INTRODUÇÃO

A PHYNANCE, enquanto empresa comprometida em imprimir o maior grau possível de governança corporativa, elaborou dentre outras políticas a presente POLÍTICA PHYNANCE DE SEGURANÇA DA INFORMAÇÃO, qual aqui apenas denominamos "política" para dirimir qualquer eventual possibilidade de risco.

Acrescente-se inicialmente que a presente política além de estar compilada neste documento encontra-se pulverizada nas demais políticas interna da empresa o que reafirma o nosso compromisso com a segurança e o valor que damos a discrição.

Nos tempos atuais a informação tornou-se o ativo mais valioso das grandes empresas, ao mesmo tempo, que passou a exigir uma proteção adequada. De forma assustadoramente crescente, as organizações, seus sistemas de informações e suas redes de computadores apresentam-se diante de uma série de ameaças, sendo que, algumas vezes, estas ameaças podem resultar em prejuízos para as empresas.

A segurança da informação visa protegê-la de um grande número de ameaças para assegurar a continuidade do negócio. Esta segurança é obtida a partir da implementação de uma série de controles, que podem ser políticas, práticas e procedimentos, os quais precisam ser estabelecidos para garantir que os objetivos de segurança específicos da organização sejam atendidos.

A política de segurança visa trazer ao ambiente da PHYNANCE regras e procedimentos que devem ser seguidos para a garantia da segurança da informação.

SEGURANÇA DA INFORMAÇÃO

A informação é um ativo que, como qualquer ativo importante para os negócios, tem um valor para a organização e consequentemente necessita ser adequadamente protegida. Para muitas empresas a informação é o maior patrimônio e protegê-la não é uma atividade simples, sendo que pode abranger várias situações, como: erro, displicência, ignorância do valor da informação, fraude, sabotagem, etc.

Define-se dados como um conjunto de bits armazenados como: nomes, endereços, datas de nascimentos, históricos de movimentação, etc. A informação é um dado que tenha sentido, como por exemplo, as notas ou informações financeiras de um cliente. O conhecimento é um conjunto de informações que agrega valor a organização.

A informação pode existir de diversas formas, ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou através de meio eletrônico, mostrada em filmes ou falada em conversas. Seja qual for a forma apresentada ou meio através do qual a informação é compartilhada ou armazenada, é recomendado que seja sempre protegida adequadamente.

Deve-se entender que segurança da informação não é uma tecnologia. Não é possível comprar um dispositivo que torne a rede segura ou um software capaz de tornar seu computador seguro. Segurança da informação não é um estado que se pode alcançar.

O que é possível fazer é administrar um nível aceitável de risco. Segurança é um processo, pode-se aplicar o processo à rede ou à empresa visando melhorar a segurança dos sistemas.

É essa a nossa intenção quando passamos a cuidar tão atentamente para esse ponto de controle dentro da nossa empresa.

ABRANGÊNCIA

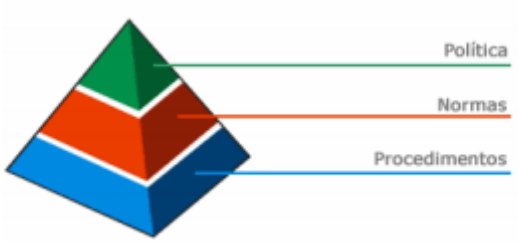
A Política Corporativa de Segurança da Informação tem como objetivo principal direcionar um programa efetivo de proteção dos ativos de informação sendo a base para o estabelecimento de todos os padrões, normas e procedimentos de Segurança. Sua abrangência é sobre todas as Dependências e ambientes e funcionários da PHYNANCE.

DEFINIÇÃO

A estrutura normativa da Segurança da Informação da PHYNANCE é composta por um conjunto de documentos com três níveis hierárquicos distintos, relacionados a seguir:

ƒ

- Política de Segurança da Informação (Política): constituída neste documento, define a estrutura, as diretrizes e as obrigações referentes à segurança da informação;
- Normas de Segurança da Informação (Normas): estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da Política, a serem seguidos em diversas situações em que a informação é tratada;
- ƒ Procedimentos de Segurança da Informação (Procedimentos): instrumentalizam o disposto nas Normas e na Política, permitindo a direta aplicação nas atividades da PHYNANCE.



CLASSIFICAÇÃO DA INFORMAÇÃO

A classificação mais comum nos dia de hoje, é aquela que divide em quatro níveis: secreta, confidencial, interna e pública.

- Secreta - Estas informações devem ser acessadas por um número restrito de pessoas e o controle sobre o uso destas informações deve ser total, são informações essenciais para a empresa, portanto, sua integridade deve ser

preservada. O acesso interno ou externo por pessoas não autorizadas a esse tipo de informação é extremamente proibido!

- Confidencial - Estas informações devem ficar restritas ao ambiente da empresa, o acesso a esses sistemas e informações é feito de acordo com a sua estrita necessidade, ou seja, os usuários só podem acessá-las se estes forem fundamentais para o desempenho satisfatório de suas funções na instituição. O acesso não autorizado à estas informações podem causar danos financeiros ou perdas de fatia de mercado para o concorrente o que impacta diretamente no desempenho da empresa.

- Interna - Estas informações devem ficar restritas ao ambiente da empresa, o acesso a esses sistemas e informações é feito de acordo com a sua estrita necessidade, ou seja, os usuários só podem acessá-las se estes forem fundamentais para o desempenho satisfatório de suas funções na instituição. O acesso não autorizado à estas informações podem causar danos financeiros ou perdas de fatia de mercado para o concorrente.

- Públicas - Informações que podem ser divulgadas para o público em geral, incluindo clientes, fornecedores, imprensa, não possuem restrições para divulgação.

Lembre-se sempre que todas as informações que tratamos prioritariamente são informações confidenciais, sendo que aquelas que não receberem esse rótulo serão devidamente sinalizadas.

CONDUTA DE TRATAMENTO DA PRIVACIDADE.

Qualquer informação que o cliente fornecer deverá ser coletada e guardada de acordo com os padrões determinado pela CVM e ANBIMA;

Toda informações que circule entre setores deve ser feita de forma criptografada para garantir uma maior segurança;

Salvo por determinação judicial, nenhuma informação coletada dos clientes poderá ser transferida a terceiros ou usadas com finalidade diferente daquela a que se propunha

quando foi fornecida. Acrescente-se que a informação colhida pode ter mais de um propósito e diante disto deverá o cliente estar devidamente ciente.

No processo de cadastramento e entrada do cliente deverão ser solicitadas informações imprescindíveis, contudo ficará a critério do cliente se fornecerá ou não tais informações, ficando desde a negativa responsável por sua repercussão. Frise-se nesse sentido que a negativa de algumas informações constitui indício de cometimento de crime de Lavagem de Capitais e deve ser imediatamente informado ao Compliance para que este tome as medidas devidas.

O acesso às informações coletadas, no âmbito interno da PHYNANCE, será restrito apenas a funcionários autorizados e previamente instruídos para o uso adequado desses dados. Desta forma, aquele que for flagrado ou denunciado contrariando a presente política poderá além de responder processo administrativo ter a repercussão criminal cabível.

DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

Independentemente do meio ou da forma em que exista, a informação está presente no trabalho de todos os profissionais. Portanto, é fundamental para a proteção e salvaguarda das informações que os profissionais adotem comportamento seguro e consistente com o objetivo de proteção.

Desta forma, todos os funcionários da PHYNANCE, independente de cargo, tempo de serviço ou função deve assumir uma postura dianteira e engajada no que diz respeito a segurança da informação.

É obrigatória a compreensão de que ameaças internas podem afetar a segurança da informação dentro da empresa, tais como vírus de computador, interceptação de mensagens eletrônicas por isso é proibido o acesso a webmails e uso de aparelhos eletrônicos por aqueles que manuseiem ou produza tal tipo de informação.

Todo funcionário deve ter o maior cuidados com os detalhes que possam por em risco a segurança não só da informação, mas também a física, dessa forma, deve-se guardar muita atenção aos cartões de acesso, chaves e senhas pessoais.

As senhas pessoais são intransferíveis, não podendo ser divulgadas nem compartilhadas. Não anote suas senhas em papel, em local visível ou sem proteção

(lembre-se que a senha é uma identidade funcional e a negligência disso pode acarretar em danos à sua reputação profissional).

Todo acesso a informação que não for explicitamente autorizado é proibido.

As informações adquiridas pela empresa não podem ser copiadas para pendrives, CDs ou qualquer outro dispositivo de armazenamento sem prévia autorização do compliance.

Nunca se sabe que pode estar ouvindo as nossas conversas. As vezes mesmo não intencionalmente pode ser dito algo que não deveria, por isso não trate de assuntos confidenciais do trabalho em ambiente público, externo ou até mesmo interno na presença de quem não deveria ter acesso àquela informação.

A política de uso de email e de internet deve ser rigorosamente seguida. Arquivos de origem desconhecidas nunca devem ser abertos ou baixados.

Toda informação impressa que tenha caráter confidencial deve ser mantida em local adequado enquanto seu manuseio, guardada em local protegido e não havendo mais necessidade o documento deve ser destruído em máquina própria. Nestes casos deverão ser respeitadas as regras quanto a manutenção do documento pelo Compliance.

Qualquer dúvida sobre como interpretar ou proceder diante da presente política deve sempre ser tomada a decisão mais conservadora e procurar imediatamente o Compliance que de pronto deverá esclarecer tal demanda.

PROTEÇÃO FÍSICA DOS DOCUMENTOS PRODUZIDOS

De início, a PHYNANCE tem por princípio construir um mundo melhor hoje e para o futuro. Desta forma o uso de material tipo impressora e papel devem ser feito de forma moderada e apenas quando necessário.

Todos os documentos devem ser produzidos em duas cópias. Uma dessas cópias será custodiada por uma empresa responsável por essa atividade e outra será arquivada dentro da PHYNANCE guardada as devidas cautelas.

As informações serão guardadas de acordo com o grau de confidencialidade, operacionalidade e importância para a atividade da PHYNANCE.

As informações devem ser mantidas por um período mínimo de 2 anos e, em casos específicos, atender a resolução própria da CVM.

AUDITORIA DE RISCO DA INFORMAÇÃO

A vulnerabilidade é o ponto onde qualquer sistema é suscetível a um ataque, ou seja, é uma condição encontrada em determinados recursos, processos, configurações, etc. Condição causada muitas vezes pela ausência ou ineficiência das medidas de proteção utilizadas de salvaguardar o bem da empresa.

Uma vulnerabilidade pode partir das próprias medidas de segurança implantadas na empresa, se existir estas medidas, porém configuradas de maneira incorreta, então a empresa possuirá uma vulnerabilidade e não uma medida de segurança.

Então, para evitar que seja colocada em risco a segurança da informação, além das cautelas de praxe é feito um sistema de auditoria semestral o qual será responsável por:

- Conferencia de aderência a presente política;
- Conferencia de adesão ao Código de Ética;
- Verificação das maquinas (computadores);
- Verificação das instalações físicas pessoais de cada funcionário;
- Propor projetos e soluções relacionados à melhoria da segurança da informação da PHYNANCE, mantendo-se atualizada com as melhores práticas existentes no mercado em relação às tecnologias disponíveis;
- Confeccionar um relatório mensal de como está o controle de segurança da informação, no sentido de realizar trabalhos de análise de vulnerabilidade, com o intuito de aferir o nível de segurança dos sistemas de informação e dos demais ambientes em que circulam as informações da PHYNANCE;
- Requisitar informações às demais áreas da PHYNANCE (diretorias, gerências coordenações etc.), realizar testes e averiguações em sistemas e equipamentos, com o intuito de verificar o cumprimento da Política e das Normas de Segurança da Informação; e
- Estabelecer mecanismo de registro e controle de não-conformidade a esta Política e às Normas de Segurança da Informação, comunicando o Compliance.

DEFINIÇÃO DO PROPRIETÁRIO DA INFORMAÇÃO

Conforme retromencionado, toda informação que circula dentro da PHYNANCE tem caráter sigiloso. O proprietário da informação é um diretor ou um gerente da PHYNANCE, formalmente indicado pela Diretoria Executiva, responsável pela concessão, manutenção, revisão e cancelamento de autorizações de acesso a determinado conjunto de informações pertencentes à PHYNANCE ou sob a sua guarda.

Desta forma, cabe à diretoria da Phynance:

- Elaborar, para toda informação sob sua responsabilidade, matriz que relaciona cargos e funções da PHYNANACE às autorizações de acesso concedidas;
- Autorizar a liberação de acesso à informação sob sua responsabilidade, observada a matriz de cargos e funções, a presente política e o Código de Ética;
- Manter registro e controle atualizado de todas as liberações de acesso concedidas, determinando, sempre que necessário, a pronta suspensão ou alteração de tais liberações. Deve ser remetidas ao Compliance cópias das liberações de acesso;
- Reavaliar, sempre que necessário, as liberações de acesso concedidas, cancelando aquelas que não forem mais necessárias;
- Analisar os relatórios de controle de acesso fornecidos pela área de Gestão de Segurança da Informação, com o objetivo de identificar desvios em relação à Política e às Normas de Segurança da Informação, tomando as ações corretivas necessárias;
- Participar da investigação de incidentes de segurança relacionados à informação sob sua responsabilidade;
- Participar, sempre que convocado, das reuniões do Comitê de Gestão de Segurança da Informação, prestando os esclarecimentos solicitados.

ATUAÇÃO DO LEGAL & COMPLIANCE

Manter as áreas da PHYNANCE informadas sobre eventuais alterações legais e/ou regulatórias que impliquem responsabilidade e/ou ações envolvendo a gestão de segurança da informação;

Arquivar cópia de todas as autorizações de acesso dadas, bem como ter acesso a relatórios periódicos de conformidade;

Incluir, na análise e na elaboração de contratos, sempre que necessário, cláusulas específicas relacionadas à segurança da informação, com o objetivo de proteger os interesses da PHYNANCE;

Avaliar, quando solicitada, as Normas e os Procedimentos de Segurança da Informação elaborados pelas diversas áreas da PHYNANCE;

Assegurar que suas equipes possuam acesso e conhecimento desta Política, das Normas e dos Procedimentos de Segurança da Informação;

Verificar periodicamente se o nível de acesso concedido condiz com a realidade da função desempenhada pelo contemplado;

Remover imediatamente todas as concessões dadas a funcionários afastados da empresa ou que tenham mudado de função;

Redigir os Procedimentos de Segurança da Informação relacionados mantendo-os atualizados

Comunicar imediatamente eventuais casos de violação de segurança da informação à área de Gestão de Segurança da Informação.

ATUAÇÃO DO R.H

Deverá o R.H colher assinatura de todos os novos contratados acerca do conhecimento do CÓDIGO DE ÉTICA E CONDUTA PROFISSIONAL PHYNANCE S/A e da presente POLÍTICA DE SEGURANÇA DA INFORMAÇÃO;

Colher a assinatura do Termo de Responsabilidade dos funcionários e estagiários, arquivando-o nos respectivos prontuários.

Informar prontamente ao Compliance do desligamento, afastamento e modificações no quadro funcional da PHYNANCE de modo que o Compliance deve tomar devidas precauções.

AVALIAÇÃO DOS RISCOS DA SEGURANÇA DA INFORMAÇÃO.

A área de Risco da PHYNANCE atua como ferramenta qual dentre das suas atribuições está a de identificação dos principais riscos aos quais as informações estão expostas; e priorização das ações voltadas à mitigação dos riscos apontados, tais como implantação de novos controles, criações de novas regras e procedimentos, reformulação de sistemas etc. que deve ser enviada ao Compliance para as devidas providências.

Essa analise pode ser setorial ou geral de acordo com a necessidade.

SEGREGAÇÃO ENTRE SETORES

Todos os acessos ao ambiente físico da PHYNANCE são controlados. Sendo assim, não é de livre acesso entre áreas. Nesse ponto é deixado claro que uma área ou setor não tem prévia autorização para frequentar o espaço físico de outra.

Essa segregação tem como objetivo principal proteger as informações. Por isso documentamos as autorizações e periodicamente será analisada necessidade de uma formulação de política própria com essa finalidade.

Será expressamente autorizado pela diretoria, através do Compliance o acesso pertencente a cada funcionário. Desta forma, uma autorização pode ser revogada a qualquer tempo.

Os setores: Administrativo, Compliance, Mesa de Operações, Modelagem, Risco e T.I possuem ambientes físicos distintos dispostos de modo a viabilizar um controle efetivo.

Isto posto é terminantemente proibida entrada no Setor Administrativo e de Compliance sem prévia autorização. Indicamos que no caso de necessidade de diálogo entre setores que este seja feita na sala de reunião e sempre acompanhada de mais de uma pessoa.

É proibida a integração de qualquer monta entre os setores com a área de modelagem que deve ser mantida completamente segregada;

Somente membros da diretoria e funcionários autorizados do T.I podem adentrar no CPD.

A integração entre as demais áreas deve guardar a maior cordialidade possível levando-se sempre em consideração o grau de importância que a informação detida por cada um e a repercussão que um vazamento mesmo que inocente poderá ter na imagem da PHYNANCE e consequentemente resvalar na sua atividade profissional

VIOLAÇÕES E CONTRARIEDADES

As violações e contrariedades a esta política, em como a qualquer outra interna da PHYNANCE tem consequências administrativa e dependendo do caso consequência legal, podendo, nos termos do retromencionado Código de Ética culminar em desligamento e eventuais processos criminais aplicados.

A PHYNANCE se resguarda o direito de manter clara a posição impoluta e ética que adota em todas suas atividades, arcando inclusive com a possibilidade de promover o desligamento do funcionário apenas pela não conformidade.

Todos os sujeitos, antes de ingressarem nos quadros de funcionários da PHYNANCE tem acesso às políticas internas e ao Código de Ética, o qual deve ler com atenção de modo a somente assinar contrato de trabalho após o aceite dessas regras.

CONCLUSÃO

Isto posto, são os parâmetros mínimos da PHYNANCE para proteção das informações e pode a qualquer tempo sem aviso prévio sofre modificações, das quais serão cientificados todos os funcionários.

DOCUMENTOS RELACIONADOS:

- Lei n° 6.385/1976: http://www.planalto.gov.br/ccivil_03/leis/L6385.htm;
- Instrução CVM n° 8/1979: http://www.cnb.org.br/CNBV/instrucoes/ins08-1979.htm;
- Instrução CVM n° 358/2002: http://www.cnb.org.br/CNBV/instrucoes/ins358-2002.htm;
- Instrução CVM n° 400/2003: http://www.cvm.gov.br/asp/cvmwww/atos/exiato.asp?file=%5Cinst%5Cinst400.htm;
- Instrução CVM nº 483/2010: http://www.cnb.org.br/CNBV/instrucoes/ins483-2010.htm;
- Política de Segurança da Informação – BMF&BOVESPA – disponível em: http://ri.bmfbovespa.com.br/upload/portal_investidores/pt/governanca_corporativa/estatutos_politicas/Politica_da_Seguranca_da_Informacao.pdf