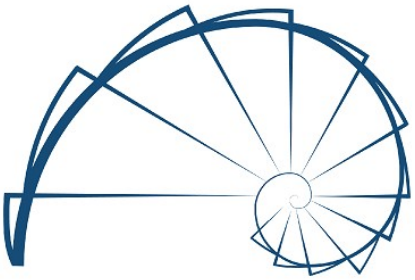

Underlying

Serviço de Auditoria de Segurança
Auditoria: 113/2022

Empresa Auditada: SIN414

Diretor: Bruno Guazzelli Batista

Equipe da Auditoria Underlying:

Ivan Leoni Vilas Boas - 2018009073

Leonardo Rodrigo de Sousa - 2018015965

Lucas Tiense Blazzi - 2018003310

Thiago Marcelo Passos - 2018002850

UNIFEI
Universidade Federal de Itajubá

IMC - Instituto de Matemática e Computação

Av. BPS, 1303 - Caixa postal 50 - 37500-903

Itajubá - MG - Brasil Telefone: 35-3629-1135

E-mail:imc@unifei.edu.br

Underlying

UNIFEI
Universidade Federal de Itajubá

ÍNDICE DE TABELA

Tabela 1 - Cronograma da auditoria SIN 414 9
Tabela 2 - Atividade de auditoria 01: Reunião 9
Tabela 3 - Atividade de auditoria 02: Planejamento 10
Tabela 4 - Atividade de auditoria 03: Seleção da equipe 10
Tabela 5 - Atividade de auditoria 04: Avaliação de controle de acesso 11
Tabela 6 - Atividade de auditoria 05: Avaliação dos sistemas 11
Tabela 7 - Atividade de auditoria 06: Avaliação nos equipamentos 12
Tabela 8 - Atividade de auditoria 07: Avaliação da rede e firewall 12
Tabela 9 - Atividade de auditoria 08: Proposta de Soluções 13
Tabela 10 - Atividade de auditoria 09: Entrega de relatórios 13
Tabela 11 - Equipe de auditores 16
Tabela 12 - Falhas se segurança da SIN413 23
Tabela 13 - Soluções propostas pela auditoria 29

Underlying

UNIFEI
Universidade Federal de Itajubá

Sumário

1. INTRODUÇÃO 4

1.1 OBJETIVO DA AUDITORIA 5

2. PLANEJAMENTO 5

2.1 ÁREA DE ABORDAGEM 5
2.2 RECURSOS 5
2.3 METODOLOGIA 6
2.3.1 AVALIAÇÃO DA SEGURNÇA 6
2.4 CRONOGRAMA DA AUDITORIA 8
2.4.1 Período de execução da Auditoria 9
2.5 ATIVIDADES DA AUDITORIA 9
2.6 ENTREVISTAS 13
2.6.1 Entrevistados Internos 13
2.6.2 Questionário aos entrevistados internos 13

3. EQUIPE DE AUDITORES 14

3.1 PROCESSO SELETIVO DOS AUDITORES 15
3.2 COMPOSIÇÃO DA EQUIPE DE AUDITORES 15

4. FALHAS ENCONTRADAS 16

5. SOLUÇÕES PROPOSTAS 24

6. AVALIÇÃO DA EQUIPE 30

7. CONCLUSÃO 31

8. FINALIZAÇÃO 32

9. ANEXO - A 33

1. INTRODUÇÃO

O presente relatório objetiva a demonstrar um processo de auditoria realizado pela empresa Underlying na multinacional SIN414 onde foi realizado a verificação de possíveis falhas nas questões de redes, nos sistemas e nos equipamentos informáticos, abrangendo contemplando todo o gerenciamento de segurança. A empresa que será auditada é a famosa multinacional SIN414 que trabalha a mais de 30 anos no fornecimento de suplementos e equipamentos agrícolas, além disso, conta com um oferecimento de cursos profissionalizantes, contando com mais de 100 mil clientes ao redor do mundo, contudo, nos últimos anos ocorreram diversos problemas relacionados à segurança. Embora a empresa SIN414 seja referência em sua área, as questões de segurança foram negligenciadas, possibilitando diversos ataques, os quais geraram prejuízos a empresa e consequentemente a insatisfação de seus clientes. Por essas e outras razões, a empresa resolveu contratar os serviços de auditoria segurança de TI da Underlying, confiando na competência da equipe para garantir a conformidade das informações.

A Underlying, por sua vez, conta com mais de 20 anos no mercado de auditoria de segurança sendo uma das empresas do ramo de auditoria e segurança mundialmente reconhecida. Atualmente possui 5 filiais ao redor do mundo e com uma equipe de mais de 500 colaboradores especializados e comprometidos com a segurança de dados. A Underlying realiza anualmente centenas de auditorias no mundo todo, no Brasil são realizadas em média 200 autoriais anuais. A SIN414 contratou os serviços de auditoria de TI da Underlying por vir negligenciando as questões de segurança pelos seus colaboradores e por consequência sofrer diversos ataques e prejuízos, sendo assim, a segurança se tornou-se um objetivo crucial da organização atualmente, uma vez que, a segurança da informação garante a integridade dos dados, confidencialidade, disponibilidade, autenticação e irretratabilidade, portanto, a garantia do devido gerenciamento da segurança da informação da empresa é crucial para o sucesso da mesma, visto que esta possui diversos dados confidenciais de seus clientes, e caso seus dados não sejam protegidos podem ser comprometidos e assim abalaria a confiança da sociedade em geral.

As atividades de auditoria realizadas na empresa multinacional SIN414 e relatadas neste documento tiveram, portanto, o objetivo de analisar todo o gerenciamento da SIN414 no que tange a segurança da informação. Essa análise tem por finalidade solucionar as questões de segurança que foram negligenciadas pela contratante ao decorrer dos anos o possibilitou os ataques e que ocasionaram prejuízos e a insatisfação de seus stakeholders que confiaram à SIN414 os seus dados confidenciais.

Para o sucesso da auditoria pela Underlying foi feito uma escolha da equipe com base em critérios estabelecidas, foi também realizado um planejamento da auditoria utilizando um questionário aplicado no setor de TI da SIN414 para coletar as informações atuais da empresa e de seus colaboradores. Em seguida foram identificados os possíveis problemas, e proposto as devidas soluções para tratar as falhas encontradas da melhor forma, por parte da equipe de auditores escolhida. Por fim foi aplicado um questionário aos funcionários de TI para avaliação dos serviços prestados pela empresa Underlying.

Desta forma, este relatório constitui um produto da auditoria realizada na empresa multinacional SIN414 no mês de junho de 2022 (ver cronograma na seção 2.6), detalhando todas as observações e conclusões da Underlying quanto a atual situação da segurança da informação.

1.1 Objetivo da auditoria

A auditoria objetivou verificar a adequação do gerenciamento de toda a segurança da empresa auditada, compreendendo a verificação dos equipamentos informáticos, dos sistemas e a verificação de todos os processos que os colaborem utilizam e que contemplam diretamente a segurança da rede e dos dados. Portanto a auditoria irá verificar toda a geração, tratamento, divulgação, acesso e arquivamento dos dados dos clientes e das informações da SIN414, de forma a garantir sua confidencialidade, integridade, disponibilidade, autenticidade e legalidade.

2. PLANEJAMENTO

O planejamento da auditoria inclui os principais pontos que devem ser levados em conta para a devida execução da mesma. As próximas seções iram abordar estes pontos que são: (I) área de abordagem, (II) os recursos necessários, (III) a metodologia de auditoria, (IV) os objetivos de controle, (V) o cronograma e (VI) as atividades da auditoria. Seguindo corretamente o devido planejamento da auditoria ela ocorreu de forma eficiente e atendeu ao seu propósito e ao cronograma.

2.1 Área de abordagem

A auditoria será realizada em toda a unidade da matriz e contemplará a averiguação dos seguintes itens:

- ✓ Sistemas utilizados;
- ✓ Sistemas administrativo-operacionais e os controles internos administrativos utilizados na gestão orçamentária, contábil, financeira, suprimentos, operacional e de pessoal;
- ✓ Equipamentos tecnológicos e informáticos
- ✓ A verificação do cumprimento das normas internas e da legislação pertinente;
- ✓ Configuração dos sistemas de controle de segurança como firewalls, IDS, IPS e antivírus
- ✓ Presença de programas maliciosos já existentes no contexto da empresa
- ✓ Necessidade da segurança física em relação a localização dos componentes de T.I da empresa

2.2 Recursos

Os principais recursos para auditoria compreendem os recursos humanos, técnicos e financeiros:

A auditoria será realizada por 4 auditores especializados (ver seção 3.2) responsáveis e possuem ciência sobre o sigilo dos dados da empresa e da importância do devido trabalho ético sobre os dados e a segurança na empresa auditada SIN414.

Além dos 4 auditores em campo para acompanhar os recursos técnicos da empresa, conta também com um suporte de dúvida ao auditor fornecido pela Underlying localizada na cede de Itajubá, Minas Gerais, Brasil. Essa equipe de suporte permite que o auditor possa ter uma terceira opinião em caso de dúvidas sobre algum problema técnico de segurança relacionada a TI. Os auditores serão de total responsabilidade da Underlying, que receberão

linhas telefônicas operacionais para que possam comunicar em tempo integral com os responsáveis da empresa auditada e com a equipe de suporte de segurança em TI e com os seus superiores em caso de irregularidades ou ainda em caso de emergências.

Em relação as finanças, nos períodos de duração da auditoria os auditores também terão direito a todas as despesas cobertas pela underlyng, entre elas as refeições e os quartos individuais de hotel para o devido descanso depois de realizarem suas jornadas de trabalhos de, no máximo, 8 horas diárias. A empresa auditada ficará responsável pelo transporte dos auditores, junto de todo os equipamentos necessários, até a localização física da SIN414.

Para o melhor desempenho e eficiência dos auditores, a underlyng irá disponibilizar aos integrantes da equipe alguns recursos técnicos para a realização da auditoria com 4 notebooks e 4 smartphones aos seus auditores.

Cabe a SIN414 fornecer aos auditores uma cópia de todos os documentos que mostrem os processos existentes da empresa relacionados a TI e a segurança, e também, se houver, forneça os manuais dos sistemas utilizados.

Caso a empresa auditada não contenha alguns ou nenhum dos recursos a ela solicitados, o serviço pode se tornar mais extenso, atrasando o cronograma.

2.3 Metodologia

A auditoria foi desenvolvida por uma avaliação de riscos e controles de gerenciamento operando na organização. Para coletar informações, primeiramente realizamos visitas à entidade auditada, observando e coletando informações a respeito da infraestrutura e organização do ambiente da empresa. Posteriormente realizamos entrevistas com gerentes, funcionários da área de TI da SIN414 e outros funcionários que possuam algum tipo de contato direto e/ou indireto com o sistema de informações da organização. Dessa forma, pudemos identificar os riscos e controles existentes no âmbito organizacional e lógico da unidade da empresa auditada.

Basicamente os procedimentos foram os seguintes:

- ✓ Visitas técnicas à unidade auditada;
- ✓ Entrevistas aos colaboradores;
- ✓ Analise de todo o gerenciamento de segurança da SIN414: verificação de documentos, manuais, e acompanhamento do trabalho dos colaboradores;
- ✓ Identificação de riscos dentro dos sistemas e dos controles existentes para permitir que os objetivos de controle sejam alcançados;

A partir desses procedimentos, identificamos deficiências nos sistemas de segurança, produzimos propostas específicas para melhorar o ambiente de controle e elaboramos uma conclusão geral sobre o projeto e operação do sistema.

2.3.1 AVALIAÇÃO DA SEGURNÇA

Para que os auditores façam os testes de segurança e identifiquem os pontos fracos e fortes da empresa diante das queixas de ataques, eles realizaram **testes de penetração** aos sistemas da empresa, **verificação de acesso** aos lugares físicos, e **avaliação do acesso (lógico), controle de autenticação dos sistemas e análise dos equipamentos tecnológicos e informáticos.**

O teste de penetração visa realizar ataques aos servidores da empresa como se fossem atacantes a fim de identificar os pontos que devem ser cobertos para que torne o acesso às informações mais complexa possível. Os testes serão realizados após o

expediente de trabalho da empresa para não afetar o desempenho do serviço da auditada, ao menos que os responsáveis pela auditada prefira outro horário.

A verificação de acesso aos lugares físicos dos equipamentos tem como objetivo avaliar as instalações da empresa para definir se são adequadas ou não, identificar todos os colaboradores que devem de fato ter acesso ao local, e, também avaliar a necessidade do colaborador, conforme sua função, possuir o acesso lógico aos dispositivos informáticos e aos sistemas e dados. Para isso será realizado a Identificação das reponsabilidades dos colaboradores, dos papéis e dos objetivos de cada área. Depois deverá ser realizada a revisão dos contratos de trabalho para incluir, se necessário, a documentação de responsabilidade sobre as políticas de segurança da empresa e o devido sigilo em relação aos dados da empresa SIN414, que mesmo após seu desligamento ficará sujeito a punições de acordo com o Comissão de Valores Mobiliários (CVM) em caso de crimes como informações privilegiada, assim como indenização da empresa em caso de vazamento de dados internos.

A auditoria aos lugares físicos deve ocorrer junto ao trabalho dos colaboradores da SIN414, juntamente com perguntas de atitudes duvidosas que possam ocorrer aos encarregados da determinada área. A avaliação da autenticação do sistema usado pela auditada deve ser feito junto com os responsáveis pelos sistemas. Caso seja um sistema adquirido, o manual deve ser provido aos auditores para estudo de questões de confiabilidade e integridade. Nesse ponto serão considerados pontos como criptografia dos dados e como é garantido a autenticidade de um usuário logado.

Para a análise dos sistemas será verificado a presença de programas maliciosos em cada contexto, sendo essencial a validação de vulnerabilidades conhecidas em relação as versões de software utilizadas, assim como a necessidade e compatibilidade de atualizações para a garantia de segurança desses componentes. Além disso, cada sistema será validado em relação ao controle deles, sendo determinado a cadeia de acesso dado o fluxo do processo da empresa em relação a esse componente, limitando da melhor forma possível o acesso de pessoas não necessitadas e não autorizadas. Dado os fatores citados, deve ser validado também a necessidade de implementação de medidas de segurança específicas para cada serviço presente no sistema, podendo ele partir da aplicação de mecanismos de registro de logs para garantia do não repúdio, como também a necessidade de monitoramento e isolamento físico dos recursos envolvidos.

Quanto aos recursos tecnológicos físicos especificamente, será necessário a validação das portas físicas dos equipamentos, mapeando toda a necessidade de comunicação de recursos externos com o dispositivo através das portas de entrada e saída, nesse contexto, todo dispositivo conectado deve ser catalogado e sua necessidade documentada, dispositivos sem viabilidade justificada devem possuir os responsáveis definidos e interrogados em relação a essa conexão. Além disso, será avaliado a presença de patchs de software em relação ao equipamento, sendo verificado a necessidade de remoção do aparelho caso o suporte fornecido tenha sido descontinuado e problemas de segurança sejam identificados sem a possível solução dado essa falta de suporte.

No processo de análise dos componentes de rede, será mapeado todos os logs existentes em relação aos roteadores, switches e servidores de aplicação, identificando comportamento que caracterize um trafego e ações maliciosas dos usuários, com a tentativa de identificar responsáveis, e principalmente mapear futuras regras de segurança dado o contexto de ataques identificado nessa etapa. Quanto as soluções de firewall, todas as regras devem ser definidas a partir da limitação total dos recursos de rede, com regras específicas para liberação de acesso e comunicação aos recursos internos, essas regras serão revisadas e a validação de versionamento e vulnerabilidades também será aplicada.

Conforme observado as metodologias abordadas na auditoria visa verificar os softwares, hardwares e controlar o acesso ao físico ao local e aos equipamentos tecnológicos e controlar a autenticação dos responsáveis aos sistemas, ou seja, quais os devidos colaboradores devem possuir acesso aos recursos utilizados pelos sistemas seja ele físico ou lógico. Essas medidas são tomadas para que não haja acesso indevido aos dados, o que pode se tornar uma vantagem competitiva para outras empresas concorrentes ou para, infelizmente, venda de informações por colaboradores mal-intencionados aos concorrentes, cuja punição já foi mencionada anteriormente. Em outro cenário, o controle também ajuda a gerenciar o acesso aos recursos físicos liberando apenas quem é de confiança e têm um contrato assinado concordando com as políticas de sigilo de dados e informações da auditada.

Toda avaliação do sistema, em sua forma física e lógica, será feita de acordo com as metodologias descritas acima. Os principais pontos observados pelos auditores, assim como a solução proposta, serão apresentados em um relatório para que a auditada possa tomar as decisões, ficando sob total responsabilidade da auditada aceitar ou não as soluções propostas pelo relatório da auditoria.

2.4 CRONOGRAMA DA AUDITORIA

Para a realização da auditoria de forma eficiente deverá ser seguido todo o planejamento realizado, assim seguiu-se rigorosamente o cronograma planejado e todas as atividades projetadas a fim de que que sua realização fosse dentro do prazo previsto e contando sempre com a compreensão e colaboração da equipe interna da empresa audita. O cronograma apresentado na tabela a seguir irá estabelecer a carga horária prevista para cada uma das atividades da auditoria:

Atividades	Auditor	Assessor	Revisor	Inicio	Fim
Reunião com o cliente	Thiago	Ivan		01/06/2022	01/06/2022
Seleção da equipe	Lucas	Ivan	Leonardo	02/06/2022	02/06/2022
Planejamento	Ivan	Lucas	Thiago	03/06/2022	04/06/2022
Avalição de controle dos dados	Leonardo	Thiago	Ivan	05/06/2022	10/06/2022
Avaliação dos sistemas	Lucas	Leonardo	Ivan	10/06/2022	20/06/2022
Avaliação dos equipamentos	Leonardo	Thiago	Lucas	20/06/2022	25/06/2022
Avaliação da rede e do firewall	Ivan	Lucas	Thiago	26/06/2022	28/06/2022
Propor soluções	Thiago	Ivan	Lucas	28/06/2022	29/06/2022

Entrega do relatório	Leonardo	Lucas	Ivan	30/06/2022	30/06/2022

Tabela 1 - Cronograma da auditoria SIN 414

2.4.1 Período de execução da Auditoria

O serviço prestado pela Underlying deve ocorrer em um período no mínimo de 1 (um) mês, cuja carga será distribuída entre 4 auditores trabalhando em uma carga horária de no máximo 8 (oito) horas por dia, exceto aos sábados e domingos. Contudo, caso a auditada não forneça alguns ou nenhum dos recursos para a auditoria, o serviço poderá se estender até 2 meses dependendo da dificuldade de avaliação sem documentação, manuais e recursos necessários.

2.5 ATIVIDADES DA AUDITORIA

O presente tópico destina-se à descrição de todos as principais atividades da auditoria. A seguir as tabelas das atividades da Auditoria Interna constarão detalhadas e especificações como: o macroprocesso, a área, os objetivos, o tipo, o local, o escopo e os riscos de cada uma das atividades.

Nº da ordem: 1	**Descrição: Reunião com o cliente**
Macroprocesso	Comunicação
Área	Auditoria
Objetivos	Reunião para recolher os dados para iniciar a auditoria
Tipo	Administrativo
Local	Sala de reuniões
Escopo	• Colher as informações necessárias para a devida realização da auditoria
Riscos	• Risco de cancelamento da reunião

Tabela 2 - Atividade de auditoria 01: Reunião

Nº da ordem: 2	**Descrição: Planejamento**
Macroprocesso	Equipe de auditoria
Área	Auditoria

Objetivos	Planejamento
Tipo	Auditoria
Local	Externo
Escopo	• Recursos necessários • Área de abordagem • Metodologia de auditoria • Forma de avaliação da segurança
Riscos	• Planejamento não contemplar todo gerenciamento de segurança existente na empresa

Tabela 3 - Atividade de auditoria 02: Planejamento

Nº da ordem: 3	**Descrição: seleção da equipe**
Macroprocesso	Processo seletivo
Área	Auditoria
Objetivos	Seleciona os melhores auditores para avaliar e propor soluções de segurança
Tipo	Administrativa
Local	Externo
Escopo	• Fazer um processo seletivo • Formalizar equipe
Riscos	• Diferença de opiniões dos membros da equipe

Tabela 4 - Atividade de auditoria 03: Seleção da equipe

Nº da ordem: 4	**Descrição: avaliação de controle**
Macroprocesso	Controle de acesso
Área	TI

Objetivos	Fazer uma análise e verificação de acesso fisio e lógico
Tipo	Operacional
Local	Toda empresa
Escopo	• Verificar permissão de acesso lógico e físico • Validar documentos de política de segurança e sigilo dos dados • Atualizar o controle de acesso dos colaboradores
Riscos	• Falha na segurança

Tabela 5 - Atividade de auditoria 04: Avaliação de controle de acesso

Nº da ordem: 6	**Descrição: avaliação dos sistemas**
Macroprocesso	Softwares
Área	TI
Objetivos	Fazer uma análise de todos os softwares instalados
Tipo	Operacional
Local	Toda empresa
Escopo	• Verificar se existe softwares maliciosos • Verificar se existem atualizações não realizadas
Riscos	• Falha na segurança

Tabela 6 - Atividade de auditoria 05: Avaliação dos sistemas

Nº da ordem: 6	**Descrição: avaliação dos equipamentos**
Macroprocesso	Hardware
Área	TI
Objetivos	Analisar todas as máquinas para ver se estão em conformidade.
Tipo	Operacional

Local	Toda empresa
Escopo	• Verificar se as máquinas estão funcionando corretamente • Verificar se há falhas de hardware
Riscos	• Falha na segurança

Tabela 7 - Atividade de auditoria 06: Avaliação nos equipamentos

Nº da ordem: 7	**Descrição: avaliação da rede e firewall**
Macroprocesso	Rede
Área	TI
Objetivos	Analisar toda a infraestrutura da rede e o sistema de firewall.
Tipo	Operacional
Local	Toda empresa
Escopo	• Verificar se a rede está livre de defeitos • Averiguar se a rede é passível de ataques • Analisar se o firewall atente as políticas de segurança e seu controle
Riscos	• Falha na segurança

Tabela 8 - Atividade de auditoria 07: Avaliação da rede e firewall

Nº da ordem: 8	**Descrição: propor soluções**
Macroprocesso	Solução
Área	Auditoria
Objetivos	Depois da análise é preciso propor soluções
Tipo	Relatório
Local	Toda empresa
Escopo	• Propor soluções

Riscos	• Não adequação dos colaboradores

Tabela 9 - Atividade de auditoria 08: Proposta de Soluções

Nº da ordem: 9	**Descrição: Entrega de relatórios**
Macroprocesso	Solução
Área	Auditoria
Objetivos	Finalização da auditoria
Tipo	Relatório
Local	Setor de TI
Escopo	• Apresentar relatório
Riscos	• Responsáveis não aceitarem utilizar as propostas

Tabela 10 - Atividade de auditoria 09: Entrega de relatórios

2.6 Entrevistas

As seções a seguir especificaram quais colaboradores e áreas de TI foram responsáveis pelo fornecimento dos dados através da entrevista e também será apresentado a entrevista que foi aplicada a estes funcionários da SIN414.

2.6.1 Entrevistados Internos

A Underlyng gostaria de agradecer os funcionários da empresa SIN414 pela assistência providenciada durante o período de auditoria, e em especial, as seguintes áreas de TI e aos membros:

- Gerente de operações: Marco Antônio de Melo
- Técnico de TI: Alfredo Bustamante Silva
- Gerente supervisor de TI: Paulo costa Figueiredo
- Administrador de redes do Windows: João Cesar Bueno Filho

2.6.2 Questionário aos entrevistados internos

A constatação da realidade de trabalho com os funcionários de TI da empresa foi obtida na observação do serviço e práticas realizadas no dia e dia, e também via questionários aplicados aos responsáveis de TI descritos anteriormente. O questionário realizado pela equipe responsável da auditoria na SIN414 encontra-se abaixo:

Questionário aos colaboradores da SIN414
1. Qual sua formação profissional para compor a equipe da empresa SIN414?

2. Possui experiências anteriores na área de segurança de TI?
3. Como é o seu relacionamento interpessoal com a equipe no setor de TI?
4. Você conhece toda infraestrutura de TI na SIN414?
5. A empresa SIN414 foca na segurança de dados dos clientes?
6. Como são armazenadas as informações dos clientes e dos produtos?
7. Você utiliza e-mail pessoal para entrar em contato com clientes? E pen drive pessoal para realizar copias dos trabalhos da empresa?
8. Em sua opinião qual sistema da empresa tem deficiência no armazenamento de dados?
9. Qual a frequência em que você utiliza a internet por interesse particular?
10. Qual a frequência que ocorre um bloqueio de acessos a sites da internet quando a utiliza?
11. Com que frequência são enviados e-mails fora do interesse organizacional?
12. Quais os tipos de ataques são enfrentados pela SIN414? Quais as medidas tem sido tomadas ate o momento para mediar os ataques?
13. A informação da empresa SIN414 é classificada em termos de seu valor, requisitos legais, sensibilidade e criticidade para a organização? Se sim, como é feita esta classificação?
14. Há algum tipo de controle de acesso físico ao sistema de informações da organização?
15. Como é feito a atualização e controle de acesso logico e físico?
16. Há na empresa uma Política de Segurança da Informação? Caso afirmativo, que aspectos ela engloba?
17. Há alguma norma que diz respeito à não divulgação de informações confidenciais entre funcionários?
18. Há algum gerenciamento de riscos e de incidentes de segurança da informação presente na organização?

3. EQUIPE DE AUDITORES

Para a realização desta auditoria, foi necessário a definição de uma equipe de auditores da Underlying capaz de realizar as entrevistas e verificar todo o ambiente de trabalho de TI da SIN414 e com capacidade de análise e conhecimento técnico para propor soluções fáceis e uteis as falhas encontradas.

Para a devida auditoria foram incluídos além dos 4 auditores da Underlying mais os 4 colaboradores internos da empresa auditada, aqueles cujo cargos de responsabilidades gerenciais eram da área de TI da empresa e que foram apresentados na seção 2.6.1. e tiveram a responsabilidade de responder os questionários.

Para a seleção dos auditores da underlying foi realizado um processo seletivo criterioso para garantir a qualidade técnica da empresa de auditoria. O próximo tópico apresenta o processo de seleção realizado com base nos conhecimentos na área de Segurança de Informação onde os candidatos com melhores resultados foram selecionados para fazer parte do grupo de colaboradores da underlying.

3.1 PROCESSO SELETIVO DOS AUDITORES

Os auditores são profissionais especializados em segurança de informação, graduados em Sistemas de Informação ou Ciência da Computação. A escolha dos profissionais para ingresso na Underlying foi um processo seletivo teórico e prático que comprovou que eles realmente entendem de segurança e que podem realizar um excelente serviço quando o assunto é segurança de informação.

O primeiro estágio do processo seletivo é uma prova que envolve termos técnicos relacionados à auditoria e segurança. Underlying precisa certificar que seus colaboradores saibam o que eles estão fazendo na prática e saibam relacionar os termos auditoria e segurança.

O segundo estágio envolve uma prova prática. Os candidatos são submetidos a um teste de penetração em um sistema fictício desenvolvido pelo gerente nacional de auditoria de segurança na Underlying. Além do teste, os candidatos devem criar um relatório detalhados das falhas que encontraram no sistema e um meio de solucionar a falha.

Cada estágio tem uma pontuação total de 100 (cem) pontos. O primeiro estágio envolvendo 50 perguntas com valor de 2 (dois) pontos cada. E a pontuação do segundo estágio será avaliada pelo gerente nacional de auditoria e segurança da Underlying.

Os candidatos aprovados são aqueles que conseguem uma pontuação de no mínimo 70 (setenta) pontos em cada prova e uma média de 80 (oitenta) pontos.

3.2 COMPOSIÇÃO DA EQUIPE DE AUDITORES

A equipe dos 4 integrantes de auditores para a realização da auditoria da SIN414 é formada pelos seguintes colaboradores da Underlying:

- Lucas: 30 anos, graduado em Sistemas de Informação, especialista em Segurança Digital. Experiência de 10 anos com auditoria em segurança. Ingressou na Underlying em 2017 com uma nota média no processo seletivo de 93 e já atuou em mais de 500 casos de a auditoria de segurança no Brasil.

- Ivan L. V. Boas: 32 anos, graduado em ciências da computação e em Sistemas de Informação, especialista em Segurança e redes de computadores. Experiência de 7 anos com segurança de informação em redes de computadores. Ingressou na Underlying em 2018 com uma nota média no processo seletivo de 92 e já realizou mais de 420 casos de auditoria de segurança no Brasil.

- Leonardo: 28 anos, graduado em Ciência da Computação, especialista em TI e segurança. Experiências de 6 anos com segurança de infraestrutura e firewall. Ingressou na Underlying em 2018 com uma nota média no processo seletivo de 91 e já atuou em mais de 410 casos.

- Thiago: 27 anos, graduado em Ciência da Computação, especialista em segurança. Experiências de 8 anos com segurança empresarial. Ingressou na Underlying em 2019 com uma nota média no processo seletivo de 90 e já atuou em mais de 312 casos.

Equipe de auditoria Underlying	
Auditores	**Cargos**
Lucas	Analista de

	Segurança Digital
Ivan	Analista de Segurança em Redes de computadores
Thiago	Analista de Segurança
Leonardo	Analista de TI e Segurança

Tabela 11 - Equipe de auditores

4. FALHAS ENCONTRADAS

A equipe atuou de forma presencial nas auditórias de todos os setores da empresa, analisando o controle de acesso e averiguando todos os equipamentos tecnológicos, os sistemas operacionais e os softwares que estavam instalados em cada dispositivo informático. Também foram feitas as identificações de diversas fraquezas no sistema de controle da empresa que podem colocar os objetivos do sistema em risco. A tabela a seguir apresenta todas as falhas que foram encontradas durante a auditoria:

Falhas encontradas na SIN413			
Processo de auditoria	**Falhas**	**Descrição das falhas**	**Justificativas (se houver)**
Ordem 05: Análise do Controle de acesso (físico e lógico)	Sem política de segurança quanto ao uso de contas e dispositivos pessoais	Os funcionários utilizam pen drive e e-mail pessoal para transferir dados pessoais e sobre a empresa.	Os colaboradores não sabiam que não era permitido o uso de dispositivos e conta pessoais, pois desconheciam as políticas de segurança. Os gerentes alegaram que o estudo de políticas técnicas está sendo estudado pela TI em conjunto com o nível estratégico da empresa

	Ausência de senhas para impedir acessos indevidos	A rede interna onde são salvos todos os documentos importantes e confidenciais da empresa é de fácil acesso, visto que não há restrição de acesso a nenhuma pasta, basta realizar o mapeamento pois não é exigida nenhuma credencial.	Justificativa dado pelo técnico de TI é que o controle de acesso estava a um bom período desatualizado e os funcionários que foram remanejados nas diversas funções continuaram com os mesmos acessos. Mas as medidas técnico/operacionais cabíveis iriam ser tomadas para impedir o acesso a tais documentos.
	Controle de administrador indevido	Os computadores de utilizam do último ano de 2021 que forem auditados estavam todos com o perfil administrador habilitado e os usuários tinham livre acesso a todas as ferramentas.	O técnico de TI alegou que teve que colocar os estagiários para realizar o controle de acesso e que não houve uma averiguação do que havia sido realizado. Mas as medidas técnico/operacionais cabíveis iriam ser tomadas para impedir o acesso a tais documentos.
	Instalação e download da internet sem algum tipo de controle	Os computadores que os funcionários utilizam durante o expediente, dentro da empresa, permitem que os usuários instalem softwares baixados da internet.	Justificativa dado pelo gerente de TI é que a maioria dos funcionários do setor precisam fazer uso da internet para realizar seus trabalhos e para serem mais independentes tem

			tais direitos. Mas que irá rever esses direitos com os gerentes dos setores e revogar de todos os desnecessários.
Ordem 06 Analise dos sistemas (programas, sistema operacional, antivírus)	SO desatualizado	Os computadores e notebooks estavam com o sistema operacional XP que é um sistema operacional legado, descontinuado e sem atualizações de segurança, representando um risco para a empresa.	Segundo os gerentes da empresa a SIN414 estava com dificuldade financeiras para realizar a troca. Então seria solicitado novamente ao setor de finanças para a liberação da compra do SO atualizado.
	SO sem licença	Em torno de 30% dos computadores auditados foram constados que não possuíam licença de sistema operacional, pois estavam todas expiradas	O técnico de TI alegou já ter encaminhado a situação para financeiro da empresa analisar.
	Antivírus desativados e desatualizados e falta de treinamento aos funcionários para manter seu uso.	Os antivírus eram de fornecedores diferentes e grande maioria estava desativado pelos colaboradores ou por não saber utilizar ou pela licença estar já expirada.	Técnico de TI alegou que não há uma padronização dos antivírus instalados nos equipamentos dos setores da empresa, os usuários das maquinas relataram aos auditores que não sabiam como utilizar os antivírus. Os gerentes alegaram que não foram informados pelos demais

			colabores da empresa e que treinamentos pela TI seriam realizados para o devido uso e que as licenças expiradas seriam renovadas de modo a padronizar o Antivírus na empresa.
	Vírus	Todas as máquinas com os antivírus desativados ou com SO ilegítimo foram encontrados softwares maliciosos, e estavam com trojans, malwares ou spywares instalados.	Os Colaboradores justificaram a ocorrência pelo antivírus ter inspirado sua validação. Os gerentes alegaram que todas as medidas seriam tomadas pela equipe de TI para o firewall e a renovação do antivírus.
	Ausência dos registros dos programas.	Não foi encontrado documentação de controle sobre os registros de todos os softwares instalados nos equipamentos tecnológicos da empresa.	Todo o departamento de TI da empresa SIN414 constatou que de fato não possui nenhum registro dos softwares instalados.
	Pacote office sem licença	Todos os computadores auditados estavam com o pacote office desatualizado e com a licença expirada.	O técnico de TI alegou ter tomado as medidas cabíveis e está sobre analise do setor financeiro.

Ordem 07 Análise dos equipamentos informáticos e tecnológicos	Sem uso de senhas fortes	O acesso do roteador de alguns setores utiliza para a configuração da rede Wi-Fi o padrão de usuário (admin) e senha (admin).	O técnico de TI alegou não ter conhecimento, mas as medidas técnico/operacionais cabíveis iriam ser tomadas pela TI para implementar política de senhas e atualizá-las.
	Defeitos na memória e na HD	Por possuírem máquinas relativamente antigas, com 6 anos de uso, alguns dos computadores falharam nos testes de hardware e apresentaram defeitos principalmente na memória e no disco rígido.	Os funcionários alegaram que este problema foi imperceptível, mas que gera um pouco de lentidão ao utilizar o PC. A Area de TI disse estar sem recursos humanos suficientes para realização de testes mais periódicos nos equipamentos informáticos, mas que semestralmente os testes são realizados.
	Ausência de backup e de controle de backup	A empresa opta por ter um servidor de armazenamento local, e com isso realiza backups apenas mensamente e sem seu devido controle e teste.	Alegação do gerente de TI é que o direcionamento da empresa que tem anos de mercado e nunca precisou restaurar um backup era de realizar apenas mensamente para economizar tempo e custo.
	Capacidade de armazenamento muito baixa	Cada usuário também possui uma cota de utilização de e-mail padrão	Os responsáveis dos setores alegaram o não

		e quando isso chega no limite a empresa não possui um servidor ou uma nuvem dedicada para armazenar esses dados. Devido a isso muitos e-mails não são recebidos pelos clientes, fornecedores ou pelos próprios funcionários da organização.	conhecimento e que iriam solicitar ao financeiro para a aquisição de dispositivo de armazenamento externo ou para armazenamento em nuvem.
Ordem 08 Análise da rede e do firewall	Firewall obsoleto	O Firewall da SIN414 está totalmente desatualizado e obsoleto, com isso ele está vulnerável a ataques e invasões.	Como não havia políticas de segurança e nenhum controle foi constatado que não há atualização do firewall a 2 anos. O gerente de TI alegou que com a implantação das novas políticas de segurança, a atualização do firewall seria realizada em seguida.
	Firewall não atende as políticas da empresa em relação de ao uso de e-mails	Problemas na utilização de e-mails, onde vários colaboradores compartilham informações fora do interesse da empresa, enviando diversos tipos de arquivo pelo e-mail eletrônico, gerando riscos de segurança pois o firewall deixa passar diversos dados com conteúdo malicioso.	Como não havia políticas de segurança e nenhum controle foi constatado que não há atualização do firewall a 2 anos. Mas as medidas técnico/operacionais cabíveis estavam sendo tomadas para a implantação de políticas de segurança e atualização do firewall.
	Firewall não	Vários sites irrelevantes ao	Como não havia

	atende as políticas da empresa em relação ao uso da internet	negócio são utilizados pelos usuários podendo expor informações da empresa a terceiros, arquivos fora do interesse organizacional são baixados e enviados sem uma fiscalização mais minuciosa do firewall.	políticas de segurança e nenhum controle foi constatado que não há atualização do firewall a 2 anos. Mas as medidas técnico/operacionais cabíveis estavam tomadas para a implantação de políticas de segurança e atualização do firewall.
	Sem controle de IP	Os equipamentos da rede não possuem nenhum registro sobre os IP de cada usuário, dos IP's de VoIP e dos IP's das impressoras.	O departamento de TI da empresa SIN414 constatou a ausência do controle sobre os IPs da rede da empresa.
Outros:	Não existe gerenciamento de risco e incidentes	Não existe na empresa a realização de um gerenciamento de riscos, de acordo com um processo formalizado, de forma a mitigar e reduzir possíveis e eventuais impactos negativos.	Os responsáveis alegaram a existência do gerenciamento de incidentes apenas de forma informal, mas de fato nem todos possuíam o conhecimento de como reagir perante os incidentes, pois não existia uma documentação e treinamento a fim de informar todos os colaborares para resolver os problemas que surgiam. Então iram tomar as medidas para formalizar o gerenciamento de

			risco e incidentes dentro da empresa.

Tabela 12 - Falhas se segurança da SIN413

A seguir serão detalhadas algumas das principais falhas mais recorrentes e de alto nível de prioridade para que sejam sanadas e não venham a prejudicar a segurança da empresa SIN414:

1. **Falta de política de segurança:** A Política de Segurança da Informação não foi amplamente divulgada a todos os usuários de recursos de TI, sejam eles internos ou externos. Esta se apresenta na intranet, porém não se implementaram ações objetivando sua disseminação rumo à mudança cultural interna da empresa. Observou-se que não existe norma interna que institui critérios para uso seguro das redes sociais, se é que deveriam ser permitidas. A ausência desse comprometimento da SIN414 com a educação de seus funcionários pode comprometer os recursos físicos e lógicos da empresa.
2. **Falta de Atualização de programas, SO e não uso de antivírus**: A instalação de um software antivírus e dos pacotes de segurança do em todos os computadores da rede se faz necessário, juntamente com a monitoração destes para garantir que eles sejam mantidos sempre atualizados. A instalação dos pacotes de segurança ajudará a garantir que a integridade do sistema e dos dados seja mantida e que as atualizações de segurança lançadas pelo fornecedor do software sejam aplicadas em tempo hábil. A falta da garantia de que os computadores da rede não possuem um software antivírus atualizado e que os pacotes de segurança recentes do sistema não estão instalados aumenta o risco de que atividades não autorizadas ocorram e que as vulnerabilidades conhecidas do Windows sejam exploradas.
3. **Ausência de controle e Configurações dos dispositivos de firewall**: Foi identificado que o monitoramento de verificação de atualização não somente do antivírus, mas como de todos os pacotes de segurança dos dispositivos de firewall que não estão sendo controladas e nem atualizadas regularmente pela atual equipe de TI da empresa. Após a definição de políticas de segurança as regras testadas e efetivas devem serem implantadas no Firewall para ajudar a minimizar os riscos de acessos na Intranet sem autorização. A revisão das regras definidas no Firewall demonstrou evidências claras de que elas são proativamente seguras. No entanto, dois pontos de preocupação foram identificados em relação à frequência de atualização de vírus e pacotes de segurança. Se o antivírus e os pacotes de segurança não são mantidos atualizados e confirmados como tal por meio da revisão periódica e testes de invasão na rede, existe um alto risco de que um acesso não autorizado possa ocorrer na Intranet da empresa auditada.
4. **Ausência de controle e testes sobre o backup dos dados**: os arquivos confidenciais da empresa e de seus clientes são armazenados no servidor, uma falha de segurança nessa rede pode ser abalar a reputação da empresa com

seus clientes. Devido aos custos a empresa opta por ter um servidor de armazenamento local, e com isso realiza backups mensamente. Isso é uma imprudência e falha de segurança gravíssima, pois se a HD do servidor for corrompida, ou se o backup for mal realizado e não foi averiguado no teste isso irá impactar diretamente na empresa e nos clientes, a empresa poderá não atender seus clientes e ainda terá de refazer retrabalhos caso perca os documentos importantes e que não sejam possíveis sua recuperação.

5. SOLUÇÕES PROPOSTAS

Após a análise realizada e os problemas esclarecidos para que a empresa auditada SIN414 consiga resolver os problemas atuais e os futuros acerca da segurança da informação será apresentado as seguintes propostas, conforme a tabela a seguir:

Soluções propostas			
Falhas	**Prioridade**	**Fase Atual**	**Soluções propostas**
Sem política de segurança quanto ao uso de contas e dispositivos pessoais	Alto	Estudo	• Realizar a implantação da política de segurança o quanto antes e realizar treinamento nos colaboradores para que tenham ciência e conhecimento do uso da mesma. • Incluir em sua política de segurança a não permissão mais a utilização de pen drives de terceiros em seus computadores. Assim, os arquivos devem ser enviados aos clientes via e-mail, evitando possível contaminação por software malicioso através de dispositivo contaminado. • Conscientizar os funcionários quanto ao compartilhamento de informações apenas de relevância ao negócio seja por e-mail eletrônico da organização e através da rede externa. • Considerar na Política de Segurança da Informação da SIN414, critérios de uso seguro das redes sociais ou bloquear o acesso a elas. • Estabelecer ações rotineiras para que as políticas e normas de segurança da informação se tornem conhecidas, acessíveis e observadas por todos os funcionários.
Setores da empresa sem	Médio	Implantação	• Atualizar frequentemente o controle de acesso limitando as permissões de usuário para evitar que

o devido controle de acesso.			os funcionários tenham acesso a recursos avançados do sistema. • A TI deve considerar que as contas de administração são restritas a usuários autorizados e que estes direitos não são concedidos a ninguém, a menos que exista um requisito essencial para sua concessão. • Apenas o setor de TI da empresa SIN414 deve ter acesso ao usuário administrador • A TI deve criar uma conta para cada usuário com privilégios de usuário comum, que estão apenas limitados a usarem o computador e notebook, mas sem poderem conseguir realizar modificações e instalações.
Ausência de senhas para impedir acessos indevidos	Médio	Implantação	• Criar senhas fortes para acesso aos dados pertinentes conforme o setor e função
Instalação e download da internet sem algum tipo de controle	Médio	Implantação	• Para que um sistema seja seguro e confiável, é necessário que se tenha um controle geral de tudo que é instalado nas máquinas, para isso, o setor de TI da SIN414 deverá permitir a instalação nos dispositivos apenas programas relacionados aos serviços utilizados pela empresa. • Estudar caso para revogar direitos de instalação de todos os funcionários e ficar apenas a cargo da TI tais responsabilidades. • Para inibir instalações indesejadas a TI deverá atualizar o controle de permissões, realizar o monitoramento e manter atualizado o firewall.
SO desatualizado	Alto	Estudo	• Realização da a troca dos sistemas operacionais das máquinas que estão utilizando Windows XP por Windows 10, pois as maquinas possuem o hardware necessário para tal mudança. • Estudar a possibilidade de implantar um SO como o Linux, levando em conta o devido treinamento para seu uso adequado.
SO sem	Alto	Estudo	• Realizar a troca para o sistema original adquirindo

licença			o seu registro • Estudar a possibilidade de implantar um SO como o Linux, levando em conta o devido treinamento para seu uso adequado • A empresa SIN414 deve adquirir licenças de sistema operacional genuínas para todas as máquinas, pois só assim elas receberão em dia os pacotes de atualizações e correções de segurança, fazendo assim que diminua o risco de invasão por parte de exploração de uma falha no sistema operacional.
Antivírus desativados e desatualizados e falta de treinamento aos funcionários para manter seu uso.	Alto	Implantação	• Padronização dos antivírus utilizados pela empresa, • Elaboração de um controle de licenças; • Treinamento e disponibilização de documentos para os usuários com passo a passo para utilização dos serviços básicos dos antivírus, a troca dos antivírus desativados e remoção do software malicioso.
Vírus	Alto	Implantação	• Devem ser adquiridas licenças do antivírus, preferencialmente padrão, para todos as estações e para o servidor de modo a realmente proteger contra trojans, malwares e spywares. • Utilizar firewall adequadamente; • Deixar antivírus sempre ativo; • Seguir rigorosamente a política de segurança definida pela organização • Atualizar sempre o SO e softwares comerciais • Não utilizar só ou programas piratas • Não abrir sites que não atendam a empresa • Não abri e-mails desconhecidos
Ausência dos registros dos programas.	Alto	Inexistente	• Implantar o gerenciamento de risco • Manter (criar e atualizar) sempre o registro e o histórico de todos os SO, e de todos os programas utilizados, principalmente os pagos. • Manter (criar e atualizar) registro de incidentes de

			todos os SO e programas utilizados.
Pacote office sem licença	Alto	Estudo	• Estudar a possibilidade de implantar sistema livre, mas levando em conta o devido treinamento para seu uso adequado • Caso não opte por software livre a empresa SIN414 deverá adquirir licença paga para todos os softwares que são utilizados por seus funcionários, visto que utilizar softwares não licenciados é prejudicial para a segurança de todo o sistema, pois softwares não licenciados não recebem atualizações de correção e melhorias, e a empresa ainda corre sério risco de sofrer com processos e multas caso opte por pirataria. • Ao realizar a aquisição original do software deverá manter todos os registros documentados
Equipamentos da rede sem uso de senhas fortes	Alto	Implantação	Reconfigurar usuário e senha do roteador para uma senha forte, utilizando letras maiúsculas, minúsculas, caracteres especiais e números.
Defeitos na memória e na HD	Médio	Reforçar melhorar	• Contratar mais profissionais Técnicos de TI para aumentar a periodicidade da realização de testes de hardware • Realizar a troca e a manutenção física dos dispositivos e equipamentos com defeitos • Realizar a manutenção mensalmente dos equipamentos pela equipe técnica de TI da empresa • Máquinas que possuem mais de 6 anos de uso devem ser substituídas para que não haja perda de desempenho no serviço por estarem obsoletas.
Ausência de backup e de controle de backup	Alto	Inexistente	• Backup podem ser programados e realizados fora do horário de trabalho economizando tempo dos colaboradores (sem necessidade de paralisá-los) e o custo em caso de perdas dos dados seria muito maior comparado ao custo de um dispositivo de armazenamento externo. • Realizar o backup diário (ou semanalmente se não for economicamente possível) • Utilizar HD externo para duplicar o backup dado a

			importância dos dados a organização ou contratar uma empresa na nuvem para manter os dados do backup seguros e fáceis de restaurar quando vier a precisar utilizá-los. • Realizar teste do backup realizado para averiguar sua conformidade • Manter (criar e atualizar) o controle de backup pela TI
Capacidade de armazenamento muito baixa	Média	Estudo	• Para armazenamento dos e-mails que passam do limite da cota deveria ser contrato o armazenamento na nuvem que são dedicados às organizações. • Compra de HD externo para armazenamento dos dados, mas atentar para a realização dos testes.
Firewall obsoleto	Alta	Implantação	• Validar as políticas de barragem do firewall, ou se possível a atualização de um firewall que dê suporte de maneira mais efetiva a toda estrutura de rede que a organização exige.
Firewall não atende as políticas da empresa em relação de ao uso de e-mails	Alta	Implantação	• Admitir funcionários de Segurança em TI qualificados que realizem a manutenção, fiscalização e monitoramento através do firewall em relação aos conteúdos acessados pelos usuários da organização. • Deve-se considerar a garantia de que a atualização do antivírus e dos pacotes de segurança dos dispositivos de firewall sejam mantidas e confirmadas como tal mediante análises periódicas de monitoramento ou testes de invasão na rede da SIN414.
Firewall não atende as políticas da empresa em relação ao uso da internet	Alta	Implantação	• Admitir funcionários de Segurança em TI qualificados que realizem a manutenção, fiscalização e monitoramento através do firewall em relação aos conteúdos acessados pelos usuários da organização. • O departamento de informática deve colocar bloqueio a sites impróprios que podem ser acessados por funcionários. • A empresa SIN414 deve investir em uma rede segura com um firewall atualizado e

			constantemente ativo, para ficar alerta e bloquear qualquer tentativa de acesso não autorizado a sua rede. • Deve-se considerar a garantia de que a atualização do antivírus e dos pacotes de segurança dos dispositivos de firewall sejam mantidas e confirmadas como tal mediante análises periódicas de monitoramento ou testes de invasão na rede da SIN414.
Sem controle de IP	Alto	Inexistente	• O departamento de informática deve manter controle sobre suas faixas de ip's e saber qual ip é destinado a cada usuário, além de separar parte da faixa apenas para impressoras e VoIP's. • Deverá manter (criar e atualizar) sempre o registro e o histórico de todos os ip's dos equipamentos da rede • Também deverá manter (criar e atualizar) registro de incidentes referentes as questões de TI, e principalmente cerca da operação para controlar a indisponibilidade da Rede.
Ausência de gerenciamento de risco	Alto	Inexistente	• Elaborar um procedimento formalizado de gerenciamento de riscos de TI e executá-lo conforme as necessidades técnicas da área e institucionais, visando a mitigação e redução dos riscos residuais e inerentes à área de TI.

Tabela 13 - Soluções propostas pela auditoria

Recomendações importantes:

- As soluções que se encontram em processo de implantação devem ser finalizadas, principalmente aquela de alta prioridade devem ter a preferência na sua conclusão.
- As soluções que se encontram em processo de estudos devem finalizar o processo de analise o quanto antes pela gerência e alta administração e também deve realizar programação da sua implantação, principalmente para aquelas de alta prioridade. Aconselha-se a empresa a realizar o investimento (aprovar) e implementar o quanto antes as soluções de alta prioridade para sanar tais falhas encontradas.
- As soluções que se encontram inexistentes devem ser estudadas, analisadas pela gerência e alta administração o quanto antes, na ordem principalmente daquelas de alta prioridade, em especial para o backup. Tais analises devem ser realizadas em todos os níveis tático, estratégico e operacional, contando com a colaboração de todos os colaborares. Aconselha-se a empresa a realizar o investimento (aprovar) e implementar o quanto antes nas soluções de alta prioridade para evitar os problemas de segurança e

melhorar o trabalho dos seus colaboradores de modo a gerar valor aos clientes da organização.

6. AVALIÇÃO DA EQUIPE

Órgão/Entidade: SIN 414 – Universidade Federal de Itajubá

Objetivo da Fiscalização: Avaliar a gestão e uso de TI.

Visando aprimorar a qualidade do serviço referente a segurança de informação da empresa Underlying solicitamos que o seguinte formulário seja preenchido conforme a satisfação referente aos tópicos indicados. A escala varia de discordo completamente até concordo completamente.

Tópico	Discordo completamente	Discordo	Neutro	Concordo	Concordo Completamente
1 – Acerca da Identificação dos problemas					
1.1 - O processo de auditoria foi realizado na data indicada?					
1.2 - A empresa foi informada com antecedência sobre a(s) data(s) da auditoria?					
1.3 - A auditoria foi encerrada no tempo proposto?					
2 - Acerca das Soluções propostas					
2.1 - As soluções propostas resolveram os problemas encontrados?					
2.2 - O custo das soluções foram aceitáveis?					
2.3 - O tempo necessário para a implementação das soluções foram aceitáveis?					
3 - Acerca da Postura profissional da equipe					
3.1 - Houve boa comunicação dos membros da equipe durante a auditoria?					
3.2 - Os problemas encontrados foram devidamente expostos e explicados no relatório e nas reuniões?					

3.2 - As soluções propostas foram devidamente expostas e explicadas no relatório e nas reuniões?					
4 - Acerca da Satisfação geral da auditoria					
4.1 - De forma geral, os serviços prestados foram satisfatórios?					
4.2 - Você recomendaria os serviços da Underlying?					
Por favor, utilize as linhas abaixo para fazer comentários, sugestões, críticas ou elogios que julgue necessário. Sua opinião é importante e contribuirá para melhorar a qualidade dos trabalhos conduzidos pela Underlying					

7. CONCLUSÃO

Após a escolha da equipe, do planejamento realizado a fim de coletar dados sobre as inconsistências na TI, foram realizadas entrevistas, observações e análise do ambiente, dos documentos, equipamentos, redes, sistemas e foram detectados alguns problemas no sistema de segurança de TI da empresa que causam prejuízos para ela, foi apresentada, por fim, diversas propostas de soluções para a SIN414.

O processo de auditoria de TI de faz extremamente necessário em todas as empresas que disponha de um setor de TI, para que possa ser feita a uma varredura completa e identificar possíveis inconformidades. Ao final da auditoria, pode perceber que as vulnerabilidades que estão presentes na empresa foram geradas por vários motivos como questão financeira, ausência de treinamento e conhecimento por parte dos colaboradores, mas em sua maior parte pelas deficiências das políticas de segurança da empresa.

A definição de políticas e a nova aderência a conformidade estabelecida pela auditoria garante que os sistemas da empresa terão uma maior cobertura dos aspectos de segurança, reduzindo o escopo de riscos em relação aos sistemas de T.I., que anteriormente era muito alta.

A implementação das soluções propostas se faz essencial dado o alto nível de vulnerabilidades graves e de alto impacto identificadas nos sistemas. Desse

modo, a garantia de segurança é necessária pela possibilidade dos danos gerados pelos ataques ao sistema, que poderiam comprometer a confiança dos clientes em relação a empresa, trazendo também diversos impactos financeiros, não só pela perda de dados e impacto da indisponibilidade da T.I. que ocasionaria a indisponibilidade dos processos de negócio, mas também pela inconformidade da empresa em relação aos órgãos reguladores, que cobram uma postura adequada da organização em relação a tecnologia, principalmente quando se tem fluxo de dados sensíveis de pessoas nos processos da empresa.

Assim, a Underlying recomenda fortemente o alinhamento das soluções tecnológicas conforme o proposto no documento, trazendo uma maior segurança para o ambiente empresarial e uma maior conformidade em relação aos órgãos reguladores, garantindo a segurança de todos os envolvidos nos processos da organização.

8. FINALIZAÇÃO

Ivan L. V. Boas

Analista de Segurança em Redes de computadores

Lucas T. Blazzi

Analista de Segurança Digital

Leonardo

Analista de TI e Segurança

Thiago

Analista de Segurança

De acordo com o documento, submeto à Diretoria as recomendações realizadas para a apreciação e, em caso de acolhimento, conversão em determinação às unidades envolvidas para que sejam cumpridas e/ou se pronunciem a respeito, conforme o caso.

Bruno Guazzelli Diretor – SIN 414

Itajubá, 25 de junho de 2022.

9. ANEXO - A

Memorando de Planejamento de Auditoria de Sistemas de Informações

Introdução

Este memorando descreve os objetivos, o escopo (abrangências) dos procedimentos a serem avaliados e as abordagens que devem ser adotadas pela equipe de auditoria de sistemas de informações que teve como objetivo verificar adequação da geração, tratamento, divulgação, acesso e arquivamento das informações do cliente SIN414 para o ano findo em 31 de dezembro de 2022. Conforme o memorando de planejamento de auditoria geral para o cliente, a extensão do uso de informática pelo SIN414 foi classificada como moderada. A equipe de auditoria das demonstrações de segurança adotou a estratégia de confiança nos controles internos de todos os sistemas de informações computadorizados.

Escopo

Conforme acordado na reunião de planejamento, o escopo do trabalho de auditoria de sistemas obedecerá ao seguinte: Entendimento global e atualização das seguintes informações: (1) Processo e workflow da classificação da informação; (2) Ambiente de Sistemas de Informações; e (3) Gestão dos Riscos de Segurança da Informação:

- Identificar e atualizar a compressão dos controles de sistemas aplicativos e os controles gerais do computador;
- Programar testes de controles que minimizam os riscos identificados para o sistema aplicativo de (Nome do sistema);
- Verificar a adequação da geração, tratamento, divulgação, acesso e arquivamento das informações na empresa SIN414.

Administração de Considerações Especiais

Data de Início: 01/06/2022

Ordem de Serviço: 113/2022

Endereço da empresa: Rua machado Belo, 50, Centro, Itajubá, MG

Pessoa chave: Bruno Guazzelli

Data limite para entrega do relatório: 31/06/2022

Formato do relatório: Padrão

Estimativa de Horas

De acordo com o tempo de execução das tarefas e os profissionais envolvidos estimamos o trabalho em 640 horas. De acordo:

_____

Bruno Guazzelli

Diretor – SIN 41

Itajubá, 01 de junho de 2022