acessível ao orçamento financeiro
Certificar-se de que o *software* autorizado seja atualmente suportado	PM: Manter os *softwares* atualizados, tanto Sistemas Operacionais que precisam de requisitos mínimos e estes devem ser atendidos, como as ferramentas de uso para a empresa, buscando qual versão ainda possui suporte com o fabricante.
Endereçar a *software* não autorizado	PM: Utilizar um software que liste os *softwares* utilizados dentro da empresa, assim identificando-os e facilitando a remoção deles, realizando o procedimento mensalmente.

Para o terceiro controle a sugestão de implementação de documentação para iniciar a implementação da gestão de dados pessoais, seguidos de um ciclo de vida estabelecido e documentado, mantendo assim uma maturidade maior sobre esse tema, as informações estão apresentadas na tabela 18:

Tabela 18 – Sugestões de melhoria para o controle Proteção de Dados

Proteção de dados	
Estabelecer e manter um processo de gerenciamento de dados	PM: Criar um diagrama que identifica todo o processo do dado na empresa, desde o cadastro destes dados até sua exclusão.
Estabelecer e manter um inventário de dados	PM: Mapear os tipos de dados, realizar contato com uma empresa especializada na conformidade LGPD, para desenhar todos os passos que envolvem o inventário. (https://bakertillybr.com.br/ferramenta-gratuita-conformidade-lgpd/ ferramenta gratuita)
Configurar listas de controle de acesso a dados	PM: Aos arquivos digitais, será estabelecido por departamento o controle de acesso aos dados de forma mais criteriosa.
Aplicar retenção de dados	PM: Estabelecer um período mínimo e máximo para retenção dos dados.
Descartar dados com segurança	PM: Para arquivos digitais, utilizar *softwares* para exclusão segura e para documentos físicos, tais como CDs, papéis e outras mídias removíveis, utilizar uma fragmentadora.
Criptografar dados em dispositivos de usuário final	PM: Utilizar uma ferramenta de criptografia, tal como o *BitLocker*® que vem sendo inativado.

Para o quarto controle as sugestões de melhoria visam a configuração segura documentada e a implementação de um *firewall* para garantir a navegação segura e uma gestão mais segura dos ativos. A proposta segue apresentada na tabela 19:

Tabela 19 – Sugestões de melhoria para configuração segura de ativos corporativos e software

Configuração segura de ativos corporativos e software	
Estabelecer e manter um processo de configuração seguro	PM: Documentar o processo de configuração segura, em cada tipo de ativo.

Estabelecer e manter um processo de configuração seguro para infraestrutura de rede	PM: Documentar o processo de configuração de dispositivos de rede, como *firewalls, switches,* roteadores.
Configurar o bloqueio automático de sessão em ativos corporativos	PM: Aplicar política em todos os usuários com bloqueio automático de sessão com período máximo de 15 minutos.
Implementar e gerenciar um firewall em servidores	PM: Implementar um Firewall que bloqueie portas, gere log e monitore o comportamento dos dados trafegados através do servidor. Recomendação: Windows Firewall
Implementar e gerenciar um firewall em dispositivos de usuário final	PM: Implementar um firewall garantindo a navegação segura dos usuários finais. Recomendação: PfSense
Gerenciar com segurança ativos corporativos e software	PM: Implementar solução para realizar varreduras periódicas buscando vulnerabilidades e atuar para aplicar os controles necessários para proteção.
Gerenciar contas padrão em ativos corporativos e software	PM: Criar rotinas de troca das senhas padrões de todos os softwares e contas padrões a cada 90 dias se não possível desativar tais contas.

Para o quinto controle as sugestões de melhoria são implementar o MFA nos acessos a contas via *web* e aplicações e assegurar o inventário de contas, se possível um relatório automatizado para evitar falhas humanas na gestão das contas. A proposta apresentada segue na tabela 20:

Tabela 20 – Sugestão de melhoria para o controle gestão de contas

Gestão de contas	
Estabelecer e manter um inventário de contas	PM: Utilizar a ferramenta do Windows Server para gerar um relatório de contas dos usuários.
Usar senhas exclusivas	PM: Utilizar uma complexidade de senhas com 14 caracteres para contas sem MFA.

Desativar contas inativas	PM: Contas sem uso por um período máximo de 60 dias devem ser desativadas.
Restringir privilégios de administrador a contas de administrador dedicadas	PM: Não utilizar contas de rede com privilégios

Para o sexto controle as sugestões são para implementar um processo documentado para futuras contratações, visto que a empresa com o amadurecimento irá expandir, criar grupos para controle de acesso e privilégio, para concessão e revogação de quando necessário, a tabela 21 apresenta as sugestões levantadas para o controle:

Tabela 21 – Sugestões de melhoria para o controle gerenciamento de controle de acesso

Gerenciamento de controle de acesso	
Estabelecer um processo de concessão de acesso	PM: Criar um diagrama que demonstre como é o processo de concessão de acesso aos usuários e grupos de usuários.
Estabelecer um processo de revogação de acesso	PM: Criar um diagrama que demonstre como é o processo de revogação de acesso e privilégio dos usuários e grupo de usuários.
Exigir MFA para aplicativos expostos externamente	PM: Habilitar MFA para produtos office.
Exigir MFA para acesso remoto à rede	PM: Não há acesso remoto à rede.
Exigir MFA para acesso administrativo	PM: Implementar MFA para acesso administrativo aos sistemas

Para o sétimo controle as sugestões de melhoria visam permitir que a empresa adquira amadurecimento compreendendo como é o processo de documentação das remediações tomadas e o conhecimento das vulnerabilidades tomadas a tabela 21 apresenta as propostas:

Tabela 21 – Sugestões de melhoria do controle gerenciamento contínuo de vulnerabilidade

Gerenciamento contínuo de vulnerabilidade	
Estabelecer e manter um processo de gerenciamento de vulnerabilidade	PM: Documentar as vulnerabilidades conhecidas, mesmo que possuam controle sugerido, porém não implementado, avaliando seu risco e sua aceitabilidade.
Estabelecer e manter um processo de remediação	PM: Documentar um processo para remediar incidentes em potencial, assim criando um processo que pode ser melhorado continuamente.
Executar um gerenciamento automatizado de patches do sistema operacional	PM: Criar rotinas de atualização de forma centralizada através de serviços de distribuição de atualizações.
Executar o gerenciamento automatizado de patches de aplicativos	PM: Criar uma rotina para atualizar os softwares quando houver atualizações disponíveis de forma centralizada.

Para o oitavo controle as sugestões são para encorajar a empresa a registrar os *logs* de auditoria de forma adequada e segura, definindo este processo permitindo futuras melhorias, a tabela 22 apresenta as propostas:

Tabela 22 – Sugestões de melhoria do controle gerenciamento de registro de auditoria

Gerenciamento de registro de auditoria	
Estabelecer e manter um processo de gerenciamento de registro de auditoria	PM: Criar um documento para definir os requisitos de registros, relatando como é coletado os registros, revisão e retenção dos *logs* de auditoria para os ativos.
Coletar registros de auditoria	PM: Definir um diretório para armazenamento e uma ferramenta para leitura dos registros.
Garantir o armazenamento adequado de registros de auditoria	PM: O diretório deve possuir acesso restrito, manter cópia de segurança e preferivelmente criptografado.

Para o nono controle as sugestões propostas visam assegurar a navegação e o envio de *e-mail*s e seu conteúdo, garantindo que a empresa não tenha sua rede comprometida, a tabela 23 apresenta as propostas:

Tabela 23 – Sugestões de melhorias para o controle proteções de *e-mail* e navegador da *web*

Proteções de *e-mail* e navegador da *web*	
Garantir o uso apenas de navegadores e clientes de *e-mail* com suporte total	PM: Manter o cliente de *e-mail* atualizado e os navegadores
Usar serviços de filtragem de *DNS*	PM: Implementar um serviço de filtragem *DNS* conhecido e confiável, como *CloudFlare DNS*

Para o décimo controle as sugestões são para proteger o ambiente corporativo de *malwares*, encorajando a empresa a adquirir um *anti-malware* capaz de identificar com maior precisão comportamentos estranhos e ser uma barreira mais robusta contra os ataques de média complexidade, a tabela 24 apresenta a proposta para o controle:

Tabela 24 – Sugestões de melhoria para o controle defesas contra *malware*

Defesas contra *malware*	
Implantar e manter um software *anti-malware*	PM: Utilizar um *software anti-malware* único para centralizar os registros e o monitoramento, recomenda-se o *Norton Defender* por ser multiplataforma e com painel *web* para monitoramento.
Configurar atualizações automáticas de assinatura *anti-malware*	PM: Configurar o *anti-malware* para atualizar de forma automática.
Desativar a execução automática e reprodução automática para mídias removíveis	PM: Garantir através de políticas de grupo que a execução e reprodução automática de mídias removíveis esteja desabilitado.

Para o décimo primeiro controle as sugestões visam que a empresa esteja preparada para incidentes não previstos e inevitáveis, onde a recuperação de dados é o caminho para não parar a operação da empresa, encorajando a empresa a categorizar os dados e realizar uma cópia de segurança em um ambiente isolado da rede interna para assegurar a integridade e a garantia de recuperação dos dados críticos, a tabela 25 apresenta a proposta para o controle:

Tabela 25 – Sugestões de melhoria para o controle recuperação de dados

Recuperação de dados	
Estabelecer e manter um processo de recuperação de dados	PM: Criar um diagrama para recuperação de dados, apresentando o processo de forma clara, documentá-lo e revisá-lo anualmente.
Executar *backups* automatizados	PM: Os *backups* são feitos através de um software, de forma automatizada, os arquivos no servidor são feitos diariamente e nos demais de forma semanal.
Proteger os dados de recuperação	PM: Os dados de recuperação são encriptados pelo software de *backup.*
Estabelecer e manter uma instância isolada de dados de recuperação	PM: Por ser na nuvem os dados de recuperação estão em uma instância isolada, sendo feita por versão, mantendo-se 5 instâncias de dados armazenados em cada ativo e 15 versões dos dados armazenados no servidor.

Para o décimo segundo controle as sugestões são para encorajar a empresa a manter todo hardware da infraestrutura de rede atualizado e mitigar os possíveis riscos

acerca de suas vulnerabilidades conhecidas, a tabela 26 apresenta a proposta para o controle:

Tabela 26 – Sugestões de melhoria para o controle gerenciamento da infraestrutura de rede

Gerenciamento da infraestrutura de rede	
Certificar-se de que a infraestrutura de rede esteja atualizada	PM: Implementar hardwares novos e preferencialmente gerenciáveis, tornando a rede mais segura e atualizável.

Para o décimo quarto controle as sugestões reforçam a importância de conscientizar cada membro da força de trabalho, encorajando a empresa a criar um programa de treinamento que aborde os assuntos acerca dos controles do *CIS Controls V8* aplicáveis de forma clara e entendível por todos, a tabela 27 apresenta as propostas para o controle:

Tabela 27 – Sugestões de melhoria para o controle conscientização de segurança e treinamento de habilidades

Conscientização de segurança e treinamento de habilidades	
Estabelecer e manter um programa de conscientização de segurança	PM: Criar um programa simples e que seja entendível por todos os colaboradores, este programa será revisado de forma anual, mantendo-o atualizado.
Treinar membros da força de trabalho para reconhecer ataques de engenharia social	PM: Explicar os processos de identificação e implementação do modelo de confiança-zero na recepção de membros externos, checagem de remetentes de mensagens, identificação
Treinar a força de trabalho em boas práticas para autenticação	PM: Explicar sobre a importância de senhas fortes, não inserir credenciais de uso corporativo em plataformas não autorizadas e o uso do MFA no ambiente corporativo.
Treinar a força de trabalho nas boas práticas para manuseio de dados	PM: Explicar sobre a importância no manuseio de dados para evitar vazão, furto e sequestro, orientando como identificar dados, armazená-los, transferir, arquivar e destruir dados, visto que esta é uma responsabilidade de cada colaborador, ensinando-os também políticas de mesa e tela limpa, bloqueio de sessão e evitar dados expostos em quadros brancos.
Treinar membros da força de trabalho sobre as causas de exposição não intencional de dados	PM: Treinar o corpo da empresa para estarem cientes das diversas causas de exposição, tais como entrega incorreta de dados via *e-mail*, perda de dispositivos portáteis que podem impactar na empresa, publicação de dados em meios não desejados, como redes sociais.

Treinar membros na força de trabalho sobre como reconhecer e relatar incidentes de segurança	PM: Treinar os membros para reconhecer incidentes de segurança, comunicando os membros responsáveis para que saibam a quem relatar os incidentes e assim tomarem medidas assertivas.
Treinar a força de trabalho sobre como identificar e relatar se seus ativos corporativos estão falhando ao realizar atualizações de segurança	PM: Explicar aos membros como identificar e relatar falhas nas atualizações de segurança dos ativos, onde notificações dos sistemas estão localizadas para averiguar e relatar apenas caso haja falhas.
Treinar a força de trabalho sobre os perigos de se conectar e transmitir dados corporativos em redes inseguras	PM: Explicar aos membros que ao se conectarem em redes inseguras ou desconhecidas, utilizem meios seguros para transmitir dados, utilizando uma VPN, como *Tunnel Bear.*

Para o décimo quinto controle as sugestões visam o inventario de provedores de serviço, facilitando que a empresa os identifique e mantenha tais informações atualizadas, a tabela 28 apresenta a proposta para o controle:

Tabela 28 – Sugestão de melhoria para o controle gestão de provedores de serviços

Gestão de provedores de serviços	
Estabelecer e manter um inventário de provedores de serviços	PM: Manter um inventário no sistema, com cadastro de todos os fornecedores e contatos para comunicação direta, revisar os contatos trimestralmente.

Para o décimo sétimo controle as sugestões objetivam que a empresa se capacite para responder a incidentes de forma ágil e assertiva, tecendo uma boa gestão de resposta a incidentes, definindo responsáveis para acompanhar e gerenciar o tratamento dos incidentes, criar uma rede de contatos para relatar os incidentes e elaborar um diagrama que apresente o processo empresarial para relatar incidentes, permitindo futuras melhorias para o controle, a tabela 29 apresenta as propostas para o controle:

Tabela 29 – Sugestões de melhoria para o controle gerenciamento de resposta a incidentes

Gerenciamento de resposta a incidentes	
Designar pessoal para gerenciar o tratamento de incidentes	PM: Com a pouca quantidade de colaboradores, o líder técnico será encarregado do gerenciamento e documentação dos esforços realizados na resposta aos incidentes, o líder técnico contará também com um agente terceirizado fixo para registrar todo o processo, supervisionado pelo líder técnico.
Estabelecer e manter informações de contato para relatar incidentes de segurança	PM: Definir contatos para relatar os incidentes, como cert.br, provedor de internet, o software que causou a vulnerabilidade, caso seja via *e-mail* relatar o provedor de *e-mail*.
Estabelecer e manter um processo empresarial para relatar incidentes	PM: Definir um diagrama para visualizar claramente a ordem correta e a quem relatar os incidentes, identificando o líder técnico e todos os membros envolvidos para cada tipo de incidente, assim sendo um processo ágil para agir na remediação dos incidentes, identificando também as etapas de remediação e pós incidente.

4 Melhorias Implementadas

Após a elaboração da proposta de melhoria a equipe se mobilizou para implementar as melhorias que foram identificadas como facilmente implementáveis na empresa, foram implementadas vinte e oito salvaguardas apresentou uma melhoria de 50%, considerando que três controles estavam em conformidade com o *CIS Controls* V8, restando vinte e cinco controles a serem implementados, conforme ilustra o gráfico 1:

Gráfico 1 – Visão total das salvaguardas do grupo IG1

Inicialmente, foi utilizado o sistema operacional Windows Server 2019 para configurar o serviço de Active Directory (AD), a fim de implementar políticas e controle de listas de controle de acesso (ACL), proporcionando consistência e viabilizando futuras melhorias nos controles de segurança. Além disso, foram criados usuários e grupos para permitir uma atribuição assertiva de privilégios e controlar ativamente o acesso aos recursos do sistema, melhorando, dessa forma, a auditoria de ações e acessos realizados na rede, foram sugeridas mudanças físicas na topologia da empresa, visando uma melhoria na segurança física, conforme indicado figura 1 e figura 2 apresentando respectivamente como era inicialmente e após a mudança física.

Figura 1 – Topologia física inicial

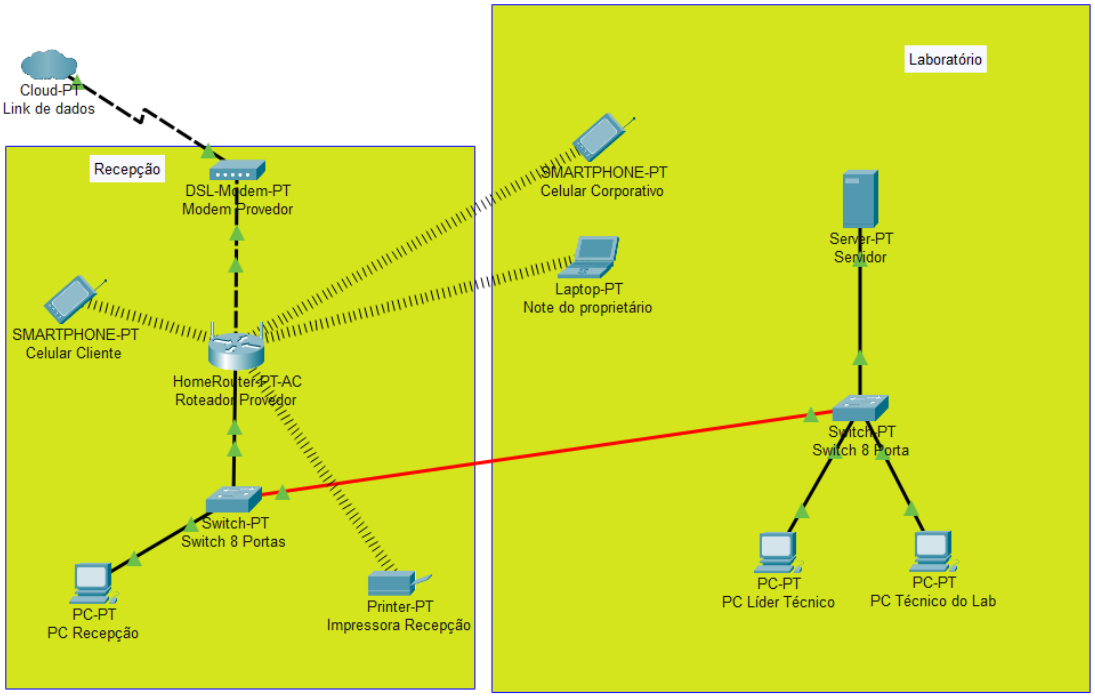
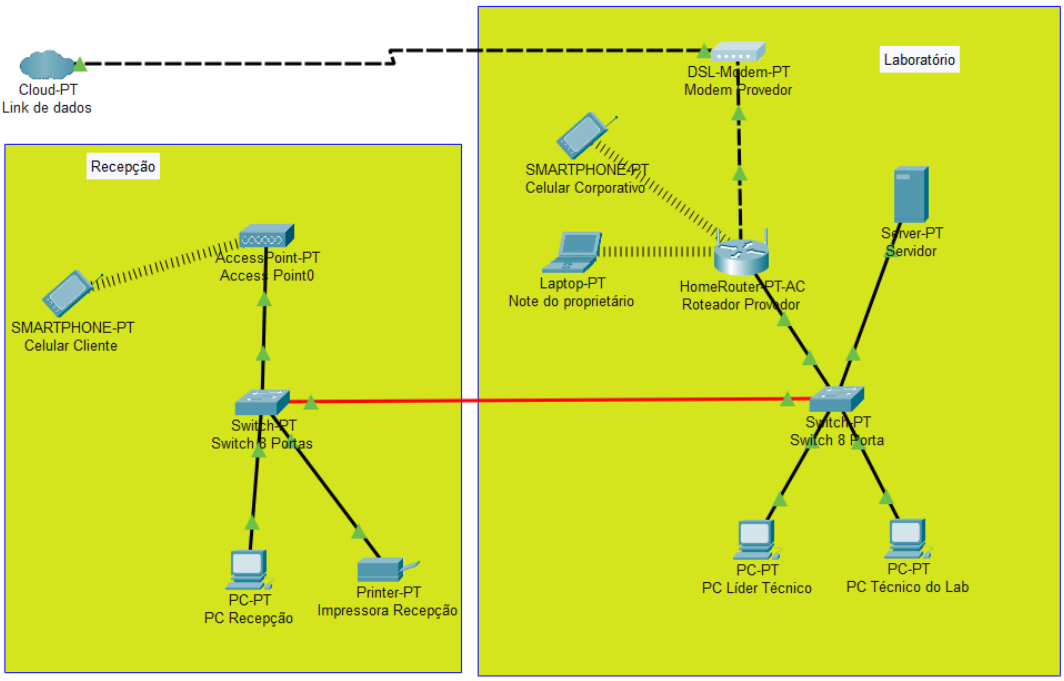


Figura 2 – Topologia física após mudança



A empresa implementou o *Spiceworks* para gerir ativamente seus ativos físicos e os aplicativos, uma ferramenta que mapeia a rede trazendo a informação de todos os dispositivos conectados e *softwares* que estão instalados nesses dispositivos, permitindo inclusive o endereçamento de ativos não autorizados, sendo o *Spiceworks* instalado no Windows Server, servindo como centralização das informações

coletadas, gerando um *dashboard* através de um painel de visualização através do navegador, buscando a conformidade com o controle de inventário de ativos da empresa e o inventário e controle de ativos de *software*.

Buscando uma melhor conformidade com o controle de proteção de dados, foi desenvolvido um diagrama, com uso da ferramenta fornecida pela empresa Baker Tilly Br, para identificar o processo da coleta de dados até o processo da exclusão, facilitando a visualização da necessidade da coleta dos dados, como é feito o cadastro, armazenamento, compartilhamento, *backup* e exclusão dos dados e assim inventariar os dados mantidos em sua posse. Realizado a configuração de controle de acesso (ACL), definindo de forma clara quais departamentos e usuários possuem acessos aos dados armazenados no servidor, definido uma retenção de dados por três anos no mínimo, habilitado em todos os equipamentos com Sistema Operacional Windows o *BitLocker*®.

Para o controle configuração segura e ativos corporativos e software, foi configurado o bloqueio automático de sessão via políticas de grupo, com período de inatividade de 15 minutos, implementado o *Norton Defender Small Business* para realizar varreduras periódicas na rede e implementado políticas de troca de senha para cada 90 dias para os usuários, contas padrões tiveram suas senhas alteradas para senhas com no mínimo 14 caracteres.

Para o controle gestão de contas, foi implementado a através do *PowerShell* a coleta do relatório de usuários do AD, criado uma rotina para gerar o relatório mensalmente, para contas de aplicativos e *e-mail* as mesmas são armazenadas em aplicativo *Evernote*, em nuvem e criptografado, com configuração de permissão de acessos, através do relatório eles desativam contas em desuso por mais de 60 dias, nenhum usuário possui privilégio, ao necessitar o mesmo é incluso no grupo de administradores de rede e retirado até o fim do dia, identificando-os através do comando *Get-ADGroupMember* via *PowerShell*.

Para o controle de gerenciamento de controle de acesso foi habilitado o MFA para os produtos Office que são facilmente acessíveis em redes externas.

Foi configurado o *Windows Server Update Services* (WSUS) para gerenciamento centralizado de atualização de patches dos Sistemas Operacionais e suas atualizações são verificadas através do *Spiceworks*.

Para o controle de gerenciamento de registro de auditoria foi definido que os logs de segurança, aplicativo, instalação e Sistema fossem salvos diretamente no Windows Server, através de uma conta de serviço, que é a única além dos usuários em *DomainAdmins*

que tem acesso a pasta de armazenamento dos registros de auditoria.

Para o controle proteções de *e-mail* e navegador da *web*, os clientes de *e-mail* e navegadores são atualizados automaticamente através do serviço dedicado de cada aplicação e para serviço de filtragem de DNS é utilizado o DNS da *CloudFlare* que é popularmente conhecido como um serviço de filtragem confiável para navegação segura.

Para o controle defesas contra *malware*, foi implantado o Norton Defender Small Business que vem com painel *web* para acompanhar os dispositivos que estão instalado os clientes e implementado as políticas definidas pelo painel do administrador da rede, contando também com atualização das assinaturas em todos os dispositivos e desativando a reprodução automática de mídias removíveis, realizando varredura automática em dispositivos conectados.

Para o controle recuperação de dados a empresa se mostrou preparada, necessitando apenas criar e documentar o processo, este não foi implementado, contudo está em desenvolvimento.

Para o controle de gestão de provedores de serviços criou-se uma planilha relacionando todos os provedores e fornecedores com seus respectivos contatos para comunicação direta e telefones, a cada trimestre é realizado pelo menos uma vez o contato com cada um a fim de verificar se o contato ainda é válido ou precisa ser atualizado.

5 Considerações finais

Após o mapeamento dos controles da Center Tech, elaborado a proposta de melhoria para as 56 salvaguardas mapeadas e aquelas que foram possíveis, o diagnóstico ofereceu uma visão clara das áreas que precisam de melhorias, identificando as principais prioridades para a organização no que diz respeito à segurança da informação. Além disso, destacou a necessidade de desenvolver um plano de ação para implementar as salvaguardas que ainda não foram implementadas, levando em consideração as necessidades específicas da organização e os riscos associados a suas operações, o que representa janelas de oportunidades para melhoria contínua.

Para garantir que a implementação das salvaguardas seja bem-sucedida, a empresa deve priorizar a conscientização e a formação dos colaboradores, além de garantir a alocação adequada de recursos e a coordenação entre as diferentes áreas envolvidas. Também é importante que a organização revise regularmente seus controles de segurança para garantir que eles estejam atualizados e adequados às mudanças no ambiente de ameaças.

Em suma, realizar um diagnóstico de maturidade utilizando o CIS Controls V8 permite que a empresa compreenda seu nível de maturidade e saiba como elevá-lo de forma efetiva e assertiva, montando um plano que a guiará até mesmo dentro de um framework complexo, mapeando seus controles implementados facilitando o reconhecimento de suas falhas e corrigindo-as, valorizando assim o esforço da organização.

BIBLIOGRAFIA:

GAT**,** **Implementação do CIS Controls V8**. Disponível em: <https://www.gat.digital/blog/implementacao-de-controles-cis/>. Acesso em: 16 fev. 2023

CENTER FOR INTERNET SECURITY**,** **Sobre nós**. Disponível em: < https://www.cisecurity.org/about-us>. Acesso em: 15 fev. 2023

FERREIRA, Luiz, **SegInfocast #79 – CIS Controls Versão 8**. Disponível em: <https://seginfo.com.br/2021/06/24/seginfocast-79-cis-controls-versao-8/>. Acesso em 12 de fev. 2023.

OSTEC, **Controles CIS**. Disponível em: <https://ostec.blog/geral/controle-cis/>. Acesso em 15 fev. 2023.

MICROSOFT, **Parâmetros da Center For Internet Security (CIS)**. Disponível em: <https://learn.microsoft.com/pt-br/compliance/regulatory/offering-cis-benchmark>. Acesso em 16 de fev. 2023.