POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

velsis

APOIO TÉCNICO CIENTÍFICO
PIRONTI ADVOGADOS

REVISÃO 03

Sumário

INTRODUÇÃO

Toda informação é um recurso fundamental e estratégico para o desenvolvimento e manutenção das atividades da VELSIS e, como tal, necessita ser protegida. A Política de Segurança da Informação (PSI) visa preservar os principais atributos da informação: a confidencialidade, a integridade e a disponibilidade da informação.

A Velsis possui uma política integrada da Qualidade e da Segurança da Informação elaborada com base nos seguintes pontos:

Oferecer soluções competitivas e seguras para o mercado de ITS (Intelligent Transportation System) e mobilidade por meio da:

I. Inovação e qualidade de seus produtos e serviços;

II. Satisfação de seus clientes internos e externos;

III. Melhoria contínua dos sistemas de gestão da qualidade e da segurança da informação com atendimento aos requisitos aplicáveis.

O termo "política" utilizado neste documento se refere as regras, procedimentos e condutas para atender a Política integrada da Qualidade e Segurança da Informação nos quesitos tecnológicos e comportamentais.

Esta política abrange todos os colaboradores, terceiros e profissionais de empresas contratadas que, de uma ou outra forma, utilizam ou manipulam as informações pertencentes à organização. A política estabelece os princípios e as diretrizes que norteiam a segurança da informação na VELSIS. Esta política foi aprovada e divulgada por decisão de toda a Diretoria da empresa, a qual apoia e fomenta as iniciativas necessárias para o alcance dos objetivos de segurança da informação aqui estabelecidos.

A presente PSI está baseada nos requisitos da norma ABNT NBR ISO/IEC 27001, reconhecida mundialmente como um código de prática para a gestão da segurança da informação.

OBJETIVO

Os objetivos específicos deste documento são:

I. Estabelecer os princípios e orientar a definição e utilização de sistemas de segurança que garantam a confidencialidade, a integridade e a disponibilidade das informações na VELSIS para preservar a continuidade dos seus negócios;

II. Definir o escopo da segurança da informação na VELSIS, suas diretrizes e procedimentos para a gestão segura dos seus ativos durante as fases de seu ciclo de vida (manuseio, armazenamento, transporte e descarte);

III. Servir de referência para auditorias internas e externas na apuração, validação e avaliação de responsabilidades.

CAMPO DE APLICAÇÃO

Os campos de aplicação desta política são:

I. Esta política aplica-se a todos os colaboradores, contratados, temporários e parceiros da companhia, ou seja, deve ser lida, conhecida e entendida por todos os usuários da informação dentro e fora dos limites da companhia.

II. Esta política se aplica tanto ao ambiente computacional quanto aos meios convencionais para manuseio, armazenamento, transporte e descarte da informação, abrangendo todos os equipamentos e recursos possuídos ou utilizados na companhia;

III. A discricionariedade (tomadas de decisões) atribuída aos gestores, quando aplicável, (6), torna-os corresponsáveis por todo o monitoramento, controle e ações para manter a conformidade com a segurança da informação, nos termos desta Política de Segurança da Informação (PSI);

IV. Caberá as áreas de negócio definir políticas específicas complementares, quando cabíveis.

É obrigação de cada colaborador se manter atualizado em relação ao conteúdo desta Política de Segurança da Informação (PSI) e dos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Gerência de Tecnologia da Informação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

APLICABILIDADE

Define-se a conformidade à esta política seguindo os critérios abaixo descritos:

I. É de responsabilidade dos usuários das informações o conhecimento desta política, devendo seguí-la rigorosamente;

II. Esta política é aplicada a todos os colaboradores, contratados, temporários e a todas as partes relacionadas de alguma forma com a companhia;

III. Via de regra, a Política de Segurança da Informação (PSI) tem a sua aplicabilidade direta, imediata e integral e entra em vigor a partir da sua data de publicação;

IV. Poderão ser produzidas políticas específicas como desdobramento de um ou mais itens deste documento, tais como: política de uso de celulares corporativos, política de uso de equipamentos móveis, entre outros;

V. A inobservância das políticas e normas de segurança da informação acarreta ao usuário sanções internas e, nos casos cabíveis, às legislações e todos os dispositivos legais.

DEFINIÇÕES

Ativos: Todo elemento que compõe os processos que manipulam e processam a informação, a contar a própria informação, o meio em que ela é armazenada, bem como os equipamentos, sistemas ou aplicativos em que ela é manuseada, transportada e descartada.

Áreas sensíveis: São áreas ou setores que concentram uma quantidade considerável de informações sensíveis e estratégicas para o negócio.

Ativos de informação: Qualquer informação que tenha valor para a organização.

Custodiante: Usuário com atribuição fornecida pelo proprietário da informação para protegê-la adequadamente.

Colaboradores: Funcionários, estagiários, terceirizados e diretores da companhia.

Confidencialidade: Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando à limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas.

Gestor: Colaboradores com nível estatutário, estratégico, gerencial, coordenação ou de supervisão.

Disponibilidade: Toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários quando os mesmos delas necessitem para executae suas atividades.

Integridade: Toda informação deve ser mantida na condição em que foi disponibilizada pelo seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais.

Impacto: Abrangência dos danos causados por um incidente de segurança sobre um ou mais processos de negócio.

Incidente de segurança: Fato ou evento decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades, levando à perdados princípios da segurança da informação (confidencialidade, integridade e disponibilidade).

Responsável pela informação: Gerador da informação ou seu principal usuário. Responsável por definir o nível de classificação da informação.

Riscos: Probabilidade de ameaças internas ou externas explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, causando impactos nos negócios.

Sistemas Corporativos: São todos os sistemas transacionais, gerenciais ou estratégicos utilizados para automatização de processos ou tomada de decisão.

Sistemas Especialistas: São sistemas específicos para automatizar processos bastante específicos, normalmente utilizado por uma área específica da organização.

Owner do Processo ou do Sistema: É o dono daquele processo ou daquele sistema, não sendo necessariamente um gestor. É o responsável pelas informações que o processo ou o sistema gera.

Terceiros: Pessoas que prestam serviços e podem possuir acesso às instalações e recursos de informação da companhia.

Usuários de Informações: Todos os usuários que de alguma forma, direta ou indireta, utilizam ou manipulam informações da empresa.

Rede corporativa VELSIS: Qualquer meio de comunicação de dados contratado pela companhia.

PSI VELSIS: Política da Segurança da Informação VELSIS.

Registro de Controle de Informações Documentadas: Lista mestra de documentos utilizados pela companhia conforme os processos da ISO9001.

Segregação de Função: Conforme o Conselho Federal de Contabilidade, na Resolução nº 1.212/2009, segregação de funções significa atribuir a "(...) pessoas diferentes as responsabilidades de autorizar e registrar transações e mantera custódia dos ativos. A segregação de funções destina-se a reduzir as oportunidades que permitam a qualquer pessoa estar em posição de perpetrar e de ocultar erros ou fraudes no curso normal das suas funções".

Menor privilégio: Consiste em conceder somente os acessos e recursos estritamente necessários para o desempenho das atividades autorizadas

OS PRINCÍPIOS E AS DIRETRIZES

A VELSIS tem o domínio de todo e qualquer materialpresente em ativosde sua propriedade e se reserva ao direito de controlar, (9) por meio de ferramentas de gerenciamento, procedimentos e auditorias, qualquer informação encontrada em um de seus ativos, com ou sem a ciência do seu funcionário ou terceiros, de modo a garantir a boa utilização e a integridade de seu sistema de informação.

PROPRIEDADE, MANUTENÇÃO DA CONFIDENCIALIDADE, INTEGRIDADE E DISPONIBILIDADE DAS INFORMAÇÕES:

As informações pertencentes à companhia devem ser preservadas em relação a sua confidencialidade, integridade e disponibilidade. Toda informação manuseada, transportada, armazenada ou descartada deve observar os seguintes princípios e diretrizes:

I. Toda informação gerada pelos usuários, utilizando integralmente ou parcialmente algum recurso da empresa, interna ou externamente, é de propriedade exclusiva da companhia;

II. As ideias, os métodos e a criação aplicados ou desenvolvidos na empresa, interna ou externamente, devem atender exclusivamente aos interesses da companhia;

III. O custodiante da informação deve prevenir-se em relação à possibilidade da ocorrência de vazamento da informação da companhia por meio de controles específicos;

IV. Qualquer divulgação de informações classificadas no Registrode Controle de Informações Documentadas deverá ser feita pelo gestor das áreas específicas;

V. Todos os colaboradores devem utilizar os recursos da empresa seguindo os princípios de segurança da informação, sem afetar ou causar prejuízo aoutrem;

VI. Qualquer descumprimento da política por qualquer usuário deve ser imediatamente comunicado a área de Tecnologia da Informação;

VII. As áreas de negócio devem manter um Sistema de Gestão de Riscos sobre o aspecto da segurança da informação. O Gerenciamento de Riscos deve ser identificado por tipo de exposição, avaliado quantoa probabilidade de incidência e o impactono negócio. O resultado desta análise poderá ser classificado como baixo, médioou alto. Identificado o risco alto, será aplicado o plano de ação para mitigação do risco;

VIII A melhoria do sistema de gestão da qualidade (ISO 9001) e da Segurança da Informação (ISO 27001) deve ser contínua;

IX Os processos e controles internos devem ser mapeados e revisados, periodicamente, quanto ao seu nível de maturidade em relação à segurança da informação;

X Adicionalmente, os dados pessoais eventualmente coletados observarão as hipóteses de tratamento previstas na legislação, em especial à Lei Geral de Proteção de Dados Pessoais (LGPD). Nestes casos, os titulares de dados serão devidamente informados sobre a finalidade dos tratamentos que serão realizados e o armazenamento respeitará padrões rígidos de segurança e confidencialidade, sendo providas todas as medidas técnicas, administrativas e institucionais cabíveis;

XI Os direitos dos titulares serão devidamente observados, sendo possível que acessem, retifiquem, solicitem a exclusão de dados, transfiram, limitem ou se oponham ao tratamento, bem como retirem eventual consentimento concedido.

GESTÃO DOS ATIVOS DE INFORMAÇÃO E CLASSIFICAÇÃO DAS INFORMAÇÕES

A classificação das informações e a gestão dos ativos de informação facilitam a implementação de controles adequados para a segurança da informação, sendo viabilizados por meio de(a):

I Identificação dos ativos de informação e permanente atualização;

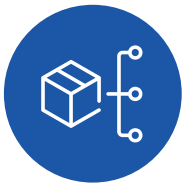
II Classificação das informações quanto a sua sensibilidade (confidencialidade), criticidade, valor (documental ou estratégico) e requisitos legais, identificando a forma adequada. Estas informações devem estar documentadas no Registro de Controle de Informações Documentadas;

III Aplicação de medidas de proteção dos ativos de forma compatível com o risco e com o valor (documental ou estratégico) da informação para os negócios da companhia. As informações devem ser classificadas sistematicamente.

Identificação das informações documentadas

As informações devem ser classificadas no documento Registro de Controle de Informações Documentadas, considerando o nível de criticidade, sensibilidade, valor e requisitos legais.

Criticidade: Define o nível de impacto que pode advir da divulgação ou uso indevido da informação. Pode ser classificada como Alto, Média ou Baixa.



Sensibilidade: Refere-se à informação de uso Restrito, Público ou Confidencial.

Valor: Define se a informação é apenas Documental ou Estratégica.

Requisitos Legais: Relaciona-se a uma lei ou normativa.

Para efeito desta política, todas as informações classificadas com a Sensibilidade "Confidencial" devem ser identificadas no rodapédos respectivos documentos ao serem manuseados ou transportados.

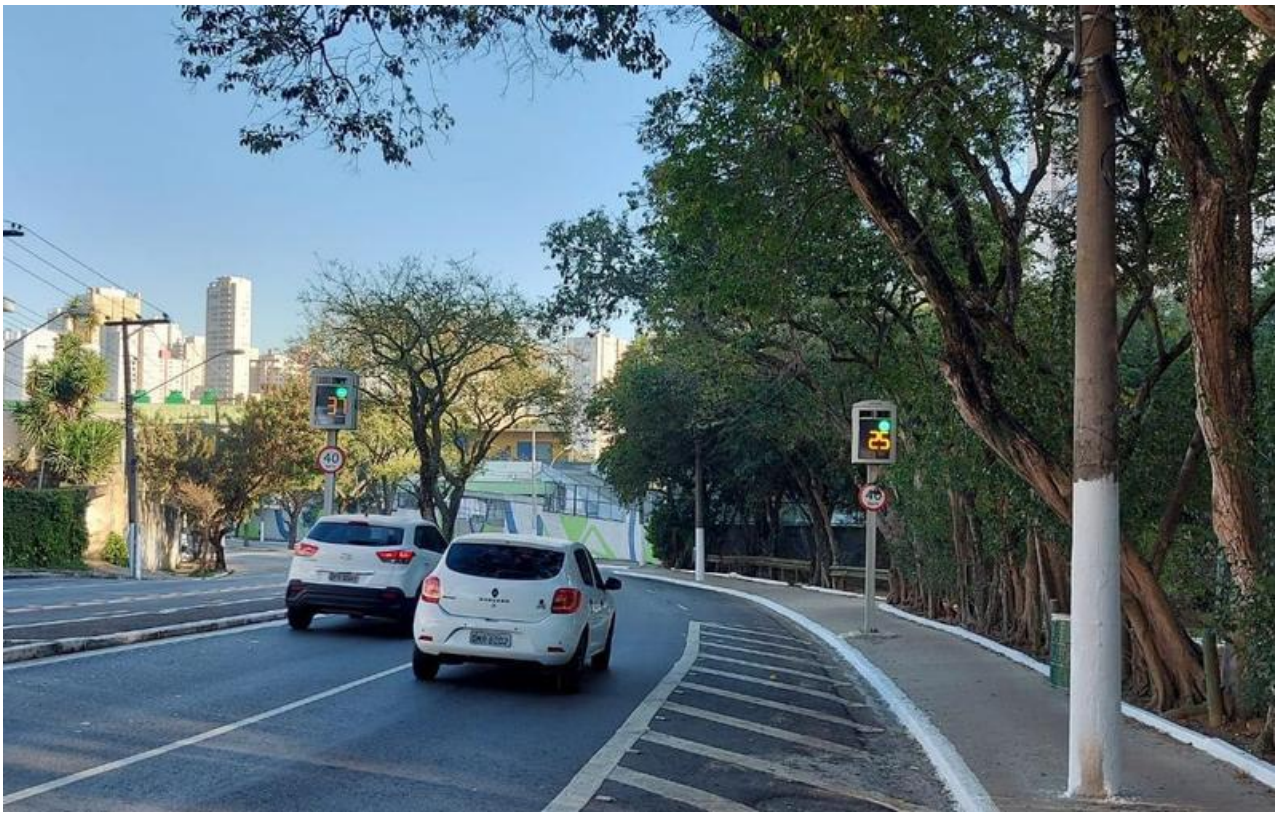
SEGREGAÇÃO DE ATIVIDADES E FUNÇÕES

Para uma gestão eficaz da segurança da informação, as atividades e funções dos usuários das informações devem ser segregadas conforme as orientações que seguem:

I. No quadro de colaboradores e terceiros, se for o caso, deve haver uma efetiva segregação de atividades e funções, ainda que de forma esporádica ou eventual, a fim de que uma mesma pessoa não assuma simultaneamente responsabilidades das quais decorram interesses conflitantes;

II. A delegação de atribuições deve ser formal, com responsabilidades claramente delimitadas mediante definição de poderes, limites e alçadas, inclusive em relação a serviços prestados por terceiros;

III. Alçadas de aprovação manual ou sistêmica devem ser implementadas quando o processo produz risco relevantes para o negócio, de forma que quem aprova nunca deve ser aquele que executa.



CONSCIENTIZAÇÃO, TREINAMENTO E PRIORIZAÇÃO DAS AÇÕES VOLTADAS A SEGURANÇA DA INFORMAÇÃO

Por ser uma questão corporativa que envolve os aspectos físicos, tecnológicos e humanos que sustentam a operação do negócio, torna-se condição imprescindível o envolvimento e apoio da alta direção nos trabalhos voltados a gestão da segurança da informação. Entende-se por apoio não só a sensibilização e a percepção adequada dos riscos e os problemas associados, mas também a consequente priorização das ações voltadas a:

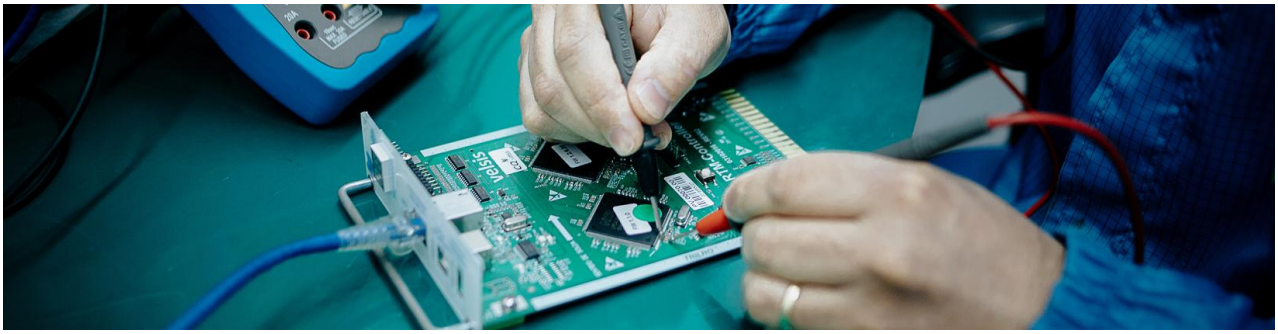
I. Existência de evidências que demonstrem a conscientização dos usuários quanto a necessidade da segurança das informações e aspectos previstos na PSI VELSIS;

II. A capacitação dos usuários em relação à correta e eficiente utilização dos recursos de acordo com as normas e políticas em vigor;

III. A Gestão da PSI VELSIS executada por colaboradores devidamente capacitados para esta função.

CONTINUIDADE DA SEGURANÇA DA INFORMAÇÃO

A continuidade da segurança da informação está orientada pelo procedimento “Plano de Continuidade da Segurança da Informação”.



CONTROLE DE ACESSOS

Na concessão de quaisquer acessos aos recursos físicos ou lógicos da empresa, devem ser observados os princípios do menor privilégio e da segregação das atividades e funções:

I. Os colaboradores e terceiros devem ter acesso físico e lógico liberado somente aos recursos e informações necessárias e indispensáveis ao desempenho de suas atividades e em conformidade com os interesses da companhia;

II. Existência de mecanismos de segurança baseados em sistemas de proteção e segregação de acessos utilizados para resguardar as transações entre redes externas e internas, bem como no uso dos sistemas corporativos;

III. As senhas e outras formas de autenticação devem ser individuais, secretas e intransferíveis, protegidas com grau de segurança compatível e regras de mudanças periódicas de acordo com a informação associada;

IV. Bloqueio ou desativação de todo o serviço (redes, sistemas, softwares, atividades, tarefas entre outros) não explicitamente autorizado pela organização;

V. O acesso às áreas sensíveis deve ser resguardado, preferencialmente por meio do uso de dispositivos de controle de acesso e utilização de câmeras de monitoração;

VI. O acesso de visitantes e colaboradores às dependências da companhia deve ser registrado pelos mecanismos de segurança vigentes, manual ou eletrônica conforme o grau de necessidade;

VII. As câmeras de segurança devem gravar as imagens captadas para posterior análise do pessoal responsável;

VIII. Não isenta de ser responsabilizado o colaborador ou terceiro que ultrapassar as áreas sensíveis o simples fato de estar sinalizado ou informado.

MONITORAMENTO E RASTREABILIDADE

Para garantir as regras mencionadas nesta Política de Segurança, a VELSIS poderá:

I. Implantar sistemas que permitam monitorar e rastrear os eventos ocorridos para dar a resposta aos incidentes de segurança de forma mais rápida;

II. Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

III. Tornar acessível as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Comitê de Segurança da Informação;

IV. Realizar, a qualquer tempo, inspeção física e lógica nas máquinas de sua propriedade;

V. Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

Para tanto, adotará, quando possível, os seguintes procedimentos:

I. Os registros de logs devem ser guardados, quando possível, de modo a auxiliar na identificação de não conformidade de segurança para caráter corretivo, legal e de auditoria;

II. O ambiente poderá ser monitorado, manual ou sistemicamente, a fim de detectar ou prever incidentes ou problemas que gerem riscos para a segurança da informação;

III. Os sistemas corporativos, quando possível, devem conter rotinas que permitam a rastreabilidade das informações incluídas, alteradas ou excluídas.

CONTROLE DE MANUSEIO, TRANSPORTE E DESCARTE DE INFORMAÇÕES

A fim de minimizar o risco de segurança da informação, o manuseio e o transporte das informações devem ser controlados:

I. As informações confidenciais não devem ser divulgadas;

II. As mídias, cópias em papel, quadros, multimídias, ou qualquer outro meio de armazenamento da informação, quando não forem mais necessárias, devem ser descartadas de forma segura, preferencialmente, destruídas ou apagadas antes do descarte propriamente dito.

MESA LIMPA E TELA LIMPA

Para reduzir os incidentes de segurança da informação, é responsabilidade de cada colaborador da Velsis:

I. Descartar os documentos dos respectivos meios de armazenamento que não sejam mais aplicáveis ao negócio, principalmente os documentos confidenciais;

II. Antes do descarte, as informações devem ser destruídas previamente para assegurar que não sejam acessadas por pessoas não autorizadas, independente do meio de armazenamento;

III. Documentos classificados como confidencias não devem ser mantidos sobre as mesas, impressoras ou estações de trabalho;

IV. Não imprimir documentos apenas para a leitura. Preferencialmente, a leitura deve ser feita na tela do seu computador;

V. Mídias removíveis não devem ser mantidas sobre a mesa, devendo ser guardadas em locais seguros;

VI. Manter a tela do computador limpa, ou seja, não devem ser gravados ícones e atalhos na tela do computador que obstrua a imagem do papel de parede padrão Velsis.

PARTES EXTERNAS E CONTRATOS

Os da contratos ou relações jurídicas externas devem preservar a segurança informação considerando que:

I. As cláusulas contratuais devem ser avaliadas criteriosamente para que haja definição clara dos papéis e responsabilidades entre as partes envolvidas, níveis de processamento necessário, segurança, monitoração, requisitos de contingência quando aplicável e necessário para garantir a segurança da informação;

II. Acordos de confidencialidade devem ser firmados para garantir a confidencialidade das informações da companhia;

III. Quando aplicável, a transferência do domínio deve ser considerada nas cláusulas contratuais quando ocorrer a falência do parceiro ou fornecedor, de forma a não impactar na integridade ou disponibilidade da informação.

Todas as informações coletadas estão sujeitas ao compartilhamento com autoridades, entidades governamentais ou outros terceiros na hipótese de conflito, ações judiciais e processos administrativos, mediante ordem judicial ou requerimento de autoridades administrativas legalmente competentes.

DOS RECURSOS TECOLÓGICOS

Caberá a área de Tecnologia da Informação definir procedimentos sistêmicos e/ou instruções de trabalho específicos, quando cabíveis.

AUTENTICAÇÕES E ACESSO AOS ATIVOS DE TI

O login e a senha é o seu passaporte para ter acessoao ambiente tecnológico da empresa, incluindo a rede corporativa e acessos aos mais diversos ativos e sistemas. A sua propriedade é única, intransferível e nominal na medida do possível.

É de responsabilidade de cada usuário manter em absoluto sigilo da sua senha pessoal, não sendo permitido a sua divulgação a outrem. Qualquer ação realizada no seu login é de sua inteira responsabilidade.

As senhas, quando possíveis de serem configuradas, deverão seguir o conceito de "senha forte",que inclui letras (A-Z, a-z), números (0-9) e caracteres especiais (@#$#, entre outros). Quando não possíveis de serem configuradas, a utilização de datas de aniversário, datas comemorativas, datas especiais, nomes, apelidos, endereços de residência, telefones e placas de veículos devem ser evitadas.

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

A área de Tecnologia da Informação aplicará a política de senha nos ativos e sistemas, quando cabível e possível, de forma geral, não sendo permitido o direito a exceções por usuários.

A concessão se dá de acordo com a natureza e função que o usuário exerce na companhia. As políticas de restrições de acesso são mantidas pela área de Tecnologia da Informação.

Não é permitido ao usuário acessar ou tentar acessar áreas que não sejam necessários para a execução de suas atividades.

Para preservara confidencialidade e a integridade das informações, é obrigatório o usuário manter o bloqueio da tela da sua estação de trabalho sempre que não estiver no local.

Acesso a sistemas de informação

A garantia da confidencialidade, integridade e disponibilidade geradas pelos sistemasde informação da companhia deve ser mantida pelos responsáveis dos processos ou sistemas que geram, manipulam e transmitem estas informações.

O acesso a estas informações deve ter o consentimento do Owner do processo ou sistema que gera ou gerou tais informações - somente ele tem a autonomia para conceder ou não o acesso. Para esta concessão deve ser observada a premissa básica de segregação de função e/ou atividade.

O processo de concessão de acesso está definido na PS – A.9-01 – Controle de Acessos.

Acesso a Banco de Dados

O acesso aos bancos de dados deve ser restrito as pessoas autorizadas e inerentes ao cumprimento de suas atividades. A concessão de acesso às informações contidas nos bancos de dados deve ser autorizada com base na regra de menor privilégio necessário para o desempenho da função.

Quando possível, é necessário que sejam criados logs nas intervenções para consulta ou manipulação de dados realizados nos bancos de dados, principalmente se o nível de privilégio concedido ao usuário em questão for alto.

Concessão de Acesso a Serviços Específicos

Compreende-se como acesso a serviços específicos aqueles que não fazem parte do dia a dia do colaborador, tais como VPN, administrador local da máquina, entre outros. Estes serviços precisam ser liberados de forma exclusiva e específica.

A autorização para a liberação é feita pelo gestor do colaborador conforme o procedimento de concessão de acessos. Quando este tipo de acesso for liberado, tanto o colaborador como gestor passam a ser diretamente responsáveis (custodiante) pelas informações produzidas ou manipuladas, independentemente de onde o colaborador se encontre fisicamente. Nestes casos, aplicam-se integralmente as regras de segurança da informação descritas neste documento.

Mesmo se tratando de concessão de acesso ao administrador local da máquina,o colaborador não está autorizado a instalar softwares sem licenças ou ilegais, realizar varredurana rede corporativa, utilizar o equipamento para fins diferentes, alterar a configuração do equipamento ou realizar intervenções que estejam fora das regras descritas na política de segurança da informação.

CORREIO ELETRÔNICO

A empresa disponibiliza cotas específicas de e-mail, podendo sofrer revisões a qualquer instante. O uso do correio eletrônico é destinado única e exclusivamente para fins profissionais e assuntos inerentes aos negóciosda companhia. A organização, o sigilo, o manuseio e o descartesão de inteira responsabilidade do usuário.

O domínio principal do e-mail corporativo é "@velsis.com.br". No entanto, conforme a necessidade da organização, é possível definir outros domínios.

A VELSIS, reserva-se o direito de monitorar qualquer conta de e-mail, a qualquer instante, com ou sem comunicação prévia, por razões legítimas de negócio, inclusive em razão da presente PSI VELSIS, para identificar situações em que haja suspeita de atividades que violem essa política. O conteúdo da mensagem de e-mail corporativo pode ser revelado sem a permissão do usuário.

As mensagens transitadas por este meio não devem ser profanas, vulgares, difamatória ou embaraçosa, de qualquer cunho discriminatória, seja racial, religiosa sexual dentre outras.

Informações de cunho confidencial (informações sensíveis) não devem ser enviadas via e-mail sem a devida proteção para fora da organização. Todos os usuários devem reconhecer que as informações transmitidas via e-mail podem conter segredos técnicos, comerciais ou informações confidenciais, e que devem ser tomadas as providências cabíveis para proteger a segurança de tais informações.

Não é permitido a utilização de e-mail particular dentro da rede corporativa da VELSIS (exemplo: gmail, hotmail, outlook entre outros). Exceções deverão ser tratadas a parte, para fins específicos e profissionais de interesse da VELSIS, com a devida autorização do gestor responsável pelo colaborador ou terceiros, desde que não se contraponha a esta política.

Assinatura do e-mail

O correio eletrônico (e-mail) deverá ser postado sempre com a assinatura corporativa padrão definida pela área de Tecnologia da Informação que deve conter:

I Nome do Colaborador

II Departamento ou Área

III Endereço do Local de Trabalho

IV Telefone de Contato (incluir o celular se for corporativo)

V Cargo do Colaborador conforme registro do empregado

VI Logo da Empresa

VII Logo de Certificações e Premiações

A companhia reserva-se no direito de, a qualquer momento, alterar o formato ou a forma de apresentação da assinatura.

Restrições no uso do e-mail

Para o uso dos serviços de e-mail, são vedados:

I Uso de programas de computador que enviem sistematicamente uma grande quantidade de mensagens através do servidor de e-mail corporativo da companhia;

II Envio de mensagens não solicitadas a múltiplos destinatários utilizando o servidor de e-mail da companhia; a menos que verificado e autorizado pontualmente pela área de Tecnologia da Informação com o objetivo de preservar que o domínio da VELSIS seja caracterizado e incluída nas mais diversas "listas negras";

III Forjar quaisquer informações do cabeçalho do remetente ou enviá-las anonimamente. A identificação do usuário remetente é sempre obrigatória

IV Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a VELSIS ou suas unidades vulneráveis a ações civis ou criminais;

V Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa concedida pelo proprietário desse ativo de informação;

VI Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas nesta política;

VII Apagar mensagens de e-mail quando qualquer uma das unidades da companhia estiver sujeita a algum tipo de investigação;

Ainda, é proibido:

Produzir, transmitir ou divulgar mensagem que:

I Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da companhia;

II Contenha arquivos com extensão: .exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf; ou qualquer outra extensão que represente um risco à segurança da informação;

III Contenha ameaças eletrônicas a segurança da informação, como: spam, mail bombing, vírus de computador;

IV Vise interromper um serviço, servidores ou rede de computadores, equipamentos de modo geral, por meio de qualquer método ilícito ou não autorizado;

V Vise obter acesso não autorizado a outro computador, servidor ou rede, senha de usuários, informações armazenadas nos meios eletrônicos;

VI Vise intervir em qualquer sistema de segurança da informação da Velsis;

VII Vise vigiar secretamente ou assediar outro usuário, colaborador, terceiros ou qualquer pessoal de forma geral;

VIII Vise acessar informações confidenciais sem explícita autorização do proprietário;

IX Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;

X Inclua imagens criptografadas ou de qualquer forma mascaradas que não façam parte do negócio ou atividade do usuário;

XI Tenha conteúdo considerado impróprio, ilícito, falso ou obsceno;

XII Tenha caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico, discriminatório entre outros;

XIII Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas pela lei;

XIV Tenha fins políticos locais ou do país (propaganda política);

XV Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

EQUIPAMENTOS DE USUÁRIO FINAL (ESTAÇÕES DE TRABALHO)

Os equipamentos (desktops, notebooks, impressoras, tablets, celulares entre outros) necessários para execução das atividades profissionais são disponibilizados pela VELSIS.

O tempo de vida útil de cada equipamento está diretamente ligado aos cuidados que cada usuário dispensa ao seu equipamento. Cabe a cada usuário zelar pelo bom uso do equipamento que a VELSIS disponibiliza para o desempenho das suas atividades e funções. Caso seja constatado que houve algum dano por imprudência ou imperícia no uso dos equipamentos, a VELSIS reserva-se o direito de solicitar reembolso por parte do funcionário, colaborador ou terceiro.

Cabe única e exclusivamente a VELSIS a escolha do tipo (desktop, notebook, tablets entre outros), modelo, fabricante, configuração, tamanho, características de cor, sistema operacional, softwares básicos dos equipamentos para o uso do colaborador, não sendo permitido que o usuário escolha tais características.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento da área de Tecnologia da Informação, ou de quem este departamento determinar.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos devem ser realizadas quando solicitadas manualmente ou automaticamente pela área de Tecnologia da Informação.

Os computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. Independentemente do nível de privilégio liberadopara o colaborador, é proibida o bloqueio ou desativação do antivírus. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar a área de Tecnologia da Informação mediante registro de chamado.

Ainda, por livre iniciativa, é vedado ao usuário, sem a devida anuência ou acompanhamento de um profissional da área de Tecnologia da Informação, realizar as seguintes intervenções:

I. Realizar a manutenção nos ativos de TI;

II. Conectar dispositivos não autorizados (roteadores, sniffers, equipamentos de wifi, switches, rubs entre outros) no sistema de rede interna da VELSIS;

III. Intervir no sistema de cabeamento lógico da rede de computadores da VELSIS;

IV. Intervir nos servidores corporativos disponibilizados em áreas específicas e sinalizadas;

V. Conectar rede móvel (3G, 4G, 5G) no computador que está ligado à rede corporativa da VELSIS;

VI. Conectar equipamentos não autorizados em qualquer outro ativo que compõe a estrutura corporativa de tráfego e armazenamento de informações da VELSIS;

VII Alterar propriedades de rede, compartilhamentos, permissões de acesso, configuração de navegadores internet, itens do painel de controle, configuração de impressoras entre outros;

VIII Instalação, desinstalação e configuração de hardware (placas, periféricos, acessórios entre outros).

E ainda, é proibido:

I Manter dados e informações referentes a sua atividade armazenadas no equipamento de usuário final (computadores, notebooks e smartphones). Os documentos eletrônicos (planilhas, documentos, dados, arquivos entre outros) devem ser guardados nos meios de armazenamento que a empresa definir conforme o procedimento de Controle de Documentos Eletrônicos;

II Armazenar dados e informações eletrônicas pessoais no equipamento de usuário final que a empresa destinou para a sua atividade;

III Utilizar a conta individual (conta de e-mail que a empresa concede ao colaborador) do pacote office para armazenar dados ou informações no OneDrive ou SharePoint. Os dados e informações da empresa devem ser armazenadas conforme orientações definidas no procedimento de Controle de Documentos Eletrônicos;

IV Alterar a configuração ou a aparência do papel de parede padrão configurada para o seu equipamento de usuário final.

Com objetivo de evitar alterações indevidas em configurações no parque de ativos de TI ou adequar os equipamentos de usuário final as regras estabelecidas nesta política, a área de Tecnologia da Informação se reserva o direito de aplicar restrições ou alterações de configuração em todo ou partes do conjunto de ativos de TI da VELSIS, a qualquer instante, sem prévio aviso. Estas alterações podem ser executadas manualmente ou automáticas através de regras implementadas da rede interna da Velsis. Qualquer exceção deve ser tratada a parte desde que não se contraponha a esta política.

Uso de Mídia Removíveis

É vetado o uso PENs Drivers ou qualquer dispositivo secundário de armazenamento tais com gravador de CD/DVD, HD externo entre outros.

Excepcionalmente, para os usuários ou atividades que necessitem do uso de tais dispositivos, é necessária a aprovação prévia do gestor responsável. A partir deste momento, o gestor e o colaborador passam a ser responsáveis para garantir a segurança da informação observando todas a regras contidas neste documento.

Informação confidencial ao negócio deve ter tratamento especial de forma a evitar qualquer risco de vazamento, devendo estar preferencialmente em formato criptografado.

A concessão de acesso para uso destes dispositivos é orientada pelo Procedimento de Controle de Acesso.

Equipamento de Terceiros

É vedado ao Terceiro conectar-se à rede de computadores da VELSIS, salvo com autorização da área de Tecnologia da Informação.

Mesmo com a autorização, caso utilize equipamento próprio,não poderá ser conectado no sistema de gerenciamento da rede da Velsis, por exemplo, Active Directory.

O contrato de prestação de serviços deve prever situações em que o terceiro utilize o seu próprio equipamento ou da empresa contratada.

As situações mínimas que devem cumpridas:

I Versão paga e atualizada do antivírus no equipamento;

II Proibição de utilização de software intrusivo na rede, como por exemplo o Sniffer. Salvo situação especial em que a empresa contratante solicite um trabalho específico que obrigatoriamente necessite de tais softwares. Neste caso, somente com autorização da área de Tecnologia da Informação;

III Proibição em conectar o computador a qualquer ponto da rede interna da VELSIS sem a devida autorização da área de Tecnologia da Informação;

IV Utilizar uma rede móvel (3G, 4G ou qualquer outra tecnologia) conectado ao equipamento e ao mesmo tempo a rede da VELSIS;

V Conectar equipamentos em qualquer outro ativo que compõe a estrutura corporativa de tráfego de informações da VELSIS.

Retirada de Ativos de TI da empresa

Não é permitida a retirada dos equipamentos e ativos da empresa, com exceção de dispositivos móveis que são regidos por políticas específicas, sem a devida autorização da área de Tecnologia da Informação. Cabe a área de Tecnologia da Informação certificar se todas as informações da Velsis armazenadas nos equipamentos estão devidamente protegidas ou excluídas antes de liberar para a retirada. Para preservar a segurança da informação, a área de Tecnologia da Informação poderá executar o procedimento de formatação do equipamento antes da retirada.

Preparado o equipamento para a retirada, não é permitido ao usuário nenhum procedimento de instalação ou cópia de novos softwares ou dados.

Durante o transporte ou manuseio de o equipamento ocorrer qualquer tipo de avalia ou quebra da segurança da informação, o usuário deve comunicar imediatamente a Área de Tecnologia da Informação para as devidas providências.

A política de segurança da informação vigora em todo o trajeto por onde este equipamento transitar. O Gestor e o colaborador passam a ser custodiantes do ativo enquanto o equipamento estiver em trânsito.

O equipamento deve ser devolvido a VELSIS em igual condição que foi retirado. Qualquer dano causado ao equipamento deve ser ressarcido.

Nota: Para maiores detalhes ver procedimento “PS–A.11.2.5-01 - Controle Retirada de Ativos de TI”.

USO DE INTERNET

A internet é uma ferramenta de comunicação e colaboração disponibilizada pela empresa para uso exclusivamente profissional. A VELSIS se reserva o direito de monitorar todos os acessosrealizados pelos seus colaboradores e terceiros. Para os colaboradores, a empresa faculta o direito de ações disciplinares ou punitivas sempre que detectada a violação de regras estabelecidas, de acordo com o Manual de Integração do Colaborador. Para terceiros, o contrato de prestação de serviços deverá prever cláusulas específicas de boas condutas de uso de recursos tecnológicos da Velsis.

O uso de sites de notícias é permitido somente para fins profissionais.

Apenas os colaboradores autorizados pela organização poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendoatender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal, à Lei Geral de Proteção de Dados Pessoais (LGPD) e demais dispositivos legais aplicáveis

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

Os colaboradores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades na VELSIS e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pelogestor.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos.

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

Não é autorizada a utilização de programas de entretenimento, jogos ou músicas, em qualquer formato.

Materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso da empresa.
Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado à VELSIS ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

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

O não cumprimento da política em relação ao uso da internet recairá na violação da política da segurança da informação cujas penalidades estão dispostas no item 9 deste documento.

ARQUIVOS E PROGRAMAS DE COMPUTADOR

A VELSIS licencia e disponibiliza programas e sistemas de computador na quantidade e versão suficiente para o desempenho das atividades de seus profisisonais de seus colaboradores.

É proibido baixar, gravar ou instalar qualquer tipo de arquivo ou programa de computador não licenciado, mesmo que faça parte da sua atividade profissional. Também é vedadocopiar, no todo ou em partes, livros, artigos, relatórios ou outros documentos, além daqueles permitidos pela lei de direito autoral.

Sobre hipótese alguma é permitido ao usuário instalar programas de computador de origem desconhecida ou não devidamente licenciada pela VELSIS, tornando-se crime de violação das leis de Copyright (fere os direitos autorais do autor do software). Esta conduta sujeitará também ao infrator as medidas disciplinares previstas no item 9 deste documento.

USO DE SOFTWARES DE COMUNICAÇÃO OU MENSAGERIA

Softwares de Comunicação ou Mensageria são ferramentas que facilitam a comunicação e trabalho colaborativo quando bem utilizadas, mas somente as definidas abaixo estão liberadas para o uso.

Microsoft Teams

O seu uso está liberado somente na conta corporativa da empresa. A VELSIS reserva-se no direito de monitorar qualquer troca de mensagens, a qualquer instante, com ou sem comunicação prévia, por razões legítimas de negócio, e inclusive em razão desta própria PSI VELSIS para identificar situações em que haja suspeita de troca de informações que violem essa política. O conteúdo da mensagem trocada ou manuseada pode ser revelado sem a permissão do usuário.

Whatsapp

O MS Teams é a ferramenta padrão de Comunicação e Mensageria da empresa. O uso do Whatsapp é restrito a trocar mensagens curtas que não comprometam a integridade e a confidencialidade da segurança da informação conforme descritos nesta política, não sendo permitido anexar arquivos de qualquer formato, natureza ou conteúdo (documentos, vídeos, fotos entre outros).

Exceção

Excepcionalmente, o whatsapp poderá ser utilizado pelo time de suporte técnico para se comunicar com os técnicos de campo e trocar imagens da situação física dos equipamentos de campo.

Skype

É utilizado nas salas de reuniões em estações próprias e por meio de contas específicas da Velsis.

Exceção

Exceção pode ser adotada pela área de Tecnologia da Informação em atividades ou setores específicos que necessitam de contato com as partes que não possuem ferramentas compatíveis com as adotadas pela Velsis. Neste caso, deverá ser criado uma certa virtual e contas especificas gerenciadas pela área de Tecnologia da Informação.

Hangout

É utilizado nas salas de reuniões em estações próprias e por meio de contas específicas da Velsis.

Zoom

É utilizado nas salas de reuniões em estações próprias e por meio de contas específicas da Velsis.

A VELSIS se reserva o direito de monitorar, sem prévio aviso, qualquer mensagem, dados ou informações trafegadas por estes meios.

As informações armazenadas ou transmitidas por este meio devem seguir as todas as orientações descritas neste documento. O não cumprimento sujeitará ao infrator as medidas disciplinares previstas no item 9 deste documento.

SERVIDOR DE ARQUIVOS

A empresa disponibiliza uma área específica para armazenamento seguro de dados e informações relativas ao negócio da empresa, com o perfil de acesso conforme a função exercida pelo usuário. Somente informações referentes as atividades profissionais do usuário deverão ser armazenadas nesta área.

A restrição de acesso é feita a nível de pastas e subpastas e são invioláveis. Qualquer tentativa de acesso a uma pasta ou arquivo armazenado em outras áreas que não sejam de interesse profissional do usuário é passível de medidas disciplinares, conforme o item 9 deste documento.

As informações armazenadas no servidor de arquivo possuem serviços de contingência para garantir a integridade e disponibilidade das informações.

Esta política de segurança da informação não autoriza ao usuário armazenar informações de domino da VELSIS em locais ou dispositivos particulares.

DISPOSITIVOS MÓVEIS CORPORATIVOS

Uso de dispositivos móveis corporativos serão tratados nos termos e limites definidos em políticas específicas, conforme abaixo indicado:

Uso de celulares corporativos: Política de Uso de Dispositivos Moveis para Fins Profissionais – Celulares.

Uso de Notebooks e Tablets: Política de Uso de Dispositivos Moveis para Fins Profissionais Notebooks e Tablets.

CRIPTOGRAFIAS

Os controles criptográficos serão utilizados para assegurar, dentre outros:

6.6.1 A confidencialidade, a integridade e a autenticidade de informações sensíveis ou críticas que se encontrem armazenadas ou em transporte físico ou eletrônico;

6.6.2 Confirmar a identidade de usuários ou serviços através de sistemas informatizados.

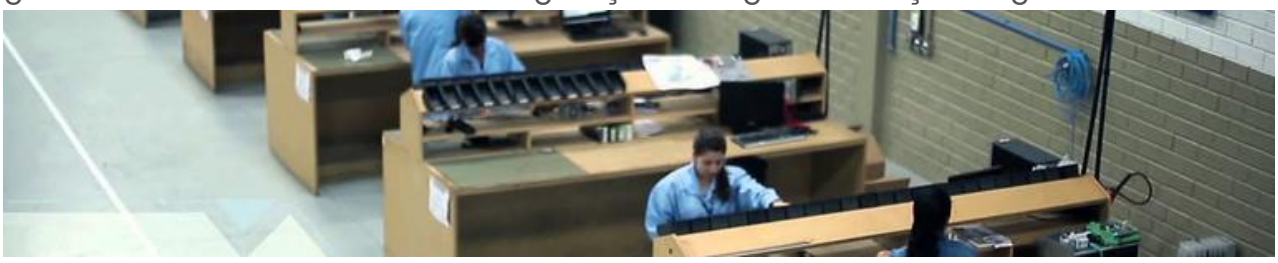
A escolha dos tipos, da qualidade e da força de algoritmos, assim como a definição de que tipo de controle criptográfico é apropriado para cada propósito e processo de negócio, tomará como base, sempre que possível, o resultado do processo de gerenciamento de riscos de segurança da informação.

Um registro de controle relacionando os controles criptográficos, quando aplicável, seus parâmetros e sua aplicação na proteção de informações classificadas serão mantidos e comunicados aos proprietários e custodiantes de ativos de informação.

Orientados pela classificação das informações, documentos de sensibilidade alta, quando armazenadas os dispositivos móveis (notebook, tablet, smartphone entre outros) ou mídias removíveis (cd, dvd, pen-drivers entre outros) devem ser criptografados para evitar a sua divulgação indevida em caso de perda ou furto do equipamento ou da mídia.

Compete aos proprietários (owners) e custodiantes dos ativos de informação aplicar adequadamente os recursos criptográficos identificados para a proteção da informação sobre sua custódia, em conformidade com as determinações deste documento.

Deve-se acionar assessoria jurídica antes de se transferir informações cifradas ou controles de criptografia para além das fronteiras jurisdicionais de modo que esta garanta a conformidade com as legislações e regulamentações vigentes em outros



INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Considera-se um incidente de segurança da informação qualquerevento adverso, confirmado ou sob suspeita, relacionado a segurança de sistemas de computação, aplicações ou redes de computadores.

Em geral, qualquer situação em que um ou mais ativos da informação está(ão) sob risco, é considerado um incidente de segurança da informação.

Na Velsis, os incidentes devem ser documentados via RNC (Registro de Não Conformidade) para a retomada o mais breve possível do(s) serviço(s) prejudicado(s) e a posterior análiseda causa raiz e ações para mitigação posterior.

Para que os incidentes de segurança da informação possam ser notificados o mais rapidamente possível quando de sua ocorrência, a Velsis possui canais de comunicação formais, acessíveis, de fácil utilização, sempre disponíveis e que, preferencialmente, preservam a identidade da pessoa que informou o incidente.

Os canais disponíveis são:

- e-mail corporativo seguranca.velsis@velsis.com.br ,

- sistema de chamados service desk.

A comunicação dos incidentes devem envolver, além do setor de tecnologia da informação, os proprietários (owners) da(s) informação(ões).

EVENTOS VERSUS INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Não se deve confundir eventos com incidentes de segurança da informação. Para tanto, seguem abaixo esclarecimentos sobre as diferenças entre os conceitos com o objetivo de facilitar sua identificação.

Eventos

Evento pode ser definido como qualquer mudança de estado que tem importância para a gestão de um item de configuração (IC) ou serviço de TI. Em outras palavras, qualquer ocorrência dentro do escopo de TI que tenha relevância para a gestão dos serviços entregues ao(s) cliente(s).

Exemplos de eventos (não exaustivo):

I. Um usuário logou no sistema;
II. Um backup agendado não ocorreu;
III. Osistema está sendo acessado pelo dobro de usuários do que o normal;
IV. Um usuário não autorizado acessou um local da rede;
V. Um sistema está mais lento do que o normal;
VI. Excesso de ligações por engano para o Service Desk;
VII. Qualquer outro que tenha relevância para quem está gerindo os serviços de TI.

O evento tem diversas naturezas, sendo categorizadas na seguinte ordem:

I. Por nomenclaturas como normal, não usual, exceção, alerta;
II. Por cores como vermelho, laranja, amarelo e verde;
III. Por criticidade como sendo crítico, tendência de ser crítico, alerta e normal.

A maioria dos eventos possíveis de serem monitorados estão implementados por meio de ferramentas específicas que sofrem melhorias a cada possibilidade de automatização.

Quaisquer outros eventos que vierem a ser detectados devem ser relatados por meio de chamados de TI no sistema de service desk ou qualquer outra ferramenta ou processo que a área de TI disponibilizar.

Incidentes de Segurança da Informação

Diferente dos eventos, os incidentes de segurança da informação são aqueles fatos cujos eventos ocasionaram alguma quebra na segurança da informação.

Assim que é detectado, um evento pode, desde já, ser classificado como um incidente ou não. A depender da natureza do que seja detectado, o processo de gestão de eventos ou de gestão de incidentes deverá tratá-lo.

OBJETIVOS DO PROCESSO

São objetivos da gestão de incidentes de Segurança da Informação:

I. Garantir a detecção de eventos e dar tratamento adequado, sobretudo na categorização destes como incidentes de segurança da informação ou não;

II. Garantir que incidentes de segurança da informação sejam identificados, avaliados e respondidos de maneira mais adequada possível;

III. Minimizar os efeitos adversos de incidentes de segurança da informação (tratando-os o mais brevemente possível);

IV. Reportar as vulnerabilidades de segurança da informação, além de tratá-las adequadamente;

V. Ajudar a prevenir futuras ocorrências, através da manutenção de uma base de lições aprendidas.

CLASSIFICAÇÃO DOS INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Os incidentes de segurança da informação são classificados, não exaustivamente, conforme abaixo:

Acesso não autorizado

São incidentes que afetam a disponibilidade da informação e podem ocorrer principalmente em três situações: (70)

I. Tentativas não autorizadas de acesso;

II. Má utilização de um sistema de informação;

III. Falhas no sistema que impedem um acesso autorizado.

Denial of Service

Significa "ataque de negação de serviço", também conhecido por DoS Attack. Trata-se de uma tentativa em tornar os recursos de um sistema ou aplicação indisponíveis para seus utilizadores, afetando o requisito de disponibilidade da informação. Não significa uma invasão propriamente dita, mas uma invalidação por sobrecarga no sistema.

Vírus de computador ou outros códigos maliciosos

O Vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.

Para que possa se tornar ativo e dar continuidade ao processo de infecção, o vírus depende da execução do programa ou arquivo hospedeiro, ou seja, para que o seu computador seja infectado é preciso que um programa já infectado seja executado.

O principal meio de propagação de vírus costuma ser os meios de armazenamento (discos rígidos, pen-drives, nuvem,memórias flash entre outros) ou ferramentas de troca de mensagens (Skype, teams, e-mail entre outros).

Os códigos maliciosos (malware) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Os códigos maliciosos podem infectar o ativo tecnológico das seguintes formas:

I. Pela exploração de vulnerabilidades existentes nos programas instalados;

II. Pelo auto execução de mídias removíveis infectadas, como pen-drives;

III. Pelo acesso a páginas Web maliciosas, utilizando navegadores vulneráveis;

IV. Pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;

V. Pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas Web ou diretamente de outros computadores (através do compartilhamento de recursos).

Outros códigos maliciosos além do próprio vírus são: Worm, Bot, Trojan, Spyware, Backdoor, Rookit entre outros. Uma vez instalados, os códigos maliciosos passam a ter acesso aos dados armazenados no computador e podem executar ações em nome dos usuários, de acordo com as permissões de cada usuário afetando a segurança das informações.

Uso Impróprio

Este tipo de incidente ocorre quando um usuário viola as políticas de segurança da informação no uso dos ativos de TI. Não se trata de uma alternativa ou tentativa de ataque, mas sim uma violação da política de segurança da informação, como por exemplo: uso de e-mail corporativo para spam ou promoção de negócios pessoais, instalação e utilização de ferramenta não autorizada, uso de pen drive de forma não autorizada, impressão ou cópia de documentos não autorizado entre outros.

RESPONSABILIDADE SOBRE A NOTIFICAÇÃO DOS INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Usuários: Terem consciência de que possuem responsabilidades com a notificação, o mais rapidamente possível, de incidentes de segurança da informação e também com os procedimentos utilizados nessa notificação. Notificar e registrar quaisquer fragilidades de segurança da informação, observada ou suspeita, nos sistemas ou serviços através dos canais disponíveis conforme item 7.

Prestadores de Serviços: Terem consciência de que possuem responsabilidades para com a notificação de incidentes de segurança da informação e também com os procedimentos utilizados nessa notificação. Notificare registrar quaisquerfragilidades de segurança da informação, observada ou suspeita, nos sistemas ou serviços.

Obs.: À exceção de pessoas autorizadas, jamais deve-se tentar averiguar os incidentes de segurança por conta própria, pois uma atitude desse tipo, além de poder ser entendida como um uso inadequado do sistema, que pode acarretar sanções previstas no item 9 deste documento contra o realizador destas ações, pode acabar provocando outros incidentes de segurança.

GESTÃO PARA INCIDENTES E SEGURANÇA DA INFORMAÇÃO

A gestão para os incidentes de segurança da informação será detalhada na PS-A.16-01 – Gestão de Incidentes de Segurança da Informação.

DOS DEVERES E RESPONSABILIDADES

DEVERES E RESPONSABILIDADES DOS COLABORADORES

Os colaboradores devem:

I. Preservar a integridade e manter sigilo absoluto sobre as operações, dados, informações, materiais, documentos, arquivos, procedimentos internos, especificações técnicas e comerciais, inovações e aperfeiçoamento tecnológicos e comerciais da VELSIS, incluindo todos os recursos de processamento de informações manuais ou sistêmicos que tenha ciência cujo acesso lhe tenha sido confiado;

II. Cumprir as determinações desta Política, sob pena de incorrer nas sanções disciplinares e legais cabíveis conforme o item 9 deste documento;

III. Responder por todo e qualquer acesso aos recursos tecnológicos ou manuais, bem como pelos efeitos desses acessos efetivados através do seu código de identificação, sua chave, ou outro atributo para esse fim utilizado;

IV. Utilizar recursos e sistemas de informações da VELSIS somente para os fins profissionais, independentemente do local onde for manuseado;

V. Comunicar e manter o registro a área de Tecnologia da Informação, o conhecimento de qualquer irregularidade ou desvio por meio de canais disponíveis.

DEVERES E RESPONSABILIDADE DOS DIRETORES E GESTORES

Os Diretores e Gestores devem:

I. Preservar a integridade e manter sigilo absoluto sobre as operações, dados, informações, materiais, documentos, arquivos, procedimentos internos, especificações técnicas e comerciais, inovações e aperfeiçoamento tecnológicos e comerciais da VELSIS, incluindo todos os recursos de processamento de informações manuais ou sistêmicos que tenha ciência, acesso o que lhe tenha sido confiado;

II. Gerenciar o cumprimento da Política de Segurança da Informação por parte de seus liderados e terceiros;

III. Disseminar o conteúdo da Política de Segurança da Informação sempre que cabíbel, bem como fomentar que seus liderados observem as regras estabelecidas neste documento;

IV. Identificar eventuais desvios praticados e adotar as medidas e ações corretivas adequadas para o negócio;

V. Impedir o acesso de empregados demitidos ou com acessos desnecessários aos ativos de TI, utilizando-se dos mecanismos de desligamento do usuário através de bloqueio destes acessos sobre sua responsabilidade;

VI. Garantir o uso adequado dos ativos de informação relacionados com o seu escopo de atuação e responsabilidade;

VII. Garantir que os seus liderados compreendam e assimilem a obrigação de proteger as informações da organização;

VIII. Comunicar formalmente a concessão de privilégios a usuários de Tecnologia da Informação e Sistema Corporativos, quais acessos e permissões devem ser concedidos aos colaboradores e terceiros sob a sua liderança;

IX. Comunicar formalmente a retirada de privilégios a usuários de Tecnologia da Informação e Sistema Corporativos, informando quais acessos ou permissões devem ser retirados de colaboradores ou terceiros demitidos sob a sua liderança.

DEVERES E RESPONSABILIDADE DOS PRESTADORES DE SERVIÇOS

Os Prestadores de Serviços devem:

I Preservar a integridade e manter sigilo absoluto sobre as operações, dados, informações, materiais, documentos, arquivos, procedimentos internos, especificações técnicas e comerciais, inovações e aperfeiçoamento tecnológicos e comerciais da VELSIS, incluindo todos os recursos de processamento de informações manuais ou sistêmicos que tenha ciência, acesso o que lhe tenha sido confiado, mesmo que não tenha sido previsto no contrato entre as partes.

II Prever nos contratos, cláusulas que contemplem a responsabilidade dos terceiros ou prestadores de serviço no cumprimento da Política de Segurança da Informação da Velsis;

III Incluir nas atividades do dia a dia, o cumprimento das regras e normas constantes na Política de Segurança da Informação da Velsis, independente onde o recurso esteja alocado.

DAS PENALIDADES

O descumprimento total ou parcial destapolítica impõe ao colaborador ou terceiros, as medidas abaixo relacionadas:

O colaborador é responsável pelo tratamento, integridade e pelo sigilo das informações recebidas sejam de maneira interna e/ou externa, de outras companhias ou partes interessadas, sendo que qualquer tentativa de violações ou infrações cometidas pelos colaboradores em relação a integridade e confidencialidade da informação estarão sujeitas a aplicação de penalidades administrativas e/ou legais.

Penalidades administrativas:

I Rescisão do contrato de trabalho por justa causa;

II Pagamento ou recomposição de todas as perdas e danos sofridos pela Velsis, inclusive de ordem moral, bem como as de responsabilidade civil e criminal com apuração através de processo administrativo ou judicial.

Penalidades legais:

III Aplicação das penas previstas nos artigos: 152 e 154 do Código Penal Brasileiro; artigo 154-A da Lei No. 12737/12; e art. 52 da Lei 13.709/18 LGPD.

As infrações cometidas por terceiros em relação a Política de Segurança da Informação da Velsis estarão sujeitas as penalidades do artigo 152 e 154 do Código Penal Brasileiro; artigo 154-A da Lei No. 12737/12 e art. 52 da Lei 13.709/18;

É facultado a Velsis impetrar ações de regresso ao colaborador ou terceiro quando cabível.

TERMO DE RESPONSABILIDADE

Eu,_____, devidamente registrado como colaborador ou prestador de serviço da VELSIS, declaro ter conhecimento da Política de Segurança das Informações Velsis – PSI VELSIS, comprometendo-me a cumpri-las de forma plena e integral, estando sujeito a ações disciplinares definidas pelo Depto. de Recursos Humanos.

_____, _____ de _____ de 20__

_____

Assinatura

velsis

APOIO TÉCNICO CIENTÍFICO
PIRONTI ADVOGADOS