d

Siglas e Definições

Informação - é o resultado do processamento, manipulação e organização de dados, de tal que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (pessoa, máquina) que a recebe.

Genericamente, o conceito de informação está intimamente ligado às noções de restrição, comunicação, controle, dados, forma, instrução, conhecimento, significado, estímulo, padrão, percepção e representação de conhecimento.

Segurança da Informação - está relacionada com proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade, não estando esta segurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento. O conceito se aplica a todos os aspectos de proteção de informações e dados.

Consistência - coerência na exposição de ideias.

Rastreabilidade - rastreamento é saber "o que" (o produto ou bem), "de onde" veio (a origem) e "para onde" foi (destino).

SGSI – Sistema de Gestão de Segurança da Informação.

DPO – Responsável pelo tratamento de Dados Pessoais.

Objetivos

Tendo como premissa o fato de que toda informação recebida ou produzida pelos colaboradores em razão das suas atividades profissionais é do Escritório, e que as exceções devem estar explícitas nos documentos contratuais a eles relacionados, essa Política de Segurança da Informação estabelece as diretrizes de padrão de conduta de todos os seus

colaboradores para garantir os princípios básicos de integridade, confidencialidade e disponibilidade de suas informações.

Abrangência

Todas as unidades do escritório.

Da Aplicação

Os itens estabelecidos na Política de Segurança da Informação são aplicáveis a todos os colaboradores, processos de negócio e sistemas de informação que manipulam direta ou indiretamente as informações de propriedade ou sob custódia do Escritório, independentemente do local e da forma como estejam armazenadas, contidas ou distribuídas no Escritório. Todos os colaboradores devem ter acesso a esta política, não sendo admitido o desconhecimento de seu conteúdo para justificar violações ou descumprimento das diretrizes estabelecidas.

A Política de Segurança, bem como, o Termo de Responsabilidade de Segurança da Informação são explanados em sua íntegra à todo colaborador, após sua contratação, por meio de uma integração. A aplicação destes termos é feita impreterivelmente pelo setor de Recursos Humanos e pelo SGSI.

Diretrizes Gerais

Quanto à Informação:

- A Organização tem políticas documentadas que contemplam a segurança e a proteção da confidencialidade da informação dos seus clientes e colaboradores e de todos os dados pessoais que possam causar riscos ou danos, inclusive morais aos mesmos;
- Toda e qualquer informação somente deve ser utilizada pelo colaborador para fins profissionais, não sendo permitida a divulgação de informações sigilosas e documentos. Casos de exceções deverão ser autorizados pelos gerentes ou proprietários da informação, e/ou ainda, sob determinação jurídica;

- Toda e qualquer informação deve ser protegida contra a modificação, destruição ou divulgação não autorizada, independente da forma em que a mesma esteja disponível (verbal, impressa ou digital);
- As informações devem ser armazenadas por tempo determinado pela organização e/ou legislação vigente, e recuperada somente quando for necessário e com autorização expressa do seu proprietário;
- No acesso à informação, somente devem ser usados recursos tecnológicos devidamente homologados e autorizados pela Organização;

Quanto aos Colaboradores:

- Todos os colaboradores devem seguir integralmente as definições estabelecidas pela Política de Segurança da Informação e cumprir com as regras do Termo de Responsabilidade da Informação do Escritório;
- É ainda dever dos colaboradores manterem-se atualizados quanto à Política de Segurança da Informação do escritório, orientando-se junto a sua liderança e/ou ao setor de Tecnologia da Informação quanto ao descarte, utilização, reaproveitamento, divulgação de informação que pertença àquela;
- Os colaboradores devem estar vinculados a instrumentos contratuais que estabeleçam os critérios de sigilo e confidencialidade eleitos pelo Escritório como necessários para a implementação de suas funções e, estão impedidos de divulgar, por qualquer meio, sem prévia e formal autorização do escritório, assuntos a ele relacionados;
- Todos os colaboradores do Escritório devem assinar o Termo de Responsabilidade da Informação sobre qualquer informação, senhas e/ou dispositivos eletrônicos de caráter pessoal ou profissional se comprometendo a não repassar qualquer informação relativa ao escritório para terceiros, tornando formal o seu conhecimento e aceite.
- É de responsabilidade do colaborador não utilizar qualquer serviço de informação do escritório para intimidar, assediar, difamar ou aborrecer qualquer pessoa.
- É de responsabilidade do colaborador não utilizar os recursos computacionais, redes sem fio e outros instrumentos de informação difamatórios que viole a privacidade de terceiros, ou que seja abusivo, ameaçador, discriminatório ou calunioso.

- Não mostrar, armazenar ou transmitir na Rede cabeada ou na Rede Wi-Fi informações que possam ser consideradas ofensivas ou abusivas.
- Não divulgar senhas, pois estas são de uso pessoal e intransferível.

Quanto ao Ambiente:

- O ambiente de armazenamento das informações deve ser apropriado e protegido contra sinistros e acessos não autorizados, garantindo a integridade, disponibilidade e confiabilidade das informações;
- Devem ser tomadas as medidas técnicas apropriadas para prevenir que ativos de sistemas de informação possam ser acessados ilegalmente, modificados sem autorização, falsificados, destruídos ou sofram interferências que afetem a confidencialidade, integridade e/ou disponibilidade das informações que eles suportam;
- A geração, uso, armazenamento, manutenção e descarte da informação devem ser feitas de acordo com as necessidades do Escritório e em conformidade com a legislação, cujos processos devem ser devidamente documentados e autorizados;
- Todo software adquirido pelo Escritório, que se utilize ou tenha acesso à informação sigilosa, deve obrigatoriamente possuir uma especificação escrita formal que tem de levar em conta a segurança dos sistemas, controle de acesso e contingência e que deve ser aprovada pelo responsável. O Escritório, por meio da seus Sócios, poderá a qualquer tempo, solicitar a auditoria de todos os sistemas de softwares utilizados, com o intuito de assegurar que o nível de segurança exigido pela sua Política de Segurança da Informação esteja sendo cumprido;
- Considerando que os equipamentos e instalações de propriedade do Escritório deverão ser utilizados única e exclusivamente como ferramenta de trabalho para o exercício das funções de cada colaborador e relacionada aos objetivos do Escritório, o Escritório reserva-se ao direito de, sempre que julgar necessário e observando os preceitos legais, monitorar, inspecionar ou auditar as informações que se encontram armazenadas em tais equipamentos e instalações ou que trafeguem pela rede do Escritório;
- Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que o Escritório julgar necessário para reduzir os riscos dos seus ativos de informação;

- Devem ser tomadas as medidas necessárias para investigar prontamente qualquer possível causa de problemas de segurança ou incidentes de segurança, bem como minimizar seus danos;
- Deverá ser realizada a manutenção da segurança física e do ambiente para que os dados e informações não sejam prejudicadas por eventos externos, mantendo instalações e infraestrutura seguras e adequadas para realização das atividades.
- O Escritório não irá se responsabilizar por atualização, manutenção e garantia de conectividade de dispositivos que não sejam de sua propriedade.
- O Escritório reserva para si o direito de monitorar, auditar e intervir nos acessos de dados de modo a salvaguardar os interesses corporativos de acordo com a Lei 12.965 (Marco Civil da Internet) e LGPD consonantes com os objetivos dessa Política.

Papéis e Responsabilidades

Todos os colaboradores:

Fazem parte das atribuições e responsabilidades de todos os colaboradores do Escritório cumprir as determinações a seguir:

- Comunicar ao SGSI qualquer fato ou indício de violação desta política e/ou seus procedimentos;
- Manter o sigilo das informações a que tenha acesso em virtude das suas atividades. As informações devem ser tratadas como sigilosas, inclusive dados cadastrais de clientes.
- ***Respeitar os requisitos legais aplicáveis às informações sob sua responsabilidade e a relação destes com controles internos;***
- Administrar de forma consciente/racional os recursos tecnológicos e mídias que contenham qualquer informação pertencente ao Escritório;
- Utilizar os recursos tecnológicos colocados à sua disposição apenas para fins profissionais e/ou para finalidades explicitamente aprovadas pelo Escritório;

- Proteger as informações de propriedade do Escritório contra acesso, modificação, destruição ou divulgação não autorizada, assim como para transmitir/divulgar qualquer material que viole os direitos de terceiros, incluindo direito de propriedade intelectual e informações de negócios.
- O colaborador não deve utilizar os recursos computacionais do Escritório, em seu benefício próprio, para fins educacionais, particulares, comerciais, políticos ou lazer.
- Não utilizar de falsa identidade ou utilizar dados de terceiros para obter acesso aos recursos computacionais e informações do Escritório.

Mesa limpa e Tela Limpa

- Os usuários têm obrigação de bloquear as estações de trabalho quando se afastarem das mesmas para impedir acesso não autorizado.
- Todas estações de trabalho são configuradas com bloqueio de tela automático, com tempo de 15 minutos, para evitar acesso não autorizado.
- Os documentos em papéis e mídias eletrônicas não devem permanecer sobre a mesa desnecessariamente, devem ser armazenados em armários ou gavetas trancadas, quando não estiverem em uso, especialmente fora do horário do expediente.
- Informações sensíveis ou críticas devem ser trancadas em local separado e seguro (um armário com chave ou cofre).
- Anotações, recados e lembretes não devem ser deixados à mostra sobre a mesa ou colados em paredes, divisórias, murais ou monitor do computador.
- Não anotar informações sensíveis em quadros brancos.
- Não guardar pastas com documentos sensíveis em locais de fácil acesso.
- Destruir os documentos impressos antes de jogá-los fora. Sempre que possível utilizar máquinas desfragmentadoras.
- Devolver todos os documentos obtidos por empréstimos de outros departamentos, quando eles não forem mais necessários.
- Guardar agendas e cadernos de anotações, assim como objetos pessoais, em gavetas ou armários trancados.

- Nunca anotar as senhas em papeis ou ativos de informação. As mesmas devem ser memorizadas.
- Preferencialmente, mesas e móveis deverão ser posicionados de forma que dados sensíveis não sejam visíveis de janelas ou corredores.
- Ao final do expediente, ou em caso de ausência prolongada do local de trabalho, a mesa de trabalho deve permanecer limpa, documentos guardados, gavetas e armários trancados e computador desligado.

Proprietário da informação:

Em relação à segurança da informação, são responsabilidades do Proprietário da Informação:

- Assegurar que suas equipes possuam acesso e conhecimento desta Política e dos Procedimentos Gerenciais e Operacionais de Segurança da Informação;
- Validar os procedimentos gerenciais e operacionais que utilizam as informações de sua responsabilidade;
- Classificar as informações sob sua responsabilidade;
- Autorizar ou delegar a responsabilidade de conceder e retirar acessos, modificar, guardar, distribuir e descartar as informações sob sua responsabilidade;
- Efetuar o controle das atualizações/alterações de acessos concedidos, solicitando sempre que julgar necessário, processo de revisão dos acessos às informações sob sua tutela podendo solicitar a remoção dos acessos sempre que considerar necessário à manutenção da segurança das informações;
- Tomar parte na investigação dos incidentes relacionados à informação sob sua responsabilidade, que possam causar qualquer tipo de impacto as diretrizes de segurança da informação;

Área de Tecnologia da Informação:

São responsabilidades da área de Tecnologia da Informação os itens abaixo:

- Definir as políticas, procedimentos e estratégias referentes à Segurança da Informação;
- Revisar as políticas anualmente ou sempre que ocorrerem mudanças significativas;
- Redigir os Procedimentos de Segurança da Informação relacionados às suas áreas, mantendo-os atualizados;

- Acompanhar o andamento dos principais projetos e iniciativas relacionados à segurança da informação;
- Manter as estratégias de divulgação da Política e dos Procedimentos gerenciais e operacionais de Segurança da Informação para todos os colaboradores do Escritório;
- Prover orientação e treinamento sobre a Política de Segurança da Informação e seus Procedimentos a todos os colaboradores do Escritório;
- Elaborar periodicamente, campanhas de conscientização dos colaboradores em relação à relevância da segurança da informação para o Escritório, mediante campanhas, palestras, treinamentos e outros meios de endomarketing;
- ***Propor projetos e iniciativas relacionados com a melhoria contínua dos processos de segurança da informação do Escritório, mantendo-se atualizada em relação às melhores práticas existentes no mercado e visando o aumento de maturidade dos processos;***
- Estabelecer procedimentos e realizar a gestão dos sistemas de controle de acesso do Escritório, incluindo os processos de concessão, manutenção, revisão e suspensão de acessos aos colaboradores;
- Efetuar levantamentos de análise de vulnerabilidade, com o intuito de aferir o nível de segurança dos sistemas de informação e dos demais ambientes e/ou ativos que suportam as informações do Escritório;
- Realizar auditorias em sistemas e processos com o intuito de verificar o cumprimento da Política e dos Procedimentos de Segurança da Informação;
- Analisar os casos de violação desta Política e dos Procedimentos de Segurança da Informação.
- Propor e validar diretrizes para utilização de rede wireless disponibilizada pelo Escritório.

Área de Infraestrutura Tecnológica:

São responsabilidades da área de Infraestrutura Tecnológica os itens abaixo:

- Disponibilizar e administrar todos os recursos e serviços relacionados à tecnologia da informação do Escritório, garantindo a máxima disponibilidade do serviço e o menor tempo possível de recuperação, em caso de desastre.
- Homologar todo hardware e software de propriedade do Escritório usado em rede cabeada, wireless e demais meios de comunicação.

DPO

São responsabilidades do DPO os itens abaixo:

- Receber reclamações e comunicações dos titulares de dados pessoais, prestar esclarecimentos e adotar as providências necessárias
- Receber comunicações da autoridade nacional de proteção de dados e adotar as providências necessárias.
- Orientar os colaboradores, terceiros contratados e demais partes do escritório do Escritório WYLB a respeito das práticas a serem tomadas em relação a proteção de dados pessoais.
- Atender as demais atribuições, conforme orientação da Autoridade Nacional De Proteção de Dados, definidas em normas complementares publicadas pelo referido órgão.
- Atuar junto ao time de Segurança da Informação no ajuste das normas e procedimentos de segurança da informação, necessários para se fazer cumprir este procedimento.
- Identificar e avaliar as principais ameaças a proteção de dados, bem como propor e, quando aprovado, apoiar a implantação de medidas corretivas para reduzir o risco.
- Tomar ações cabíveis para se fazer cumprir os termos desta política.
- Apoiar a gestão das violações de dados pessoais, garantindo tratamento adequado e comunicando, em prazo razoável, a autoridade nacional e titulares afetados pela violação sempre que esta representar risco ou dano relevante aos titulares.

Gestão Jurídica:

Cabe à área Jurídica:

- Incluir, na análise e na elaboração de contratos, cláusulas específicas relacionadas à segurança da informação;
- Avaliar, quando solicitada, as Normas e os Procedimentos de Segurança da Informação elaborados pelas diversas áreas do Escritório;
- Imputar as medidas legais cabíveis em caso de não cumprimento de alguma das cláusulas desta política representadas pelo termo de responsabilidade e sigilo.

Gestão de Recursos Humanos:

Cabe à área de Recursos Humanos:

- Informar, prontamente, à área de Segurança da Informação, todos os desligamentos, afastamentos e modificações no quadro funcional da empresa com ao menos 20 minutos de antecedência de o colaborador envolvido ser alertado sobre a ocorrência, e ainda, em caso de exceções que não for possível respeitar o prazo, que seja ao mínimo, em tempo hábil para garantir a segurança das informações.

Gestão Administrativa:

Cabe às áreas Administrativas:

- Assegurar que as informações confidenciais e assuntos estratégicos da Escritório, aos quais os prestadores de serviços terceirizados contratados tenham acesso direto ou indireto, sejam tratados dentro do âmbito da atuação objeto do contrato, considerando as diretrizes descritas nesta Política com relação à confidencialidade e ao sigilo sobre o armazenamento, o uso, a disponibilização e a divulgação das informações.

Contas de Acessos a Sistemas

A concessão aos colaboradores de contas de acesso aos sistemas corporativos é feita de acordo com o estabelecido pelo setor de Tecnologia da Informação/Administrativo em conformidade com as necessidades de acesso em razão das atividades desenvolvidas pelo colaborador.

Revisão de Perfis

Cabe a cada gestor a atualização do nível dos perfis de acesso dos colaboradores vinculados à sua responsabilidade, a fim de manter o adequado nível de privilégio necessário às suas funções nos sistemas do Escritório.

Acesso a Sistemas Corporativos

Os acessos aos sistemas corporativos seguirão as premissas estabelecidas pelo setor de Tecnologia da Informação em conformidade com o solicitado pelo Supervisor Direto do colaborador.

Sistema de Comunicação Eletrônica

Os sistemas de comunicação eletrônica das unidades do Escritório tais como e-mail e serviço de mensagem instantânea, deverão ser usados apenas para atividades de negócios e devem estar de acordo com os padrões de conduta ética do Escritório e de boas práticas do mercado de trabalho.

Advertências

Conforme presente no documento, em nenhum momento será admitido, a qualquer colaborador, invocar o desconhecimento das normas aqui descritas para justificar violações ou descumprimento das diretrizes definidas.

Todo e qualquer caso de descumprimento ou inobservância destas normas serão passíveis de suspensão do acesso e sanções contratuais ou dispositivas constantes em Lei.

Considerações Finais

Todos os casos que não se enquadrarem nos descritos anteriormente deverão ser levados à área de segurança da informação que submeterá, se necessário, aos Sócios, que após análise, poderá ou não solicitar a revisão da Política de Segurança da Informação do Escritório.

A alegação de desconhecimento desta política não exime o infrator da responsabilidade sobre as infrações cometidas bem como as possíveis sanções a ele impostas.

Em caso de dúvidas, quanto ao teor deste documento ou para relatar qualquer incidente de risco de segurança da informação, o colaborador deverá utilizar o e-mail: dpo@wambier.com.br.

Documentos de Referência para Atendimento às Diretrizes

Norma ABNT ISO/IEC 27001 – Tecnologia da Informação – Técnicas de Segurança – Sistema de gestão de segurança da informação - Requisitos.

Norma ABNT ISO/IEC 27002 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação.

Norma ABNT NBR 15999-1:2007 - Gestão da continuidade de negócios – Parte 1: Código de prática.

Constituição Federal de 1988 – Ultima Emenda Constitucional em 06/06/2013.

Código Civil Brasileiro - (Lei 10.406 de 10 de janeiro de 2002) em vigor desde 11 de janeiro de 2003, sendo a última atualização pela LEI Nº 12.607, DE 4 DE ABRIL DE 2012.

Marco Civil da internet - (Lei N° 12965/2014)

LGPD – (Lei N° 13709/2018)