

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

PETRONECT

PARA QUE SERVE?

- **Estabelecer** diretrizes que permitam aos Colaboradores da Petronect seguir padrões, no tocante à Segurança da Informação, adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.
- **Nortear** a definição de procedimentos específicos de Segurança da Informação, bem como a implementação de controles e processos para atendimento da mesma.
- **Viabilizar** e **assegurar** a proteção dos serviços, das operações, dos desenvolvimentos, dos ativos da Petronect e de seus Clientes e Colaboradores, de ameaças, tanto internas quanto externas, deliberadas ou acidentais, em seus Processos de Negócio.



DEFINIÇÕES IMPORTANTES

- **Declaração de Conformidade de Sigilo** - o Portal de Compras e Contratações possui desde 2005 o Certificado que atesta a conformidade da Declaração de Sigilo das Propostas de Fornecedores com os requisitos da Norma ISO 17050-1. Periodicamente uma empresa certificadora avalia a conformidade desta declaração, ratificando o compromisso da Petronect com a manutenção da Segurança da Informação de seus Clientes.
- **Classificação das Informações** - O Portal de Compras e Contratações possui desde 2005 o Certificado que atesta a conformidade da Declaração de Sigilo das Propostas de Fornecedores com os requisitos da Norma ISO 17050-1. Periodicamente uma empresa certificadora avalia a conformidade desta declaração, ratificando o compromisso da Petronect com a manutenção da Segurança da Informação de seus Clientes.
- **Desenvolvimento Seguro** - é uma prática, utilizada pela Petronect, que define ações relacionadas à segurança no desenvolvimento de software, incluindo, modelagem de ameaças, análise estática do código, revisão de código, testes de segurança direcionados e uma revisão final de segurança, a fim de minimizar a quantidade de vulnerabilidades e falhas de segurança nos produtos ofertados.



AÇÕES E RESPONSABILIDADES

- Viabilizar o tráfego de processos de contratações, de cadastro de fornecedores, obter cotações, disponibilizar operações financeiras, e desenvolver soluções eletrônicas são os negócios da Petronect.
- A confidencialidade, disponibilidade, a integridade e a transparência de procedimentos e a lisura de ações caracterizam a Petronect, desde a sua criação e terão cada vez mais demandas de nosso público usuário.
- Sinergia de todos os componentes desta força de trabalho, para entender, divulgar e cumprir este conjunto de diretrizes, regras e práticas que direcionam e controlam o modo pelo qual cada um de nós deverá contribuir para proteger estes ativos de nossas operações, pois a segurança da informação na Petronect a fará sobreviver por muitos anos agregando o valor que dela se espera.



DIRETRIZES DE A-Z

- a) A informação é um recurso fundamental para o desenvolvimento das atividades da Petronect e, como tal, necessita ser protegida. A segurança da informação visa preservar as informações da Petronect quanto à: confidencialidade, integridade e disponibilidade.
- b) A Política de Segurança da Informação é o documento que estabelece as diretrizes corporativas para a proteção dos ativos de informação da Petronect. É aprovada pela Diretoria e divulgada pelo Comitê de Segurança da Informação da Petronect. Deve, portanto, ser cumprida e aplicada em todas as áreas da empresa.
- c) A implementação desta política é importante para manter e demonstrar a integridade dos processos, produtos e serviços da Petronect nos acordos estabelecidos com seus Clientes e fornecedores, no cumprimento da Política de Privacidade e na Declaração de Conformidade de Sigilo publicada em seu site.
- d) Toda informação produzida ou recebida pelos Colaboradores como resultado da atividade profissional contratada pela Petronect, pertence à Petronect.
- e) Os computadores, sistemas e informações da Petronect são utilizados pelos Colaboradores para a realização das atividades profissionais para as quais o Colaborador foi designado.
- f) Todos os softwares desenvolvidos e\ou alterados por meio de contratação de serviços realizadas pela Petronect são de propriedade intelectual da Companhia.
- g) Os processos de desenvolvimento e manutenção de software devem seguir as boas práticas para o Desenvolvimento e Manutenção Segura de Software, descritas nos documentos Padrão de Gestão de Desenvolvimento Seguro e no Padrão de Processo de Desenvolvimento de Soluções e Melhorias.
- h) A Petronect reserva-se o direito de monitorar e registrar todo o uso das informações geradas, armazenadas ou veiculadas na empresa.
- i) A Política de Segurança da Informação deverá ser comunicada a todos os Colaboradores da Petronect, visando assegurar que todas as pessoas tenham ciência da mesma e a pratiquem na empresa.
- j) O Comitê de Segurança da Informação é o fórum para encaminhamento de todas as questões corporativas relacionadas à Gestão da Segurança da Informação.
- k) Todos os incidentes que afetam a Segurança da Informação devem ser reportados, indiferente da causa ou origem.
- l) Todos os Colaboradores da Petronect devem ter ciência e serem orientados nos procedimentos de segurança e no uso correto dos ativos disponibilizados pela Petronect dentro do período definido, de acordo com o gestão de acessos Petronect após concessão dos acessos para realização das atividades. Treinamentos devem ser oferecidos conforme julgamento das gerências.
- m) Todas as mudanças em processos, procedimentos e tecnologias devem ser formalmente avaliadas considerando o atendimento aos requisitos desta Política.
- n) As medidas de proteção aos recursos da Petronect devem ser aplicadas nos processos de mudança dos sistemas com administração sob responsabilidade da Petronect, como o SRM, onde serão avaliados os riscos e o valor da informação (impactos) para os negócios da Petronect, garantindo a correta manutenção dos níveis de confidencialidade, integridade e disponibilidade das suas informações.
- o) Quando razões tecnológicas ou determinações superiores tornarem impossível o uso apropriado de controles mínimos adequados à garantia da segurança dos ativos de informação, devem ser implementadas medidas que minimizem os riscos. As justificativas e as medidas alternativas devem ser registradas, assim como as devidas aprovações.
- p) A Petronect reserva-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, adotar as medidas legais cabíveis e punir os infratores, no caso de uso indevido de recursos.
- q) Esta Política está implementada na Petronect através de procedimentos específicos, obrigatórios para todos os Colaboradores, independentemente do nível hierárquico ou função na empresa.
- r) Os Colaboradores e terceiros devem ter acesso físico e lógico liberado somente aos recursos de informação necessários e indispensáveis ao desempenho das atividades e em conformidade com os interesses da Petronect, de forma a garantir a proteção da informação contra acesso não autorizado ou revelação indevida a pessoas não autorizadas através de ações deliberadas ou descuidadas.
- s) O grau de proteção das informações deve ser proporcional ao nível de classificação da confidencialidade e ao valor atribuído a essa informação.
- t) A Petronect incentiva todos os Colaboradores a relatarem, de forma direta e imediata, vulnerabilidades ou incidentes de segurança da informação identificados.
- u) Todo Colaborador deve ter uma identificação única, pessoal e intransferível, tal como crachá, para acesso físico e usuário e senha para acesso lógico à Petronect, qualificando-o, inequivocamente, como responsável por qualquer atividade desenvolvida sob esta identificação, conforme as regras estabelecidas nos procedimentos internos. Os Colaboradores temporários devem ter uma identificação com prazo limitado à execução da sua atividade.

DIRETRIZES DE A-Z

- v) Os ativos de informação compartilhados devem ser utilizados de forma que outros Colaboradores não sejam afetados ou prejudicados nos critérios referentes à Confidencialidade, Integridade e Disponibilidade das suas informações. (Exemplo: acesso indevido, códigos maliciosos, quebra de sigilo, compartilhamento indevido de informações sensíveis e classificadas).
- w) É obrigação de cada Colaborador manter-se atualizado em relação a esta Política e aos procedimentos e normas relacionadas, buscando orientação do seu superior ou da Gerência responsável sempre que não estiver absolutamente seguro quanto à sua aplicação.
- x) A Petronect entende que todos os seus controles relacionados à Segurança da Informação devem atender e cumprir os requisitos de negócio de seus Clientes definidos de acordo com a Declaração de Conformidade de Sigilo das propostas de fornecedores publicada no Portal da Petronect
- y) A Petronect entende que deve cumprir toda condição de contrato com Clientes relacionado à segurança da informação.
- z) A Petronect possui o compromisso de estimular ações que promovam a melhoria contínua em Segurança da Informação, de modo a assegurar o avanço nesta área.

RELACIONAMENTO COM CADEIA DE SUPRIMENTOS

Os requisitos de segurança da informação devem ser acordados com o provedor externo e a fim de mitigar os riscos associados com o acesso dos provedores externos aos ativos da Petronect.

O acordo firmado com o provedor externo deve contemplar todas as diretrizes desta política que são aplicáveis ao prestador de serviço.

Para os serviços terceirizados de Tecnologia da Informação, o Acordo de Responsabilidade e Confidencialidade da Informação deve ser estendido por toda a cadeia de suprimento do provedor externo.

Um processo formal para gestão de provedor externo deve ser estabelecido.

A aderência a esta política por parte do provedor externo deve ser monitorada sistematicamente pela Petronect.



DISPOSITIVOS MÓVEIS

Devem ser tomados cuidados ao se utilizarem dispositivos móveis em locais públicos, salas de reuniões e outras áreas desprotegidas.

Devem ser estabelecidas proteções para evitar o acesso não autorizado ou a divulgação de informações armazenadas e processadas nesses dispositivos. Os dispositivos móveis devem ser também protegidos fisicamente contra roubo, especialmente quando deixados, por exemplo, em carros ou em outros meios de transporte, quartos de hotéis, centros de conferência e locais de reunião.

Deve ser estabelecido um procedimento específico que leve em consideração requisitos legais, securitários e outros requisitos de segurança da organização para casos de furto, roubo ou perda de dispositivos móveis.

Os dispositivos móveis que contêm informações importantes, sensíveis e/ou críticas para o negócio, não devem ser deixados sem observação e, quando possível, estejam fisicamente trancados com o uso de travas especiais, para proteger esses dispositivos móveis.

Deve ser agendado treinamento para as pessoas que usam dispositivos móveis, como forma de aumentar a conscientização quanto aos riscos adicionais decorrentes desta forma de trabalho, e os controles que se recomenda implementar.

TRANSPORTE E RETIRADA DE ATIVOS DA PETRONECT

Devem ser claramente identificados os funcionários, fornecedores e partes externas que tenham autoridade para permitir a remoção de ativos para fora do local.

Devem ser estabelecidos limites de tempo para a retirada de equipamentos do local, e a devolução seja controlada.

Sempre que necessário ou apropriado, é recomendado que seja feito um registro da retirada e da devolução de ativos, quando do seu retorno.

A identidade, atribuição e função de qualquer pessoa que manuseia ou utiliza os ativos estejam documentados, e que esta documentação seja devolvida com o equipamento, a informação ou software.

TRABALHANDO EM ÁREAS SEGURAS

Definição: São ambientes físicos onde que contém os recursos de processamento das informações e as informações da Petronect.

O pessoal só terá conhecimento da existência de áreas seguras ou das atividades nelas realizadas, apenas se for necessário.

Deve ser evitado o trabalho não supervisionado em áreas seguras, tanto por motivos de segurança como para prevenir as atividades mal-intencionadas.

As áreas seguras, não ocupadas, devem ser fisicamente trancadas e periodicamente verificadas.

Não é permitido o uso de máquinas fotográficas, gravadores de vídeo ou áudio ou de outros equipamentos de gravação, tais como câmeras em dispositivos móveis, salvo se for autorizado.

As normas para o trabalho em áreas seguras incluem o controle dos funcionários, fornecedores e partes externas que trabalham em tais áreas, cubram todas as atividades nestas áreas.

Os equipamentos devem ser acondicionados em local apropriado de forma a minimizar danos causados por poeira, efeitos químicos, interferência ou radiação eletromagnética e vandalismo.

Os locais que possuem equipamentos devem ter a temperatura e umidade do ar constantemente monitoradas para evitar que ambas afetem negativamente os equipamentos.

A movimentação e a instalação de equipamentos (com exceção de dispositivos móveis) só podem ser feitas pelo time de Infraestrutura.

A manutenção dos equipamentos deve ser realizada apoiada em bases de conhecimento e especificações do fabricante para garantir a integridade e disponibilidade dos mesmos. Os equipamentos que passarem por manutenção devem ser inspecionados para garantir que não estão em mau funcionamento antes de entrar em operação.

A remoção de equipamentos do local de origem deve ser feita de forma controlada e somente mediante autorização.

Os equipamentos e outros ativos da Petronect que operam fora dos perímetros de segurança definidos, devem possuir medidas de segurança implementadas para minimizar os riscos inerentes ao ambiente externo.

Os equipamentos devem ser inspecionados antes da reutilização ou descarte para averiguar quanto à existência de informação sensível armazenada. Caso o equipamento inspecionado em questão contenha informação sensível, a mesma deve ser sobrescrita de forma segura antes da reutilização ou descarte.

Para os equipamentos que não estão sendo monitorados continuamente pela Petronect, devem ser implementadas medidas de segurança como a conscientização e a responsabilização dos usuários destes equipamentos quanto à proteção da informação existente nos mesmos.

No Data Center, os equipamentos devem ser protegidos contra indisponibilidades causadas devido à falta ou interrupções no suprimento de serviços como energia elétrica e ar-condicionado por meio de redundância.



DESCARTE E REUTILIZAÇÃO DE MÍDIA

Os equipamentos devem ser inspecionados para verificar se a mídia está ou não armazenada, antes do descarte ou reutilização.

As mídias de armazenamento que contém informações confidenciais ou de direitos autorais devem ser destruídas fisicamente, ou as informações devem ser destruídas, apagadas ou sobre-gravadas por meio de técnicas que tornem as informações originais irrecuperáveis, em vez de se usarem as funções-padrão de apagar ou formatar.

No caso de dispositivos defeituosos que contenham informações sensíveis, pode ser necessária uma avaliação de riscos para determinar se convém destruir fisicamente o dispositivo em vez de mandá-lo para o conserto ou descartá-lo.

Adicionalmente à remoção segura das informações contidas no disco, a encriptação completa do disco reduz o risco de revelação de informação confidencial quando o equipamento é descartado ou reparado, a encriptação do dispositivo pode ser feita em alternativa à sua destruição.

As ferramentas usadas para sobregravar devem ser analisadas criticamente para assegurar que elas são aplicáveis à tecnologia usada para o armazenamento da mídia.



POLÍTICA DE MESA LIMPA

As informações do negócio sensíveis ou críticas, por exemplo, em papel ou em mídia de armazenamento eletrônicas, devem ser guardadas em lugar seguro (idealmente em um cofre, armário ou outras formas de mobília de segurança) quando não em uso, especialmente quando o escritório está desocupado.

Os computadores e terminais devem ser mantidos desligados ou protegidos com mecanismo de travamento de tela e teclados controlados por senha, token ou mecanismo de autenticação similar quando sem monitoração e protegida por tecla de bloqueio, senhas ou outros controles, quando não usados.

Devem ser evitados o uso não autorizado de fotocopiadoras e outra tecnologia de reprodução (por exemplo, scanners, máquinas fotográficas digitais).

Os documentos que contêm informação sensível ou classificada devem ser removidos de impressoras imediatamente.



AÇÃO DE CONTINGÊNCIA

Exceções a esta política deverão ter seus pleitos formalizados ao Comitê de Segurança da Informação onde serão deliberados e, caso assim sejam julgados, aprovados em caráter excepcional (aprovação por exceção).

DOCUMENTOS COMPLEMENTARES

- POLÍTICA DE PRIVACIDADE
- DECLARAÇÃO DE CONFORMIDADE DE SIGILO - A Petronect > Segurança da Informação
- GESTÃO DE ACESSOS PETRONECT
- DESENVOLVIMENTO SEGURO
- CLASSIFICAÇÃO E TRATAMENTO DE INFORMAÇÕES
- PROCESSO DE DESENVOLVIMENTO DE SOLUÇÕES E MELHORIAS

HISTÓRICO DE VERSÕES

1. Original

The logo for Petronect features the word "Petronect" in a bold, italicized, dark blue sans-serif font. A green circular graphic, composed of two curved segments, is positioned behind the letter "o".

Petronect