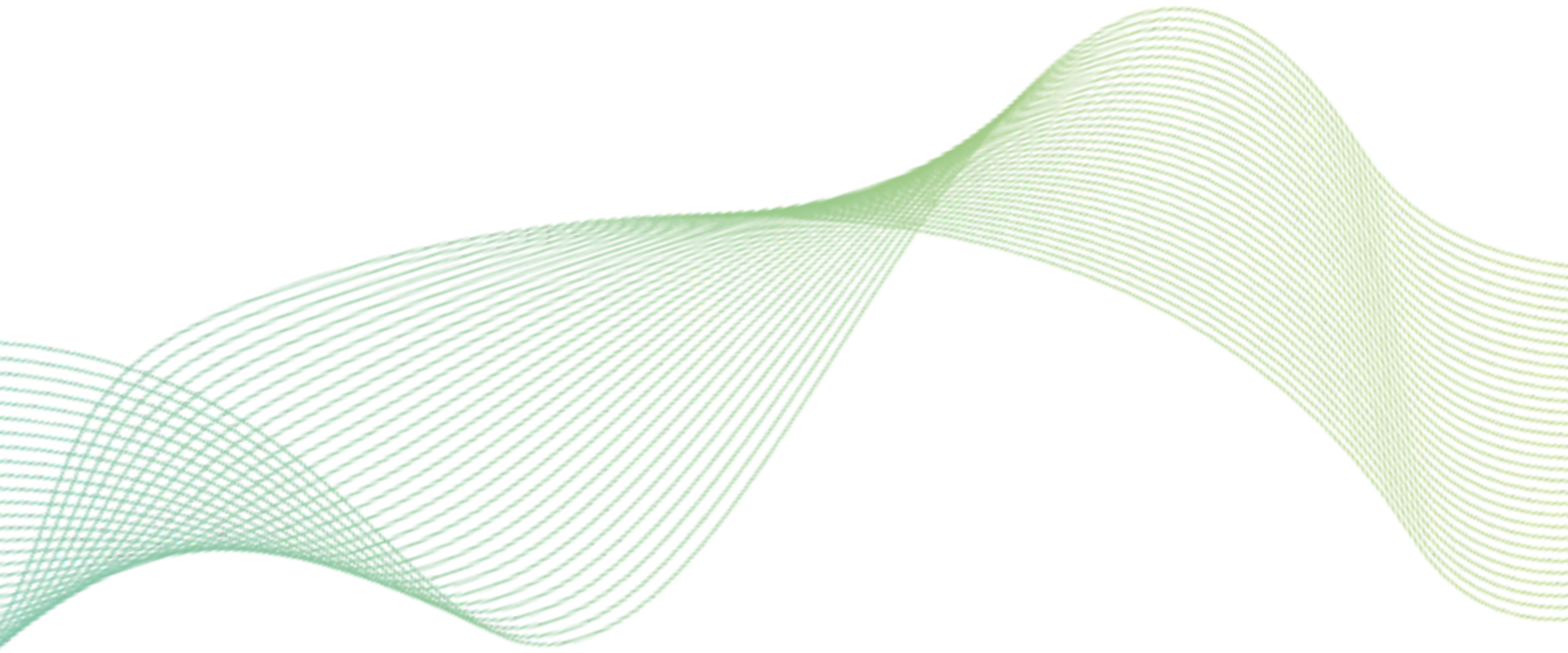
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO



2024

DA DISTRIBUIÇÃO E VIGÊNCIA

A Política de Segurança da Informação (PSI) da Aptum Tecnologia, traz as diretrizes para a proteção de ativos e prevenção de responsabilidades, relacionadas à Segurança da Informação.

Todos os membros da Alta Direção, coordenadores, colaboradores, incluindo terceirizados, estagiários e jovens aprendizes (“Colaboradores”) da empresa devem definir seus direcionamentos a partir das orientações previstas na presente Política, considerando as necessidades específicas e os aspectos legais e regulatórios a que estão sujeitas.

A PSI será revisada anualmente, podendo ser alterada, quando mudanças forem necessárias e aprovadas.

DO CONTROLE DE VERSÕES

A PSI da Aptum Tecnologia, ao ser anualmente revisada, e vindo a ser alterada, irá manter um controle atualizado de versões, com as respectivas datas de Controle de Aprovação e de Modificações Aprovadas. A tabela a seguir apresentada, apresenta um modelo de Controle de Versões, a ser praticado.

VERSÃO	DATA DA ELABORAÇÃO	AUTOR	Revisor	CONTROLE DE MODIFICAÇÃO
01	21/05/2024	Antônio J. A. Cebalho	Victória da S. Oliveira	Criação do Documento

Sumário

1. INTRODUÇÃO

A Segurança da Informação (SI) é a proteção da informação, contra vários tipos de ameaças, objetivando, garantir a continuidade do negócio, minimizando os riscos e maximizando o retorno sobre os investimentos e as oportunidades para a Aptum Tecnologia e seus clientes.

A Gestão da Segurança da Informação, não é um exercício pontual, mas uma atividade permanente de melhoria contínua. A Segurança da Informação é obtida a partir da implementação de um conjunto de controles, incluindo tecnologia, políticas, processos, procedimentos, conscientização e a própria estrutura organizacional da empresa. Esses controles além de serem estabelecidos, implementados, analisados criticamente, sempre que necessário, serão continuamente melhorados e atualizados, para garantir que os objetivos de segurança da informação da Aptum Tecnologia, sejam atendidos.

Internamente, considera-se como Informação, toda a base de conhecimento, conteúdo, dados, conceito envio ou recebimento de mensagens, processo ou fato existente, em meio físico ou eletrônico, que compõe documentos e informações de propriedade e do interesse ou posse da Aptum Tecnologia. Isto inclui, mas não se limita a, qualquer dado, material, processo, especificações, inovações e aperfeiçoamento técnicos e comerciais, que agreguem valor para o negócio da empresa, assim como todas as informações confidenciais dos nossos clientes, colaboradores, prestadores de serviços e terceiros sob custódia da empresa.

A Aptum Tecnologia, faz o acompanhamento do ciclo de tratamento dos dados, garantindo que as informações sejam confiáveis e estejam devidamente protegidas. Nesse sentido, a presente Política apresenta diretrizes gerais de conduta, bem como obrigações a serem seguidas na Aptum a fim de mitigar eventuais riscos e danos relacionados a ameaças externas ou internas, deliberadas ou acidentais, que possam impactar na confidencialidade, integridade e disponibilidade das informações de qualquer natureza.

O ciclo de vida dos dados é o processo que descreve o caminho dos dados da organização, desde o momento em que o dado é coletado por consentimento ou outra base legal até o arquivamento ou eliminação deles.

2. DA ALTA DIREÇÃO

A efetividade da Política de Segurança da Informação, depende fundamentalmente do comprometimento da Alta Direção, dessa forma a Alta Direção da Aptum Tecnologia demonstra através deste documento, esse comprometimento com a sua PSI, para que todos os seus colaboradores se sintam motivados a cumpri-la, uma vez que a Segurança da Informação se faz com a participação de todos.

A Alta Direção da Aptum Tecnologia, registra e espera que através desta PSI, que todas as recomendações aqui citadas, sejam consideradas aprovadas por essa Alta Direção e que com a sua divulgação, elas sejam entendidas e seguidas por seus colaboradores, colaborando assim para a proteção dos dados da empresa.

3. NORMAS E REFERÊNCIAS

A Política de Segurança da Informação (PSI) da Aptum Tecnologia, está fundamentada nos objetivos de controle elencados na Norma ABNT NBR ISO/IEC 27002, assim como as publicações NIST (National Institute of Standards and Technology – Instituto Nacional de Padrões e Tecnologia), agência regulatória que estabeleceu o Cybersecurity Framework (Estrutura de Segurança Cibernética), reconhecida mundialmente na área de Segurança da Informação, além de seguir as recomendações da Lei 13.709/2018 (LGPD - Lei Geral de Proteção de Dados).

São considerados como principais atributos da Segurança da Informação:

A Confidencialidade:

A informação só deve ser disponibilizada para quem estiver devidamente autorizado para acessá-la, ou seja, não é permitido a disponibilização ou exposição da informação para indivíduos, entidades ou processos não autorizados expressamente, seja por contratos ou outros instrumentos formais.

A Integridade da Informação:

Toda informação deve ser mantido exatamente no seu formato e conteúdo original, tal como foram criadas ou recebidas, utilizando tecnologias, controle e processos que

garantam esse requisito, pelo próprio criador dos produtos e sistemas da Aptum Tecnologia.

A Disponibilidade da Informação:

Os Sistemas e Informações pertencentes ao ecosistema tecnológico da Aptum Tecnologia, deverão estar disponíveis para os seus clientes, associados e colaboradores, atendendo também a confidencialidade das informações e a integridade das informações, formando assim, uma tríade de segurança de qualidade a ser cumprida (Confidencialidade, Integridade e Disponibilidade).

Da Privacidade e Proteção dos Dados Pessoais

Os dados pessoais contidos nas informações, devem ser protegidos com a adoção de medidas técnicas e organiozacionais de Segurança da Informação, nos termos impostos pela Lei 13.709/2018, conhecida por Lei LGPD ou Lei Geral de Proteção de Dados, a qual é seguida e apresentada pela Aptum Tecnologia, em outro documento.

4. OBJETIVOS DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

A Política de Segurança da Informação (PSI) da Aptum Tecnologia, tem como objetivo, orientar, estabelecer normas, diretrizes corporativas e procedimentos para a proteção dos ativos de informação e prevenção de responsabilidade legal para todos os usuários, com foco na segurança das informações, afim de que se garanta:

- A Confiabilidade das Informações através da preservação da confidencialidade, integridade e disponibilidade dos dados da empresa;
- O compromisso da Aptum Tecnologia com a proteção das informações de sua propriedade e/ou sob a sua guarda;
- A participação e comprometimento de todos os colaboradores, nos processos e controles de Segurança da Informação, com o dever de cumpri-los;

5. POR QUE OS COLABORADORES DEVEM SE PREOCUPAR COM A SEGURANÇA DA INFORMAÇÃO?

Não adianta a Alta Direção e a Área da Tecnologia da Informação impor controles e medidas técnicas, se não existir a participação e a colaboração dos gestores de

colaboradores da Aptum Tecnologia em cumpri-los. Ou seja, por exemplo, de nada vale a implantação de barreiras e portas de controle de acesso eletrônico, se um colaborador que tem acesso legítimo a determinada área restrita, resolver divulgar informações confidenciais que estavam devidamente protegidas.

A Área da Tecnologia da Informação (TIC) da Aptum Tecnologia, é a área responsável pela guarda dos dados da Aptum Tecnologia, mas o processo de Segurança da Informação, deve ser observado por todos os gestores e colaboradores da empresa, independentemente do nível hierárquico, posto que, de posse de uma informação específica, qualquer pessoa pode, por descuido e/ou má intenção, se tornar um agente de divulgação de informação não autorizada. Assim, é importante e obrigatório que todos colaborem com a área de Tecnologia da Informação e cumpram as medidas de segurança da informação, para que elas sejam efetivas, garantindo assim o seu objetivo.

6. CLASSIFICAÇÃO DAS INFORMAÇÕES

A Informação é tida como um ativo e possui valor diferente, dependendo do seu conteúdo. Os controles de proteção desses ativos, podem aumentar de acordo com o seu valor. A classificação das informações pode definir assim, quais controles de proteção precisam ser implementados.

Podemos entender a classificação das informações, também como uma escala de proteção a ser aplicada na mesma.

Para a Aptum Tecnologia, existem quatro níveis de classificação da informação em ordem crescente de importância e sigilo, a seguir relacionadas:

6.1. Informação Pública:

São todas as informações que já são de conhecimento público e que já estão disponibilizadas para os clientes, colaboradores e público em geral, seja através da Internet, ou veiculadas em documentos publicados em jornais, revistas, folders, redes sociais, panfletos, avisos ou paletestas autorizadas.

6.1.1. Exemplos de Informações Públicas: site Web da Aptum Tecnologia, folder da Aptum Tecnologia, tais como: informações pertinentes ao patrimônio público, utilização de recursos públicos, licitações e contratos administrativos, catálogo de serviços, eventos, cursos e palestras realizadas etc.

6.2. Informação Interna:

São todas as informações que estão disponíveis aos colaboradores por meio de ferramentas privadas, com armazenamento inyerno, em computadores servidores Aptum Tecnologia ou terceiros autorizados (na nuvem, por exemplo). As informações internas estão disponíveis aos colaboradores da Aptum Tecnologia, para a execução das suas tarefas rotineiras, não se destinando, portanto, ao uso do público externo.

A informação classificada como “Interna”, não poderá ser encaminhada, divulgada ou publicada em quaisquer meios, para terceiros não autorizados, devendo a sua disponibilização ser restrita ao ambiente de trabalho da Aptum Tecnologia e o seu uso limitado aos colaboradores ou terceiros (mediante assinatura do Termo de Confidencialidade ou de Não Divulgação (NDA), que realmente necessitem ter acesso a tais informações.

6.2.1. Exemplos de informações internas: e-mails e telefones, procedimentos e avisos internos, reuniões de alinhamento e feedbacks que acontecem entre líderes e equipe, trabalhos internos, etc.

6.3. Informação Restrita:

A informação classificada como “Restrita”, sómente poderá ser acessada pela área, departamento, divisão ou função dentro da Aptum Tecnologia que classificou a informação. Normalmente são informações de uma determinada área que não debvemser restritas a certa pessoas da empresa.

6.3.1. Exemplos de Informações Restritas: documento com dados pessoais e dados de saúde dos colaboradores que ficam no RH da empresa, salário dos colaboradores, estratégias de marketing, Livros e Registros Contábeis Empresariais, Operações Bancárias, Registro da Propriedade Intelectual, Projetos, Investigação de Responsabilidade de Servidor,

6.4. Informação Confidencial:

A informação classificada como “Confidencial”, deve ser mantida em arquivos físicos ou eletrônicos, com níveis de segurança compatíveis com a relevância da informação, tais como cofres, armáriose gavetas com chaves, diretórios criptografados e só podem ser enviados, sómente apos a inclusão de mecanismos de segurança (criptografia

ou senha).

A transmissão de arquivos confidenciais só deverá ser feita utilizando meios de transmissão seguros, para as partes préviamente autorizadas, com contrato de sigilo claro e dentro da validade, sejam as partes: funcionários, colaboradores, associados, fornecedores ou qualque tipo de parceiro de negócios que precisam: criar, armazenar ou processar qualquer tipo de informação CONFIDENCIAL.

6.4.1. Exemplos de Informações Confidenciais: registro de propriedade intelectual da Aptum Tecnologia, informações financeiras e tributárias da Aptum Tecnologia, informações financeiras sensíveis, por exemplo, números de contas bancárias, números de cartões de crédito, histórico de transações e outras informações relacionadas às finanças dos clientes ou da própria empresa, senhas de acesso a um sistema, senha de acesso ao e-mail, acordos e regulamentos direcionados aos funcionários, estratégias de mercado, técnicas de produção, dinâmicas de funcionamento, ideias inovadoras, contratos firmados pela da Aptum Tecnologia, etc.

O colaborador, o prestador de serviço e/ou consultor, deverão informar imediatamente a seu superior hieráquico dentro da Aptum Tecnologia, e por escrito (e-mail), sobre qualquer uso ou violação ou revelação indevida ou outra situação que caracterize o descumprimento dessa Política.

Excentuam-se da obrigação de manutenção de confidencialidade disposta nesta Política,o atendimento a quaisquer determinações decorrentes de Lei ou por ordem de autoridades judiciais.

As claúsulas de ciência, responsabilidade e confidencialidade quanto à política e diretrizes de Segurança da Informação, visam alertar e responsabilizar o colaborador, o prestador de serviço e/ou consultor, de que o acesso e o manuseio de informações devem se restringir ao exercício da respectiva função ou processo que requer essa informação, sendo proibido o seu uso para qualquer outro propósito distinto do designado.

7. DOS DEVERES E RESPONSABILIDADES

7.1. COLABORADORES

Será de inteira responsabilidade dos funcionários e demais colaboradores da Aptum Tecnologia:

- Cumprir fielmente a Política, as Normas, os Procedimentos de Segurança da Informação da Aptum Tecnologia;
- Proteger as informações contra acesso indevido, divulgação indevida, modificação ou destruição não autorizada pela Aptum Tecnologia;
- Garantir que os equipamentos e recursos tecnológicos à sua disposição, sejam utilizados apenas para as finalidades aprovadas pela Aptum Tecnologia;
- Fazer o descarte adequado de documentos e mídias de acordo com o seu grau de classificaão.

7.2. GESTORES DE PESSOAS E/OU PROCESSOS

Em relação à Segurança da Informação e suas atualizações, cabe aos gestores de pessoas e/ou processos:

- Aprovar a Política de Segurança da Informação e suas atualizações;
- Ter postura exemplar em relação à Segurança da Informação, servindo como modelo de conduta, para os colaboradores sob a sua gestão;
- Dar ciência, na fase de contratação e formalização de contratos individuais de trabalho, à responsabilidade do cumprimento da PSI da Aptum Tecnologia;
- Cumprir e fazer cumprir esta Política e os Procedimentos de Segurança da Informação da PSI da Aptum Tecnologia;
- Exigir de parceiros, prestadores de serviços e outras entidades externas a assinatura do Termo de Confidencialidade referente às informações às quais terão acesso;
- Elaborar com o apoio do Divisão de Gestão de Processos e Tecnologia da Informação, os Procedimentos de Segurança da Informação relacionados às suas áreas, fornecendo as informações necessárias e mantendo-as atualizadas;
- Informar sempre que necessário, as atualizações referentes a processo e/ou cadastro de funcionários para que as pemissões possam ser concedidas ou revogadas de acordo com a necessidade;
- Tomar as decisões administrativas referentes aos descumprimentos da PSI da Aptum Tecnologia;

7.3. DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

Cabe ao Divisão de Tecnologoa de Informação (TIC):

- Definir as regras para instalação de software e de hardware da PSI da Aptum Tecnologia;
- Monitorar os acessos às informações e aos ativos de tecnologia (sistemas, banco de dados, recursos de rede, mídias removíveis), tendo como referência a Política e as

Normas de Segurança da Informação;

- Manter registro e controle atualizados de todas as liberações de acesso concedidas, providenciando sempre que demandado formalmente, a pronta suspensão ou alteração de tias liberações;
- Propor as metodologias e processos referentes à Segurança da Informação, como classificação da Informação, avaliação de risco, análise de vulnerabilidades, etc;
- Analisar criticamente, Incidentes de Segurança;
- Manter uma comunicação efetiva sobre possíveis ameaças e novas medidas de segurança;
- Buscar alinhamento com as diretrizes da PSI da Aptum Tecnologia;

8. UTILIZAÇÃO DA REDE E DA INTERNET DA APTUM TECNOLOGIA

O ingresso na rede interna da Aptum Tecnologia, deve ser devidamente controlado para que os riscos de acessos não autorizados e/ou indisponibildades das informações sejam minimizados.

Dessa forma, é necessário instaurar algumas regras, listadas a seguir:

- A Aptum Tecnologia poderá permitir acesso à Internet e a navegação em sites de conteúdo, sempre de acordo com a sua Política de Segurança da Informação, ou seja, em função do tipo de atividade que o colaborador e o prestador de serviço, necessite utilizar para desempenhar suas funções, entretanto, cabe ressaltar que haverá a possibilidade de bloqueios de sites classificados como inseguros ou não confiáveis.
- É explicidamente proibido a transferência de arquivos por envio de quaiquer protocolos, aplicativos ou ferramentas que não forem prévia e expressamente aprovados pela área de Segurança da Informação da Aptum Tecnologia.
- A Aptum Tecnologia, reserva-se o direito de monitorar e registar o acesso à rede e à Internet como forma de inibir a proliferação de programas maliciosos, garantindo a integridade da rede, sistemas e dados internos.
- Os equipamentos, tecnologias e serviços fornecidos para o acesso à Internet e que sejam de propriedade da Aptum Tecnologia, poderão ser analisados e, se necessário, sserem bloqueados qualquer arquivo, correio eletrônico, ou aplicação, visando assegurar o cumprimento de sua Política de Segurança da Informação;
  A Internet disponibilizada pela Aptum Tecnologia aos seus colaboradores,

independentemente de sua relação contratual, pode ser utilizada para fins pessoais para resolução de problemas pessoais, desde que seja autorizado por escrito e não prejudique o andamento dos trabalhos nos divisãoes/unidades internas;

- A Internet disponibilizada pela Aptum Tecnologia aos seus colaboradores, independentemente de sua relação contratual, não pode ser utilizada para jogos, entreterimentos (sites de musicas, de filmes, de esportes, de azer);
- Para os colaboradores em home office, ou em viagem a serviço da empresa, o acesso a Intranet da Aptum Tecnologia, deverá ser feito exclusivamente através de equipamento corporativo da mesma, e via VPN, garantindo assim a segurança à rede interna da Aptum Tecnologia.
- Salvo se realizada pelo divisão de Tecnologia da Informação, não será permitida a alteração das configurações de rede e de inicialização das máquinas, bem como modificações que possam trazer algum problema.
- O Departamento de Recursos Humanos da Aptum Tecnologia é reponsável por comunicar formalmente, ao divisão de Tecnologia da Informação da Aptum Tecnologia, sobre desligamentos de colaboradores para o devido cancelamento do login e senha, de e-mail corporativo, bem como o descadrastamento de outros eventuais acessos existentes;
- É proibida a divulgação e/ou o compartilhamento indevido de informações internas, confidenciais e restritas, em listas de discussões, sites, redes sociais, fóruns, comunicadores instantâneos ou qualquer outra tecnologia correlata que use a Internet como via, de forma deliberada ou inadvertidamente, sob a possibilidade daquele que o fizer, sofrer penalidades previstas nos procedimentos internos e/ou ma forma da Lei.
- Os colaboradores com acesso à Internet, só poderão fazer o download de programas homologados e licenciados pela TIC da Aptum Tecnologia, e com origem confiável;
- Os colaboradores com acesso à Internet, devem comunicar a TIC da Aptum Tecnologia, e as eventuais ocorrências de avisos de virus ou agentes maliciosos em sua máquinas;
- O uso, a cópia ou a distribuição não autorizado de softwares que tenham direitos autorais. Marca registrada ou patente, são expressamente proibidos. Qualquer software não autorizado será exclído pelo divisão competente;
- Os colaboradores não poderão, em hipótese alguma, utilizar os recursos da Aptum Tecnologia, para fazer download ou distribuição de software ou dados pirateados, atividade consideradas delituosa de acordo com a legislação nacional;
- O uso do e-mail corportativo da Aptum Tecnologia, é de uso exclusivo para atividades relacionadas a serviços oficiais do colaboradores e/ou consultores da mesma;
- Os colaboradores e consutores da Aptum Tecnologia, com acesso à Internet, devem se atentar aos acessos e ações relacionadas aos crimes e às tipificações

de formas de crimes cibernéticos comuns, a seguir relacionadas, que são extremamente proibidas pelo Código Penal Brasileiro (CP):

Crime	**Tipificação**
Crime Estelionato e furto eletrônicos (fraudes bancárias).	Arts. 155, §§ 3º e 4º, II, e 171 do CP - Código Penal.
Invasão de dispositivo informático e furto de dados.	Arts. 154- A do CP - Código Penal.
Falsificação e supressão de dados.	Arts. 155, 297, 298, 299, 313-A, 313-B do CP - Código Penal.
Armazenamento; produção; troca; publicação de vídeos e imagens contendo pornografia infantojuvenil.	Arts. 241 e 241-A, do ECA (Lei nº 8.069/1990).
Assédio e aliciamento de crianças.	Art. 241-D, do ECA (Lei nº 8.069/1990) Arts. 147 do CP - Código Penal.
Ameaça.	Art. 147 do CP - Código Penal.
Cyberbullying (veiculação de ofensas em blogs e comunidades virtuais)	Arts. 138, 139, 140 do CP - Código Penal.
Interrupção de serviço.	Art. 266, parágrafo 1º, do CP - Código Penal.
Incitação e apologia de crime.	Arts. 286 e 287 do CP - Código Penal.
Prática ou incitação de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.	Art. 20 da Lei nº 7.716/1989.
Crimes contra a propriedade intelectual artística e de programa de computador.	Art. 184 do CP - Código Penal e Lei nº 9.609/1998.
Venda ilegal de medicamentos.	Art. 273 CP - Código Penal.

- Esses tipos de materias não poderão ser acessados, expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de quaququer recurso da Aptum Tecnologia, ou seja documentos digitais de condutas considerada ilícitas, como as aparentadas na tabela anteriormente mostrada, são expressamente proibidos.
- Os colaboradores não poderão usar os recursos da Aptum Tecnologia, para deliberada ou inadvertidamente propagar, qualquer tipo de virus, worms, cavalos de tróia, spam, ou programas de acesso e controle remoto de outros computadores;
- Apenas os colaboradores de TIC da Aptum Tecnologia, poderão usar os recursos da Aptum Tecnologia, para acesso e controle remoto de outros computadores ou equipamentos de rede e de segurança da informação, desde que seja para atividades de suporte técnico remoto, autorizado;

- Não são permitidos os acessos a softwares peer-to-peer, tais como: Kazaa, Bit Torrente, e afins;
- Não são permitidos os acessos a sites de compartilhamento de arquivos, tais como> mega,uploaded, bitshare, depositfiles, etc;
- Não são permitidas tentativas de burlar os controles de acesso e de visualização de conteúdo de computadores/rede da Aptum Tecnologia, usando sniffers ou proxies anônimos e estratégias de bypass de Firewall;
- Não são permitidos o uso de dispositivos de reconhecimento de vulnerabilidades, análise de tráfego, ou qualquer outro que possa causar sobrecarga ou rejudicar o bom funcionamento e a segurança da rede interna, salvo os casos em que o objetivo for realizar Auditorias de Segurança, e quando a área/divisão competente deverá estar devidamente ciente e ter autorizado tal tipo de procedimento.
- Os arquivos inerentes à Aptum Tecnologia, deverão ser armazenados em pasta compartilhada de cara área/divisão, localizada no computador servidor de arquivos, para a garantia de backup destes documentos. É terminantemente proibido armazenar estes tipos de arquivos em equipamentos e mídias removíveis pessoais;
- A Aptum Tecnologia, poderá quando desejar, realizar a geração de relatórios de sites e de downloads acessados e realizados pelo seu colaboradores e consultores;

9. POLÍTICAS DE SENHAS

A senha é a forma mais convencional de identificação e acesso do usuário, sendo um recurso pessoal e intransferível que protege a identidade do colaborador, evitando que uma pessoa se faça passar por outra.

O uso de dispositivos e/ou senhas de identificação por outra pessoa, que não seja a titular, constitui crime tipificado no Código Penal Brasileiro (Art. 307 - Falsa Identidade). Assim com o objetivo de orienta a criação de senhas seguras, estabelecem- se as seguintes regras:

- A senha é de total responsabilidade do colaborador, sendo expressamente proibida a sua divulgação, ou emprétimo, devendo a mesma ser imediatamente alterada após o primeiro login e no caso de suspeita de sua divulgação ou descoberta po terceiros;
- A senha inicial, só será fornecida ao próprio colaborador, pessoalmente ou via comunicação segura. É terminantemente proibido o fornecimento de senha via telefone, comunicador instantâneo, ou outra forma que não assegure a identidade do colaborador;

- É proibido o compartilhamento de login para funções de administração de sistemas da Aptum Tecnologia;
- As senhas de uso pessoal, não devem ser anotadas ou deixadas próximas ao teclado, mousepad, computar ou monitor de vídeo (debaixo do teclado, colada no monitor de vídeo, etc);
- As senhas deverão seguir os seguintes pre-requisitos:
  - Tamanho mínimo: 8 caracteres;
  - Existência de caracteres com: pelo menos três dos seguintes gurpos: letras maiúsculas, letras minúsculas, números e carateres especiais;
  - Não se deve utilizar senhas baseadas em informações pessoais e de fácil dedução, tais como: data do aniversário, nome do conjuge, número da placa do carro, etc);

- O acesso do usuário deverá ser imediatamente cancelado nas seguintes situações:
  - Desligamento do colaborador e/ou consultor, do quadro da Aptum Tecnologia;
  - Mudança de função do colaborador e/ou consultor;
  - Quando e por qualquer razão, cessar a necessidade de acesso do usuário ao sistema ou informação;

Para os cancelamentos acima mencionados, o divisão de Recursos Humanos (RH) da Aptum Tecnologia, ficará responsável por informar prontamente ao divisão de Tecnologia da Informação, acerca dos desligamentos e mudanças de função dos colaboradores.

10. CORREIO ELETRÔNICO (E-MAIL)

O correio eletrônico (e-mail) é uma das principais formas de comunicação. No entanto, é também, uma das principais vias de disseminação de malwares (“softwares maliciosos” - projetados para se infiltrarem no dispositivo do usuário, sem seu conhecimento, causando dano ou falhas no sistema, ou roubando dados). Assim, surge a necessidade de normalização da utilização dete recurso:

- O e-mail corporativo da Aptum Tecnologia é destinado a fins profissionais, relacionados às atividades dos colaboradores;
- Os e-mails enviados ou recebidos de endereços externos poderão ser monitorados pela Aptum Tecnologia, com o intuito de bloquear spams, malwares ou outros conteúdos maliciosos que violem a Política de

Segurança da Informação (PSI) da Aptum Tecnologia;

- É proibido enviar, com endereço eletrônico corporativo, mensagens com anúncios particulares, propagandas, vídeos, fotografias, músicas, mensagens do tipo “corrente”, campanhas e promoções;
- É proibido abrir arquivos com origens desconhecidadas anexados às suas mensagens eletrônicas;
- É proibido enviar qualquer mensagem por meios eletrônicos, que torne a Aptum Tecnologia vulnerável a ações civis ou criminais;
- É proibido falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetente e/ou destinatários;
- É proibido produzir, transmitir ou divulgar mensagem que:
  - Contenha ameaças eletrônicas como: spam. Phishing, mail bombing, mawares;
  - Contenha arquivos com código executável (.exe, .cmd, . pif, .hta, . src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
  - Vise obter acesso não autorizado a outro computador ou servidor da rede;
  - Vise interromper um serviço, servidores ou rede de computatores por meio de qualquer método ilícito ou não autorizado;
  - Vise burlar qualquer sistema de segurança;
  - Vise vigiar secretamente ou assediar outro usuário;
  - Vise acessar informações confidenciais sem a explícita autorização do proprietário;
  - Tenha conteúdo considerado impróprio, obsceno ou ilegal;
  - Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pronográfico entre outros;
  - Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos;
- O uso de e-mails pessoais é aceitável, se usado com moderação, em caso de necessidade e quando:
  - Não contrariar as normas aqui estabelecidas;
  - Não interferir, negativamente nas atividades profissionais individuais ou na de outros colaboradores;
  - Não interferir, negativamente, na imagem da Aptum Tecnologia.

11. DO USO DAS ESTAÇÕES DE TRABALHO

As estações de trabalho devem permanecer operáveis durante o maior tempo

possível para que os colaboradores, não tenham suas atividades prejudicadas. Assim, algumas medidas de segurança devem ser tomadas:

- É de responsabilidade do colaborador zelar por seu equipamento, mantendo-o em boas condições;
- Ao se afastar do seu posto de trabalho, o colaborador deve bloquear o acesso à sua estação de trazbalho;
- Não é permitido personalizar o equipamento com adesivos, fotos, riscos, bem como raspar ou retirar a etiqueta de patrimônio;
- É vedada a abertura de computadores para qualquer tipo de reparo pelos colaboradores. Caso seja necessário, o reparo deverá ser feito pela equipe competente (Divisão de TI);
- As estações de trabalho só estarão acessíveis aos colaboradores através de contas de usuário limitadas (login e senha pessoal);
- É proibida a instalação de softwares ou sistemas de trabalho pelos usuários finais. Este procedimento só poderá ser realizado pela equipe competente (Divisão de TI);
- É proibida também a instalação de softwares que não possuam licença e/ou não sejam homologados pela equipe competente (Divisão de TI);
- As estações de trabalho, devem permanecer bloqueadas (logoff), nos períodos em que o colaborador se ausentar do seu posto de trabalho;
- Os documentos e arquivos relativos à atividade desempenhada pelo colaborador, deverão ser armazenadas em local poróprio, no computador servidor da rede, o qual possui rotinas de backup e controle de acesso adequado;
- Os documentos, inclusive críticos e/ou confidenciais, só podem ser armazenados no computador servidor da rede, nunca em disco local da estação de trabalho do colaborador;
- É proibido o uso das estações de trabalho para:
  - Tentar ou obter acesso não autorizado a outro computador, servidor ou rede da Aptum Tecnologia;
  - Burlar quaisquer sistemas de segurança da Aptum Tecnologia;
  - Interromper um serviço, servidores ou rede de computadores da Aptum Tecnologia, por meio de qualquer método ilícitp ou não autorizado;
  - Cometer ou ser cumplice de atois de violação, assédio sexual, pertubação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular da Aptum Tecnologia;
  - Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país , a moral, os bons costumes e a ordem pública;

- O técnico de informática não se responsabiliza por prestar manutenção ou instalar softwares que não sejam da Aptum Tecnologia;
- As estações de trabalho possuem códigos internos, os quais permitem que sejam identificadas na rede, tudo que for executado na estação de trabalho, é de responsabilidade do colaborador;

12. DO USO DE EQUIPAMENTOS PARTICULARES E DISPOSITIVOS MÓVEIS

O objetivo da Aptum Tecnologia é maximizar a agilidade e a eficiência da realização das tarefas dos colaboradores, contando com todos os recursos dos equipamentos disponíveis, mas não se pode deixar de considerar os requisitos de Segurança da Informação.

São exemplos de equipamentos móveis particulares/privados: notebooks, smartphones, pendrives, discos rígidos removíveis, ou quaisquer outros dispositivos portáteis que permitam armazenar e/ou processar dados.

Quando autorizado o uso de equipamentos móveis particulares/privados, o dispositivo pessoal deve ficar restrito à rede de convidados/guest da Aptum Tecnologia,

Não é permitido a conexão de dispositivos não corporativos às redes internas, cabeadas ou sem fio, da Aptum Tecnologia.

Não é permitida a utilização de pendrives, discos rígidos removíveis.

Os colaboradores que precisam fazer uso de dispositivos móveis, para o desempenho das suas funções e rtarefas especificas, o farão, utilizando equipamentos fornecidos pela Aptum Tecnologia, com os devidos controles e proteções técnicas aplicadas, e mediante autorização por escrito do seu supewrior hierárquico.

A não observância desta regra ensejará na aplicação das penalidades previstas nesta PSI, sem a exclusão de outras, porventura cabiveis.

13. DO USO DE MULTIFUNCIONAIS

O uso de multifuncionais (impressoras) na Aptum Tecnologia, deve seguir as seguintes regras:

- É proibida a impressão e cópia de documentos de uso pessoasl e/ou ilegal;
- A configuração e manutenção das impressoras só poderá ser realizada pela equipe técnica da Aptum Tecnologia, ou por prestador de serviços devidamente contratado e qualificado para este fim;
- As impressoras da Aptum Tecnologia, devem estar ligadas na energia, e serão proibidas de sofrerem intervenções por parte de qualquer colaborador da Aptum Tecnologia, que não seja do Divisão de TI, ou ou por prestador de serviços devidamente contratado e qualificado para este fim;
- As impressoras que forem por ventura locadas, deverão indicar a possibilidade de reimpressão e , em sendo o caso, para substituição da máquina, por qualquer motivo, deverá ser feita a exclusão do histórico/arquivo com a aparesentação do respectivo comprovante dete ato, pela empresa locadora.

14. O BACKUP

Um dos procedimentos mais básicos da Segurança da Informação é a implantação de uma Política de Backup (cópia de segurança). Uma organização tem que estar preparada para recuperar (restaurar) todos os seus dados de forma íntegra, caso um incidente de perda de dados venha a ocorrer.

Assim, estabelecem-se as seguintes regras:

- Todo sistema ou informação relevante para a operação da Aptum Tecnologia, deve possuir cópia dos seus dados de produção, para que em caso de eventual acidente de indisponibilidade de dados, seja possível recuperar ou minimizar os impáctos nas operações da empresa;
- Os gestores da Aptum Tecnologia por classificar os dados de acordo com a sua relevância, esperam que o Setro de TI, realize os devidos backups necessários, observando o tempo de retenção destas cópias;
- Todos os backups devem ser automatizados por sistemas de agendamento para que sejam, preferencialmente, executados fora do horário comercial, durante os períodos de pouco ou nenhum acesso de usuários ou processos aos sistemas de informática;

- As mídias de backup, devem ser acondicionadas em local seco, seguro (de preferência em cofres corta-fogo, em confirmidade com a Norma ABNT), e preferencialmente, distantes o máximo possível do ambiente do Rack do Data Center;
- Toda infraestrutura de suporte aos processos de backup e restauração, deve possuir controle de segurança, para a prevenção contra acessos não autorizados, bem como mecanismos que assegurem o seu correto funcionamento;
- O setro ou restador de serviço, responsável pela área de TI da Aptum Tecnologia, deve preparar semestralmente um plano de execução de testes de restauração de dados, com escopo definido emconjunto com as demaisáreas/divisãoes da Aptum Tecnologia. Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente dio original, para que assim não sobreponha os arquivos válidos;
- Na situação de eventual ocorrência de erro de backup e/ou restore é necessário que ele seja feito no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema. Caso seja extremamente negativo o impácto da lentidão dos sistemas derivados desse backup, eles deverão ser executados apenas mediante justificativa dessa necessidade;

15. DA POLÍTICA DA MESA LIMPA

Todos os colaboradores da Aptum Tecnologia, deverão obedecer as regras de limpeza e organização do ambiente de trabalho a fim de não expor desnecessáriamente, as informações classificadas da Aptum Tecnologia.

Os documentos impressos e anotações que precisam estar em um papel (impresso ou de anotações), devem permanecer nas mesas em caráter temporário, devendo ser guardados em compartimentos fechados (gavetas, armários) que possuam fechadura/chave, ou descartados de forma rasgada e/ou picotada.

Toda informação que permanecer nas mesas poderá e deverá ser destruída pelo colaborador responsável, ou por qualquer outro colaborador que assim o quiser fazê-lo, exercitando assim as boas práticas de proteção de informações da Aptum Tecnologia.

16. DA SEGURANÇA DO AMBIENTE DE TI

Estrutura física do Rack do Data Center

As máquinas (computadores servidores) que armazenam os sistemas da Aptum Tecnologia, deverão estar em área considerada protegida, no caso do ambiente do Rack do Data Center estar localizado dentro da empresa.Todos os sistemas ou equipamentos considerados como críticos, devem ser mantidos em áreas seguras do Rack do Data Center.

A entrada no ambiente do Rack do Data Center, dever ser protegida com soluções de segurança de controle de acesso físico, tais como câmera de CFTV IP, controle de acesso biométrico. A área do Rack do Data Center deve permanecer fechada, com mecanismo de autenticação individual (biometria digital).

A porta de acesso ao ambiente do Rack do Data Center deve permanecer fechada, com mecanismo de autenticação individual (biometria digital). O acesso às dependências do ambiente do Rack do Data Center, com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só pode ser feito a partir da autirização da equipe de Segurança e mediante supervisão.

O acesso às dependências do ambiente do Rack do Data Center sem as devidas identificações só poderá ocorrer, em situações de emergência, quando a segurança física do referido ambiente for comprometida, como por exemplo, no caso de ecorrêcia de sinistro, tal como: incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação não estiver funcionando.

Caso haja a necessidade do acesso não emergencial, o requisitante deve solicitar autorização com antecedência á área responsável pelo ambiente do Rack do Data Center. O referido ambiente, deve ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente, somente poderá ser realizado com a colaboração dos funcionários designados para a limpeza.

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável. A instalação ou desinstalaçao de quaiquer equipamentos no ambiente do Rack do Data Center, somente se dará, através da emissão de Ordem de Serviço, devidamente autorizada pelo gestor responsável.

17. DA ESTRUTURA ORGANIZACIONAL DA ÁREA DE SEGURANÇA DA INFORMAÇÃO

O gestor de Segurança da Informação terá como competências:

- Coordenar, executar e acompanhar as atividades de tratamento e respostas a incidentes de segurança na rede corporativa da Rack do Data Center da Aptum Tecnologia;
- Coordenar, executar e acompanhar a análise dos sistemas comprometido, buscando levantar as causas, danos e responsáveis;
- Coordenar, executar e acompanhar a avaliação, auditoria e testes das condições de segurança da rede corporativa da Aptum Tecnologia;
- Coordenar, executar e acompanhar a análise dos ativos de informação e estruturas constitutivas dos ambientes de tecnologia da informação, presentes na Aptum Tecnologia;
- Desenvolver a aplicar um Plano de Conscientização em Segurança da Informação e Comunicaões, a fim de que todos os colaboradores da Aptum Tecnologia;, tenham ciência do assunto;
- Manter em condições adequadas de segurança o acervo de informações relativas aos incidentes de segurança na rede corporativa da Aptum Tecnologia;
- Participar da definição e acompanhar os indicadores de incidentes de segurança na rede corporativa da Aptum Tecnologia;
- Prestar assessoria técnica na elaboração de Políticas, Normas, Procedimentos, Pareceres, e na especificação técnica de produtos e equipamentos direcionados Segurança da Informação e Comunicações;
- Participar da proposição de recursos necessários às ações de Segurança da Informação e Comunicações;
- Executar outras atividades correlacionadas que lhe forem demandadas;

18. DA PROTEÇÃO CONTRA MALWARE

A detecção e remoção de malware nos equipamentos da Aptum Tecnologia, deve observar os seguintes pontos:

- Deverá ser realizado o monitoramento através do uso de antivírus e firewall, com gerenciamento em nuvem, conforme os casos aplicáveis, pela Área da TI.
- Deverão ser realizados a geração de relatórios das detecções ocorridas, com os respectivos status de bloqueio de ataques associados e de movimentação para quarentena.

19. DO TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

- **Serviços Reativos:**

  Tratamento de Incidentes de Segurança em Redes de Computadores;

  Tratamento de artefatos maliciosos;

  Tratamento de vulnerabilidades;

- **Serviços Proativos:**

  Detecção de Intrusão: Todo e qualquer servidor deve estar ciente que o tratamento de incidentes, vida minimizar os impáctos de um incidente nos processos em curso na Aptum Tecnologia, sendo assim voltado à redução e contenção dos efeitos técnicos indesejáveis e seu monitoramento.

  Quaisquer falhas, anomalias, ameaças ou vulnerabilidades observadas, devem ser notificadas o mais rápido possível, para o gestor da Segurança da Informação.

  Deve-se obter informações quantitativas acerca dos incidentes ocorridos que descrevam: sua natureza, as causas, as datas de ocorrência, a sua frequência e os custos resultantes. Tais informações serverm com indicadores da eficácia das políticas e da relação custo-benefício dos controles de segurança.

  Após o levantamento dos dados, o incidente deverá ser tratado e documentado, visando manter um histórico dos incidentes e ainda uma cultura acerca deles.

  O monitoramento e a detecção dos ataques DDoS, serão realizados via Firewall e o outro necanisnos aplicáveis. O sistema deve estar preparado para mitigar esses tipos de ataque. Esse sitema também monitorará arquivos, contra ataques de códigod maliciosos.

  Quando um ataque é detectado, o administrador deverá ser notificado e irá avaliar se foi de fato um ataque ou um falso positivo. No caso de ataques DDoS, o sistema de defesa deverá bloquear os principais endereços de origem associados.

Caso sejam detectados códigos maliciosos, eles deverão ser imediatamente interrompidos a as suas origens isoladas, até a avaliação do adminstrador.

20. DA SEGURANÇA FÍSICA DO AMBIENTE

É necessário estabelecer o perímetro de segurança física de modo a preservar o acesso somente a pessoas autorizadas, sendo obrigatório o uso de identificação visual (crachá), para colaboradores, visitantes, clientes, fornecedores e prestadores de serviços.

Para controle da segurança física o acesso dos colaboradores na Aptum Tecnologia, deve ser feito por meio de sistema de controle de acesso biométrico, ressaltando que haverá controle e monitoramento por filmagem ambiental em vários divisãoes/salas da empresa. Os referidos arquivos de controle de acesso físico, deverão ser mantidos pelo prazo ínimo de 30 (trinta) dias (salvo exceção justificada), e o descarte feito com segurança.

21. DA VIOLAÇÃO DA POLÍTICA E SUAS PENALIDADES

As violações de segurança devem ser informadas à área de Tecnologia e Segurança da Informação (TIC), por escrito, via e-mail. Toda violação ou desvio devem ser investigados por esse divisão, podendo contar com auxílio de outros que se mostrem necessários, para a determinação das medidas cabíveis, visando a correção da falha ou reestruturação de processos.

Exemplos que podem ocasionar sanções, dentre outras que tenham sido mencionadas nesta PSI:

- Uso ilegal de software;
- Introdução (intencional ou não) de vírus de informática;
- Tentativas de acesso não autorizadas a dados e sistemas;
- Compartilhamento de informações sensíveis do negócio;
- Divulgação de informações de clientes e operações;

Os princípios da segurança estabelecidos na presente política, possuem total aderência da alta administração da Aptum Tecnologia e devem ser observados por todos

na execução de suas funções.

A não conformidade com as diretrizes desta política e a violação das normas derivadas da mesma, sujeia os colabotadores da Aptum Tecnologia, às penas de responsabilidade civil e criminal na extensão que a Lei permitir e a recisão de contratos.

Em caso de dúvidas quanto aos princípios e responsabilidades descritas nesta PSI, o colaborador deve entrar em contato com o Gestor responsável pela Segurança de Informação (TIC).

No caso de não cumprimento das normas estabelecidas nesta PSI, o colaborador poderá sofrer as seguintes Penalidades:

Advertência verbal: O colaborador será comunicado verbalmente que está infringindo as normas da PSI da Aptum Tecnologia e será recomendado a releitura da mesma.

Advertência formal: A primeira notificação será enviada ao colaborador, informando o descumprimento da norma, com a indicação precisa da violação cometida. A segunda notificação será encaminhada para a chefia imediata do infrator.

Suspensão: Pelo período de 30 dias, visa a punição do colaborador (a) que violou as regras da empresa ou que não cumpriu com os seus deveres previstos npo contrato de trabalho. A penalidade poderá ser aplicada também, em caso de ato faltoso cometido durante o período em que cumpre o aviso prévio.

Demissão por justa causa: Possibilidade que a empresa tem de dispensar um colaborador (a) por justa causa, caso ele tenha cometido algum ato considerado grave ou reiterado, de acordo com o artigo 482 da clt.

22. CONSIDERAÇÕES FINAIS

As dúvidas decorrentes dos fatos descritos neta PSI, deverão ser encaminhadas aos Gestores da Aptum Tecnologia, para avaliação e decisão, sempre com suporte técnico do responsável pela Segurança da Informação.

Esta PSI, entra em vigor a partir da data de sua publicação, e pode ser alterada a qualquer tempo, por decisão da Alta Direção da Aptum Tecnologia, com o apoio do Gestor de Segurança da Informação, Coordenador(a) de Compliance, e quando surgirem fatos e

situações relevantes e que não tenham sido contemplados neste documento.

Agradecemos o seu apoio!