A.S
ALMEIDA SANTOS
ADVOGADOS

POP – Procedimento Operacional Padrão					
Equipe: 17 TECNOLOGIA DA INFORMAÇÃO					
Atividade: PSI – Política de Segurança da Informação					
Elaborado por:	**Aprovado por:**	**Publicado em:**	**Prox. revisão:**	**Ciclo:**	**ID:**
SJV	JR	16/09/2021	16/09/2026	Anual	17.01
Nome do arquivo: PSI - Politica De Segurança Da Informacao.Docx					

Sumário

Objetivos

Estabelecer diretrizes que permitam aos colaboradores e clientes da **Almeida Santos** seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Aplicação da PSI

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço e fornecedores, e se aplicam à informação em qualquer meio ou suporte.

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, sem prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de cada colaborador manter-se atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Gestão de TI sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar a **Almeida Santos** e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

Regras

Definições

Informações Confidenciais são consideradas não disponíveis ao público, que:

- identifiquem dados pessoais ou patrimoniais;
- sejam objeto de acordo de confidencialidade celebrado com terceiros;
- identifiquem ações estratégicas cuja divulgação possa prejudicar a gestão dos negócios ou reduzir sua vantagem competitiva;
- o colaborador utilizar para autenticação de sua identidade (senhas de acesso ou crachás) de uso pessoal e intransferível.

Não se caracteriza descumprimento desta Política a divulgação de informações confidenciais quando em atendimento a determinações decorrentes do Poder Judiciário ou Legislativo, de órgãos fiscalizadores e reguladores. E quando a divulgação se justificar, por força da natureza do negócio, a advogados, auditores e contrapartes.

Ataque Cibernéticos/Cibersegurança: Os ataques cibernéticos mais comuns são:

- Malware – softwares desenvolvidos para corromper os computadores e redes, como: Vírus: software que causa danos à máquina, rede, softwares e Banco de Dados; Cavalo de Troia: aparece dentro de outro software criando uma porta para a invasão do computador; Spyware: software malicioso para coletar e monitorar o uso de informações; e Ransomware: software malicioso que bloqueia o acesso aos sistemas e base de dados, solicitando um resgate para que o acesso seja reestabelecido.

- Engenharia social – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito, como exemplo: Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento; Phishing: links vinculados por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais; Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais; Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais; e Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes, a fim de captar qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

- Ataques de DDoS (distributed denial of services) e botnets – ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição.

- Invasões (advanced persistent threats) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Disposições Gerais

Preservar as informações da **Almeida Santos** quanto à:

- **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Disponibilidade:** garantia de que os colaboradors autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

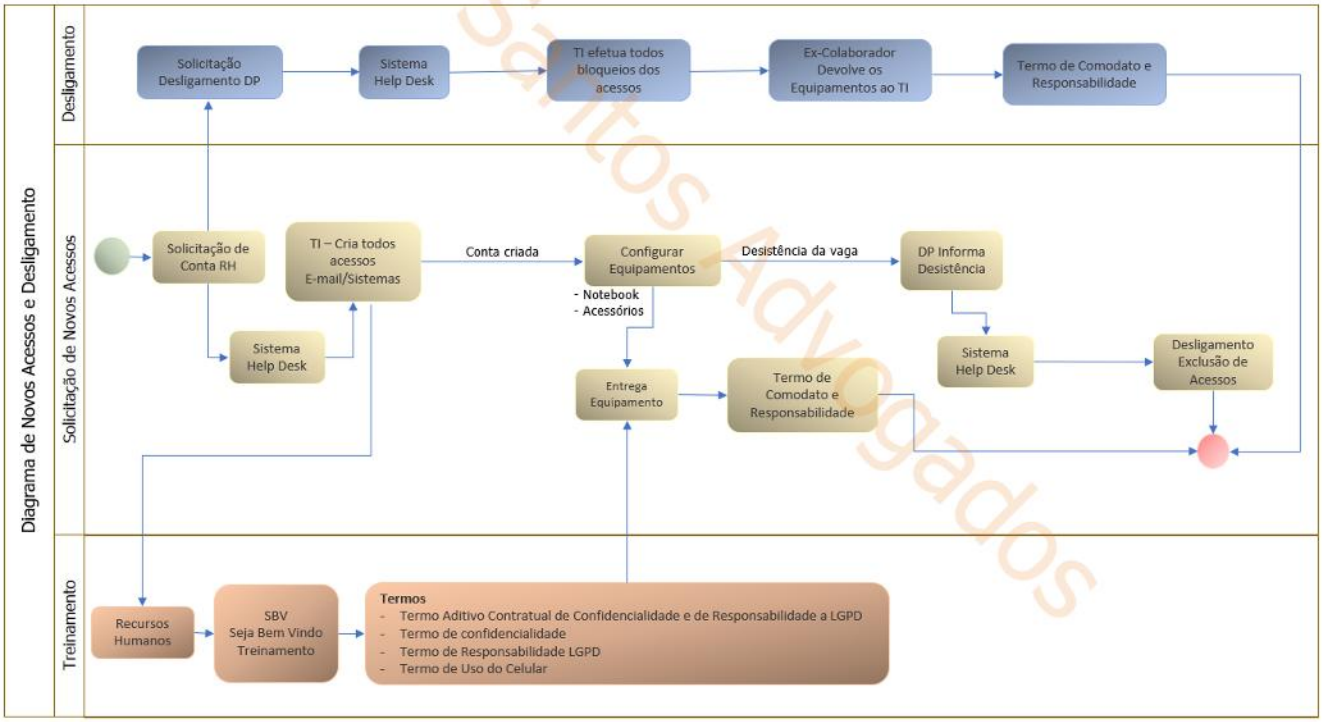
As seguintes diretrizes devem ser seguidas por todos os colaboradores:

- As informações confidenciais devem ser tratadas de forma ética e sigilosa e de acordo com as leis e normas internas vigentes, evitando-se mau uso e exposição indevida.
- A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada.

- A concessão de acessos às informações confidenciais deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades.
- A identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.
- Segregação de instalações, equipamentos e informações comuns, quando aplicável.
- Qualquer risco ou ocorrência de falha na confidencialidade e na segurança da informação devem ser reportados a equipe de TI.

Solicitação de Novos Acesso e Desligamento

O processo de novos acesso e desligamento segue de acordo com as normas estabelecidas no documento 17.08_GC - Gestao_da_Conectividade.



Havendo a necessidade de bloqueio imediato dos acessos.

O Gestor, Departamento Pessoal ou Recursos Humanos estiverem impossibilitados de acessar o sistema Help Desk para enviar a solicitação de bloqueio da conta poderá fazê-lo por e-mail, Teams, WhatsApp, Telefone.

E no primeiro momento que houver oportunidade e acesso registrar a solicitação no sistema Help Desk.

Gerenciamento dos Dados

Nossos dados estão armazenados e disponibilizados em nuvem, no ambiente da Microsoft - SharePoint.

Configurado de forma segura, o compartilhamento externo é bloqueado, somente pessoas da organização pode ter acesso aos links.

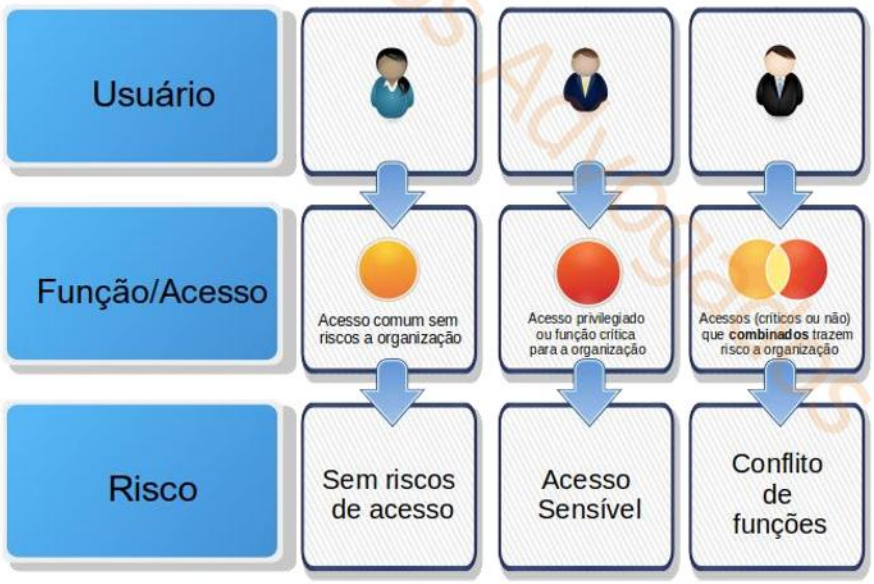
Processos e Controles

Controle de Acesso

Todos os colaboradores do escritório possuem usuário/senha para acessar as informações da rede local e SharePoint em nuvem, que são configurados para acessar somente as informações necessárias para o desenvolvimento de sua rotina de trabalho.

Segregação de Acessos

A Gestão de Acessos a Rede e Sistemas da empresa é feito pela equipe de TI apenas.
Seguindo parametrizações e cuidados para com os usuários, funções e riscos.



Definição:

Para o acesso ao SharePoint existe grupos de acessos com permissionamento de Leitura ou Escrita as pastas Departamentais, somente o Gestor pode autorizar o acesso através de solicitação no sistema Help Desk da empresa.

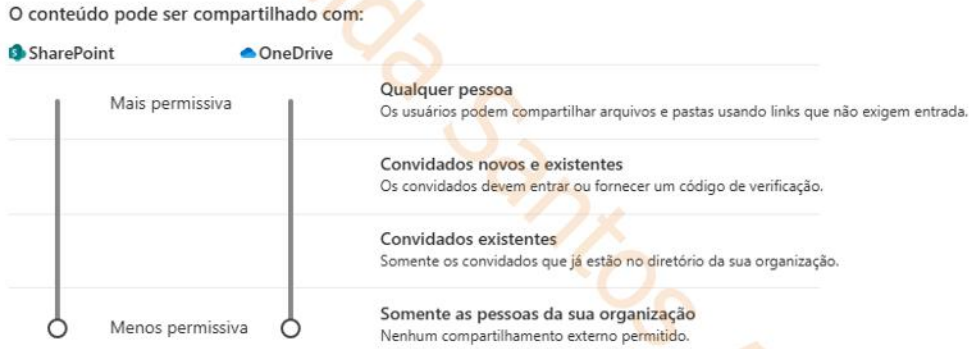
- Grupos de Acessos às pastas somente leitura por equipe;
- Grupos de Acessos às pastas somente escrita por equipe;

Para acesso ao Sistema Jurídico e Financeiro existe grupos de cada equipe com o permissionamento ao que necessita executar em sua rotina diária, somente o Gestor pode autorizar o acesso através de solicitação no sistema Help Desk da empresa.

- Grupos por equipe com acesso aos módulos e funções a sua rotina apenas.

Compartilhamento externo

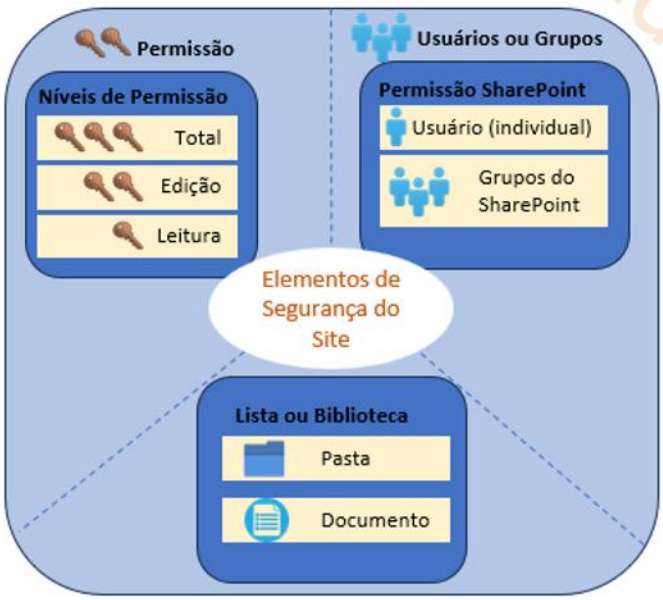
Somente as pessoas da sua organização
Nenhum compartilhamento externo permitido.

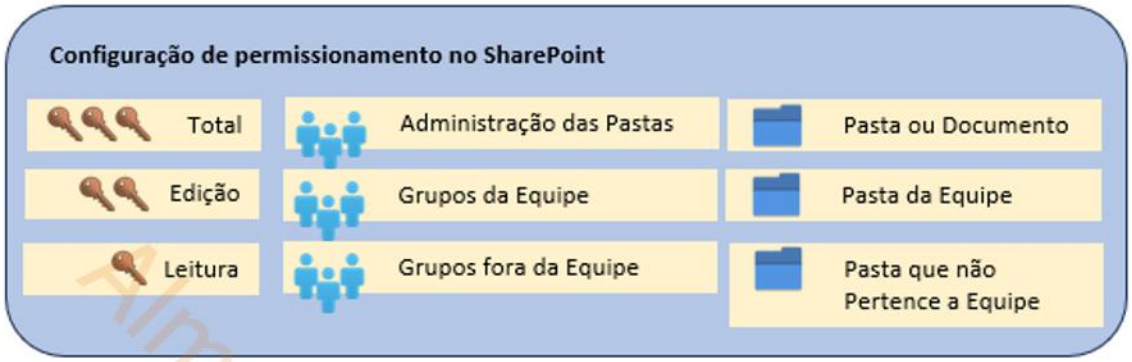


Links de arquivo e pasta

Nenhum link externo permitido.

Relacionamento entre permissões, usuário e grupos e objetos de segurança





- ✓ Somente a conta do TI possui permissão elevada para administrar os acessos
- ✓ O acesso é concedido aos colaboradores de acordo com a equipe que atua
- ✓ Para obter acesso há uma pasta que não seja de sua equipe.
- ✓ É necessário abrir uma solicitação no sistema Help Desk da empresa e se aprovado pelo Gestor proprietário da pasta o acesso é concedido de acordo com sua necessecidade

  - *Escrita* (onde o usuário pode incluir, excluir e editar arquivos e pastas)

  - *Leitura* (onde o usuário poderá consultar o conteúdo da pasta)

- ✓ Nenhum colaborador tem permissão para compartilhar links ou acessos as pastas com usuários externos, mesmo que aprovado pela sua Gestão, a polícita da empresa não permite tal compartilhamento.

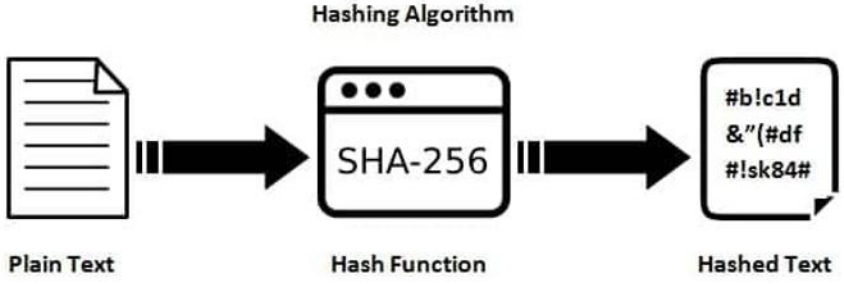
VPN

O acesso a VPN é protegido por criptografia.

Fase 1:	**Fase 2**:
Diffie-Hellman Group: 16 Criptografia: AES-256 Hash: SHA-384	Criptografia: AES-256 Hash: SHA-384 Modo de Cifra de Bloco: CBC

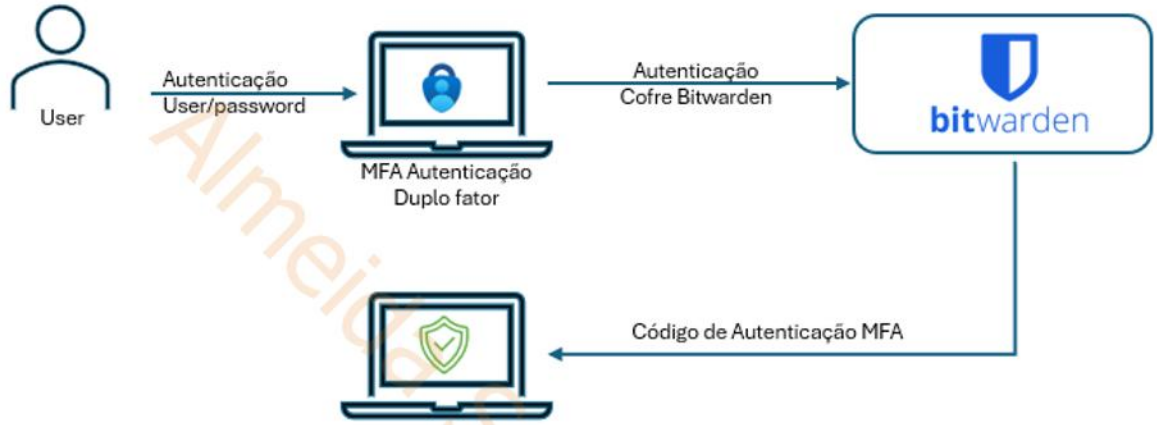
Sistema Jurídico e Financeiro – SSL

O sistema da empresa possui certificado SSL SHA256 (criptografia)

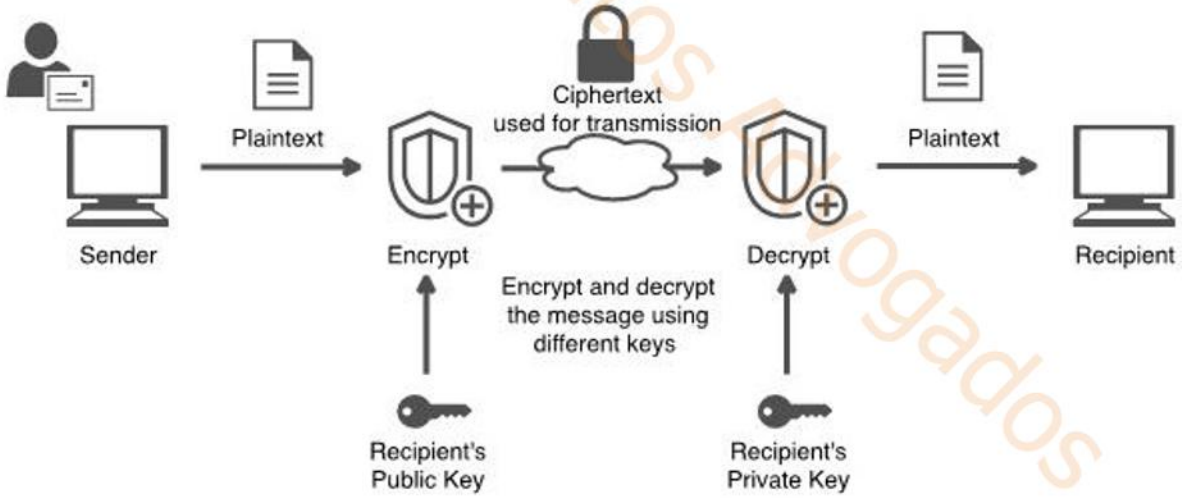


Identidade e Acessos

Microsoft MFA - Autenticação de dois fatores



Criptografia TLS Key



Sistema Jurídico e Financeiro - Monitoramento

Microsoft Defender for Cloud

- Microsoft SQL Server 2016 (SP3) (KB5003279) - 13.0.6300.2 (X64)
- Alertas por métricas:
  . CPU
  . Disco
  . Rede
  . Memória
- Vulnerabilidade do sistema o que deve ser remediado

Certificado Digital A1

Loy Legal

Sistema para proteção e monitoramento do uso do certificado digital A1.

O certificado não é instalado localmente nos Notebooks apenas no sistema.

Captura as intimações eletrônicas diretamente nos portais de justiça que não disponibilizam no diário oficial Ex: E-Proc, Projudi e outros.

Utilizamos o certificado A1 para peticionamentos eletrônicos, salvo em nuvem, criptografado e também geramos uma contra senha, sendo esta, específica apenas para protocolar, garantindo assim maior segurança para o dono do Certificado.

Grupos de acesso

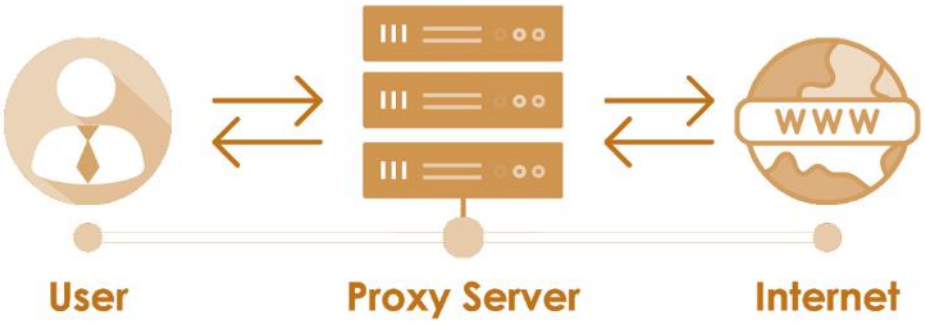
- Consulta Processual
- Peticionamentos
- Leituras de intimações
- Assinador de documentos
- Bloquear nos finais de semana
- Bloquear nos feriados
- Restrição por horários

Acesso WiFi

O acesso ao WiFi é liberado apenas para colaboradores conectarem o Notebook da empresa, a fim de seguirem com seu trabalho, estando no ambiente da empresa é aplicado as segurança de nosso Firewall e Proxy.

Gestores tem acesso em seus dispositivos móveis, demais MacAddress são bloqueados

A segurança aplicada nos equipamentos é o protocolo de criptografia WPA2.



Mesa e Tela Limpa

Para **reduzir os riscos de acesso não autorizado, perda de informações ou danos às informações** durante e fora do horário de expediente, devemos adotar uma política de **"mesa limpa e tela limpa"**, visando o resguardo de informações constante em documentos e/ou impressos durante a ausência do funcionário do seu local e/ou estação de trabalho.

Essa política ajuda a prevenir o acesso não autorizado a informações sensíveis e a proteger os dados da organização. Além disso, está alinhada com normas e estruturas de segurança da informação, como a ISO 27001, que recomendam práticas de mesa limpa e tela limpa como parte das medidas de segurança.

Informações deixadas sobre as mesas de trabalho são passíveis de serem danificadas ou destruídas de diversas formas. O objetivo da política é a redução de risco de uma violação de segurança, fraudes e roubo de informações causadas por documentos que estão sendo deixados sozinhos nas instalações da organização.

A política de mesa limpa e tela limpa faz parte do Código de Conduta da **Almeida Santos**.

Esta política deve ser lida por todos colaboradores, que atuem com as atividades nela descritas.
Institui regras sobre os cuidados a proteção da informação através da mesa limpa e tela limpa.

Tela Limpa

Durante a ausência do local de trabalho, todas as informações sensíveis e confidenciais não podem ficar expostas ou desprotegidas. Arquivos devem ser fechados.

Os usuários têm obrigação de bloquear as estações de trabalho quando se afastarem das mesmas para impedir acesso não autorizado. Ao final do dia dispositivos devem ser desligados, principalmente os conectados às redes e internet.

Mesa Limpa

Os colaboradores devem manter papeis e informações seguras, utilizando locais para armazenamento principalmente quando o ambiente estiver vazio.

Os papéis (com dados dos clientes/acordos) devem ser armazenados em armários trancados e/ou em outras formas de mobiliário de segurança, quando não estiverem em uso;

Anotações, recados e lembretes não devem ser deixados à mostra sobre a mesa ou colados em paredes, divisórias, murais ou nos monitores do computador. Informações sensíveis não devem ser anotadas em quadros brancos.

Os colaboradores não devem deixar pastas com documentos sensíveis em locais de fácil acesso. Devem, ainda, destruir os documentos impressos antes de jogá-los fora, usando, sempre que possível, máquinas fragmentadoras.

Proteção às impressões

Os colaboradores não devem imprimir documentos apenas para lê-los, mas lê-los nas telas dos ativos de informações, preferencialmente.

Quando estritamente necessário, os documentos impressos devem ser removidos imediatamente evitando acúmulo em local público.

Quando aplicável, a utilização de senhas personalizada no local do equipamento compartilhado deve ser utilizada.

Princípios da PSI

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

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso de equipamento pessoal é proibido pelas normas da empresa, casos específicos devem ser tratados e aprovados pela TI junto a Diretoria.

A **Almeida Santos**, por meio do sistema que monitora as máquinas, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

Requisitos da PSI

Para a uniformidade da informação, a PSI deverá ser comunicada a todos os colaboradores da **Almeida Santos** a fim de que a política seja cumprida dentro e fora da empresa.

Deverá haver um comitê multidisciplinar responsável pela gestão da segurança da informação, doravante designado como Comitê de Segurança da Informação.

Tanto a PSI quanto as normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Comitê de Segurança.

Deverá constar em todos os contratos da **Almeida Santos** 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 empresa.

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 um termo de comodato e responsabilidade.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à Equipe de TI e ela, se julgar necessário, deverá encaminhar posteriormente ao Comitê de Segurança da Informação para análise.

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.

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.

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a empresa julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas comerciais e financeiros desenvolvidos pela **Almeida Santos** ou por terceiros.

Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

A **Almeida Santos** 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.

Esta PSI será implementada na **Almeida Santos** por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.

O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação acarretará violação às regras internas da empresa e sujeitará o colaborador às medidas administrativas e legais cabíveis.

Das Responsabilidades Específicas

Dos colaboradores em Geral

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da empresa.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar a **Almeida Santos** e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

Dos Colaboradores em Regime de Exceção (Estagiários)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Comitê de Segurança da Informação.

A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

Dos Gestores de Pessoas e/ou Processos

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI da **Almeida Santos**.

Exigir dos colaboradores a assinatura do Termo de confidencialidade, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da **Almeida Santos**.

Antes de conceder acesso às informações da empresa, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender ao Procedimento Opracional Padrão (POP).

Da Área de Tecnologia da Informação

Infraestrutura – Computadores, Sistema e Rede

Atender a todos colaboradores da empresa através de sistema automatizado – Help Desk de acordo com a documentação 17.13_HP - Help Desk.

Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI, seguindo o mesmo padrão para o perfil de colaboradors sem privilégio algum para instalação e/ou remoção de programas, com acessos de sua equipe e pelos Procedimentos de Segurança da Informação complementares.

Os administradores e operadores da equipe de TI podem, pela característica de seus privilégios como colaboradors, acessar os arquivos e dados de outros colaboradors. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

Segregar as funções administrativas, operacionais e de gestão a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs de auditoria das suas próprias ações.

Garantir segurança especial para sistemas e rede, incluindo o ambiente externo, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

Gerar e manter os sistemas de monitoramento atualizados para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para os logs gerados e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-los juridicamente válidos como evidências.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para o **Almeida Santos**.

Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante.

Quando ocorrer movimentação interna dos ativos de TI especificamente equipamentos de Gestores, garantir que as informações do Gestor não será removido de forma irrecuperável antes de disponibilizar o ativo para outro colaborador, os demais não mantemos as informações locais, as máquinas são formatadas sem nenhum tipo de backup e disponibilizada para outro colaborador.

Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas.

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

os colaboradors (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.

os colaboradors (logins) individuais de estagiários serão de responsabilidade dos próprios contratados.

os colaboradors (logins) individuais de advogados serão de responsabilidade dos próprios advogados.

Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

Definir as regras formais para instalação de software e hardware, exigindo o seu cumprimento dentro da empresa.

Realizar auditorias periódicas de configurações técnicas e análise de riscos.

Garantir que os certificados digitais sejam disponibilizados aos colaboradores após seu treinamento e assinatura de Termo de Responsabilidade pelo uso e manuseio.

Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de colaboradors por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.

Garantir que todos os servidores, estações e demais dispositivos com acesso à rede interna da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

Monitorar o ambiente de TI, gerando indicadores e históricos de:

- ✓ Uso da capacidade instalada da rede e dos equipamentos;
- ✓ Tempo de resposta no acesso à internet e aos sistemas críticos da **Almeida Santos**;
- ✓ Períodos de indisponibilidade no acesso à internet, vpn e aos sistemas críticos da **Almeida Santos**;
- ✓ Incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
- ✓ Atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);

Segurança da Informação

Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.
Propor e apoiar iniciativas que visem à segurança dos ativos de informação da **Almeida Santos**.

Publicar e promover as versões da PSI e as Normas de Segurança da Informação aprovadas pelo Comitê de Segurança da Informação.

Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio da **Almeida Santos**, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.
Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

Analisar criticamente incidentes em conjunto com o Comitê de Segurança da Informação.

Apresentar as atas e os resumos das reuniões do Comitê de Segurança da Informação, destacando os assuntos que exijam intervenção do próprio comitê ou de outros membros da diretoria.
Manter comunicação efetiva com o Comitê de Segurança da Informação sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar **Almeida Santos**.

Buscar alinhamento com as diretrizes corporativas da empresa.

Do Comitê de Segurança da Informação

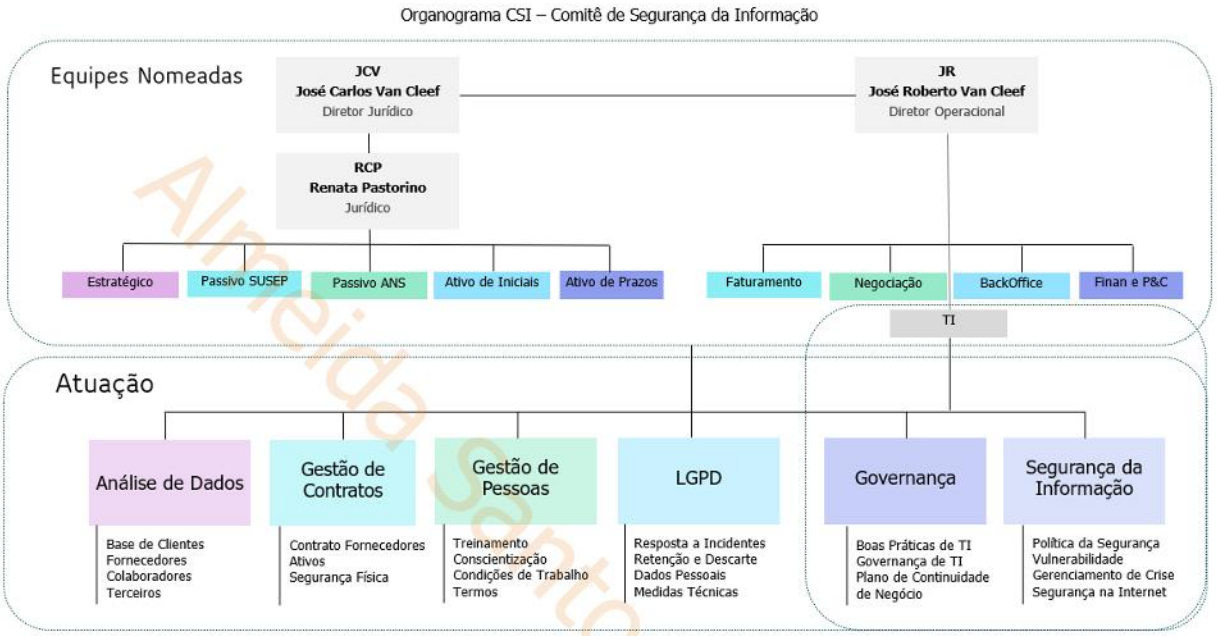
Deve ser formalmente constituído por colaboradores com nível hierárquico mínimo coordenação, nomeados para participar do grupo pelo período de um ano.

Deverá o CSI reunir-se formalmente pelo menos uma vez a cada seis meses. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para a **Almeida Santos**.

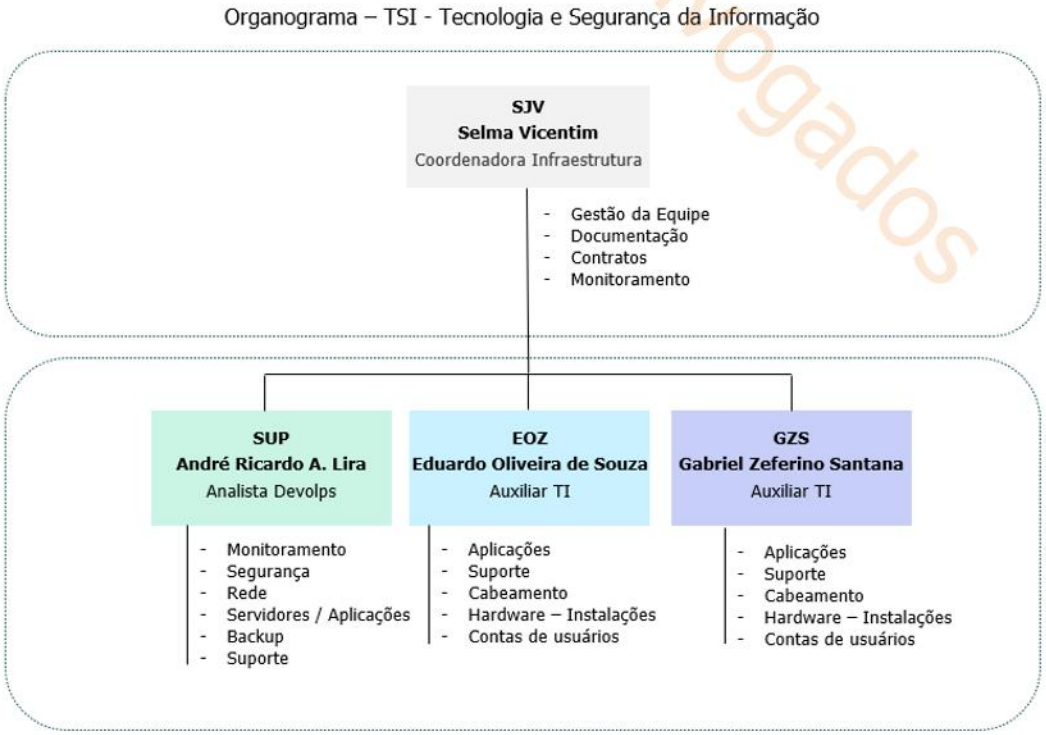
O CSI poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.
Cabe ao CSI:

- ✓ propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos;
- ✓ propor alterações nas versões da PSI e a inclusão, a eliminação ou a mudança de normas complementares;
- ✓ avaliar os incidentes de segurança e propor ações corretivas;
- ✓ definir as medidas cabíveis nos casos de descumprimento da PSI e/ou das Normas de Segurança da Informação complementares.

Organograma CSI – Comitê de Segurança da Informação



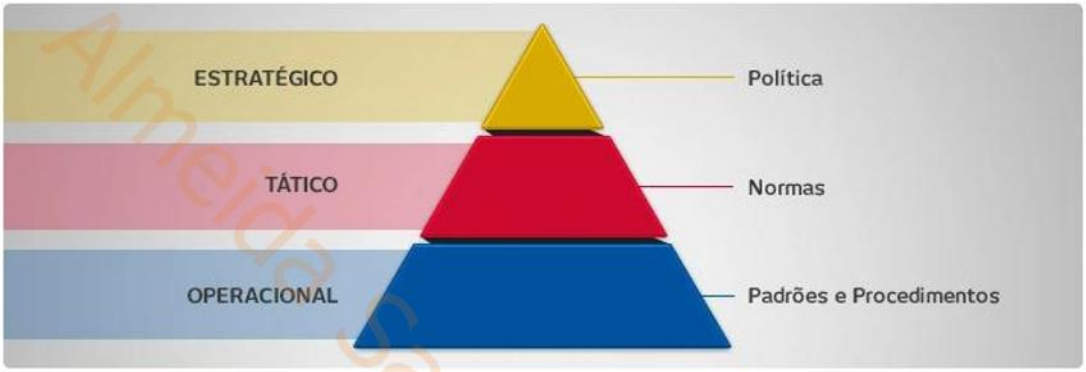
Organograma – Equipe TI



Disponibilização da Informação

Em nossa Intranet disponibilizamos Documentação, Fascículos aos colaboradores com relação a

SGSI – Sistema de Gestão e Segurança da Informação



LGPD – Lei Geral de proteção de Dados

ESG - Environmental, Social and Governance

Práticas Ambientais, Sociais e de Governança

Do Monitoramento e da Auditoria do Ambiente

Para garantir as regras mencionadas nesta PSI, a **Almeida Santos** implantou um sistema de Monitoramento denominado **Workmonitor** nas estações de trabalho.

- Produtividade

Em tempo real o que cada colaborador produz e análise coletiva e individualmente o trabalho desenvolvido por eles.

- Comparar entre colaboradores.
- Visualizar horas mais e menos produtivas.
- Construir rankings de produtividade.
- Informações valiosas para fomentar o aumento da produtividade.

- Monitoramento

Monitoramento de aplicações e sites.

- Busca por palavras e encontramos o exato momento em que um site ou aplicação foi usado.
- Acompanhamos em tempo real o que todos os colaboradores produzem.

- Segurança

Segurança nas informações da empresa.

- Alarmes para sermos avisado imediatamente caso alguém acesse programas ou sites específicos.
- Se acessou, estará gravado em vídeo. Se digitou, estará registrado na base de dados da ferramenta.
- Todas as informações geradas pelo WorkMonitor estarão armazenadas em ambientes seguros e criptografados.
- Bloqueio imediato das estações em caso de desligamento ou atividade suspeitas.

- Investigação Forense

Tecnologia que ativa um mecanismo de rastreio, de forma on-line, nas máquinas, permitindo analisar qualquer informação, voltados a atividades suspeitas.

Características:

- Acesso a máquina dos usuários de forma silenciosa;
- Gera laudos criminais, coletando tudo que for catalogado como evidência o que dará peso aos indícios e as referências;

Capturar a informação visualizada e transmitida pelos usuários.

RRM - Módulos

Inventário - Controle de Hardware e Software

Características gerais do módulo:

- Inventaria de forma completa todos os componentes de hardware e software em tempo real;
- Não trabalha por varredura, garantindo estabilidade nas máquinas e na rede;
- Permite executar, de maneira customizada e por demanda, a varredura dos discos para que todo o arquivo do tipo ZIP, MP3, DLL, entre outros, possa ser inventariado;
- Trabalha em tempo real, garantindo que todo e qualquer software executado seja listado e pré-classificado no inventário;
- Permite que seja feito o cadastro completo e automatizado de todas as licenças existentes na rede;
- Recursos para customização de formulários personalizados e interativos;
- Possui um nível avançado de identificação de hardware, evitando a necessidade de abrir computadores para upgrade.

Tático - Controle Remoto

- Suporta múltiplas conexões remotas, tanto cliente quanto servidor;
- Permite controlar múltiplos computadores remotos e visualizar múltiplas sessões na mesma tela;
- Bloqueio do teclado e mouse do computador remoto durante a conexão;
- Possibilita o controle remoto via web (Internet Explorer/Netscape/Firefox/Chorme);
- Transferência de arquivos;
- Impressão remota de arquivos;
- Mensagem de início/final de controle remoto;
- Log detalhado das ações realizadas durante o controle remoto;
- Acesso autorizado ao registro do Windows;
- Customização do consumo do controle remoto;
- Não necessita a montagem de bookmarks. Possui uma interface que permite visualizar os micros disponíveis para controle remoto, agrupando no formato organizacional (setores ou localidades);
- Autorização de conexão e desconexão por parte do cliente;

- Possibilita modo somente visualização, conforme o perfil do operador;
- Executa processos e serviços remotamente sem o uso do controle remoto;
- Permite efetuar shutdown remoto sem conectar ao computador remoto;
- Suporta alta resolução;
- Possibilita ligar computadores de forma remota (função wake-up on lan);
- Permite visualizar os softwares instalados e todos os componentes de hardware do equipamento remoto;
- Dependência de plugin do fabricante, o que garante velocidade e sigilo nas informações trafegadas.

Distribuição de Software

- Possui velocidade na entrega dos pacotes, não consumindo recursos da rede;
- Possibilita criar regras para distribuição, podendo executar eventos antes e depois do envio;
- Proporciona ao administrador todos os logs de falha e sucesso na entrega ou instalação do pacote;
- Possibilita o agendamento da distribuição de pacotes;
- Permite a instalação silenciosa de pacotes;
- Possui um componente auxiliar ao qual integra diversos arquivos e diretórios em um único executável, o que facilita o trabalho para o administrador na construção do pacote;
- Dispõe de recursos para efetuar gravação de movimentos do mouse como auxílio na instalação do pacote. Utiliza-se este recurso quando o software não possui instalação silenciosa;
- A entrega do pacote pode ser compactada e criptografada;
- Suporte a plataforma Linux e Windows, uso de multicast;
- Integração com múltiplos servidores de pacotes;
- Permite criar dependência de pacotes;
- Possui controle de número de entregas simultâneas;
- Permite enviar pacotes sem a necessidade de compartilhamentos.

Correio Eletrônico

O objetivo desta norma é informar aos colaboradores da **Almeida Santos** quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico da **Almeida Santos** é para fins corporativos e relacionados às atividades do colaborador colaborador dentro da empresa. A utilização desse serviço para fins pessoais não é permitido.
Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico da **Almeida Santos**:

- enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da empresa;

- enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de colaborador de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a **Almeida Santos** ou suas unidades vulneráveis a ações civis ou criminais;
- divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades da **Almeida Santos** estiver sujeita a algum tipo de investigação.
- produzir, transmitir ou divulgar mensagem que:
  - ✓ contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da **Almeida Santos**;
  - ✓ contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
  - ✓ 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;
  - ✓ vise obter acesso não autorizado a outro computador, servidor ou rede;
  - ✓ vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
  - ✓ vise burlar qualquer sistema de segurança;
  - ✓ vise vigiar secretamente ou assediar outro colaborador;
  - ✓ vise acessar informações confidenciais sem explícita autorização do proprietário;
  - ✓ vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
  - ✓ inclua imagens criptografadas ou de qualquer forma mascaradas;
  - ✓ contenha anexo(s) superior(es) a 50 MB para envio (interno e internet) e 50 MB para recebimento (internet)
  - ✓ tenha conteúdo considerado impróprio, obsceno ou ilegal;
  - ✓ seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
  - ✓ contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
  - ✓ tenha fins políticos locais ou do país (propaganda política);
  - ✓ inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador
- Departamento
- Telefone com Ramal - se possuir
- Correio eletrônico
- Nome da empresa

Internet

Todas as regras atuais da **Almeida Santos** visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da empresa com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a **Almeida Santos**, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da empresa, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

A **Almeida Santos**, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a empresa cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela empresa aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos nas unidades.

Como é do interesse da **Almeida Santos** que seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

Somente os colaboradores que estão devidamente autorizados a falar em nome da **Almeida Santos** para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

Apenas os colaboradores autorizados pela empresa poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de batepapo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Os colaboradores com acesso à internet não poderão fazer o download (baixa) programas mesmo sendo eles ligados às suas atividades na **Almeida Santos** deverão solicitar a equipe de TI através de chamado

no sistema Help Desk para que providencie a instalação, e o mesmo somente se seguirá se a empresa for retendora de licença, sendo programa livre – homologado pela TI.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela equipe de TI e reportado ao DP e seu Gestor direto.

Os colaboradores não poderão em hipótese alguma utilizar os recursos da **Almeida Santos** para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso. Caso seja necessário, grupos de segurança deverão ser criados para viabilizar esse perfil de colaborador especial e seus integrantes definidos pelos respectivos gestores.

Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado a **Almeida Santos** ou de dados de sua propriedade.

Os colaboradores não poderão utilizar os recursos da **Almeida Santos** para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins), serviços de streaming (rádios on-line, canais de broadcast e afins) não serão permitidos. Já os serviços de midia sociais (Facebook, Youtube e afins) serão permitidos a grupos específicos que necessitam dos acessos pera execução de seu trabalho e desde que aprovador pelo seu Gestor e Diretoria. Porém, os serviços de comunicação instantânea (WhatsApp e afins) serão inicialmente disponibilizados aos colaboradors e poderão ser bloqueados caso o gestor requisite formalmente à Equipe de TI, ou se identificarmos mal uso da aplicação.

Não é permitido acesso a sites de proxy de navegação anônima.

Identificação

Os dispositivos de identificação e senhas protegem a identidade do colaborador, evitando e prevenindo que uma pessoa se faça passar por outra perante a **Almeida Santos** e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

Todos os dispositivos de identificação utilizados na **Almeida Santos**, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira, e de acordo com a documentação 17.08_GC - Gestao_da_Conectividade.

O colaborador, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a empresa e a legislação (cível e criminal).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante a **Almeida Santos** e a legislação (cível e criminal) será dos colaboradors que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

É proibido o compartilhamento de login para funções de administração de sistemas.

O Departamento Pessoal da **Almeida Santos** é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.

A Equipe de TI responde pela criação da identidade lógica dos colaboradores na empresa, nos termos do Procedimento 17.08_GC - Gestao_da_Conectividade para Gerenciamento de Contas de Grupos e Colaboradors.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local.

Os colaboradors que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 8 (oito) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) caixa-alta (maiúsculo).

Já os colaboradors que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

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

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.

Após 3 (três) tentativas de acesso, a conta do colaborador será bloqueada. Para o desbloqueio é necessário que o colaborador entre em contato com a Equipe de TI da **Almeida Santos**.

Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).

Os colaboradors devem comunicar a equipe de TI imeditamente se suspeitarem que terceiros obtiveram acesso indevido ao seu login/senha.

A periodicidade para troca das senhas não está definida definida devido a decentralização entre o sistema, e-mail e rede, isso traria uma grande confusão nos acessos pelos colaboradors. Estamos seguindo com um projeto de migração de todas nossas contas de e-mail para os servidores da Microsoft para regularizarmos essa situação.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum colaborador for demitido ou solicitar demissão, o Departamento Pessoa deverá imediatamente comunicar tal fato ao Departamento de Tecnologia da Informação através de chamado no sistema Help Desk da empresa, a fim de que essa providência seja tomada. A mesma conduta se aplica aos colaboradors cujo contrato ou prestação de serviços tenha se encerrado, bem como aos colaboradors de testes e outras situações similares.

Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca à área técnica responsável para cadastrar uma nova.

Computadores e Recursos Tecnológicos

Os equipamentos disponíveis aos colaboradores são de propriedade da **Almeida Santos**, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da empresa, bem como cumprir as recomendações constantes no Termo de Comodato e Responsabilidade.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico da Equipe de TI da **Almeida Santos**, ou de quem este determinar. As gerências que necessitarem fazer testes deverão solicitá-los previamente à Equipe de TI através de chamado no sistema Help Desk da empresa.

Todas as atualizações do sistema operacional estão programadas para ocorrerem automaticamente nas estações, porém a Equipe de TI envia comunicados periodicamente orientando aos colaboradores sobre a prática e como checar e efetuar as atualizações recomendadas pela Microsof, os demais sistemas que exijam atualização são feitos automaticamente pela ferramenta RMM sem a interferência do colaborador.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O colaborador, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar a Equipe de TI responsável mediante registro de chamado no Help Desk.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes ao negócio da **Almeida Santos** (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao colaborador.

Documentos imprescindíveis para as atividades dos colaboradores da empresa deverão ser salvos em drives de rede. 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 colaborador.

Os colaboradores da **Almeida Santos** e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da Equipe de TI.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas.

Todos os computadores de uso individual deverão ter senha de Bios para restringir o acesso de colaboradores não autorizados. Tais senhas serão definidas pela Equipe de TI da **Almeida Santos**, que terá acesso a elas para manutenção dos equipamentos.

- Os colaboradores devem informar a Equipe de TI qualquer identificação de dispositivo estranho conectado ao seu computador.
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da Equipe de TI da **Almeida Santos** ou por terceiros devidamente contratados para o serviço.
- É expressamente proibido o consumo de alimentos, bebidas ou fumo próximo aos equipamentos.
- O colaborador deverá manter a configuração do equipamento disponibilizado pela **Almeida Santos**, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelo Termo de Comodato e Responsabilidade, assumindo a responsabilidade como custodiante de informações.
- Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os computadores e notebooks quando não estiverem sendo utilizados.
- Todos os recursos tecnológicos adquiridos pela **Almeida Santos** devem ter imediatamente suas senhas padrões (default) alteradas.
- Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da **Almeida Santos**.

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.
- Burlar quaisquer sistemas de segurança.
- Acessar informações confidenciais sem explícita autorização do proprietário.
- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).

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

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;

- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

Data Center

De acordo com a Documentação 17.14_GAI - Gestão da Area de Infraestrutura.

O acesso ao Datacenter somente deverá ser feito pela Equpe de TI autorizada por meio de chave.

Nas localidades em que não existam colaboradores da área de tecnologia da informação, pessoas de outros departamentos deverão receber previamente a autorização da Equipe de TI para que possam exercer as atividades operacionais dentro do Datacenter, como: suporte em eventuais problemas, e assim por diante.

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado, que deverá solicitar o acesso através do Sistema Help Desk preenchendo o formulário Controle de Acesso ao Datacenter, bem como assinar o Termo de Responsabilidade.

Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização com antecedência a Equipe de TI liberação de acesso, conforme lista salva em Procedimento de Controle de Acesso ao Datacenter.

Deverão existir duas cópias de chaves da porta do Datacenter. Uma das cópias ficará de posse do coordenador responsável pelo Administrativo, a outra, de posse do coordenador de infraestrutura.

O Datacenter deverá ser mantido limpo e organizado.. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do Departamento de Serviços Gerais.

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.

A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com o preenchimento da solicitação de liberação pelo colaborador solicitante e a autorização formal desse instrumento pelo responsável do Datacenter, de acordo com os termos do Procedimento de Controle e Transferência de Equipamentos.

GPO – Group Policy Objects

Os administradores gerenciam as GPOs a partir do Active Directory. aplicadas em diferentes níveis, como:

- **Domínio:** Afeta todos os dispositivos e usuários conectados ao domínio.
- **Unidade Organizacional (OU):** Políticas específicas a grupos
- **Computadores Locais:** Aplicada diretamente em dispositivos específicos.

Backup

Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas "janelas de backup" – períodos em que não há nenhum ou pouco acesso de colaboradors ou processos automatizados aos sistemas de informática, seguindo a documentação 17.09_Gestao_da_Seguranca.

Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

Para Microsoft Office SharePoint Online, o tempo de retenção é de 93 dias. Ele começa quando você exclui o item de seu local original. Quando você exclui o item da lixeira do site, ele entra na lixeira do conjunto de sites. Ele permanece lá pelo restante dos 93 dias e, em seguida, é excluído permanentemente.

Além deste período concedido pela Microsoft, temos um sistema interligado de Backup – Veem

Diariamente recebemos o resultado dos JOB.

Interligado ao sistema Veem, temos uma unidade interna do tipo NAS que faz um espelhamento de todos arquivos na nuvem.

O Backup dos arquivos do Sistema utilizado pela empresa é feito na Nuvem (Azure), controlado e por empresa terceira contratada.

Os backups históricos ou especiais deverão ser armazenadas discos externos, Mantidos em ambiente externo ao Datacenter.

Os backups imprescindíveis, críticos, para o bom funcionamento dos negócios da **Almeida Santos**, exigem uma regra de retenção especial, conforme previsto nos procedimentos específicos e de acordo com a Norma de Classificação da Informação, seguindo assim as determinações fiscais e legais existentes no país.

Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

Quaisquer atrasos na execução de backup ou restore deverão ser justificados formalmente pelos responsáveis nos termos do Procedimento de Controle de Backup.

Testes de restauração (restore) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do backup.

Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

Para formalizar o controle de execução de backups e restores, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pelo coordenador de infraestrutura, nos termos do Procedimento de Controle de Backup e Restore.

Os colaboradores responsáveis descritos nos devidos procedimentos e na planilha de responsabilidade poderão delegar a um custodiante a tarefa operacional quando, por motivos de força maior, não puderem operacionalizar. Contudo, o custodiante não poderá se eximir da responsabilidade do processo.

Backup em repouso

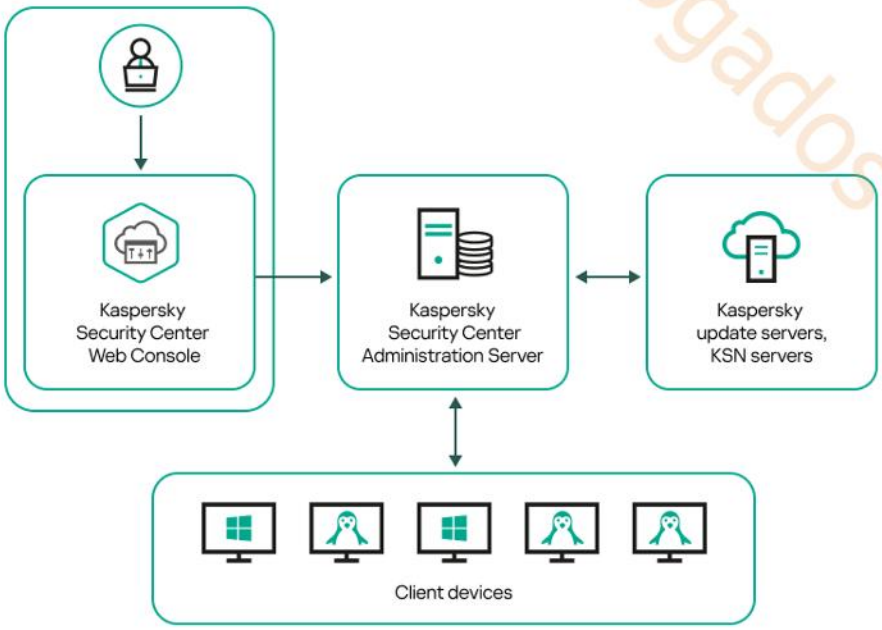
A criptografia em repouso é usada para ajudar a proteger os dados armazenados em um disco (incluindo unidades de estado sólido) ou mídia de backup. Todos os dados armazenados pela **Almeida Santos** são criptografados na camada de armazenamento pelo algoritmo padrão de criptografia avançada (AES, na sigla em inglês), AES-256.

Antivirus

Kaspersky Security Center Cloud Console

- Instalação dos aplicativos da Kaspersky em dispositivos logados a rede e gerenciar os aplicativos instalados.
- Hierarquia de grupos de administração de dispositivos clientes.
- Servidores de Administração virtuais e hierarquicamente.
- Dispositivos de rede, incluindo estações de trabalho e servidores:
- Gerencia remota dos aplicativos da Kaspersky instalados nos dispositivos clientes.
- Implementação centralizada de chaves de licença para aplicativos da Kaspersky nos dispositivos cliente.
- Políticas de segurança para dispositivos da rede.
- Gerencia tarefas para aplicativos instalados em dispositivos na rede.
- Relatórios sobre o status do sistema de segurança para cada cliente individualmente.

O Servidor de Administração e o DBMS (Sistema de Gerenciamento de Banco de Dados) conectado são implantados em um ambiente em nuvem. A manutenção do servidor de administração e do DBMS está incluída como parte do serviço. Todos os componentes de software do Kaspersky Security Center Cloud Console são mantidos atualizados. É feito o backup regular do Servidor de Administração e dos objetos criados (como políticas e tarefas) para mantê-los seguros.

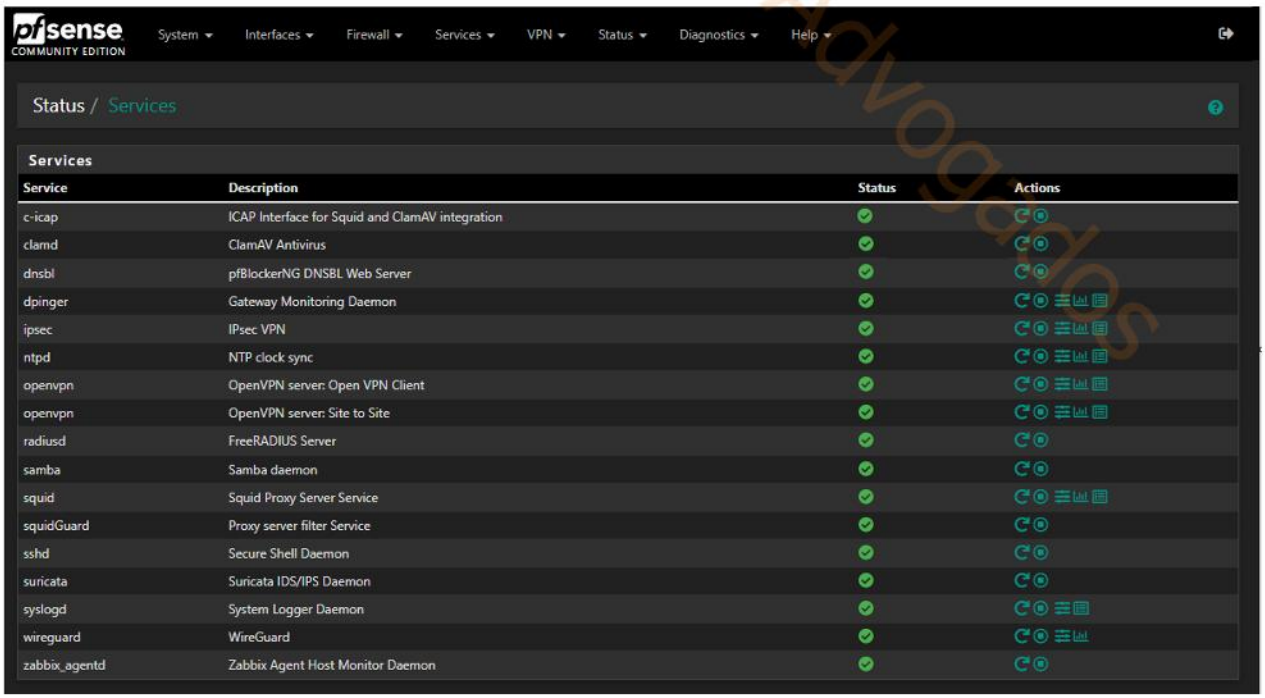


Política de Ameaças

Microsoft Defender 365

Firewall

PFSense – Services status



Das Disposições Finais

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da **Almeida Santos**. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela empresa.

Controle de Atualização

Versão	Data	Alterações
01	16/09/2021	Versão Inicial
02	16/09/2022	Versão Revisada
03	16/09/2023	Versão Revisada
04	16/09/2024	Versão Final