Política, Normas e Procedimentos de Segurança da Informação e Trabalho Remoto

Sumário

Introdução e Compliance

1.1. Introdução, propósitos e objetivos

1.1.1. A Política, Normas e Procedimentos de Segurança da Informação e trabalho remoto, também referida como PNPSITR, é o documento que orienta e estabelece as diretrizes corporativas da Enfoque para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas e pessoas atuantes na empresa.

1.1.2. Para o propósito da presente PNPSITR, trabalho remoto se aplica igualmente ao trabalho remoto em desktop/ notebook, celular e dispositivos móveis.

1.1.3. Mediante ao atual cenário tecnológico e de inovação e com o intuito de maximizar a eficácia e produtividade dos funcionários, mas ao mesmo tempo permitir que estes tenham maior flexibilidade em suas vidas profissionais, a empresa estabelece e apoia o trabalho remoto.

1.1.4. Para viabilizar o método de trabalho, a Enfoque estabelecerá padrões e proverá ferramentas para estabelecer o trabalho remoto com a adoção de práticas que atendam às necessidades do negócio, da equipe e do indivíduo. Isso maximizará nossa capacidade de fornecer alta qualidade de serviços e, ao mesmo tempo, gerenciar nossos custos operacionais.

1.1.5. A Enfoque garantirá que todos os usuários que trabalham em casa ou remotamente estejam cientes do uso aceitável e com segurança de dispositivos portáteis de computador e trabalho remoto. Tanto equipamentos quanto qualquer informação armazenada neles devem ser reconhecidos como valiosos ativos da Enfoque e, portanto, devem ser apropriadamente manipuladas, arquivadas e, quando necessário, descartadas.

1.1.6. A presente política está amparada exclusivamente em 3 pilares: (1) na estrutura atual da empresa, (2) na necessidade atual da empresa com relação aos ativos de informação e (3) na evolução tecnológica e novas ameaças e vulnerabilidades. A mesma poderá ser revista à medida em que aspectos relacionados aos pilares se modifiquem. A Enfoque atualizará e divulgará amplamente a todos os envolvidos quaisquer mudanças necessárias às práticas do dia-a-dia.

1.2. Compliance

1.2.1. Devem cumprir a presente política todos os funcionários, contratados em período integral ou meio período, por contratos permanente ou temporário, parceiros, fornecedores e terceirizados que venham a ter acesso às informações geridas ou produzidas pela Enfoque, em qualquer meio ou suporte, aos sistemas de informação ou equipamentos de

TI (incluindo dispositivos de mídia removíveis). Por definição, todos aos quais se aplicam esta política serão denominados 'colaboradores'.

1.2.2. Qualquer pessoa que venha a violar essa política estará sujeita à Demissão ou rescisão contratual da atividade junto a Enfoque. Violações graves dessa política podem ser consideradas uma má conduta grave, sujeitando sujeitará o colaborador às medidas administrativas e legais cabíveis. Caso haja algum ponto não compreendido e suas implicações, procurar a orientação do responsável pelo TI e Recursos Humanos – Eduardo Artiaga (eduardo.artiaga@enfoquepesquisa.com.br).

1.2.3. O Eduardo Artiaga é o líder dos processos de segurança física e eletrônica, atualmente auxiliado pelo consultor contratado da Rada Serviços em Informática Ltda. Portanto, além das dúvidas da presente política, o Eduardo é o ponto focal para quaisquer dúvidas ou suposto incidente que envolva a segurança física e eletrônica de dados recebidos, geridos ou produzidos pela Enfoque.

1.2.4. Fica estabelecido que é também obrigação de cada colaborador manter-se atualizado em relação a esta PNPSITR e aos procedimentos e normas relacionadas, buscando orientação do seu responsável pelo TI e Recursos Humanos sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

1.3. Gestão de Incidentes de Segurança da Informação

1.3.1 Foram criados canais de comunicação direta de atendimento aos Funcionário, Contratados, parceiros e Terceirizados para receber as primeiras notificações e chamados de incidentes adequadamente; Os canais disponibilizados são por e-mail ISI@enfoquepesquisa.com.br ou por telefone (21) 98057-0027;

1.3.2 A equipe responsável pelo tratamento de incidentes de segurança tem por objetivo receber, filtrar e responder as solicitações e alertas através da análise dos incidentes de segurança, procurando impedir a continuidade da ação maliciosa, e também a identificação de tendências.

1.3.3 A equipe responsável pelos incidentes deve realizar o tratamento das informações de forma a viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações, observando sempre a legislação em vigor.

1.3.4 Durante o gerenciamento de incidentes de segurança, havendo indícios de ilícitos criminais, o responsável pela Segurança da Informação deve preservar as evidências e acionar de forma imediata a diretoria e setor jurídico da empresa para que seja adotado os procedimentos legais cabíveis;

1.3.5 Qualquer tentativa de alteração nos parâmetros de segurança, por qualquer usuário, sem credenciamento ou autorização para tal, será considerado inadequada, e os riscos relacionados serão informados ao colaborador e ao seu gestor.

1.3.6 O descumprimento ou inobservância de quaisquer regras ou diretrizes definidas neste instrumento serão tratadas como "falta grave", e o colaborador classificado dessa forma estará sujeito aplicação de medidas administrativas, cíveis e judiciais cabíveis.

Estrutura

2.1. Esta política foi separada em duas categorias:
2.1.1. Todos os aspectos referentes à Segurança Física do trabalho remoto
2.1.2. Todos os aspectos referentes à Segurança da Informação

2.2. A presente política aplica-se ao uso correto e seguro de dispositivos que garantem a comunicação e produtividade dos projetos e demais atividades cotidianas desempenhadas para a empresa. Engloba:
2.2.1.1. Computadores portáteis
2.2.1.2. Desktops
2.2.1.3. Telefones celulares, incluindo smartphones
2.2.1.4. Dispositivos móveis como pendrivers e conexões HDMI

2.3. Por definição, usaremos a referência ‘colaboradores’ para todos Tanto para os aspectos de Segurança física quanto para a Segurança da Informação, é essencial para o desempenho do trabalho remoto em casa que se disponibilize um quarto ou área da casa s:

Da Segurança Física

3.1. É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos concedidos ao uso dos colaboradores do inventário da Enfoque.

3.2. Papéis, anotações e lembretes da sua mesa de trabalho devem ser mantidos sempre que possível fora da superfície da mesa (mesa limpa);

3.3. Papéis, mídias eletrônicas ou qualquer informação confidencial não devem ser deixados na mesa, quando o colaborador for se afastar. Neste caso devesse guardar a informação nas suas gavetas ou em armários de documentos que fiquem trancados. A escolha do local vai depender do tempo de afastamento.

3.4. Todo colaborador deve ao deixar a sua estação de trabalho bloquear ou mesmo desligar o seu computador

3.5. Ao final do dia todos os documento e meios eletrônicos devem ser devidamente guardados/organizados com proteção adequada, de preferência em lugares trancados;

3.6. Os papéis (relatórios) e mídias eletrônicas devem ser armazenados em locais trancados adequados quando não estiverem em uso, especialmente fora do horário do expediente.

AVISO: Cada colaborador é responsável pela segurança da informação, sendo de inteira responsabilidade, de cada um, todo o prejuízo ou dano que vier a causar em decorrência da não obediência as normas e procedimentos específicos da empresa.

Da Segurança da Informação

4.1. Das informações gerais:

4.1.1. Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela Enfoque pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

4.1.2. Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

4.1.3. A Enfoque, por meio de equipe responsável pelo TI e Recursos Humanos, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

4.1.4. Deverá constar em todos os contratos da Enfoque o anexo de Acordo de Confidencialidade ou Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.

4.1.5. A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar o termo de responsabilidade contido desse documento.

4.1.6. O colaborador assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na Enfoque, mesmo depois de terminado o vínculo contratual mantido com a instituição.

4.1.7. O colaborador é responsável pelas consequências da manipulação de qualquer ativo de informação que decida enviar, compartilhar, armazenar ou descartar. Assim, exige-se do colaborador atenção redobrada ao transferir informações ou arquivos da empresa por qualquer meio, com destino a ou copiando qualquer destinatário, independentemente da finalizada.

4.1.8. Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente ao responsável pelo TI e Recursos Humanos.

4.1.9. Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

4.1.10. Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

4.1.11. A Enfoque exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

4.1.12. A utilização dos equipamentos de informática e comunicação, sistemas e informações pelos colaboradores devem ser de forma consciente, de maneira que algumas medidas devem ser adotadas:

4.1.12.1. Não deixar o equipamento com a tela do equipamento sem proteção e/ou sem bloqueio ao se afastar do mesmo;

4.1.12.2. Deixar sua área de trabalho (Desktop) do computador o mais limpo possível, ou seja, livre de arquivos soltos e ícones sem necessidade. O ideal é reservar alguns poucos minutos no final do dia e remover ou realocar as tudo que foi criado durante o dia de trabalho;

4.1.12.3. Realizar ou solicitar que seja realizado (caso não tenha autorização devida) a remoção de atalhos de desktop e de programas que não tenham mais utilidade, esvaziamento de lixeira, limpeza de arquivos temporários, verificação de programas funcionando em background, entre outros.

4.1.12.4. Nunca deixar os arquivos confidenciais no seu desktop quando não estiverem sendo utilizados. Sempre optar por salvar estes tipos de arquivos na nuvem.

4.1.12.5. Não salvar itens pessoais ou baixar programas no seu desktop sem a devida autorização;

4.2. Das senhas de acesso utilizadas:

4.2.1. Os usuários (logins) individuais de colaboradores serão de responsabilidade do próprio colaborador.

4.2.2. Os usuários (logins) de terceiros serão de responsabilidade do analisa/ gestor responsável pelo projeto específico em execução.

4.2.3. É de responsabilidade de cada usuário a criação e memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

4.2.4. As senhas devem respeitar o nível de complexidade exigido por cada dispositivo e provedor de acesso provido pela empresa. Contudo, independentemente do dispositivo, software ou provedor de acesso, é essencial que as senhas:

4.2.4.1. Não sejam baseadas de informações pessoais de fácil identificação como datas, nomes, número de telefones, etc.

4.2.4.2. Não sejam reutilizadas em diferentes tipos de acessos exatamente a mesma senha

4.2.4.3. Não sejam utilizadas concomitantemente para fins pessoais como senhas de sites online, redes sociais, fóruns, etc.

4.2.4.4. Nunca seja divulgada a terceiros, mesmo que para outros colaboradores que compartilhem de tarefas. As senhas são individuais e intransferíveis.

4.2.5. Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ao responsável pelo TI e Recursos Humanos que procederá o cadastramento de uma nova.

4.2.6. As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

4.2.7. Deverá ser respeitado em sua integralidade o processo para a renovação de senha (conforme política própria de acesso em nuvem e de correio eletrônico), contemplando aqui a periodicidade máxima demandada. Não podem ser repetidas as 3 (três) últimas senhas. Os sistemas forçarão a troca das senhas dentro dos prazos máximos de segurança de cada sistema.

4.2.8. Os colaboradores serão responsáveis por alterar a própria senha, conforme orientação do responsável de TI, além de o fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

4.2.9. Deverão ser protegidos por senha (bloqueados), todos os terminais de computador e impressoras quando não estiverem sendo utilizados.

4.2.10. Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum colaborador for demitido ou solicitar demissão, o responsável pelo TI e Recursos Humanos deverá ser imediatamente comunicado, a fim de que essa providência seja tomada. A mesma conduta se aplica aos colaboradores cujo contrato ou prestação de serviços tenha se encerrado, aos colaboradores de testes, temporários e outras situações similares.

4.3. Do uso do correio eletrônico:

4.3.1. O uso do correio eletrônico da Enfoque é para fins corporativos e relacionados às atividades do colaborador usuário para fins profissionais. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a Enfoque e também não cause impacto no tráfego da rede.

4.3.2. Atenção redobrada ao recebimento de links ou solicitações de origem duvidosa. Em caso de dúvidas, entrar em contato imediatamente com o responsável por TI.

4.3.3. Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico da Enfoque:

4.3.3.1. enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
4.3.3.2. enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
4.3.3.3. enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Enfoque ou suas unidades vulneráveis a ações civis ou criminais;
4.3.3.4. divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins
sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
4.3.3.5. falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
4.3.3.6. produzir, transmitir ou divulgar mensagem que:
4.3.3.6.1. contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Enfoque;
4.3.3.6.2. contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
4.3.3.6.3. contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
4.3.3.6.4. vise obter acesso não autorizado a outro computador, servidor ou rede;
4.3.3.6.5. vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
4.3.3.6.6. vise burlar qualquer sistema de segurança;
4.3.3.6.7. vise vigiar secretamente ou assediar outro usuário;
4.3.3.6.8. vise acessar informações confidenciais sem explícita autorização do proprietário;
4.3.3.6.9. vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
4.3.3.6.10. inclua imagens criptografadas ou de qualquer forma mascaradas;
4.3.3.6.11. contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet)
4.3.3.6.12. tenha conteúdo considerado impróprio, obsceno ou ilegal;
4.3.3.6.13. seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
4.3.3.6.14. contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
4.3.3.6.15. tenha fins políticos locais ou do país (propaganda política);
4.3.3.6.16. inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

4.3.4. As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:
4.3.4.1. Nome do colaborador
4.3.4.2. Departamento ou cargo ocupado
4.3.4.3. Nome da empresa e logo
4.3.4.4. Telefone(s) de contato

4.4. Do armazenamento de dados e ativos de informação:

4.4.1. Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em serviço em nuvem. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

4.4.2. Os colaboradores da Enfoque e/ou detentores de contas privilegiadas não deve executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da Gerência de Sistemas.

4.5. Do uso de computadores, equipamentos e recursos de informática:

4.5.1. Todos os computadores de uso individual deverão ter senha de Bios para restringir o acesso de pessoas não autorizados. Tais senhas serão definidas pelo próprio colaborador.

.

4.5.2. Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.

4.5.3. É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática do inventário da Enfoque para qualquer tipo de reparo que não seja realizado por um técnico designado pelo responsável pelo TI e Recursos Humanos.

4.5.4. O colaborador ao usar equipamento do inventário da Enfoque deverá manter a configuração do equipamento disponibilizado, seguindo os devidos controles de segurança exigidos pela presente política, assumindo a responsabilidade como custodiante de informações. A mesma regra aplica-se a configuração do sistema operacional instalado que não deve ser alterado sob pena de torná-lo vulnerável.

4.5.5. O colaborador é responsável pela atualização do sistema operacional, software antivírus e outros softwares assim que demandando por mensagens automáticas dos próprios softwares no equipamento usado.

4.5.5.1. Em caso de dúvidas sobre a autenticidade da solicitação da atualização, o colaborador deve entrar em contato com o responsável de TI e confirmar.

4.5.5.2. Em caso de atualização cuja finalidade é correção de debilidades do sistema à novas e graves ameaças de segurança, o responsável de TI fará reforço da urgência da atualização através de comunicação interna por correio eletrônico. Se já não houver feito, o colaborador deverá realizar imediatamente atualizações dessa categoria e o responsável de TI fará verificação remota da realização da ação.

4.5.6. Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da Enfoque:

4.5.6.1. Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.

4.5.6.2. Burlar quaisquer sistemas de segurança.

4.5.6.3. Acessar informações confidenciais sem explícita autorização do proprietário.

4.5.6.4. Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).

4.5.6.5. Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.

4.5.6.6. Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;

4.5.6.7. Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

4.5.6.8. Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

4.5.7. A Enfoque, na qualidade de proprietária dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

4.6. Dos dispositivos móveis – computadores portáteis, telefones celulares, tablets, pendrivers e conexões HDMI

4.6.1. Todas as regras anteriormente listadas para o uso de equipamentos são válidas também para os dispositivos móveis.

4.6.1.1. Assim como dispositivos não-móveis, o colaborador é responsável pela atualização do sistema operacional do seu dispositivo móvel, mesmo o de dispositivos menores como smartphones e tablets, por exemplo. Em caso de dúvidas, o colaborador deve entrar em contato com o responsável de TI para se informar e obter uma verificação periódica da atualização dos dispositivos móveis utilizado.

4.6.2. Todo colaborador deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel. Deverá, também, manter estes backups separados de seu dispositivo móvel, ou seja, não os carregar juntos.

4.6.3. O suporte técnico aos dispositivos móveis de propriedade da Enfoque e aos seus colaboradores deverá seguir o mesmo fluxo de suporte contratado pela instituição.

4.6.4. Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel. É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes.

4.6.5. Os colaboradores devem tomar o devido cuidado e atenção aos dispositivos portáteis ao se deslocarem de casa para outro local. Devido à alta incidência de roubos de carros, laptops ou outros equipamentos portáteis nunca devem ser deixados sem vigilância em carros ou levados para áreas vulneráveis.

4.6.6. É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela Enfoque, notificar imediatamente seu gestor direto e o responsável por TI

e Recursos Humanos. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

4.7. Política de Gestão de Ativos

Objetivo

Estabelecer padrões para que os ativos de tecnologia da informação da Enfoque sejam identificados; definir responsabilidades apropriadas para proteção e divulgação da gestão dos ativos da informação, por meio do estabelecimento e manutenção de inventários, além de assegurar que o ciclo de vida dos ativos seja realizado e gerenciado para garantir a Segurança da Informação e o atendimento as políticas, normas e boas práticas recomendadas

Controle de Ativos

Os ativos são divididos nos seguintes grupos:

Ativos físicos - Equipamentos que compõem os recursos de tecnologia e de informática, como computadores, mídias removíveis, equipamentos de comunicação e conectividade, entre outros;

Ativos de softwares- Os programas, sistemas, ferramentas e utilitários adquiridos e/ou desenvolvidos pela Enfoque e que fazem parte das atividades em seu dia a dia.

Ativos de informação - São dados em tráfego ou armazenados em sistemas de informação, estejam estes em formato lógico (elétrico, magnético ou ótico) ou físico (impressos).

Aquisição

A aquisição de ativos é uma etapa importante que certamente influenciará os três pilares da gestão de ativos: custo, desempenho e risco

A prática mostra que adotar como critério apenas o custo inicial de compra, na maioria das vezes, não é a melhor alternativa, pois outros aspectos precisam ser avaliados já na etapa de especificação:

- Condições de regime normal de trabalho do equipamento;
- Custos durante o ciclo de vida;
- Riscos associados à falha;
- Eficiência energética e consumo de energia;

Estes são apenas alguns exemplos, pois existem muitos outros aspectos a serem avaliados, de acordo com o negócio da empresa

Ciclo de vida

a) Um processo de gestão de ativos deve ser estabelecido e documentado, para garantir que os ativos de tecnologia da informação sejam gerenciados e monitorados;

b) O processo de gestão de ativos deve levar em consideração as fases do ciclo de vida do ativo:

I. Planejamento – Fase de alinhamento das ações com a estratégia corporativa. Esta fase envolve a revisão dos ativos que são atualmente usados em toda a organização e análise dos custos de compra e instalação de novos ativos de TI.

II. Aquisição – Fase de definição do padrão técnico, empresas fornecedoras, contratações e estabelecimento de acordo contratuais;

III. Implantação - Fase de configuração/instalação técnica e disponibilização conforme padrões estabelecidos;

IV. Gerenciamento - Fase de controle, apoio técnico, manutenção, atualização e monitoração;

V. Descarte – Processo realizado quando um bem perde sua utilidade e torna-se antieconômico. Esta fase corresponde a transferência de um bem para uma outra categoria, que são: material obsoleto, inservível ou excedente.

c) O planejamento das ações relacionados à gestão de ativos devem estar em conformidade com o plano estratégico da área de tecnologia da informação da empresa;

d) Na aquisição de ativos físicos ou de software da Enfoque deve-se estabelecer formalmente uma área única responsável pela aquisição;

e) Os ativos físicos ou de software da empresa devem ser padronizados, para serem adquiridos e disponibilizados conforme perfil funcional e homologados baseado nestes padrões;

f) As licenças de ativos de software e períodos de garantia dos ativos físicos devem ser controlados pela área técnica da empresa;

g) Para cada ativo físico da empresa identificado, deve ser definido e nomeado o seu respectivo responsável funcional;

h) Um fluxo com critérios específicos deve ser estabelecido para o descarte dos ativos físicos e de software, levando em consideração a máxima utilização, o que, por que, como e onde descartar;

i) A área de gestão de ativos da Enfoque deve ser responsável, mas não somente, por:

I. Estabelecer os padrões funcionais para aquisição;

II. Assegurar que as aquisições de ativos físicos e de software sejam antecedidas por um estudo técnico;

III. Assegurar um tratamento adequado na designação dos ativos;

IV. Assegurar o gerenciamento do ativo ao longo do seu ciclo de vida;

V. Assegurar que os ativos sejam inventariados e protegidos;

VI. Assegurar um tratamento adequado no descarte do ativo;

Inventário

a) Os ativos de tecnologia da informação da empresa devem ser inventariados, claramente identificados e registrados;

b) As áreas de patrimônio com o apoio da área de gestão de ativos da empresa têm a responsabilidade de realizar periodicamente os inventários e armazenar os resultados por um período de 2(dois) anos para fins de auditoria interna;

c) Periodicamente deve haver uma revisão pela área técnica de segurança da informação para assegurar que os ativos de tecnologia da informação da empresa estejam em conformidade com o inventário;

Descarte de ativos

Os custos envolvidos na vida de um ativo devem incluir os custos para descarte ou reciclagem face às responsabilidades ambientais que as empresas assumem e à legislação pertinente a que estão submetidas.

Ao final da vida útil do ativo, para cumprir com a responsabilidade assumida sobre ele, a empresa pode escolher o destino que lhe for mais conveniente: recuperá-lo, reciclá-lo, vendê-lo para outra empresa ou, até descartá-lo. Todas estas opções envolvem custo, desempenho e risco, portanto é necessário realizar uma análise para que seja tomada a decisão mais adequada para cada caso.

O descarte de ativos deve seguir o Item 5.5.6 desta Política de Segurança.

4.8. Gestão das Ameaças e Vulnerabilidades

4.8.1. Consiste no processo de identificação, classificação e tratamento das ameaças e vulnerabilidades, ou seja, busca a correção e a aplicação de controles para minimizar a probabilidade de exploração ou impacto dos negócios;

4.8.2. Deve obter informações sobre as ameaças e as vulnerabilidades em tempo hábil, avaliando a sua exposição e aplicando as medidas apropriadas para lidar com os riscos;

4.8.3. Deve-se manter um inventário completo e atualizado para servir como base da avaliação de riscos e das ações a serem tomadas, como por exemplo:

- Aplicação de Patches;
- Bloqueios de estações de trabalho comprometidas;
- Adaptação ou Agregação de controles;
- Aumento do monitoramento;
- Aumento da conscientização.

4.8.4. O processo sobre as funções e responsabilidades da equipe/colaboradores da empresa deve seguir o mesmo formato da Gestão de Incidentes e/ou do Plano de Continuidade de Negócios e Análise de Impacto.

4.8.5. Está gestão deve ser alinhada com o processo de Gestão de Incidentes, documentada e monitorada.

Sobre a Detecção de Ameaças e Vulnerabilidades

As principais ações relacionadas à detecção de ameaças e vulnerabilidades têm como enfoque definir e refinar o escopo que será avaliado; preparar as ferramentas necessárias e verificar sua integridade; e realizar testes e verificar resultados, ou seja, uma detecção eficaz de vulnerabilidades deve ser capaz de encontrar vulnerabilidades e reportá-las em tempo hábil para sua correção, de forma a impedir que sejam exploradas.

Recomenda-se que as verificações de ameaças e vulnerabilidades cubram os ativos internos e externos à rede de produção.

- As ferramentas devem ser configuradas e ajustadas adequadamente de acordo com o escopo avaliado.
- Os tipos de varreduras e os tipos de teste devem ser avaliados e ajustados para que sejam congruentes com o escopo avaliado.
- A frequência de testes de segurança deve levar em consideração os requisitos legais, regulamentares e contratuais que a empresa deve cumprir e os riscos associados aos ativos avaliados.
- As varreduras de ameaças e vulnerabilidades na rede corporativa devem ser realizadas por períodos determinados ou após alteração significativa na rede.
- Os testes de segurança devem utilizar o feed de vulnerabilidade mais recente, de forma a evitar que determinadas vulnerabilidades não sejam detectadas.
- Para cada teste, é necessário verificar a integridade da ferramenta utilizada e se ela varreu corretamente os ativos analisados e se existem exceções de ameaças e vulnerabilidades.
- As ferramentas utilizadas devem ser ajustadas continuamente, de forma a evitar que varreduras feitas por ferramentas distintas gerarem resultados distintos.
- O teste de invasão ou o teste de penetração (Pentest) deve ser realizado conforme critério de necessidade da empresa ou pelo menos semestralmente, a fim de fornecer as informações mais precisas e relevantes sobre as ameaças e vulnerabilidades atuais, sem afetar o funcionamento normal da empresa;
- A integridade do resultado de detecção de ameaças e vulnerabilidades deve ser avaliada antes de sua comunicação, de forma a evitar inconsistências, contradições ou resultados incompletos.
- A detecção manual de ameaças e vulnerabilidades deve ser considerada como complemento à detecção automática.

Sobre a Elaboração e manutenção dos relatórios

- O responsável pelo TI deve elaborar relatórios após cada ciclo de detecção para auxiliar a empresa a entender e mensurar as ameaças e vulnerabilidades existentes.
- Os resultados da varredura devem passar por análise para que possíveis falsos positivos possam ser identificados e eliminados.
- Deve-se adotar métricas para os relatórios de ameaças e vulnerabilidade e determinar o valor percentual dos ativos de informação por gravidade e/ou CVSS.
- A quantidade e a porcentagem de novas ameaças e vulnerabilidades devem ser monitoradas por: severidade; grupos funcionais; tipo de ambiente; tipo de sistema; e tipo de vulnerabilidade.
- O relatório deve ser classificado, durante e após a sua elaboração, de acordo com a sensibilidade das informações presentes nele.
- Todas as versões do relatório devem ser remetidas ao Diretor de Compliance e ao gestor de segurança de informação.

Sobre a Classificação de Ameaças

A empresa deve seguir o critério da Norma ISO/NRB 27005:2011, onde a classificação das ameaças se dá pela sua origem - de natureza humana deliberada, acidental e ambiental e com o tipo, conforme quadro abaixo:

TIPOS DE AMEAÇAS	DESCRIÇÃO
Dano físico	Incidente com equipamento, instalação, mídia ou substância que foram comprometidos.
Eventos naturais	Incidentes com fontes de água, do solo, do subsolo ou do ar
Paralisação de serviços essenciais	Incidentes em serviço de energia elétrica, água encanada, esgoto, condicionamento de ar etc
Distúrbio causado por radiação	Incidentes causados por radiação térmica ou eletromagnética
Comprometimento da informação	Interceptação, destruição, furto, cópia indevida, adulteração de hardware ou software.
Falhas técnicas	Falha, defeito, saturação ou violação das condições de uso de equipamento de informática.
Ações não autorizadas	Uso, cópia ou processamento ilegal de dados
Comprometimento de funções	Uso errado, abuso de direitos, falsificação de direitos, repúdio de ações, indisponibilidade de pessoas.

Sobre a Identificação de Ameaças

A tabela abaixo contém exemplos de ameaças típicas de acordo com a Norma ISO/NRB 27005:2011.

TIPO	AMEAÇAS
Dano Físico	Fogo, Água, Poluição, Acidente grave, Destruição de equipamento ou Mídia, Poeira, Corrosão e Congelamento
Eventos Naturais	Fenômenos Climáticos, sísmicos, vulcanicos, meteriológicos e Inundação
Paralisação de serviços essenciais	Falha do ar condicionado ou do sistema de suprementos de água, Interrupção do suprimento de energia e Falha do equipamento de telecomunicação
Disturbios causado por radiação	Radiação eletromagnética, térmica e Pulsos eletromagnéticos
Comprometimento da informação	Interupção de sinais de interferência comprometedores, Espionagem à distância, Escuta não autorizada, Furto de mídia ou documentos, Furto de equipamentos, Recuperação de mídia reclicada ou descartada, divulgação indevida, Dados fontes não confiáveis, Alteração de hardware e software, Determinação da localização
Falhas técnicas	Falha de equipamento, Defeito de equipamentos, Saturação do sistema de informação, Defeito de software e Violação das condições de uso do sistema de informação que possibilitam sua manutenção
Ações não autorizadas	Uso não autorizado de equipamentos, Cópia ilegal de software, Uso de cópias de software falsificadas ou ilegais, Comprometimento dos dados e Processamento ilegal de dados
Comprometimento de funções	Erro durante uso, Abuso de direitos, Forjamento de direitos, repúdio de ações e Indisponibilidade de recursos humanos.

Priorização e correção de ameaças e vulnerabilidades

O monitoramento proativo de vulnerabilidades e ameaças em dispositivos, se remediadas, reduzirá ou eliminará o potencial de exploração e economizará os recursos necessários para responder a incidentes após a exploração.

O tratamento de vulnerabilidades deve ser priorizado com base em sua classificação de risco e criticidade, tempo esperado para correção, grau de risco, impacto em caso de exploração e no valor que o ativo tem para o negócio.

As vulnerabilidades devem ser tratadas de acordo com o seu nível de severidade e nos prazos estipulados abaixo. Exemplo de classificação:

Nível de severidade	Prazo de correção	Descrição do risco
Muito Crítico (6)	Até [2 dias]	Condição totalmente inaceitável quando medidas imediatas devem ser tomadas para eliminar a materialização do risco e mitigar perigos e impactos.
Crítico (5)	Até [30 dias]	Pessoas mal-intencionadas podem facilmente obter o controle do host, o que pode comprometer toda a sua rede. As vulnerabilidades incluem acesso de leitura e gravação a arquivos, execução remota de comandos e backdoors.
Alto (4)	Até [45 dias]	Pessoas mal-intencionadas podem obter o controle do host ou coletar informações altamente confidenciais, incluindo acesso de "leitura" ao arquivo, backdoors em potencial ou uma lista de todas as contas de usuário no host.
Médio (3)	Até [90 dias]	Pessoas mal-intencionadas podem obter acesso às configurações de segurança no host, o que pode levar ao acesso a arquivos e à divulgação de conteúdo de arquivos, navegação em diretórios, ataques de negação de serviço e uso não autorizado de serviços.
Baixo (2)	Até [120 dias]	Pessoas mal-intencionadas podem coletar informações confidenciais do host, como versões de software instaladas, que podem revelar vulnerabilidades conhecidas.
Muito baixo (1)	Até 180 dias	Pessoas mal-intencionadas podem coletar informações sobre o host por meio de portas ou serviços abertos, o que pode levar à divulgação de outras vulnerabilidades.

É fundamental que a empresa seja capaz de estabelecer essa classificação de risco de acordo com suas demandas e necessidades internas.

- Os testes que forem concluídos com falha devem ser examinados novamente até que sua execução seja concluída com êxito. Caso não seja possível, deve-se avaliar se a vulnerabilidade será incluída na lista de exceções por pessoal autorizado, com base no processo de aceitação de risco.

- Devem-se estabelecer mecanismos para obter atualizações de software quando emitidas pelo fabricante ou fornecedor oficial regularmente, utilizando recursos autorizados, tais como sites de fornecedores de sistemas, fóruns e grupos de notícias, bancos de dados de gerenciamento de vulnerabilidades e diferentes ferramentas para rastrear as vulnerabilidades mais recentes.

- Quando as vulnerabilidades não puderem ser corrigidas dentro do prazo o responsável polo TI deve enviar um aviso contendo as seguintes informações:
    - Detalhes do sistema ou ativo.
    - A justificativa para a solicitação.
    - Detalhes dos controles existentes (se houver).
    - Novo prazo de correção.
    - Plano de ação da remediação (obedecendo o novo prazo de correção).

- Os alertas de vulnerabilidades, as correções de patches e as ameaças emergentes que correspondam aos recursos informacionais relacionados no inventário de sistema e ativos de informação devem ser monitorados.

Revisões sobre a gestão de ameaças e vulnerabilidades

A gestão de ameaças e vulnerabilidades deve ser revisadas periodicamente ou quando houver necessidade. Essa revisão será feita através de fatores que devem estar documentados, como: teste de ameaça e vulnerabilidades, ocorrência de um incidente de informação, inserção de ativos informacionais, mudança de objetivos do negócio, etc.

Práticas gerais para a condução de operações de segurança SOC:

· Siga as funções da estrutura de segurança cibernética como parte das operações.

- Detectar a presença de adversários no sistema.
- Responder rapidamente investigando se é um ataque real ou um alarme falso.
- Recuperar e restaurar a confidencialidade, a integridade e a disponibilidade da carga de trabalho durante e após um ataque.

Reconheça rapidamente um alerta. Um adversário detectado não deve ser ignorado enquanto os responsáveis pela defesa fazem a triagem de falsos positivos.

Reduza o tempo para corrigir um adversário detectado. Reduza o tempo de oportunidade para conduzir, atacar e alcançar sistemas confidenciais.

Priorize os investimentos em segurança em sistemas com valor intrínseco alto. Por exemplo, contas de administrador.

Busque proativamente adversários à medida que seu sistema amadurece. Esse esforço reduzirá o tempo que um adversário mais experiente pode operar no ambiente. Por exemplo, habilidoso o suficiente para evitar alertas reativos.

Ferramentas

Ferramentas do Azure que a equipe do SOC pode usar para investigar e corrigir incidentes.

Ferramenta	Finalidade
Microsoft Defender para Nuvem	Geração de alertas. Use o guia estratégico de segurança em resposta a um alerta.
Azure Monitor	Logs de eventos do aplicativo e dos serviços do Azure
NSG (Grupo de segurança de rede do Azure)	Visibilidade das atividades de rede.
Proteção de Informações do Azure - Purview	Proteja o e-mail, os documentos e os dados confidenciais que você compartilha fora da sua empresa.

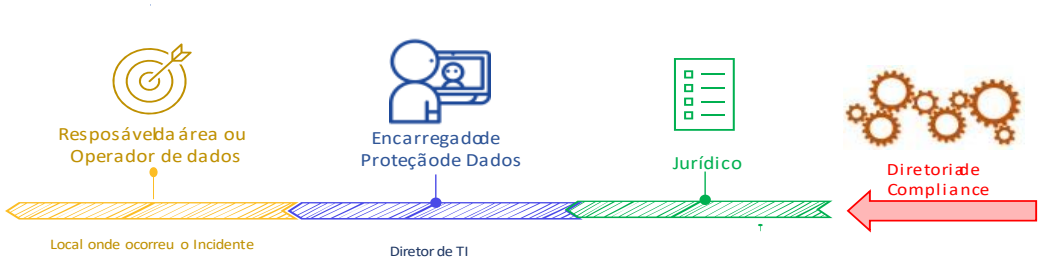
Atribuir contato de notificação de incidente

Os alertas de segurança serão emitidos para setores designados. Na maioria dos casos, essas notificações indicam que o recurso está comprometido. Isso permite que sua equipe de operações de segurança responda rapidamente e corrija possíveis riscos de segurança.

Resposta a incidente

A organização está efetivamente monitorando a postura de segurança entre cargas de trabalho, com os recursos e ferramentas da plataforma de segurança Azure, monitorando dados de telemetria relacionados à segurança e investigando possíveis violações de segurança. As atividades de comunicação, investigação e busca precisam ser alinhadas com as equipes de acesso TI e ADM.

Fluxo de resposta de Incidentes



4.9. Da atualização de Softwares – Gestão de Patches

4.9.1. A atualização dos softwares instalados nos computadores, equipamentos e recursos de informática são de extrema importância, uma vez que, são feitas alterações na versão que está instalada na máquina com o propósito de: correção de falhas (inclusive de segurança), melhorias de usabilidade, confiabilidade e funcionalidade.

4.9.2. Como mencionado nos itens anteriores, é de responsabilidade do setor técnico e dos colaboradores manter as máquinas atualizadas. E por ser uma tarefa básica, não pode ser esquecida ou negligenciada, sob pena de sanções, conforme mencionado no item 9.2 deste documento.

4.9.3. Gestão de patches – Visa a correção dos softwares através da identificação de disponibilidade e vulnerabilidade. Isso é feito com a revisão, execução e confirmação dos patches, que tem a finalidade de atualizar todo sistema para reduzir e/ou sanar quais quer riscos. Para que isso seja possível, o responsável pelo setor técnico deve:

- Realizar periodicamente um inventário de todos os sistemas da empresa;
- Tentar a padronização dos sistemas;
- Listar todos os controles de segurança que estão em vigor;
- Avaliar as vulnerabilidades relatadas no inventário, sempre comparando com o inventário anterior, de forma a ordenar o que precisa ser corrigido primeiro;
- Aplicar os patches para reduzir e/ou sanar os riscos do sistema;
- Verificar se os patches foram instalados corretamente e as correções bem-sucedidas.

4.10. Da proteção antivírus

4.10.1. O responsável por TI e Recursos Humanos e/ou consultoria especializada instalará um programa antivírus por assinatura atualizado nos equipamentos de todos os colaboradores em trabalho remoto. Os colaboradores devem garantir que seus equipamentos estejam disponíveis para acesso remoto para permitir a atualização do software antivírus sempre que necessário.

4.11. Do descarte das informações

4.11.1. Visando a preservação do meio ambiente, algumas das nossas mídias são reaproveitadas, mas sempre utilizando os procedimentos de reutilização com segurança, apagando todas as informações do antigo usuário. As que não podem ser reaproveitadas, com informações confidenciais, são apagadas e destruídas manualmente, e outras são trituradas para reciclagem, mas sempre um funcionário nosso acompanhando todo o processo;

4.11.2. No caso de documentos impressos com informações confidenciais não há reutilização, logo, são destruídos manualmente e outros são triturados, mas sempre um funcionário nosso acompanhando todo o processo;

4.11.3. As informações contidas em mídia eletrônica são excluídas definitivamente utilizando a técnica WIPE;

4.11.4. Utilizamos como padrão o tempo de 6 meses para descarte, salvo quando especificado em contrato tempo diferente. O responsável pela Área fica a cargo de acompanhar o processo e realizar as comunicações quando devidas.

Normas de Classificação da Informação

5.1 Tem por objetivo garantir o tratamento e proteção adequado a todas as informações, sendo impressas ou eletrônicas, produzidas ou não pela Enfoque, que sejam manuseadas pelos colaboradores, respeitando sempre as melhores práticas de gerenciamento e a legislação vigente, assim como as definições que são adotados nesta PNPISTR.

5.2 Principais tipos de documentos:

- ATA – É um documento formal escrito com base em redação oficial, utilizado em âmbito interno que tem por objetivo registrar reuniões, assembleias e conferências, dela constando, normas, fatos, votações, ocorrências, resoluções, recomendações, determinações, decisões, debates, disposições, etc. Deve ser lavrada pelo secretário de forma objetiva e resumida, das deliberações, resoluções e demais ocorrências de uma reunião ou evento. Após assinada por todos os presentes, inclusive o secretário, a ata, passa a constituir prova de que

houve a reunião, com decisões nela tomadas e das manifestações de todos os participantes. Por conta do seu valor jurídico, deve ser lavrada sem rasuras ou emendas, para que se evite futuras modificações;

- CONTRATO – É um documento que estabelece um vínculo jurídico firmado, via de regra, por escrito, entre dois ou mais sujeitos correspondido pela vontade e com responsabilidade do ato firmado, resguardado pela segurança jurídica em seu equilíbrio social, ou seja, é um acordo de duas ou mais vontades, na conformidade da ordem jurídica, destinado a estabelecer uma regulamentação de interesses entre as partes, com o escopo de adquirir, modificar ou extinguir relações jurídicas de natureza patrimonial;
- DOSSIÊ – É um arquivo e/ou uma coleção de documentos que contém informações relativas aos funcionários, colaboradores, procedimentos administrativos e jurídicos, entre outros. Podem estar em papel ou em formato digital. Geralmente é de âmbito interno, porém, quando solicitado por algum agente externo, pode ser disponibilizado, uma vez que tenha autorização do gestor imediato.
- MEMORANDO e OFÍCIO – São documentos formais de âmbito interno (Memorando) e / ou externo (Ofício) elaborados em papel oficial da empresa (timbrado) e enviado normalmente a funcionários, colaboradores, autoridades públicas, participantes, etc. São os tipos mais comuns de correspondência expedido pela empresa. O conteúdo em via de regra é uma matéria administrativa, mas pode vincular também uma matéria de caráter judicial ou social;
- PROPOSTA COMERCIAL – É um documento formal, utilizado no âmbito interno/externo, que deve apresentar basicamente um escopo dos serviços, preço, cronograma, informações de suporte e da empresa, Termos, Condições e campos de assinatura das partes. Elaborada em papel com timbre da empresa, a proposta comercial tem por objetivo formalizar em contrato a solução oferecida.
- RELATÓRIOS - É um documento formal, utilizado no âmbito interno, com o propósito de reportar através de narrativa escrita e circunstanciada os fatos ocorridos e/ou constatados, ou seja, apresenta o resultado por escrito de uma investigação ou de um trabalho de análise de uma determinada situação. Podendo conter sugestões e recomendações.

5.3 Classificação

5.3.1 É de responsabilidade do colaborador classificar toda informação produzida e manipulada, utilizando os critérios apresentados na planilha abaixo, de forma a garantir a disponibilidade das informações, em conformidade com sua respectiva classificação.

Classificação	Critérios	Consequências de eventual vazamento	Permissão de acesso	Exemplo de documentos
PÚBLICA	Informações que podem ser de conhecimento público	Nenhum	Qualquer pessoa, física ou jurídica, interna ou externa	Informações disponíveis no site ou mídias sociais;
	Informações cujo conhecimento é do interesse de toda EMPRESA e podem ser divulgadas sem	Fornecimento de informações a público externo pode contribuir para eventuais incidentes	Todos os colaboradores, funcionários, e contratados pela EMPRESA, Diretores e Conselheiros. E quando	Balancetes Mensais, Políticas Internas (alçadas, contratação de terceiros), normativos internos (organização e regimentos

CORPORATIVA	restrição, apenas para o público interno		solicitado, por órgão de fiscalização externa.	internos); Documentos Institucionais; Relatório Anual de Atividades da Diretoria Listas de e-mail, ramais, escalas de funcionários
INTERNA	Informações de conhecimento exclusivo do corpo de funcionários da EMPRESA, podendo ser divulgadas para terceiros ou público externo desde que com autorização do Gestor ou em razão de exigência legal	Estas informações podem causar perdas à EMPRESA, caso seja acessada, manipulada ou destruída de forma não autorizada.	Todos os colaboradores, funcionários, Conselheiros e Dirigentes da EMPRESA. Para terceiros ou público externo, desde que com autorização do Gestor ou em razão de exigência legal	Relatórios, Relatório Gerencial; Demonstrações Contábeis e Financeiras; Relatório de conciliação das contas patrimoniais e de resultado; Declarações oficiais exigidos pela Receita Federal do Brasil; Contratos com fornecedores diversos; Plano de Cargos e Salários; Peças Jurídicas protocoladas em processos sem segredo de justiça; Contratos, ...
PRIVADA	Informações protegidas que requerem cuidados especiais quanto à preservação de seus atributos e cuja divulgação indevida sujeita a EMPRESA a riscos consideráveis dirigidas ao gestor da unidade	Estas informações podem causar perdas consideráveis à EMPRESA caso seja acessada, manipulada ou destruída de forma não autorizada, violando ajustes contratuais, sigilo fiscal, tributário ou leis de acesso	Funcionários da EMPRESA membros de grupos específicos de trabalho que necessitam de acesso à informação para o exercício de suas funções. Para terceiros ou público externo, desde que com autorização do Gestor ou em razão de exigência legal. Requerem citação explícita das pessoas ou grupos autorizados	Relatórios, Solicitações, Orçamento, Autorizações para pagamentos, Informações mensais para ABEP;; Cadastros e dossiês de funcionários ou clientes; Dados bancários,
CONFIDENCIAL	Informações cuja preservação de seus atributos seja fundamental para a continuidade dos negócios e cuja divulgação sujeita a EMPRESA a riscos muito elevados. São informações sigilosas, pessoais e estratégicas.	Estas informações podem causar perdas à EMPRESA caso seja acessada, manipulada ou destruída de forma não autorizada. Um impacto substancial é esperado caso estas informações sejam divulgadas de forma não autorizada.	Gestores e funcionários da EMPRESA, estes com acesso previamente autorizado pela diretoria, que necessitam de acesso à informação para o exercício de suas funções. Informações pessoais e estratégicas, com citação explícita das pessoas ou grupos autorizados	Planejamento Estratégico; Relatório; Processos ; Fluxo de caixa; Saldos Bancários; Folha de Pagamento dos funcionários; Ações judiciais; Relatórios de processos judiciais; Cadastros de Diretores; Atas de reunião.

5.4. Responsabilidade e Rotulação

5.4.1 É de responsabilidade do colaborador rotular devidamente toda informação produzida e/ou manipulada, seja digital ou impressa, utilizando os "critérios de classificação da informação" presentes nesta PNPSITR. A rotulação deve ser feita preferencialmente no cabeçalho, podendo também ser feita no rodapé, sempre de fácil visualização.

5.5. Tratamento das informações

As informações listadas abaixo seguem as normas de classificação e tem por objetivo estabelecer os cuidados necessários ao se criar, manusear, transmitir, armazenar, manipular e transportar as informações de forma a garantir a sua integridade, disponibilidade e confidencialidade

5.5.1. Grau de sigilo

- **Pública** – Podem ser de conhecimento público;
- **Corporativa** – Para conhecimento e interesse de todos os membros da empresa;
- **Interna** – Para conhecimento exclusivo dos funcionários da empresa;
- **Privada** – Para conhecimento de grupos e pessoas autorizadas, através de citação explícita;
- **Confidencial** - Para conhecimento de grupos e pessoas autorizadas, através de citação explícita, pois são informações pessoais e estratégicas.

5.5.2. Disponibilidade

- **Pública** – Disponível para o público interno e externo;
- **Corporativa** – Disponível apenas para o público interno;
- **Interna** – Disponível para o público interno, podendo ser difundido para fora em caso de interesse de negócios ou requisição legal;
- **Privada** – Disponível para todos os colaboradores da empresa, podendo ser apresentado a terceiro, desde que, o acesso seja controlado e monitorado. Não deve ser encaminhada para fora da empresa, salvo quando compor acervo patrimonial.
- **Confidencial** - Disponível para todos os colaboradores da empresa, sendo obrigatório indicar o nome das pessoas e cargos que poderão acessar a informação. Não deve ser encaminhada para fora da empresa, salvo quando compor acervo patrimonial

5.5.3. Divulgação/Transmissão

TIPOS	Pública	Corporativa	Interna	Privada	Confidencial
Correio	Sem precauções adicionais	Usar correspondência envelopada registrada	Usar correspondência envelopada registrada e que possa ser rastreada	Uso Desaconselhado. Caso necessário, deve haver anuência prévia do gestor da informação e enviada correspondência que possa ser rastreada, de preferência com portador e recibo de entrega, ou, na falta, SEDEX ou correlato	Não é permitido, a não ser em casos necessário, com a anuência do gestor da informação, observados os cuidados das restritas
Correio eletrônico - Interno	Sem precauções adicionais			Utilizar com precaução	Uso desaconselhado
Correio eletrônico - Externo	Sem precauções adicionais	Usar, apenas, quando houver interesse negocial, aprovado pelo gestor da informação		Utilizar com precaução. Evitar máximo	Não é permitido
Sítio da internet	Sem precauções adicionais	Não é permitido, a não ser quando expressamente autorizado pela Diretoria Executiva			
Reuniões	Sem precauções adicionais	Em ambiente interno. Tomar precauções em relação ao sigilo	Atentar para que apenas as pessoas autorizadas acessem a informação		
Telefone fixos e Celulares	Sem precauções adicionais	Tomar precaução em relação ao sigilo	Tomar precaução em relação ao sigilo. Precaver- se contra a aproximação de pessoas não autorizadas	Precaver- se contra a aproximação de pessoas não autorizadas. Uso de vivavoz, apenas, em áreas fechadas.	Precaver- se contra a aproximação de pessoas não autorizadas. Vedado o uso de viva voz. Em casos necessários, utilizar em local restrito e tom de voz moderado.
E-mail pessoal	Vedado o uso				

5.5.4. Reprodução

- **Pública** – Pode ser realizada por todos os colaboradores;
- **Corporativa e Interna** – Permitida, desde que mantida a integridade da informação e seja para uso exclusivo no desenvolvimento das atividades profissionais;
- **Privada** – A reprodução deve ser previamente autorizada pelo gestor da informação. Atentar para a integridade e confidencialidade. Se for cópia digital, os arquivos temporários devem ser eliminados;
- **Confidencial** – Vedada a cópia de todo ou parte. Permitido somente para colaboradores autorizados previamente pelo gestor da informação e em processo de backup.
-

5.5.5. Armazenamento/Guarda

TIPOS	Pública	Corporativa	Interna	Privada	Confidencial
Impressos, formulários e anotações	Sem precauções adicionais	Guardar em local trancado		Guardar em local restrito e trancado (preferencial-mente em armário de segurança) quando não estiver sendo usada. Acesso, apenas, para as pessoas que necessitam pela natureza de seu trabalho	Guardar em local restrito e trancado (preferencial-mente em armário de segurança), com controle e registro de acesso. Disponível apenas para pessoal previamente autorizado pelo gestor da informação
Informações eletrônicas (em geral)	Sem precauções adicionais	Armazena- mento apenas na rede corporativa	Armazena- mento apenas na rede corporativa. Acesso restrito ao público interno	Armazena- mento apenas na rede corporativa em ambiente compatível com a criticidade	Armazena- mento apenas na rede corporativa, em locais específicos, e que possuam rotina de *backup* e registros de log
E-mail corporativo	Armazenamento apenas em bases corporativas				Armazenamento em bases corporativas com cripto
Mídias removíveis	Sem precauções adicionais	Guardar em local de acesso exclusivo para público interno	Guardar em local restrito e trancado. Acesso apenas para as pessoas que necessitam pela natureza do seu trabalho		Guardar em local restrito, trancado e com controle e registro de acesso. Disponível apenas para pessoal previamente autorizado pelo gestor da informação

5.5.6. Descarte e/ou destruição

Abaixo vamos apenas detalhar os cuidados necessários para realização do descarte e/ou destruição da informação, pois este tema já foi abordado no item 4.8 desta PNPSITR.

TIPOS	Pública	Corporativa	Interna	Privada	Confidencial
Impressos, formulários e anotações	Sem preocupações adicionais	Utilizar fragmentadora			
Formulários, impressos e anotações (timbrado)	Utilizar fragmentadora				
Disquetes, CD's e DVD's (mídias removíveis)	Sem preocupações adicionais		Utilizar fragmentadora, perfurador ou picotar com tesoura		
Pen drive, HD externo e interno (mídias removíveis)	Sem preocupações adicionais		Utilizar ferramenta corporativa para formatar a mídia antes de ser descartada		
Fitas (mídias removíveis)	Sem preocupações adicionais		Retirar a fita e picotar com tesoura		
Dispositivos móveis (notebooks e celulares)	Sem preocupações adicionais		Utilizar ferramenta corporativa para formatar a mídia antes de ser descartada		

OBS: Qualquer equipamento que foi utilizado para manter informações Privadas ou Confidenciais devem passar pelo processo WIPE antes do descarte.

5.6. Reciclagem

- **Pública** – Os documentos impressos, formulários, questionário, anotações, entre outros com está classificação podem ser reciclados sem preocupação adicional.
- **Corporativo, Interna, Privada e Confidencial** – Os documentos impressos, formulários, questionário, anotações, entre outros, devem ser destruídos utilizando fragmentadora antes da reciclagem.

5.7. Reutilização

- **Pública** – As mídias removíveis, dispositivos móveis, documentos impressos, formulários, questionário, anotações, entre outros, com está classificação podem ser reutilizados sem preocupação adicional.
- **Corporativo, Interna, Privada e Confidencial** – As mídias removíveis, dispositivos móveis, entre outros, com está classificação, devem ser formatados antes de serem reutilizados e/ou destruídos. Já os documentos impressos, formulários, questionário, anotações, entre outros com está classificação, não podem ser reutilizados.

5.8. Backup

- Backup de informações deve ser realizados pela equipe de Tecnologia, em nuvem, para garantir o retorno das operações em caso de falhas na infraestrutura, sistemas ou equipamentos, deverá obrigatoriamente manter o mesmo nível de proteção das informações que foram copiadas, em especial a necessidade de criptografia.

Procedimentos e controles implementados

6.1 Atendendo ao objetivo de monitorar e mensurar a performance e efetividade da presente política, nos próximos itens consta uma tabela contendo as atividades de controles com seus respectivos métodos, responsáveis, envolvidos, prazos de implementação e registros de execução.

6.2 Todos os colaboradores serão informados quanto da necessidade de disponibilização dos recursos necessários sob sua responsabilidade para que as atividades de controle sejam realizadas. Se houver necessidade de agendamento prévio, o mesmo será realizado em dia e horário de mútua conveniência desde que não desrespeite os prazos aqui informados.

6.3 Tabela de controles detalhada:

Atividade de controle	Método	Responsável	Envolvidos	Prazos/ períodos de recorrência	Registro de resultados para análise
Verificação de logs de acesso aos ativos de informação	Por software	Responsável TI em conjunto com consultor	Diretoria, em caso de não conformidade	Mensal	Relatório de não conformidade com a política
Verificação de logs de backup	Por software	Responsável TI em conjunto com consultor	Diretoria, em caso de não conformidade TI	Mensal	Relatório de não conformidade com a política
Verificação de funcionamento de antivírus e riscos a segurança em todos os dispositivos	Manual remoto	Responsável TI em conjunto com consultor	Todos os colaboradores	Trimestral	Listas de verificação e relatório de não conformidade
Verificação de funcionamento do sistema de correio eletrônico e riscos de segurança	Manual remoto	Responsável TI em conjunto com consultor	Todos os colaboradores	Trimestral	Listas de verificação e relatório de não conformidade
Análise de risco gerais da empresa	Reunião pessoal	Responsável TI em conjunto com consultor	Diretoria, em caso de não conformidade TI	Trimestral	Carta de registro e relatórios de não conformidade para alteração da presente política
Deliberar e controlar procedimentos de certificação digital e recursos criptográficos	Manual remoto + Reunião de equipe e diretoria	Responsável TI em conjunto com consultor	Todos os colaboradores	Semestral	Listas de verificação e Carta de registro

Noções básicas sobre PII (Informações de Identificação Pessoal)

7.1 Personally identifiable information (**PII**, informação pessoal identificável em tradução livre) – São dados que podem ser usados para identificar, contatar ou localizar um indivíduo ou distinguir uma pessoa de outra. Exemplos:

- Nomes completos
- Endereços postais
- Endereços de e-mail
- Número da carteira de habilitação
- Números de RG e CPF

- Datas de nascimento
- Entre outros

7.2 Segundo a Amazon Macie Clssic, existe uma classificação de objetos de PII, da seguinte forma:

- **Alto** – Quando se tem mais de 50 nomes ou e-mails e qualquer outra informação pessoal. Exemplo: João da Silva e CPF: 057.111.321-00;
- **Moderada** – Quando se tem de 5 a 50 nomes ou e-mails e qualquer outra informação pessoal;
- **Baixa** – Quando se tem de 1 a 5 nomes ou e-mails e qualquer outra informação ou apenas qualquer outra informação pessoal de atributos do PII.

Termo de Compromisso, Sigilo e Confidencialidade

Modelo

Eu, _____, nacionalidade, inscrito(a) no CPF/ MF sob o nº 00000, para tanto, declaro ter lido, estou ciente e de acordo com a **Política, Normas e Procedimentos de Segurança da Informação e trabalho remoto**, bem como suas diretrizes, obrigações, deveres, recomendações e penalidades nela prevista.

Comprometo-me a manter absoluto sigilo com relação a toda e qualquer informação a que tiver acesso da Enfoque e a não utilizar informações confidenciais, para gerar benefício próprio ou de outrem, presente ou futuro, responsabilizando-se por todas as pessoas que vierem ter acesso através do meu intermédio.

Declaro estar ciente que a **Política, Normas e Procedimentos de Segurança da Informação e trabalho remoto** está à disposição através do contato com o responsável pelo TI e Recursos Humanos, portanto pode ser solicitada a qualquer momento através do e-mail do colaborador responsável. Declaro, também, estar ciente de que os acessos por mim realizados no sistema em nuvem, o conteúdo das mensagens enviadas através do Correio Eletrônico corporativo, assim como o uso dos recursos de TI disponíveis são restritos somente ao uso profissional e que são de minha inteira responsabilidade.

Cidade, _____ de _____ de _____

_____ _____

Nome Legível: (Funcionário)

CPF: 0000

Eduardo Artiaga - TI e Recursos Humanos

CPF: 0000

TESTEMUNHAS:

1)_____

2)_____

Sanções

9.1 O colaborador é responsável por qualquer atividade a partir de sua conta (login e senha) e também por seus atos no uso dos recursos oferecidos. Assim, o mesmo responderá por qualquer ação judicial e administrativa apresentada à Enfoque e que envolva a sua conta.

9.2 Todas as práticas que representam ameaça à segurança da informação serão tratadas com a aplicação de ações disciplinares. Na ocorrência de violação desta política, de deliberações internas ou externas, ou de determinação de superiores, ficam os infratores sujeitos a advertência verbal, advertência por escrito, suspensão, demissão sem ou com justa causa e outras medidas cabíveis.

9.3 Todos os usuários são responsáveis pelo uso correto dos recursos informática de propriedade da Enfoque. A instalação ou utilização de softwares não autorizados constitui crime de propriedade intelectual e o infrator estará sujeito à pena de detenção e multa de acordo com a Lei 9.609 de 19 de fevereiro de 1998, pela LGPD e demais leis vigentes relacionadas a esta política.

9.4 A Enfoque se reserva no direito de impor sanções e penas aos que violarem esta Política, nos termos das demais normas legais e internas da Instituição.

Aprovação

Este documento foi aprovado em 18/08/2022 pela Diretoria de Compliance e pelo Comitê Gestor de Segurança e é válido a partir da data de sua publicação para todos os colaboradores que utilizam recursos computacionais.

Histórico de Revisão

VERSÃO	DATA	ITEM OU PÁGINA	HISTÓRICO
1.0	01/07/2019	Todas	Emissão do documento
2.0	15/01/2020	Item 1.2	Modificação
3.0	23/11/2021	Itens 5, 7 e 9	Inclusão
4.0	14/03/2022	Item 4.6	Inclusão
5.0	15/08/2022	Itens 4.7 e 4.8	Inclusão