NEO CONSIG

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

OBJETIVO

O presente documento constitui uma declaração formal da NEOCONSIG acerca de seu compromisso com a proteção das informações de sua propriedade ou sob sua custódia, devendo ser cumprido por todos os seus diretores, gestores, empregados, estagiários, aprendizes e prestadores de serviços.

ABRANGÊNCIA

Esta política se aplica à Empresa, Diretoria, colaboradores e prestadores de serviços.

DEFINIÇÕES

- **Política de Segurança da Informação:** é o documento que orienta e estabelece as diretrizes corporativas da NEOCONSIG 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 da instituição.
- **Informação:** A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, consequentemente, necessita ser adequadamente protegida. A informação pode existir em diversas formas, podendo ser impressa, escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma de apresentação ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.
- **Segurança da Informação:** É a proteção da informação de vários tipos de ameaças, a fim de garantir a continuidade do negócio, minimizar os riscos, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

  Os princípios da segurança da informação abrangem, basicamente, os seguintes aspectos:
  - **Integridade:** somente alterações, supressões e adições autorizadas pela empresa devem ser realizadas nas informações;
  - **Confidencialidade:** somente pessoas devidamente autorizadas pela empresa devem ter acesso à informação;
  - **Disponibilidade:** a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado.

- **Ameaça:** Causa potencial de um incidente indesejado, que pode resultar em dano para o sistema ou organização.
- **Áreas críticas:** Dependências da NEOCONSIG ou de seus clientes, onde esteja situado um ativo de informação relacionado às informações críticas para os negócios da empresa ou de seus clientes.
- **Ativo:** Qualquer coisa que tenha valor para a organização.
- **Ativo de Informação:** Qualquer componente (humano, tecnológico, físico ou lógico) que sustenta um ou mais processos do negócio de uma unidade ou área do negócio.
- **Controle:** Forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.
- **Evento de segurança da informação:** Ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

- **Gestão de riscos:** Atividades coordenadas para direcionar e controlar a organização no que se refere a riscos
- **Incidente de segurança da informação:** Qualquer fato que afete um dos pilares do CID, Confidencialidade, Integridade e Disponibilidade
- **Informação:** agrupamento de dados que contenham algum significado
- **Informações críticas para os negócios da NEOCONSIG:** Toda informação que, se for alvo de acesso, modificação, destruição ou divulgação não autorizada, resultará em perdas operacionais ou financeiras à NEOCONSIG ou seus clientes. Cita-se, como exemplo, uma informação que exponha ou indique diretrizes estratégicas, contribua potencialmente ao sucesso técnico e/ou financeiro de um produto ou serviço, refira-se a dados pessoais de clientes, fornecedores, empregados ou terceirizados, ou ainda que ofereça uma vantagem competitiva em relação à concorrência.
- **Risco:** Combinação da probabilidade de um evento e de suas consequências.
- **Vulnerabilidade:** Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

NORMAS, PROCEDIMENTOS E REQUISITOS DE COMPLIANCE

- **ABNT NBR ISO 27001:2022 -** Sistemas de gestão de segurança da informação, segurança cibernética e proteção à privacidade – Sistemas de gestão da segurança da informação - Requisitos.

RESPONSABILIDADES

É dever de todos os seus diretores, gestores, empregados, estagiários, aprendizes e prestadores de serviços, conhecer, ter acesso e cumprir a presente Política.

DETALHAMENTO

ESTRUTURA DA POLÍTICA

Esta política contém 4 seções de controles de segurança da informação, que juntas trazem para conhecimento das principais categorias de segurança uma seção introdutória das normas internas da NEOCONSIG.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Política de Segurança da Informação

"Promover a cultura da segurança da informação em toda a organização através da implementação de processos adequados para prevenção e mitigação de incidentes de segurança, protegendo a confidencialidade, integridade, disponibilidade e privacidade dos dados, cumprindo os requisitos regulamentares e buscando a melhoria contínua de nossos processos".

A Política de Segurança da Informação, é o documento que orienta e estabelece as diretrizes corporativas da NEOCONSIG 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 da instituição.

DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

A NEOCONSIG adota as seguintes diretrizes para assegurar a proteção das informações sob sua custódia:

- Classificação e Tratamento da Informação
  Todas as informações devem ser classificadas de acordo com sua criticidade e confidencialidade (pessoal, seletiva, setorial, interna ou pública).
  O tratamento da informação deve respeitar sua classificação, garantindo o acesso apenas a pessoas devidamente autorizadas.

- Controle de Acesso
  O acesso às informações será concedido conforme o princípio do menor privilégio e da necessidade de saber.
  Cada colaborador e prestador deve utilizar credenciais individuais e intransferíveis para acesso aos sistemas e informações.
  É proibido compartilhar senhas, tokens, certificados digitais ou outros meios de autenticação.

- Uso Aceitável dos Ativos de Informação
  Os ativos de informação (computadores, e-mails, sistemas, redes, dispositivos móveis e documentos) devem ser utilizados exclusivamente para fins profissionais.
  É proibido instalar softwares não autorizados, acessar conteúdos ilícitos ou utilizar os ativos de forma que comprometa a segurança da empresa.

- Proteção Física e Lógica
  Áreas críticas devem ter controle de acesso físico restrito.
  Equipamentos e mídias que contenham informações sensíveis devem ser protegidos contra roubo, perda ou dano.
  Dispositivos móveis devem utilizar criptografia e senha de bloqueio.

- Backup e Continuidade de Negócio
  Cópias de segurança devem ser realizadas periodicamente, armazenadas de forma segura e testadas regularmente.
  Planos de continuidade de negócios e recuperação de desastres devem estar implementados e atualizados.

- Tratamento de Incidentes de Segurança
  Todo incidente de segurança da informação deve ser registrado e comunicado imediatamente ao Gestor do SGI.
  Medidas corretivas e preventivas devem ser aplicadas para evitar recorrências.

- Privacidade e Proteção de Dados Pessoais
  O tratamento de dados pessoais seguirá as disposições da LGPD (Lei 13.709/2018) e da ISO 27701, garantindo os direitos dos titulares.
  Dados pessoais só devem ser coletados, armazenados e processados para finalidades legítimas e previamente autorizadas.

- Conscientização e Treinamento
  Todos os colaboradores e prestadores de serviços devem participar de treinamentos periódicos sobre segurança da informação e privacidade.
  A responsabilidade individual pelo uso adequado das informações é permanente.

- Conformidade e Auditoria
  O cumprimento desta política está sujeito a auditorias internas e externas.
  O descumprimento das diretrizes poderá resultar em medidas disciplinares, contratuais e legais cabíveis.

Consultar MA-02 Manual de Recurso Humanos item 7.1.9 para mais informações.

POLÍTICA EMPRESARIAL DE PRIVACIDADE E PROTEÇÃO DE DADOS

A política de privacidade pode ser encontrada no PO-37 Política Empresarial de Privacidade e Proteção de Dados.

CONTROLES ESPECÍFICOS:

- **Sistemas NEOCONSIG:** Os sistemas devem assegurar a rastreabilidade das ações por meio de registros que permitam identificar a origem, o responsável e o conteúdo da ação realizada.
- **Rede dos Colaboradores:** O acesso à internet é monitorado via proxy, e os logs do servidor Windows Server devem garantir a rastreabilidade dos acessos e atividades na rede interna.
- **Gestão de Incidentes:** A comunicação de incidentes e a gestão deve observar o fluxo definido no procedimento relacionado a gestão de incidentes incluindo análise, resposta e plano de ação.

POLÍTICA DE SENHAS

- Se estiver criando senha não-numérica, crie senhas combinando letras maiúsculas e minúsculas (Aa), números (58) e símbolos (#@), com no mínimo 12 caracteres conforme definido pela GPO e nos servidores linux conforme política do PAM, evitando seguir uma lógica que possa ser adivinhada como números sequenciais, datas, telefones entre outros. Observe que para arquivos comprimidos com senha a mesma deve ter as mesmas características, porém 12 caracteres.
- O sistema Neoconsig e suas derivações utiliza senhas numéricas, neste caso crie a senha dentro das políticas do sistema, digite sempre números seguros que somente você conheça, evite alterar a senha dos sistemas em computadores ou aparelhos fora das nossas dependências. Não utilize em nenhuma hipótese: CPF, data de nascimento, número de telefones ou outros números que sejam

conhecidos por outras pessoas além de você. Proibido: senha sequencial tal como 102030, 203040, etc. Exemplo de senha segura: 234591 (não usar esta).
- Toda senha deve ser pessoal e intransferível.
- Altere todas as suas senhas a cada 45 dias, isso pode ser parametrizado de maneira diferente no caso dos sistemas web em que há restrições diferenciadas para um determinado convênio.

CLASSIFICAÇÃO OU CONFIDENCIALIDADE DA INFORMAÇÃO EM DOCUMENTOS

Todos os documentos emitidos pelos colaboradores da NEOCONSIG devem ser classificados conforme abaixo:

- Pessoal – Somente podem ser conhecidos e acessados pela própria pessoa como por exemplo sua própria senha pessoal (Classificação 1);
- Seletiva – Somente podem ser conhecidos e acessados pelo superior imediato da pessoa que emitiu o documento e pela pessoa para quem foi compartilhada a informação. (Classificação 2);
- Setorial – Podem ser conhecidos e acessados pelas pessoas do próprio setor, pela direção ou pelas pessoas dos setores a quem é emitido o documento. (Classificação 3);
- Interna – Podem ser conhecidos e acessados por todos da empresa (Classificação 4);
- Pública – Podem ser conhecidos e acessados publicamente. (Classificação 5)

Para tal classificação, deve-se acrescentar ao cabeçalho uma nota, Ex. : Classificação: 5 – Pública ou Confidencialidade 5 - Pública.

Para mais informações sobre como utilizar a classificação ou confidencialidade em documentos utilize o documento PR-01 Procedimento para Elaboração, Revisão e Controle de Documentos e Registros.

CLASSIFICAÇÃO DA INFORMAÇÃO EM E-MAILS

Para classificar informações transmitidas por e-mails, a classificação deverá constar acima da assinatura do e-mail.

TROCA DE INFORMAÇÕES

Cada classificação da informação deve possuir uma especificação para troca de informações baseada nas descrições que se seguem:

– Troca de informações para classificação 1
Sem permissão para troca, exceto com aval assinado pelo administrador de segurança ou na ausência desse, pelo próprio gestor, com obrigação de comunicação futura ao administrador de segurança. Este estabelecerá um método para a troca da informação, que já esteja cadastrado para a classificação seguinte (classificação 2).

– Troca de informação para classificação 2:
Troca da informação falada: Estabelecer quais pessoas devem ter o conhecimento da informação. Fazer a troca da informação em sala de reunião adequada e devidamente fechada. Se fizer

anotações, devem ser depois digitadas em computador em arquivo protegido por senha pessoal de 12 caracteres de letras e números e símbolos, e depois o papel descartado corretamente.
Troca da informação em documento físico: Estabelecer quais pessoas devem ter o conhecimento da informação.
Troca de informação em documento eletrônico: Criptografar a informação com chave ou senha que impeça sua abertura (sugestão arquivo RAR com senha). Utilizar Senha de 12 caracteres combinando letras, números e símbolos à ser transferida por meio diferente do que foi usado para transferir o arquivo.
Enviar o arquivo por e-mail, mas transmitir a senha por outro meio para evitar interceptação da mesma no mesmo arquivo, tal qual telefone fixo ou a rede Microsoft Teams, outro modo permitido é o uso do par de chave pública/privada utilizando GPG.

Exceções: Somente se autorizado pelo administrador de segurança da informação por outro meio comprovadamente criptografado ou na falta deste pelo superintendente da área de tecnologia

- Troca de informação para classificação 3
  Através do sistema de e-mail (Office 365) da empresa, mas sde o gestor necessitar de mais segurança através das mesmas políticas da classificação 2.

- Troca de informação para classificação 4
  Através do sistema de e-mail da empresa ou através de reunião com todos da empresa sem pessoa de fora da empresa.

- Troca de informação para classificação 5:
  Livre.

Devem acontecer treinamentos com todos os funcionários a respeito desta classificação e ela deve ser objeto de auditoria interna, conforme descrito no MA-01 item 7.2.3.

PAPEIS E RESPONSABILIDADES NA SEGURANÇA

Empregados, Estagiários, Aprendizes e Prestadores de Serviços:

- Zelar continuamente pela proteção das informações da Organização ou de seus clientes contra acesso, modificação, destruição ou divulgação não autorizada;
- Assegurar que os recursos (computacionais ou não) colocados à sua disposição sejam utilizados apenas para as finalidades estatutárias da Organização;
- Garantir que os sistemas e informações sob sua responsabilidade estejam adequadamente protegidos;
- Garantir a continuidade do processamento das informações críticas para os negócios da NEOCONSIG;
- Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual;
- Atender às leis que regulamentam as atividades da Organização e seu mercado de atuação;

- Selecionar de maneira coerente os mecanismos de segurança da informação, balanceando fatores de risco, tecnologia e custo;
- Comunicar imediatamente ao Administrador de Segurança da Informação qualquer descumprimento da Política de Segurança da Informação.

Departamento de Tecnologia da Informação:

- Propor ajustes, aprimoramentos e modificações na estrutura normativa da segurança submetendo à aprovação da Diretoria;
- Redigir o texto das normas e procedimentos de segurança da informação, submetendo à aprovação da Diretoria;
- Requisitar informações das demais áreas da NEOCONSIG, através das diretorias, gerências e supervisões, com o intuito de verificar o cumprimento da política, das normas e procedimentos de segurança da informação;
- Receber, documentar e analisar casos de violação da política e das normas e procedimentos de segurança da informação;
- Estabelecer mecanismos de registro e controle de eventos e incidentes de segurança da informação, bem como, de não conformidades com a política, as normas ou os procedimentos de segurança da informação;
- Notificar as diretorias quanto a casos de violação da política e das normas e procedimentos de segurança da informação;
- Receber sugestões dos gestores da informação para implantação de normas e procedimentos de segurança da informação;
- Propor projetos e iniciativas relacionadas à melhoria da segurança da informação;
- Acompanhar o andamento dos projetos e iniciativas relacionados à segurança da informação;
- Realizar, sistematicamente, a gestão dos ativos da informação;
- Gerir a continuidade dos negócios, demandando junto às diversas áreas da empresa, planos de continuidade dos negócios, validando-os periodicamente;
- Realizar, sistematicamente, a gestão de riscos relacionados à segurança da informação.

Administrador de Segurança da Informação:

- O Administrador de Segurança da Informação, contratado pela NEOCONSIG, designado pela alta direção como responsável pela qualidade da segurança da informação.
- É dado a ele, portanto, a liberdade para cobrar, auditar e avaliar ou até mesmo criar exceções dentro da política da informação com o auxílio e aprovação ou repulsa da alta direção.
- É proibido ocultar do administrador de segurança da informação, informações relevantes do incidente, pois ele é único que pode responder adequadamente a tais tentativas e tomar as corretas providências.

Gerências e Superintendências:

- Cumprir e fazer cumprir a política, as normas e procedimentos de segurança da informação;
- Assegurar que suas equipes possuam acesso e entendimento da política, das normas e dos procedimentos de Segurança da Informação;
- Redigir e detalhar, técnica e operacionalmente, as normas e procedimentos de segurança das informações relacionadas às suas áreas, quando solicitado pelo departamento técnico.

- Comunicar imediatamente ao departamento técnico, eventuais casos de violação da política, de normas ou de procedimentos de segurança da informação.

Área Jurídica:

- Manter as áreas da NEOCONSIG informadas sobre eventuais alterações legais e/ou regulatórias que impliquem responsabilidade e ações envolvendo estas políticas.
- Incluir na análise e elaboração de contratos, sempre que necessárias cláusulas específicas relacionadas à segurança da informação, com o objetivo de proteger os interesses da NEOCONSIG;
- Avaliar, quando solicitado, a política, as normas e procedimentos de segurança da informação.

Gerência de Recursos Humanos:

- Assegurar-se de que os empregados, estagiários, aprendizes e prestadores de serviços comprovem a participação da integração na NEOCONSIG, sendo obrigatório a realização da avaliação online no ambiente de treinamento interno.
- Criar mecanismos para informar, antecipadamente aos fatos, ao canal de atendimento técnico mais adequado, alterações no quadro funcional da NEOCONSIG.

Auditoria:

- Todo ativo de informação sob responsabilidade da NEOCONSIG é passível de auditoria em data e horários determinados pelo administrador de segurança da informação com aprovação da diretoria da TI. Podendo este, também, ocorrer sem aviso prévio. Como segunda opção podem tais auditorias ser encomendadas ao analista pelas gestões ou diretoria da empresa.
- Durante a auditoria deverão ser resguardados os direitos quanto a privacidade de informações pessoais, desde que estas não estejam dispostas em ambiente físico ou lógico de propriedade da NEOCONSIG ou de seus clientes de forma que se misture ou impeça o acesso às informações de propriedade ou sob responsabilidade da NEOCONSIG.
- Ao entrar com aparelhos que possuam rede sem fio ou com fio na empresa, o colaborador concorda em caso de evidências de acesso, informar o MAC ADDRESS de tais equipamentos se solicitado para garantir que eles não estão sendo usados para acessar ou tentar burlar a rede da NEOCONSIG.
- Com o objetivo de detectar atividades anômalas de processamento da informação e violações da política, das normas ou dos procedimentos de segurança da informação, a área de Segurança da Informação poderá realizar monitoramento e controles proativos, mantendo a confidencialidade do processo e das informações obtidas.
- Em ambos os casos, as informações obtidas poderão servir como indício ou evidência em processo administrativo e/ou legal.

Diretoria:

- Aprovar a política e as normas de segurança da informação e suas revisões;
- Aprovar a composição do departamento técnico quanto à segurança.
- Nomear os analistas de segurança ou administradores de segurança quando em acordo, conforme as indicações da área de tecnologia de informação.
- Para o bem da organização, seguir as políticas de segurança fielmente.

COMITÊ DE SEGURANÇA DA INFORMAÇÃO (CSI):

Esse comitê deverá ser constituído pelos Diretores e gestores de áreas com a atribuição de aprovar as diretrizes da Política de Segurança da Informação, assim como modificá-las conforme as necessidades da **NEOCONSIG.**

Ainda, a revisão e a manutenção desta política são de responsabilidade do comitê. A periodicidade da revisão será anual ou realizada sempre que for conveniente para a **NEOCONSIG**.

São atribuições do Comitê de Segurança da Informação:

- Propor ajustes, aprimoramentos e modificações desta Política;
- Propor melhorias e aprovar as Normas de Segurança da Informação;
- Definir a classificação das informações pertencentes e/ou custodiadas pela **NEOCONSIG** com base na política de classificação da informação;
- Analisar os casos de violação desta Política e das Normas de Segurança da Informação;
- Realizar reuniões quando solicitadas, aprovar e propor adequações relacionados à melhoria da segurança da informação da **NEOCONSIG**.
- Educar os usuários sobre os princípios e procedimentos de Segurança da Informação.
- As reuniões do CSI devem ser realizadas semestralmente podendo haver convocação em frequência maior ou extraordinariamente, sempre que necessário e devem ser registradas em ata. De acordo com a necessidade, outros representantes de outras áreas da **NEOCONSIG** e convidados externos poderão participar das reuniões do CSI.

USO DE ARQUIVOS COMPARTILHADOS NA REDE (EXCETO SHAREPOINT)

É obrigatório que sejam seguidos os procedimentos abaixo:

Criar arquivo: os arquivos devem ser criados na área de trabalho e após concluído serem copiados para a rede. Os nomes dos arquivos devem ser “breves” e não podem conter símbolos e/ou acentos, pois deixa a indexação dos arquivos lenta, torna os arquivos inacessíveis, pode travar o servidor ou até dificultar a restauração do backup.

Acessar arquivo: O acesso simultâneo de um mesmo arquivo salvo na rede causa impacto quando coincidir com a execução do backup, podendo corromper o arquivo, além de acarretar perda parcial do backup, bem como o travamento total do servidor.

Edição e Exclusão de arquivos: Somente edite ou exclua um arquivo que seja de sua autoria. Redobre sua atenção quando for editar ou excluir qualquer arquivo. Na dúvida consulte seu superior imediato.

O uso dos diretórios é destinado somente a arquivos pertinentes a empresa e ao negócio, portanto, fica proibido salvar quaisquer tipos de arquivos pessoais (sem relação com a empresa) na rede, evitando lentidão na recuperação dos backups e/ou outros possíveis problemas no servidor.

GESTÃO DE ATIVOS

É compromisso de todos gerenciar os ativos físicos e suas informações de forma a promover o bem-estar e o desenvolvimento de uma gestão de informação segura, sustentável e confiável, através do atendimento aos requisitos regulatórios, legais e os subscritos pela NEOCONSIG, atendendo às necessidades dos públicos de relacionamento, sem comprometer a saúde e a segurança dos colaboradores e do ambiente em que está inserida e promover a melhoria contínua do seu sistema de Gestão de Ativos.

A equipe de TI deverá utilizar o sistema OCS Inventory para apoiá-los na gestão de ativos de tecnologia que estejam em rede e permitam a instalação do agente do OCS Inventory, os ativos de hardware que não permitem a instalação do agente OCS Inventory serão gerenciados na planilha FO-76 Formulário Ativos de Hardware Não Gerenciaveis pelo OCS Inventory.

Os ativos em estoque deverão ser armazenados de forma a garantir sua conservação na sala de estoque que é protegida por chave, e serão gerenciados pela aba estoque da FO-76 Formulário Ativos de Hardware Não Gerenciaveis pelo OCS Inventory.

Os ativos relacionados a informação deverão receber um código ou tarja de identificação.

Os ativos tais como teclado, mouse, headsets, fontes, pentes de memória, processadores, cabos ou ainda hardwares de baixo custo de aquisição são considerados bens de consumo e não possuem código de identificação na gestão de ativo, o mesmo pode ser aplicado à ativos que não estão relacionados a informação.

No MA-02 Manual de Recursos Humanos também são descritas questões referentes a gestão de ativos, como por exemplo os termos TU-21 Termo de Responsabilidade para Utilização de Recursos de TI.

Em caso de extravio de um ativo, a equipe de infraestrutura e segurança deverá ser informada imediatamente bem como a diretoria de TI para as devidas providências.

AQUISIÇÃO

Os novos ativos deverão ser adquiridos com suas características funcionais em linha com a estratégia da empresa, a matriz de riscos e a criticidade da função que será exercida, mensuradas através de indicadores específicos que garantam:

- Uma maior facilidade na atuação da manutenção;
- Um atendimento adequado às funções requeridas em um tempo definido e sob um determinado contexto operacional (Confiabilidade);
- Uma estratégia de manutenção e operação baseada em confiabilidade, alinhando as atividades com um adequado suporte logístico;

OPERAÇÃO E MANUTENÇÃO

Os ativos deverão ser operados e mantidos focando na otimização da disponibilidade, eficiência de custo e atendimento aos requisitos regulatórios, através:

- Do cumprimento adequado dos planos e estratégias de manutenção e operação;
- Da melhoria contínua dos processos com inovações, novas tecnologias e boas práticas;
- Da consolidação de uma visão integrada dos ativos de gestão no compartilhamento de recursos;
- Do gerenciamento adequado das informações sobre os ativos para suportar as análises e garantir decisões fundamentadas em critérios técnicos;
- Do gerenciamento proativo dos custos, no qual as decisões de gastos sejam baseadas em um modelo multicritério e em linha com a estratégia da empresa;
- De uma força de trabalho interna e/ou externa capacitada, motivada e responsável pelos resultados.

BACKUP E ARMAZENAGEM DE INFORMAÇÕES:

Em relação ao backup e armazenagem de informações considera-se o seguinte para cumprir as determinações de segurança da empresa:

Categoria	Incluído no Backup	Notas
Sistema de Consignação	Sim	Dados sensíveis armazenados aqui são incluídos no backup.
Arquivos Armazenados no AD	Sim	Incluídos no backup.
Arquivos Armazenados em Computador Local	Não	Vetado armazenar dados sensíveis em computadores locais. Não há backup desses arquivos.
SharePoint (Revisão e Versionamento de Documentos)	Sim	Utiliza revisão de documentos que permite o versionamento, garantindo controle sobre diferentes versões e possibilitando a recuperação de versões anteriores.

A política de backup da empresa é meticulosamente projetada para garantir a segurança dos dados sensíveis. Os backups incluem o sistema de consignação, arquivos armazenados no AD (Active Directory), e os documentos no SharePoint. O SharePoint utiliza uma funcionalidade de revisão de documentos que permite o versionamento deles, garantindo controle sobre diferentes versões e possibilitando a recuperação de versões anteriores.

É estritamente proibido armazenar arquivos com dados sensíveis em computadores locais, uma vez que esses arquivos não são incluídos nos backups regulares. Essa medida visa garantir que os dados sensíveis não sejam comprometidos.

USO DA INTERNET:

O uso das redes dos colaboradores é restrito exclusivamente às atividades relacionadas aos objetivos da empresa. Dessa forma, é fundamental ressaltar que o acesso à Internet para fins pessoais não é autorizado. Da mesma maneira, o acesso a redes sociais deve ser feito somente pelos departamentos que as utilizam para suas funções corporativas, sendo proibido o uso de redes sociais pessoais em equipamentos da organização.

Também estão proibidos os acessos à sites de pornografia, fakenews, malware e outros.

USO DA IMPRESSORA:

O uso das impressoras é restrito as necessidades profissionais e atividades diretamente relacionadas às operações. A utilização de impressoras para fins pessoais não é permitida, visando preservar os recursos e manter o foco na eficiência e eficácia.

É esperado que cada funcionário use as impressoras de maneira responsável, garantindo que todos os documentos impressos estejam em conformidade com as necessidades e objetivos da empresa.

USO E COLETA DE INFORMAÇÕES:

O uso e coleta de informações deve-se restringir ao estritamente necessário para o desempenho das atividades da empresa.

Todas as informações à disposição da Neoconsig possuem como único fim permitir desempenhar com segurança suas atividades (gestão da informação da margem consignável e atividades relacionadas), não tendo o colaborador ou quem quer que seja permissão para fazer qualquer outro uso desta informação.

POLÍTICA PARA MESA E TELA LIMPA

É responsabilidade dos colaboradores manter a mesa e tela limpa em relação a informações dos colaboradores e clientes mantendo a confidencialidade das informações (evitando ícones na área de trabalho), bem como manter a tela bloqueada ao se ausentar de sua mesa, o documento PR-05 Procedimento de Mesa e Tela Limpa descreve em detalhes como funciona o processo de mesa e tela e limpa.

POLÍTICA PARA INSTALAÇÃO DE SOFTWARES

Toda a instalação de softwares deverá ser solicitada via sistema de chamados para o Núcleo de Infraestrutura e Segurança da Informação e somente este, poderá realizar as instalações de softwares conforme o documento PR-113 Instalação de Softwares Licenciados.

Para o controle do inventário de Softwares, é utilizado a ferramenta de agente OCS Inventory.

VIOLAÇÕES E SANÇÕES

São consideradas violações à política, às normas ou aos procedimentos de segurança da informação as seguintes situações, não se limitando às mesmas:

- Qualquer ação ou situação que possa expor a NEOCONSIG, direta ou indiretamente, a perdas financeiras ou danos à imagem, tanto reais quanto potenciais, comprometendo seus ativos de informação;

- Utilização indevida de dados corporativos, divulgação não autorizada de informações, segredos comerciais ou outras informações sem a permissão expressa do Administrador de Segurança da Informação;

- Uso de dados, informações, equipamentos, software, sistemas ou outros recursos tecnológicos, para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos e externos, da ética ou de exigências de organismos reguladores da área de atuação da NEOCONSIG ou de seus clientes;

- A não comunicação imediata ao Administrador de Segurança da Informação de quaisquer descumprimentos da política, de normas ou de procedimentos de Segurança da Informação, que porventura um gestor, empregado, estagiário, aprendiz ou prestador de serviços venha a tomar conhecimento ou chegue a presenciar.

Sanções

A violação à política, às normas ou aos procedimentos de segurança da informação ou a não aderência à política de segurança da informação da NEOCONSIG são consideradas faltas graves, podendo ser aplicadas penalidades previstas em lei ou conforme a política da empresa descrita em MA-02 Manual de Recursos Humanos.

POLÍTICA DE USO DE DISPOSITIVOS MÓVEIS

Os dispositivos móveis da Neoconsig são para uso exclusivo para fins de trabalho, conforme TU-21 Termo de Responsabilidade para Utilização de Recursos de TI e armazenados conforme o item 6.3.4 da PO-02 Politica Gestão de Acessos.

POLÍTICA PARA CONTINUIDADE DE NEGÓCIOS

A continuidade de negócios é declarada conforme os procedimentos em PR-119 Procedimento para Continuidade de Negócio, o objetivo da continuidade de negócios é garantir que os sistemas continuem em funcionamento mesmo no caso de queda dos sistemas principais.

COMUNICAÇÃO DAS INFORMAÇÕES DA POLÍTICA

Todas as alterações relevantes neste documento serão informadas aos clientes externos e fornecedores através de um informativo no site da Neoconsig, que ficará disponível durante, pelo menos, 15 dias.

NEOCONSIG TECNOLOGIA S.A.

* Versão Documento: 07
** Atualizado em 21/08/2025