POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

Prefácio

A informação é um dos principais patrimônios do mundo dos negócios. Um fluxo de informação de qualidade é capaz de decidir o sucesso de um empreendimento.

Mas esse poder, somado à crescente facilidade de acesso, faz desse "ativo" um alvo de constantes ameaças internas e externas.

Quando não gerenciados adequadamente, esses riscos e ameaças podem causar consideráveis danos a **VEMCARD**, e prejudicar nosso crescimento e vantagem competitiva.

Atentos a isso, publicamos a Política de Segurança da Informação, o alicerce dos esforços de proteção à informação da **VEMCARD**.

Política da Informação

Esse documento tem caráter confidencial e restrito a **VEMCARD**, não podendo ou devendo ser redistribuído, sendo a infração passível de punição pelas regras disciplinares internas, bem como ações legais.

1. Introdução

A segurança da informação é um dos assuntos mais importantes dentre as preocupações de qualquer instituição.

Confidencialidade, integridade e disponibilidade da informação estão diretamente ligadas à segurança.

Confidencialidade**:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

Disponibilidade**:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Temos neste documento um conjunto de instruções e procedimentos para normatizar e melhorar nossa visão e atuação em segurança.

1.1 O que é informação?

A informação é um ativo que, como qualquer outro é importante para os negócios, tem um valor para a organização e consequentemente necessita ser adequadamente protegida.

A informação pode existir de diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou através de meios eletrônicos, mostrada em filmes ou falada em conversas. Seja qual for a forma pela qual ela é apresentada, transmitida, armazenada ou compartilhada, é recomendado que a mesma seja protegida adequadamente.

1.2 O que é segurança da informação?

A segurança da informação protege a informação de diversas ameaças para garantir a continuidade dos negócios, a integridade e a disponibilidade dela.

1.3 O que é uma política de segurança da informação?

Política de segurança é uma série de normas internas padronizadas pela instituição que devem ser seguidas à risca para que todas as possíveis ameaças sejam minimizadas e combatidas eficientemente pela equipe de segurança.

1.4 A instituição e a política de segurança da informação

Todas as normas aqui estabelecidas deverão ser seguidas à risca por todos os funcionários, parceiros e prestadores de serviços. Ao receber essa cópia da política de segurança, o(a) Sr.(a) comprometeu-se a respeitar todos os tópicos aqui abordados e está ciente de que seus e-mails e navegação na internet podem estar sendo monitorados. A equipe de Tecnologia e Segurança da Informação, encontra-se a total disposição para saneamento de dúvidas e auxílio técnico.

1.5 O não cumprimento dessa política?

O não cumprimento dessas políticas acarretará medidas disciplinares.

2. Educação e segurança

Todo funcionário deve ser treinado adequadamente para as questões de segurança.

Nenhum pré-requisito técnico é necessário, visto que o treinamento abordará o contexto comportamental do usuário, e não os aspectos técnicos, os quais serão delegados à equipe especializada.

2.1 Autenticação

A autenticação nos sistemas de informática é feita por meio de senhas.
Senhas como nome do usuário, combinações simples (abc123), substantivos (casa, meia, cadeira, Brasil), datas (11092001), números de telefones e outros são extremamente fáceis de descobrir.

2.1.1 Política de senhas

A senha deverá conter no mínimo oito (8) caracteres alfanuméricos (letras, números e caracteres especiais) com diferentes caixas (maiúsculo e minúsculo).

Para facilitar a memorização das senhas, utilize padrões mnemônicos.

Por exemplo:

• eSus8C (eu SEMPRE uso seis 8 CARACTERES)

• 9SSgianc (9 Senhas Seguras garantem integridade a nossa corporação)

• s3Nh45 (palavra senha onde o “3” substitui o “E”, o “4” o “A” e o “5” o “S”).

Como selecionar e manter senhas.

As senhas são efetivas apenas quando usadas corretamente, requer alguns cuidados na sua escolha e uso, como:

- ✓ Não utilize palavras que estão no dicionário (nacionais ou estrangeiros);
- ✓ Não utilize informações pessoais fáceis de serem obtidas, como o número de telefone, nome da rua, nome do bairro, cidade, data de nascimento etc.;
- ✓ Não utilize senhas somente com dígitos ou com letras;
- ✓ Utilize senha com, pelo menos, oito caracteres;

- ✓ Misture caracteres maiúsculos e minúsculos;
- ✓ Misture números, letras e caracteres especiais;
- ✓ Inclua, pelo menos, um carácter especial;
- ✓ Utilize um método próprio para lembrar da senha, de modo que ela não precise ser escrita em nenhum local, em hipótese alguma;
- ✓ Não anote sua senha em papel ou em outros meios de registro de fácil acesso;
- ✓ Não utilize o nome do usuário;
- ✓ Não utilize o primeiro nome, o nome do meio ou o sobrenome;
- ✓ Não utilize nomes de pessoas próximas, como da esposa(o), dos filhos, de amigos;
- ✓ Não utilize senhas com repetição do mesmo dígito ou da mesma letra;
- ✓ Não forneça sua senha para ninguém, por razão alguma;
- ✓ Utilize senhas que podem ser digitadas rapidamente, sem a necessidade de olhar para o teclado.

LEMBRE-SE:

Sua senha não deve ser jamais passada a ninguém, nem mesmo para a equipe de segurança.

Caso desconfie que sua senha não está mais segura, sinta-se à vontade para mudá-la.

Tudo que for executado com a sua senha será de sua inteira responsabilidade, por isso tome todas as precauções possíveis para mantê-la secreta.

2.2 E-mails

Grande parte de nossa comunicação do dia a dia passa-se através de e-mails. Mas é importante lembrar, que hoje, os grandes incidentes com informações, chegam por meio eletrônico.

Devemos lembrar que os vírus atuais são mandados automaticamente. Isso significa que um e-mail de um cliente, parceiro ou amigo, pode não ter sido encaminhado por ele, o que chamamos de **e-mail malicioso**.

2.2.1 Política de e-mail

Nossos servidores de e-mail encontram-se protegidos contra vírus e códigos maliciosos, mas algumas atitudes do usuário final são requeridas:

O e-mail deve ser utilizado de forma consciente, evitando qualquer tipo de perturbação a outras pessoas, seja através da linguagem utilizada, frequência ou tamanho das mensagens.

Desconfie de todos os e-mails com assuntos estranhos ou em idioma estrangeiro.

Evite o envio de grande quantidade de mensagens de e-mail (spam) que, de acordo com a capacidade técnica da Rede, seja prejudicial ou gere reclamações de outros usuários.

Isso inclui qualquer tipo de mala direta, como, por exemplo, publicidade, comercial ou não, anúncios e informativos, ou propaganda.

Não reenvie e-mails do tipo corrente, aviso de vírus, avisos da Microsoft, AOL, Symantec, criança desaparecida, criança doente, pague menos em alguma coisa, não pague alguma coisa, etc.

Evite o uso do e-mail da instituição para assuntos pessoais, para tal, utilize seu e-mail particular.

As contas de e-mail, terminadas em **@vemcard.com.br**, não são de propriedade particular e sim institucional e, como tal, poderão passar por auditorias, onde, constatando-se irregularidades, o usuário prestará contas de seu uso.

Não mande e-mails para mais de 10 pessoas de uma única vez.

Evite anexos muito grandes. O tamanho do e-mail mais o anexo está limitado em 10Mb.

Não clique em links do tipo “Clique para remover”.

Os seguintes anexos estão bloqueados em nossos servidores de e-mail: EXE, BAT, SRC, LNK, COM, DLL, SHS, VBS.

Caso algum cliente ou fornecedor necessite enviar um e-mail com um dos anexos citados, você deverá entrar em contato com o departamento de TI (Tecnologia da Informação) que providenciará uma solução para sua necessidade.

Caso a **VEMCARD**, julgue necessário, haverá bloqueios:

1. De e-mail com arquivos anexos que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos;

2. De e-mail com arquivos anexos, em Planilhas Eletrônicas e Arquivos Compactados;

3. De e-mail para destinatários ou domínios que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos;

• É proibido, forjar qualquer das informações do cabeçalho do remetente;

• Não é permitido, má utilização da linguagem em respostas aos e-mails comerciais, como abreviações de palavras, uso de gírias;

• É obrigatória a manutenção da caixa de e-mail, evitando acúmulo de e-mails e arquivos inúteis;

• Para certificar-se que a mensagem foi recebida pelo destinatário, deve-se, se necessário, utilizar procedimentos de controles extras para verificar a chegada da mensagem, devem ser solicitadas notificações de “recebimento” e “leitura”;

• Não execute ou abra arquivos anexados enviados por emitentes desconhecidos ou suspeitos;

• Não abra arquivos anexados com as extensões .bat, .exe, .src, .lnk e .com se não tiver certeza absoluta de que solicitou este e-mail;

• Não devem ser enviadas mensagens de correio eletrônico cujo conteúdo seja confidencial, não podendo tornar-se público, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei.

2.3 Internet

A Internet é indiscutivelmente uma das mais poderosas ferramentas de trabalho.

Devemos encará-la dessa forma dentro da instituição, porém, no ambiente de trabalho, o uso recreativo da Internet não é permitido.

2.3.1 Política de Internet

Esse tópico visa definir as normas de utilização da Internet que engloba desde a navegação a sites, downloads e uploads de arquivos.

O uso e o acesso à Internet serão restritos aos seguintes tópicos:

• somente a navegação de sites é permitida. Casos específicos que exijam outros protocolos deverão ser solicitados diretamente à equipe de segurança com prévia autorização do supervisor do departamento.

• Acesso a sites com conteúdo pornográfico, jogos, bate-papo, apostas e assemelhados estará terminantemente proibido e monitorado na tentativa do acesso.

• é proibido o uso de ferramentas P2P (Kazaa, Morpheus, eMule, Torrent e etc).

• A utilização de serviços streamming (videos do youtube, globo esporte e

afins) estarão sujeitos a monitoramento para controle de uso de banda,

para que seja evitada a queda no desempenho de navegação web.

• é proibida a divulgação de informações confidenciais da **VEMCARD**, em grupos de discussão, listas ou bate-papo, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei;

Caso a **VEMCARD,** julgue necessário haverá bloqueios de acesso à:

1. arquivos que comprometa o uso de banda ou perturbe o bom andamento

dos trabalhos;

2. sites de Mensageria, como por exemplo, WhatsApp Web e de Comunicação, como por exemplo, Skype;

3. domínios que comprometa o uso de banda ou perturbe o bom andamento

dos trabalhos;

Obrigatoriedade da utilização do programa Mozilla Firefox, Internet Explorer e Google Crome, ou outro software homologado pelo departamento técnico, para ser o cliente de navegação;

Lembrando novamente que o uso da Internet estará sendo auditado constantemente e o usuário poderá vir a prestar contas de seu uso.

2.4 Utilização da Rede

Esse tópico visa definir as normas de utilização da rede que abrange o login,

manutenções de arquivos no servidor e tentativas não autorizadas de acesso.

Estes itens serão abordados para todos os usuários dos sistemas e da rede de computadores da **VEMCARD.**

2.4.1 Política de utilização da Rede

Não são permitidas tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta. Isso inclui acesso aos dados

não disponíveis para o usuário, conectar-se a servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes.

Não são permitidas tentativas de interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui ataques, tentativas de provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor e tentativas de invadir um servidor.

Antes de ausentar-se do seu local de trabalho, o usuário deverá fechar todos os programas em uso, evitando, desta maneira, o acesso por pessoas não autorizadas, efetuar o logout/logoff da rede ou bloqueio do computador através de senha.

O usuário deve fazer manutenção no diretório pessoal, evitando acúmulo de arquivos desnecessários.

Material de natureza pornográfica e racista não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede. Sendo que serão passiveis de punição os usuários que fizerem uso deste.

Jogos ou qualquer tipo de software/aplicativo não pode ser gravado ou instalado no diretório pessoal do usuário, no computador local e em qualquer outro diretório da rede, podem ser utilizados apenas os softwares previamente instalados no computador e homologados pela equipe de TI da VEMCARD.

Não é permitido criar e/ou remover arquivos fora da área alocada ao usuário e/ou que venham a comprometer o desempenho e funcionamento dos sistemas. As áreas de armazenamento de arquivos são designadas conforme abaixo.

Compartilhamento das áreas de armazenamento de arquivos;

Diretório Departamental - Arquivos do departamento em que trabalha

Diretório Público - Arquivos temporários ou de compartilhamento geral, para todos os funcionários.

Em alguns casos pode haver mais de um compartilhamento referente aos arquivos do departamento em qual faz parte.

A pasta Público, não deverá ser utilizada para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza sensível, devem ser armazenadas apenas informações comuns a todos.

Haverá limpeza trimestral dos arquivos armazenados na pasta Público, para que não haja acúmulo desnecessário de arquivos.

É proibida a instalação ou remoção de softwares que não forem devidamente acompanhadas pelo departamento técnico, através de solicitação escrita que será disponibilizada, e deve conter autorização do coordenador da área do solicitante.

Não são permitidas alterações das configurações de rede e inicialização das máquinas bem como modificações que possam trazer algum problema futuro.

É obrigatório armazenar os arquivos inerentes à instituição no servidor de
arquivos para garantir a cópia de segurança deles. O departamento de TI não se responsabilizará pela eventual perda de arquivos armazenados localmente.

É proibida a abertura de computadores para qualquer tipo de reparo, seja isto feito em departamentos ou laboratórios de informática, caso seja necessário o reparo deverá ocorrer pelo departamento técnico.

Quando ocorrer a admissão de funcionário, o coordenador responsável, deve formalizar através de abertura de chamado, para a equipe de TI, providenciar a ativação dos acessos do usuário aos recursos necessários da rede.

Quando um funcionário é transferido entre departamentos, o coordenador que transferiu deve certificar-se de que todos os direitos de acesso aos sistemas e outros controles de segurança ainda serão necessários na sua nova função e formalizar através de abertura de chamado, para equipe de TI, qualquer modificação necessária;

Quando ocorrer a demissão do funcionário, o coordenador responsável, deve formalizar através de abertura de chamado para equipe de TI, para providenciar a desativação dos acessos do usuário a qualquer recurso da rede. Deve-se verificar a necessidade de troca de senhas de contas de uso comum ao departamento, evitando o acesso às informações.

O acesso às informações é feito através da conta criada pela equipe de segurança através de solicitação do coordenador responsável pelo setor. Cada usuário deverá possuir uma conta de acesso própria, sendo que empréstimos não são permitidos.

O acesso a diretórios ou compartilhamentos dos departamentos deve ser fornecido somente em caso de necessidade de acesso.

2.4.2 Política de utilização da Rede sem fio “Wireless”

A rede Wireless do VEMCARD deve atender as Normas descritas pela Tecnologia da Informação, além de políticas internas.

O usuário que acessa a rede wireless da **VEMCARD**, deve obedecer às normas abaixo:

1. O Acesso e utilização da rede Wireless (Sem fio), só poderá ser realizada dentro das dependências da **VEMCARD**.

2. Não é permitido qualquer tipo de scanner na rede Wireless (Sem fio), mesmo que seja para testes. Somente será concedido direito para scanner, solicitações encaminhadas para a TI.

3. A tentativa de acesso, ou o acesso a computadores não autorizados; a tentativa de quebra, ou a quebra de sigilo de senhas alheias; o acesso e modificação de arquivos pertencentes a outros usuários sem a sua autorização; são considerados delitos graves, puníveis com o cancelamento da conta eletrônica infratora em todos os computadores da **VEMCARD,** e podendo inclusive resultar em ação legal.

4. Não é permitido desenvolver, manter, usar ou divulgar meios que possibilitem a violação de computadores da rede. O desrespeito a esta regra também será punido com a exclusão da conta eletrônica envolvida e o impedimento de obtenção de novas contas eletrônicas pelo usuário em questão.

5. Toda documentação ou informação obtidas através da rede, que tenham propriedade registrada, não podem ser copiadas, modificadas, disseminadas ou usadas, no todo ou em parte, sem permissão expressa do detentor dos direitos autorais.

6. Os recursos computacionais da **VEMCARD** não podem ser usados para mostrar, armazenar ou transmitir texto, imagem ou som que possam ser considerados ofensivos ou abusivos.

7. Os administradores dos sistemas computacionais da **VEMCARD**, podem ter

acesso aos arquivos dos usuários quando for indispensável para a manutenção do sistema e em falhas de segurança.

3. Estações de trabalho

Cada estação de trabalho tem códigos internos que permitem que ela seja identificada na rede, e cada indivíduo possui sua própria estação de trabalho. Isso significa que tudo que venha a ser executado de sua estação acarretará responsabilidade sua. Por isso sempre que sair da frente de sua estação tenha certeza de que efetuou logoff ou travou o console.

A estação de trabalho, não é de propriedade particular e sim institucional e, como tal, poderão passar por auditorias, onde, constatando-se irregularidades, o colaborador prestará contas de seu uso.

3.1 Política de uso de estação de trabalho

Lembramos que sua estação é sua ferramenta de trabalho, mas também é um importante componente de segurança. Por isso observe as seguintes orientações:

• Não instale nenhum tipo de software / hardware sem autorização do departamento de TI

• Não tenha MP3, filmes, fotos e softwares com direitos autorais ou qualquer outro tipo de pirataria.

• Todos os dados relativos à instituição devem ser mantidos no servidor, onde existe um sistema de backup diário e confiável. Caso não saiba como fazer isso, entre em contato com o departamento de TI. Através de abertura de chamado, na Central de Serviços

• Todo periférico (impressora, scanner, mouse, teclado etc.) que está conectado à sua estação de trabalho faz parte dela, sendo assim não é permitida a utilização dos mesmos para uso pessoal.

3.2 Política de uso de notebooks

Por se tratar de um equipamento com grande mobilidade e de custo elevado devemos tomar alguns cuidados especiais para o bom funcionamento deles.

• Quando você estiver fora da instituição, nunca deixe seu notebook dentro do veículo estacionado, seja em ruas, em estacionamentos ou mesmo em sua residência.

• Somente retire o notebook da instituição se você for utilizá-lo em viagens ou em trabalhos externos.

• No caso de um sinistro, é obrigatória a elaboração de Boletim de Ocorrência Policial, descrevendo detalhadamente as circunstâncias do evento com o Notebook.

• No caso de perda por acidente é obrigatória a elaboração de uma declaração do ocorrido.

• A instituição reserva-se no direito de ser ressarcida, caso julgar que houve desleixo na guarda ou descumprimento das normas pelo funcionário com relação ao Notebook.

• Para facilitar o seu dia a dia, todas as informações necessárias para o seu trabalho estão dentro do notebook, sendo assim você deve fazer backups das suas informações preferencialmente no servidor da rede.

4. Cópias

• Não será permitido copiar softwares, arquivos e e-mails em cd, dvd, pen-drive, em serviços de armazenamento na Nuvem ou qualquer outro meio de reprodução.

• Os arquivos copiados deverão ter uso estritamente pertinentes aos interesses da instituição.

• Os backups que venham a ser necessário deverão ser efetuados somente na rede corporativa.

• Exceções somente serão permitidas após parecer do setor de TI e autorizados pela coordenadoria.

5. Vírus e códigos maliciosos

São os maiores geradores de problemas de segurança. Alguns procedimentos simples podem evitar grandes transtornos:

• Mantenha seu antivírus atualizado. Provavelmente nossa equipe técnica irá se encarregar disso, mas caso não tenha sido feito ou você perceba que a atualização não está funcional, entre em contato com ela para que a situação possa ser corrigida.

• Reporte atitudes suspeitas em seu sistema a equipe técnica, para que possíveis vírus possam ser identificados no menor espaço de tempo possível.

• Suspeite de softwares que "você clica e não acontece nada".

6. Social

Como seres humanos, temos a grande vantagem de sermos sociáveis, mas muitas vezes quando falamos sobre segurança, isso é uma desvantagem. Por isso observe os seguintes tópicos:

• Não fale sobre a política de segurança da instituição com terceiros ou em

locais públicos.

• Não diga sua senha para ninguém. Nossa equipe técnica jamais irá pedir sua senha.

• Não digite suas senhas ou usuários em máquinas de terceiros, especialmente fora da instituição.

• Somente aceite ajuda técnica de um membro de nossa equipe técnica previamente apresentado e identificado.

• Nunca execute procedimentos técnicos cujas instruções tenham chegado por e-mail.

• Relate à equipe de segurança pedidos externos ou internos que venham a discordar dos tópicos anteriores.

7. Política da Mesa limpa e Tela limpa

A política de mesa limpa deve ser considerada para os departamentos e utilizada pelos Colaboradores da **VEMCARD**, de modo que papéis e mídias removíveis não fiquem expostas à acessos não autorizados.

A política de tela limpa deve considerar que se o usuário não estiver utilizando a informação ela não deve ficar exposta, reduzindo o risco de acesso não autorizado, perda e danos à informação.

Os papéis ou mídias de computador não devem ser deixados sobre as mesas, quando não estiverem sendo usados devem ser guardados de maneira adequada, em preferência em gavetas ou armários trancados.

Os ambientes dos departamentos devem ser mantidos limpo, sem caixa ou qualquer outro material sobre o chão de modo que possa facilitar o acesso de pessoas que estiverem no departamento.

Sempre que não estiver utilizando o computador não deixar nenhum arquivo aberto, de modo que as informações possam ser visualizadas por outras pessoas que estiverem no departamento.

Agendas, livros ou qualquer material que possam ter informações sobre a instituição ou informações particulares devem sempre ser guardadas em locais fechados, evitando o acesso.

Chaves de gavetas, armários, de portas de acesso à departamento, de laboratórios de informática devem ser guardadas em lugar adequado, não devem ser deixadas sobre a mesa ou guardadas com o Colaborador.

Ao utilizar impressoras no ambiente da **VEMCARD**, certifique-se de não deixar nenhum impresso com informações referentes à instituição.

8. Continuidade de negócios

De nada adianta uma informação segura se ela estiver indisponível para quem necessita dela. Para que a segurança da informação aconteça precisamos que as pessoas que compõem a instituição, deixem de estar apenas “envolvidas com a segurança”, para estarem “comprometidas com a segurança”.

9. Medidas e Procedimentos de Segurança da Informação

Medidas da área de Segurança de Informações, que servem de estratégia da **VEMCARD,** na busca de minimizar os riscos com segurança cibernética, com base em um conjunto de ações de segurança, visando garantir um nível de maturidade e um padrão adequado de proteção no tratamento de dados pessoais.

1) Inventário e controle de ativos corporativos

- 1.1 Estabelecer e manter um inventário detalhado de ativos corporativos
- 1.2 Endereçar ativos não autorizados

2) Inventário e controle de ativos de software

- 2.1 Estabelecer e manter um inventário de software
- 2.2 Assegurar que o software autorizado seja atualmente suportado
- 2.3 Endereçar o software não autorizado

3) Proteção de dados

- 3.1 Estabelecer e manter um processo de gestão de dados Dados
- 3.2 Estabelecer e manter um inventário de dados Dados
- 3.3 Configurar listas de controle de acesso a dados Dados
- 3.4 Aplicar retenção de dados Dados
- 3.5 Descartar dados com segurança Dados
- 3.6 Criptografar dados em dispositivos de usuário final. Dispositivo

4) Configuração segura de ativos corporativos e software

- 4.1 Estabelecer e manter um processo de configuração segura
- 4.2 Estabelecer e Manter um Processo de Configuração Segura para a Infraestrutura de Rede
- 4.3 Configurar o bloqueio automático de sessão nos ativos corporativos
- 4.4 Implementar e gerenciar um firewall nos servidores
- 4.5 Implementar e gerenciar um firewall nos dispositivos de usuário final
- 4.6 Gerenciar com segurança os ativos e softwares corporativos
- 4.7 Gerenciar contas padrão nos ativos e softwares corporativos

5) Gestão de contas

- 5.1 Estabelecer e manter um inventário de contas
- 5.2 Usar senhas exclusivas
- 5.3 Desabilitar contas inativas
- 5.4 Restringir privilégios de administrador a contas de Administrador dedicadas

6) Gestão do controle de acesso

- 6.1 Estabelecer um Processo de Concessão de Acesso
- 6.2 Estabelecer um Processo de Revogação de Acesso
- 6.3 Exigir MFA para aplicações expostas externamente
- 6.4 Exigir MFA para acesso remoto à rede
- 6.5 Exigir MFA para acesso administrativo

7) Gestão contínua de vulnerabilidades

- 7.1 Estabelecer e manter um processo de gestão de vulnerabilidade
- 7.2 Estabelecer e manter um processo de remediação
- 7.3 Executar a gestão automatizada de patches do sistema operacional
- 7.4 Executar a gestão automatizada de patches de aplicações

8) Gestão de registros de auditoria

- 8.1 Estabelecer e manter um processo de gestão de log de auditoria
- 8.2 Coletar logs de auditoria
- 8.3 Garantir o armazenamento adequado do registro de auditoria

9) Proteções de e-mail e navegador Web

- 9.1 Garantir o uso apenas de navegadores e clientes de e-mail suportados plenamente
- 9.2 Usar serviços de filtragem de DNS

10) Defesas contra malware

- 10.1 Instalar e manter um software anti-malware
- 10.2 Configurar atualizações automáticas de assinatura anti-malware
- 10.3 Desabilitar a execução e reprodução automática para mídias removíveis

11) Recuperação de dados

- 11.1 Estabelecer e manter um processo de recuperação de dados
- 11.2 Executar backups automatizados
- 11.3 Proteger os dados de recuperação

- 11.4 Estabelecer e manter uma instância isolada de dados de recuperação

12) Gestão da infraestrutura de rede

- 12.1 Assegurar que a infraestrutura de rede esteja atualizada

13) Monitoramento e defesa da Rede

14) Conscientização sobre segurança e treinamento de competências

- 14.1 Estabelecer e manter um programa de conscientização de segurança
- 14.2 Treinar membros da força de trabalho para reconhecer ataques de engenharia social
- 14.3 Treinar membros da força de trabalho nas melhores práticas de autenticação
- 14.4 Treinar a força de trabalho nas Melhores Práticas de Tratamento de Dados
- 14.5 Treinar membros da força de trabalho sobre as causas da exposição não intencional de dados
- 14.6 Treinar Membros da força de trabalho no Reconhecimento e Comunicação de Incidentes de Segurança
- 14.7 Treinar a força de trabalho sobre como identificar e comunicar se os seus ativos corporativos estão faltando atualizações de segurança
- 14.8 Treinar a força de trabalho sobre os perigos de se conectar e transmitir dados corporativos em redes inseguras

15) Gestão de provedor de serviços

- 15.1 Estabelecer e manter um inventário de provedores de serviços

16) Segurança de aplicações

17) Gestão de respostas a incidentes

- 17.1 Designar Pessoal para Gerenciar Tratamento de Incidentes
- 17.2 Estabelecer e manter informações de contato para relatar incidentes de segurança
- 17.3 Estabelecer e manter um processo corporativo para relatar incidentes

18) Testes de invasão.