DeVivo Castro Advogados

De Vivo, Castro, Cunha e Whitaker Advogados

Política de Segurança da Informação

De Vivo, Castro, Cunha e Whitaker Advogados

São Paulo, 17 de novembro de 2023

Rua Leopoldo Couto de Magalhães Jr. 758 – 10º andar
Itaim Bibi – São Paulo – SP – 04542-000
Tel: 55 11 3048-3266 E-mail: info@devivocastro.com.br
www.devivocastro.com.br

SUMÁRIO

1. Objetivo

O objetivo deste documento é estabelecer os padrões e regras necessários para a elaboração dos controles e dos documentos referentes a Segurança da Informação do **DVC**.

2. Cumprimento e restrições

É obrigação de todos os colaboradores incluídos no âmbito do **DVC** observar o cumprimento desta política, comunicando imediatamente seu superior sobre qualquer dúvida, atividade anormal ou ilícita dentro do ambiente da empresa.

3. Prefácio

3.1. Introdução

DeVivo Whitaker e Castro Advogados – **DVC** contrariando o senso comum, caracteriza-se por ser um escritório de clientes, e não apenas de casos e processos. Com tal filosofia, o escritório elegeu como seu principal foco de atenção o cliente, seja ele pessoa física ou jurídica, bem assim os seus negócios, objetivos e particulares expectativas.

É justamente por conta disso que o escritório procura estar o mais próximo possível de seus clientes, conhecendo-os por inteiro, por dentro e por fora, interagindo com suas áreas, departamentos e demais divisões. É a típica e sincera relação de parceria, verdadeira via de mão dupla, sem a qual se torna impossível desenvolver a moderna advocacia e prestar bom atendimento.

A Política de Segurança descreve em maiores detalhes as normas de segurança do **DVC** por área.

Este documento é de leitura mandatória por todos os empregados e sócios responsáveis pela Segurança de Informações dentro da organização (por ex.: gestores, *Security Officer*, administradores de segurança, coordenadores, auditores entre outros) e **deve** ser entendido e usado como necessário para realizar seus deveres e atribuições dentro da organização.

Um pequeno resumo que pode ser encontrado neste mesmo documento é destinado como a introdução de um documento local planejado para todos os empregados e sócios, este documento **deve** considerar todas as práticas locais (requisitos legais, práticas comuns, entre demais aspectos). É de responsabilidade do **Departamento de Segurança da Informação** assegurar que qualquer versão

contenha tanto quanto possível as condições normativas, contratuais e legais, bom como práticas de mercado adotadas.

Este é um documento de política e como tal não provê detalhes de implementação.

3.2. Escopo

Esta política é mandatória para a segurança dos processos de negócio interno e externos (relacionados com o cliente) do **DVC** e se aplica a todos os empregados, sócios, fornecedores e consultores em todo **DVC**.

A política é aplicada a todas as formas intelectuais e físicas de ativos da informação tanto próprios, como usados ou mantidos em custódia pelo **DVC**. Estas formas incluem *hardware*, redes, *software* e dados, tanto armazenados e processados em computadores, transmitidos através de redes, impressos ou escritos, enviados por fax, armazenados em mídias removíveis (por ex.: CDROM, fitas, Dispositivos de armazenamento conectados em interface USB) ou falados em conversas e ligações telefônicas ou postadas na Internet, como por exemplo em redes sociais, chats, *wikis* ou assemelhados.

3.3. Arquitetura da Segurança

Para permitir uma abordagem estruturada para a Segurança de Informações foi definida uma arquitetura em camadas. A estrutura consiste nos seguintes elementos:

3.3.1. Política de Segurança da Informação

Nesta política os objetivos globais de Segurança da Informação do **DVC** são definidos através de um conjunto de normas de segurança. A política demonstra o compromisso do **DVC** com a Segurança de Informações. **Deve** ser vista como uma referência a todas as decisões relacionadas à segurança.

3.3.2. Controles de Segurança de Informações

Os controles de segurança consistem em um conjunto amplo de medidas de segurança, compreendendo práticas de segurança comuns, e são necessários para implementar a política de segurança do **DVC**. Os controles de segurança são baseados na norma de segurança aceita internacionalmente (ISO 27001, ISO 27002, Código de Prática para Gestão da Segurança de Informações, entre demais referências normativas e boas práticas de mercado).

3.3.3. Padrões, Diretrizes e Procedimentos de Segurança de Informações

Esta camada consiste de um conjunto de normas técnicas, procedimentos e diretrizes detalhadas para apoio adicional na implementação da política de segurança. Por exemplo: em uma plataforma específica ou em um serviço específico são descritos os passos para gestão de uma ferramenta de segurança.

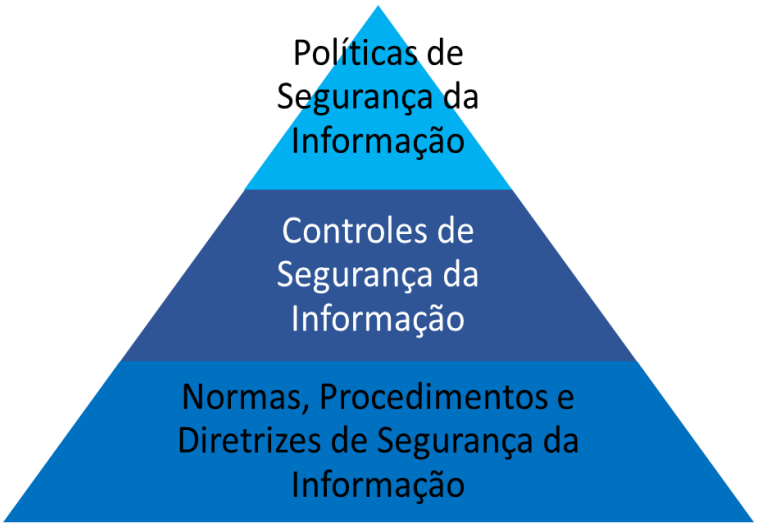

*Figura 1 - Arquitetura de Segurança do **DVC***

3.4. Terminologia e Conceitos de Segurança da Informação

A Segurança de Informações salvaguarda a confidencialidade, integridade, disponibilidade, autenticidade, legalidade e não-repúdio da informação e sistemas da informação. Estes aspectos têm o seguinte significado:

- **Confidencialidade**: A Informação não é disponibilizada ou divulgada a indivíduos, entidades ou processos não autorizados.
- **Integridade**: É compreendida por:
  - Integridade de dados: Dados não são alterados ou destruídos de forma não autorizada.
  - Integridade de Sistemas: O sistema executa a sua função da maneira prevista, sem que haja manipulações deliberadas ou acidentais não autorizadas.
- **Disponibilidade**: Ativos que são acessíveis a partes autorizadas nos momentos apropriados.
- **Autenticidade**: É um processo que se estabelece a validade.
- **Legalidade**: A informação é armazenada, transmitida, acessada e retida de acordo com os termos legais existentes.
- **Não-repúdio:** São as partes envolvidas em uma transação que são capazes de provar, posteriormente, o que aconteceu.

Sempre que o termo ‘colaboradores’ (ou ‘colaboradores do **DVC**’) é mencionado nesta política, significa todos os empregados e sócios do **DVC** incluindo fornecedores e funcionários temporários. Neste documento todas as entidades de negócio dentro do **DVC** são chamadas de ‘organizações’ e os gestores que são responsáveis por elas são chamados de ‘gestão de linha’ (ou ‘gerentes de linha’).

3.5. Procedimento de Exceções à Política

Todos os itens descritos como “**deve**”, “**devem**”, “**deverão**” ou “**deverá**” são mandatórios e estão relacionados principalmente a requisitos estatutários ou mínimos. Itens rotulados como “recomendável” são vistos como boas práticas e normalmente **devem** ser cumpridos. Exceções **não devem** colocar em risco outras partes do **DVC,** seus clientes ou fornecedores e ser formalmente aprovadas conforme alçadas de risco.

3.6. Propriedade, Manutenção e Análise crítica

Os sócios seniores do **DVC** é proprietária desta política de Segurança de Informações. O **Departamento de Segurança da Informação** é responsável pela gerência dos aspectos de segurança da informação e conta com a ajuda de organizações operacionais e de todos os colaboradores do **DVC**. **Esta política será revisada anualmente** ou no caso de uma alteração maior.

A Gestão de Segurança valoriza suas opiniões e sugestões; após receber o parecer do *Security Officer* local, quaisquer observações a esta política de segurança ou sugestões para sua melhoria **devem** ser encaminhadas para o **Departamento de Segurança da Informação** através do correio eletrônico: **compliance@dwca.com.br**.

4. Declaração da Política de Segurança da Informação

4.1. Objetivo

O objetivo da Segurança da Informação é assegurar a continuidade do negócio e minimizar danos causados pelo impacto de incidentes de segurança.

- A finalidade da Política de Segurança da Informação é proteger os ativos de Informação do **DVC** e seus respectivos clientes, conforme firmado em contrato, contra todas as ameaças, sejam elas internas ou externas, propositais ou acidentais.
- A Política de Segurança da Informação se aplica a todos os colaboradores do **DVC**, incluindo fornecedores, contratados e recursos temporários e a todas as informações, sejam elas de propriedade do **DVC**, mantida sob sua custódia para os clientes ou utilizadas pelo **DVC**.
- É Política da empresa assegurar que:
    - As informações serão protegidas contra acesso não-autorizado;
    - A confidencialidade das informações será assegurada;
    - A Integridade das informações será mantida;
    - Requisitos do negócio quanto à disponibilidade da informação e sistemas serão atendidos;
    - A Gestão de Risco será executada para identificar e avaliar riscos de segurança para que medidas apropriadas possam ser adotadas;
    - A classificação de ativos de informação será aplicada;

- Requisitos legais e regulatórios do país, bem como requisitos contratuais de segurança, serão atendidos; e
- Treinamento em Segurança de Informações é mandatório para todos os colaboradores.

- O **Departamento de Segurança da Informação**, é responsável por garantir a segurança e a organização de segurança dentro do **DVC**. Tal departamento é diretamente responsável por manter a Política de Segurança, metas anuais de segurança e prover aconselhamento e assistência em sua implementação. Para esta missão ele conta com uma estrutura global de apoio.
- Padrões, procedimentos e diretrizes adicionais **deverão** ser elaborados localmente para apoiar a implementação da política global de acordo com a legislação local. Estas regras definem o nível mínimo de conformidade para todos os funcionários sobre Segurança da Informação.
- Todos os gestores são diretamente responsáveis pela Implementação da Política dentro de suas áreas de negócio e pela adesão a mesma pelas suas equipes.
- É responsabilidade de cada funcionário aderir à Política de Segurança da Informação e aos padrões, procedimentos e diretrizes relacionados. Violações podem resultar em ações disciplinares, até e inclusive demissão.
- Todos os colaboradores **devem** reportar violações de Segurança de Informações, reais ou potenciais, ao seu gestor ou ao *Security Officer*. No caso de um incidente de segurança ações imediatas **devem** ser tomadas para reduzir os riscos e impactos de danos para o **DVC** e nossos clientes.
- Exceções a esta Política de Segurança da Informação requerem aprovação do **Departamento de Segurança da Informação.**
- Nesse contexto, os domínios de segurança lógica e segurança física (pessoas e sites) contribuem para reforçar a proteção das informações.

5. Política de Segurança da Informação

5.1. Organização

5.1.1. Gestão da Segurança da Informação

Uma estrutura de gestão **deve** ser estabelecida para iniciar e controlar a implementação de Segurança de Informações dentro do **DVC**. Os sócios seniores do **DVC devem** aprovar e apoiar os desenvolvimentos da política de segurança, avaliações de normas de segurança e implementação de segurança dentro da companhia.

Uma organização de gestão de segurança corporativa foi estabelecida, o **Departamento de Segurança da Informação,** com a tarefa de promover boas práticas de Segurança de Informações em toda o DVC e é responsável por ajudar gestores, usuários, colaboradores de TI e outros a cumprir suas responsabilidades de Segurança de Informações.

Os Gestores da empresa no País e/ou Filial ou do Grupo de Serviço pertencentes ao **DVC** são responsáveis pela Segurança da Informação dentro de seu campo de autoridade. É recomendável que cada grupo de serviço e organização de país tenha uma função de gestão de segurança, responsável pela coordenação da política de segurança tanto para serviços de clientes internos como externos do **DVC**.

Gestores são responsáveis pela Segurança de Informações dentro de suas próprias áreas de responsabilidade. Medidas **devem** ser tomadas para coordenar a atividade de Segurança de Informações dentro de sua área de negócios.

É responsabilidade de cada membro dos colaboradores do **DVC** estar em conformidade com esta política.

5.1.2. Cooperação com Terceiros (Parcerias, Joint Ventures, Fornecedores, Contratados)

Sempre que o **DVC** entrar em parcerias, *joint ventures, insourcing* ou outros acordos com terceiros, é recomendável realizar uma análise de risco com relação a questões de segurança. Esta análise de risco fornecerá os controles e procedimentos de segurança, que **devem** ser acordados e definidos em um contrato seguindo os controles de negócio normais deste tipo de acordo.

Contratos do **DVC** com fornecedores **devem** incluir uma cláusula declarando que seus funcionários estarão em conformidade com a política, padrões e procedimentos de segurança. É responsabilidade da gestão local, assegurar que

funcionários que não pertençam a empresa são informados sobre a política de segurança.

5.1.3. *Outsorcing* de Atividades do DVC para Terceiros

Outsourcing de sistemas de informação ou processos de negócios necessitam de uma análise de risco. Esta análise indicará os controles e procedimentos a serem implementados no contrato.

5.1.4. Níveis de Segurança

É meta o **DVC** entregar aos seus clientes serviços de alta qualidade. Assim um nível de segurança básico **deve** ser incorporado aos serviços entregues pelo **DVC**. É recomendável que este nível de segurança básico seja consistente com "controles de segurança geralmente aceitos" para serviços de TI. É recomendável que o "nível de segurança básico" de um serviço seja definido e documentado nas Descrições de Serviço do **DVC** mantidas pela organização, países ou departamentos de entrega de serviço.

Quando a infraestrutura, instalações e recursos de TI do **DVC**, são compartilhados entre clientes múltiplos, o nível de segurança básico será o nível mínimo. Este nível não pode ser reduzido, porque isto pode comprometer o nível de segurança de outros clientes.

Se uma organização tem *outsourcing* ou recursos conjuntos de seus serviços de TI para com o **DVC**, o nível de segurança de recursos compartilhados **deve** ser levado até pelo menos ao "nível básico de segurança" do **DVC**.

Para atender os requisitos dos clientes, níveis adicionais de segurança podem ser selecionados para prover serviços de segurança estendidos aos clientes, com um custo adicional.

É recomendável que o nível de segurança de serviços globais entregues pelo **DVC** tenha um padrão mínimo acordado em cada grupo local de entrega.

5.1.5. Criação de serviço

Quando o **DVC** estiver desenvolvendo novos serviços, uma análise dos riscos e requisitos de segurança **deve** ser realizada. Como parte do processo de criação, é recomendável que os níveis de segurança básicos do **DVC** e possivelmente de níveis estendidos para este novo serviço, sejam declarados nas descrições de serviços do **DVC**.

O DVC irá considerar em suas análises de risco, questões relacionadas às etapas de identificação de riscos, análise e avaliação de riscos, tratamento dos riscos, monitoramento e comunicação dos riscos em acordo às normas ISO 27005 e ISO 31000, e, aspectos relacionados à mensuração dos níveis de risco, critérios de risco e o respectivo apetite ao risco de acordo com critérios estabelecidos pelo DVC

5.1.6. Contratos

Boas práticas de segurança são frequentemente o resultado da cooperação entre o **DVC**, seus clientes e outros fornecedores. Portanto, as responsabilidades de todas as partes para o nível de segurança acordado **devem** ser descritas em propostas iniciais, contratos resultantes e Acordos de Nível de Serviço.

Se, a pedido de um cliente, o nível de segurança a ser implementado para um serviço em particular for inferior ao nível básico de segurança do **DVC**, o nível de segurança acordado e as tarefas e responsabilidades do **DVC** e do cliente **devem** ser explicitamente declarados no contrato ou acordo de nível de serviço. Também será adicionado que os riscos correspondentes são de inteira responsabilidade do Cliente e que o **DVC** é dispensado de qualquer responsabilidade resultante dessa implementação. Como resultado, o **DVC** será formalmente dispensado de suas obrigações de fornecer um nível básico de segurança para estes serviços. Reduzir o nível de segurança para um cliente nunca pode levar risco a outros clientes e, portanto, pode exigir algumas medidas adicionais.

Quando o **DVC** adquire novos contratos de *outsourcing* ou de recursos conjuntos, o nível de segurança do ambiente do cliente **deve** ser analisado criticamente e avaliado como parte do *due diligence*. O nível e riscos de segurança **devem** ser claramente documentados antes dos contratos serem formalizados.

5.2. Classificação

5.2.1. Propriedade

Para manter a proteção adequada de ativos, todos os ativos mais importantes **devem** ser inventariados (*hardware* e *software*) e ter um proprietário nomeado (*hardware*, *software* e informação). Colaboradores específicos, envolvidos na operação dos processos de negócio da companhia, que possuem habilidades específicas, conhecimento e experiência de difícil substituição, também pode ser

considerado como um dos ativos importantes e **devem** ser identificados em um plano de sucessão.

5.2.2. Classificação da Informação

Para assegurar que a informação recebe um nível adequado de proteção, é recomendável que seja classificada de acordo com o padrão de classificação do **DVC**, para ocorrer o nível adequado de proteção.

Na criação da informação, o criador da mesma é responsável por sua classificação imediata. O proprietário da informação é responsável pela correta classificação e é recomendável que analise criticamente a classificação de acordo com procedimentos de controle de documentos do **DVC**. Maiores informações disponíveis no documento **PSI 002 - Política de Classificação da Informação**.

O Colaborador ou Terceiro **deverá** consultar o **Departamento de Segurança da Informação** caso haja qualquer dúvida a respeito da classificação de uma informação pela sua sensibilidade.

5.2.3. Salvaguarda de Registros da Companhia

Registros importantes da companhia **devem** ser protegidos contra perda, destruição e falsificação. Alguns registros podem necessitar de retenção segura para atender a requisitos estatutários ou regulamentares, bem como apoiar atividades essenciais de negócios.

Exemplos disso são registros que podem ser exigidos como evidência de que uma empresa opera dentro de regras estatutárias ou regulamentares, ou para assegurar defesa adequada contra ação criminal ou civil potencial, ou para confirmar o status financeiro de uma companhia com relação a acionistas, sócios e auditores. A lei ou regulamentação nacional pode definir o período e conteúdo de dados para retenção de informações. Quando são escolhidos meios eletrônicos de armazenagem, procedimentos para assegurar a capacidade para acessar dados (tanto a legibilidade da mídia quanto do formato) por todo o período de retenção, para salvaguardar contra perda devido à mudança futura de tecnologia.

O sistema de armazenagem e manuseio de registros **deve** assegurar a clara identificação de registros e de seu período de retenção estatutário ou regulamentar. **Deve** permitir a destruição apropriada dos registros após esse período se o **DVC** ou seus Clientes não mais necessitarem deles.

Para atender estas obrigações, os seguintes passos **devem** ser considerados por cada País e/ou departamento:

a. É recomendável emitir diretrizes sobre a retenção, renovação, armazenagem, manuseio e descarte de registros e informações de negócios;

b. É recomendável esboçar um programa de retenção identificando tipos essenciais de registro de negócios e o período de tempo que eles **devem** ser retidos;

c. É recomendável manter um inventário de fontes de informações de negócios-chave; e

d. É recomendável programar controles adequados para proteger registros e informações de negócios essenciais contra perda, destruição, acesso não autorizado e falsificação.

5.2.4. Classificação de Ativos de Clientes

É recomendável que o **DVC** estimule e incentive seus clientes a classificar seus ativos. Esta classificação auxiliará o cliente a tomar decisões sobre medidas de segurança (adicionais) que possam ser necessárias para certas informações, incluindo requisitos de contingência e recuperação.

5.3. Segurança dos Colaboradores

5.3.1. Segurança no Trabalho – Definição e Recursos

5.3.1.1. Triagem de Colaboradores

O recrutamento de colaboradores para cargos sensíveis pode exigir triagem adicional de seus empregos anteriores e referências, de acordo com a natureza da posição a ser preenchida. Isto será conduzido de acordo com a legislação vigente no país. A triagem é responsabilidade da Gerência de Recursos Humanos e aplica-se a todos os colaboradores do **DVC**, contratados e outros funcionários temporários. Maiores informações disponíveis no documento **NSI 002 - Norma de Segurança em Recursos Humanos**.

5.3.1.2. Termos e Condições de Emprego

Os termos e condições de emprego do **DVC devem** incluir uma cláusula com a qual os funcionários estão familiarizados e concordam com a **Declaração da Política de Segurança** do **DVC** (ver Capítulo 4). No caso de uma violação da Política de Segurança, pode ser tomada ação disciplinar. Essa ação pode variar de uma

advertência verbal (com ou sem observação no arquivo pessoal) até e inclusive demissão. A gravidade do incidente **deve** orientar a severidade da ação a ser tomada.

É recomendável que os termos e condições para fornecedores, contratados e funcionários temporários trabalhando para o **DVC** sejam definidos em contratos formais, que especifiquem as condições de segurança necessárias para assegurar a conformidade com a Declaração de Política de Segurança do **DVC**. O contrato **deve** estar estabelecido antes que seja permitido o acesso às instalações, recursos e/ou informações do **DVC**.

5.3.1.3. Acordos de Confidencialidade

Os funcionários do **DVC devem** assinar um acordo de confidencialidade que normalmente é parte de seus termos e condições de emprego.

Fornecedores, contratados e outros funcionários temporários, se não estiverem cobertos por um contrato entre empresas já existente contendo uma declaração de confidencialidade, **devem** assinar um acordo deste tipo, antes de seu emprego e conexão com as instalações do **DVC**.

É recomendável que os acordos de confidencialidade sejam analisados criticamente quando houver alterações nos termos e condições de emprego, particularmente quando funcionários estão em vias de deixar a organização, ou os contratos em vias de expirar.

5.3.1.4. Segurança nas Descrições dos Cargos

É recomendável que as tarefas e responsabilidades de segurança sejam aprovadas pela gestão e, incluídas nas descrições de cargo onde adequado. Assim como as tarefas e responsabilidades relacionadas à segurança consistente com as Políticas de Segurança do **DVC** sejam conhecidas por aqueles envolvidos em gestão de segurança ou na entrega de serviços de segurança e outras partes interessadas.

5.3.1.5. Código de Conduta

O Código de Conduta do **DVC** descrito no documento **Código de Ética e Conduta do DVC** define regras para conduta pessoal, que cada membro da equipe é recomendado a seguir e **deve** incluir segurança e questões relacionadas.

5.3.1.6. Encerramento de Contrato de Emprego

Quando um membro da equipe deixa o **DVC**, o gestor é responsável por assegurar que ele ou ela devolvam tudo o que é de propriedade do **DVC** e que todos os privilégios de acesso sejam imediatamente removidos.

5.3.1.7. Segregação de Funções

Quando apropriado, a gestão **deve** separar os cargos, tarefas e responsabilidades para evitar que um indivíduo subverta um processo crítico do **DVC** ou de cliente.

5.3.1.8. Nível de Autorização de cargo

A gestão **deve** certificar-se que os colaboradores desempenham somente aquelas funções exigidas para seu cargo dentro da companhia. Eles também são responsáveis por verificar se os funcionários somente têm as autorizações necessárias para desempenhar esse cargo.

5.3.2. Educação, Treinamento e Conscientização

É recomendável que os colaboradores recebam treinamento e educação em bases regulares para assegurar que estão conscientes da política e padrões de segurança do **DVC**, e equipados para apoiar a implementação das normas no transcorrer de seu trabalho normal.

5.3.3. Notificando Incidentes de Segurança

Incidentes de segurança **devem** ser notificados à gestão responsável o mais rápido possível. Gestores são responsáveis por tomar ações para resolver incidentes em suas áreas. É recomendável que todos os membros da equipe estejam conscientes dos procedimentos para notificar incidentes de segurança conforme definido na organização local. Maiores informações disponíveis no documento **NSI 007 - Norma de Tratamento de Incidente em Segurança da Informação**.

5.3.3.1. Notificando Fragilidades na Segurança

É recomendável que fragilidades na segurança sejam notificadas à gestão responsável. Os gestores são responsáveis por avaliar o risco de segurança, tomar ação em suas áreas de responsabilidade quando exigido, e **devem** estar conscientes dos procedimentos para notificar incidentes de segurança, conforme definido na

organização local. Tais fragilidades **não devem** ser testadas sem o acordo escrito de um nível adequado de gestão.

5.4. Segurança Física e do Ambiente

As áreas de computação e rede do **DVC** (por ex. centros de computação, sites de servidores e outras instalações de TI, como por exemplo e centros de publicação) devem ser operadas como instalações fechadas com acesso controlado, permitido somente a pessoal autorizado. É recomendável que o acesso seja limitado somente aos colaboradores do **DVC** que tenha um requisito de negócio válido para acesso.

No ambiente do servidor, local que contém os dados sensíveis do **DVC**, é **PROIBIDO** qualquer tipo de gravação de áudios e vídeos, a não ser em um local designado (mediante a liberação do gestor de TI) especificamente para essa finalidade. Essa regra é aplicada para todos os usuários, sem qualquer exceção.

É recomendável que procedimentos especiais sejam aplicados para visitantes e a pessoa responsável pela segurança física da área analise criticamente autorizações de acesso pelo menos uma vez por ano. Assim como os sistemas do **DVC,** localizados em sites de clientes, sejam instalados em uma área ou sala controlada pelo **DVC**. É recomendável que as áreas de entrega especial e de carga sejam controladas e, se possível, isoladas das áreas de computação do **DVC**. Maiores informações disponíveis no documento **NSI 003 - Norma de Segurança Física e do Ambiente** e **NSI 015 - Norma de Segurança de Acesso Físico**.

É recomendável que as áreas de computação e rede do **DVC** sejam fisicamente protegidas contra ameaças à segurança e que os equipamentos estejam localizados de forma a reduzir os riscos de ameaças ambientais e perigos, tais como incêndio e dano por fumaça, inundação, falha de energia, problemas de umidade, iluminação, mau-funcionamento técnico, sabotagem e roubo. É recomendável que o equipamento seja mantido de acordo com os procedimentos documentados de fornecedores, para assegurar sua disponibilidade contínua. Assim como os controles adequados sejam determinados com base em uma avaliação de risco

A gestão de linha **deve** autorizar de maneira auditável o uso de equipamento para processamento de informação fora das instalações do **DVC** e é recomendável que esse equipamento receba proteção adequada. Isto também se aplica a computadores laptop usados fora das instalações do **DVC**.

É recomendável que o acesso à informação sensível em mídia removível ou papel seja protegido por controles adequados. Assim como uma informação sensível não seja deixada onde possa ser acessada, lida, copiada ou levada por pessoal não autorizado a fazê-lo.

É recomendável que estações de trabalho e servidores sejam protegidos contra acesso não autorizado (Por ex. Proteção de tela protegida por senha) quando não estão sendo usadas. Isto também se aplica a equipamento eletrônico portátil (por ex. notebooks, *smartphones* e *tablets*).

Quando equipamento e mídia que contêm informações sensíveis são descartados, é recomendável que o processo assegure que as informações não podem ser recuperadas posteriormente.

5.5. Segurança de rede

5.5.1. As Redes do DVC

As redes do **DVC devem** ser separadas de redes externas.

As redes privadas são as sub-redes, contendo todos os colaboradores e os recursos internos do **DVC** para apoiar os processos de negócios. Elas são acessíveis somente aos colaboradores do **DVC** e subcontratados.

As redes de serviço são as sub-redes que o **DVC** utiliza para entregar serviços a clientes. É recomendável que apoiem tanto a gestão de serviço quanto as atividades de entregas de serviços.

É recomendável que o acesso a dados transportados pela rede seja restrito somente às pessoas autorizadas, para proteger sua integridade e confidencialidade. Normalmente, dados transportados pela rede não são criptografados, a menos que seja solicitado pelo **DVC**, cliente, ou por lei ou regulamentação do país.

Não é permitido aos colaboradores do **DVC** tentar qualquer tipo de acesso ou uso não-autorizado aos sistemas ou redes internas do **DVC**, clientes ou terceiros usando recursos de computadores do **DVC**, seus próprios ou do cliente. Maiores informações disponíveis no documento **NSI 011 - Norma de Segurança de Rede**.

Somente softwares e ferramentas padrão aprovados do **DVC** (ou do cliente) são permitidos em computadores e redes do **DVC**. *Software* ou ferramentas extras necessárias além desses **devem** ser formalmente autorizados de maneira auditável pelo seu gestor (e/ou cliente).

Não é permitido aos colaboradores do **DVC** instalar qualquer ferramenta de categoria "*hacking*" na rede do **DVC** ou de clientes e/ou em estações de trabalho (computadores desktop ou notebooks), incluindo, mas não se limitado a, produtos como crackers de senha, *war dialers*, *port scanners*, ferramentas *peer-to-peer*, ferramentas de compartilhamento de arquivos, *packet sniffers*, etc a menos que explicitamente autorizado pela gestão, de acordo com diretrizes de segurança; estas ferramentas **devem** ser autorizadas em bases individuais e não podem ser compartilhadas com ninguém mais. Qualquer um que tenha estas ferramentas tem que removê-las imediatamente, ou solicitar seu uso à gerência com uma justificativa de negócios.

Todas as práticas intencionais que coloquem em perigo a segurança da rede do **DVC** são proibidas e as consequências de fazê-las são descritas na seção referente a processos disciplinares.

5.5.2. Conexões com Internet Pública

Todas as conexões entre as redes do **DVC** (**REDES DE SERVIÇO** e **REDES PRIVADAS**) e a **Internet** (ou qualquer outra rede pública) para acessar serviços de rede **devem** incluir arquitetura de 'firewall' para filtrar tráfego e bloquear acesso não-autorizado. Todo tráfego entrando e saindo **deve** passar por este firewall.

Somente será permitida passagem através do firewall de serviços de rede para os quais existe uma necessidade do negócio. Todos os firewalls **devem** ser configurados e gerenciados para atender aos requisitos de segurança.

O estabelecimento de uma conexão direta entre os sistemas de computação do **DVC** e sistemas de computador em organizações externas via Internet ou outra rede pública **devem** ser apoiadas por uma autenticação forte e criptografia de tráfego, dependendo da classificação de informação.

5.5.3. Conexões de Terceiro

Redes de terceiros **não devem** ser conectadas diretamente às redes do **DVC** (REDES DE SERVIÇO e REDES PRIVADAS). Todas as conexões entre as redes do **DVC**, redes de terceiros **devem** passar através de um 'gateway' seguro para filtrar tráfego / protocolos e bloquear acesso não-autorizado. Todo o tráfego entre as redes do **DVC** e a rede de terceiros (entrando e saindo) **deve** passar por este gateway.

Conexões entre a REDES DE SERVIÇO e redes de terceiros exigem uma análise de risco.

É recomendável que os requisitos de segurança do **DVC** sejam incorporados a contratos, que definem as responsabilidades do **DVC** e da empresa terceira.

5.5.4. Acesso remoto

Acesso remoto às redes do **DVC** serão disponibilizados aos colaboradores do **DVC** com base na "necessidade do negócio", a critério de seu gestor. Acesso remoto **deve** ser restrito a membros autorizados.

Somente será permitido acesso remoto usando soluções padrão do **DVC**.

Quando a Internet ou uma conexão dedicada de terceiro é usada para acessar as redes do **DVC**, **deve** ser usada autenticação forte, juntamente com criptografia.

É recomendável que os colaboradores do **DVC** que utilizem facilidades de acesso remoto, protejam adequadamente suas estações de trabalho para evitar acesso não-autorizado à rede do **DVC** ou de clientes. Eles são pessoalmente responsáveis pela proteção de sua estação de trabalho e uso correto das facilidades de acesso remoto do **DVC**.

É recomendável que o acesso remoto seja realizado através de uma VPN e seja respectivamente configurado, de tal forma que todo o tráfego seja roteado, apenas, pela VPN, prevenindo a conexão simultânea a qualquer outra rede.

Quando facilidades de acesso remoto forem oferecidas, a estação de trabalho (computadores desktop ou notebooks) usada **deve** estar rodando a última versão de ferramenta antivírus juntamente com os arquivos de vacina atualizados e **deve** estar continuamente habilitada, monitorando constantemente por vírus e suas atividades.

O acesso direto a redes de cliente, por colaboradores do **DVC**, através de qualquer tipo de instalação de acesso remoto não é permitido, a menos que explicitamente acordado pelo cliente e mencionado no Acordo de Nível de Serviço; neste caso, o cliente **deve** dispensar o **DVC** de qualquer responsabilidade sobre danos potenciais resultantes de tais acessos.

5.6. Segurança do Host / Sistema

5.6.1 Medidas Gerais de Segurança

Os colaboradores do **DVC** são responsáveis pela proteção de suas estações de trabalho (computadores *desktop* ou *notebooks*) em todo o tempo. A fim de reduzir o risco de acesso não autorizado aos computadores desktop ou notebooks, é recomendável bloqueá-los e utilizar uma proteção de tela protegida por senha quando abandonadas.

É recomendável atribuir senhas de BIOS para oferecer maior proteção de dados em caso de perda ou extravio deste equipamento.

Todos os computadores desktop ou notebooks do **DVC devem** estar equipados com *firewall* pessoal e/ou aplicativo de proteção/detecção de intrusão do equipamento e ainda as medidas de segurança, padrão do **DVC**, para *anti-spyware* e outros *malwares*.

Atualização dos sistemas e aplicações com patches de segurança são obrigatórios.

5.6.2. Identificação e Autenticação

A **autenticação** de usuários nos sistemas do **DVC** é efetuada **mediante senha**; os usuários **devem** manter a sua senha em segredo, modificá-la regularmente, **não devem** armazená-las em seus computadores sem usar arquivos criptografados, e **não devem** tentar descobrir senhas pertencentes a outras pessoas. Devido à responsabilidade pessoal, o uso de credenciais de acesso funcionais ou compartilhadas não é permitido. Exceções podem ser concedidas desde que procedimentos adequados para o acesso controlado as credenciais de acesso funcionais ou compartilhados sejam aplicados.

A gestão de sistemas **deve** estabelecer um procedimento para redefinir senhas, que inclua disposições para identificação positiva do solicitante. É recomendável que o usuário altere imediatamente estas senhas iniciais.

É recomendável que medidas adicionais e mais fortes de identificação e autorização sejam implementadas para usuários e clientes do **DVC** quando necessário. Para um perfil com privilégios especiais, é recomendável considerar o uso de técnicas mais rígidas de autenticação, tais como *tokens* ou pergunta/resposta.

Identificação e autenticação são realizadas por um sistema de autenticação dependente de plataforma. É recomendável que este procedimento de acesso

autenticado ofereça informações mínimas sobre o sistema para evitar fornecer a um usuário não-autorizado, assistência desnecessária. Ao realizar uma tentativa de autenticação em um sistema, se qualquer parte do processo estiver incorreto, é recomendável não fornecer ao usuário *feedback* específico indicando a fonte do problema. Caso contrário, é recomendável simplesmente informar ao usuário que o processo de autenticação está incorreto. Maiores informações disponíveis no documento **NSI 005 - Norma de Controle de Acesso Lógico**.

Onde a identificação do usuário não for possível, por ex. acesso via rede pública ou comunicação entre aplicativos, é recomendável tomar medidas adicionais. Estas medidas incluem roteamento forçado a serviços predefinidos, aplicativo via gateways de rede ou aplicativos de confiança.

É recomendável considerar, para certos usuários, restrições em horários de conexão para sistemas críticos ou sensíveis. Também é recomendável considerar um sistema de usuário com um log-off automático, ativado automaticamente após um período de inatividade.

5.6.3. Autorização

Controle de acesso é exigido para sistemas e dados compartilhados com outros. O proprietário da informação em um sistema compartilhado é responsável por decidir quem poderá acessar e que autoridades serão concedidas.

Deve existir um processo formal de autorização para assegurar acesso aos sistemas. É recomendável que o acesso ao sistema seja alocado com base na "necessidade de uso". O uso de "privilégios de sistema" ou utilidades de sistema **deve** ser restrito aos responsáveis pela gestão de sistema. Como responsáveis pela custódia destes sistemas, a gestão de sistema **deve** ter um processo estabelecido para implementar o acesso de usuário a qualquer sistema sob seu controle.

5.6.4. Administração de Segurança

É recomendável haver um procedimento de registro de usuário para entrada de novos usuários em um sistema. Somente pedidos aprovados pelo proprietário da informação em um sistema, podem ser implementados. Um registro de todos os usuários registrados para usar o sistema **deve** estar disponível.

É responsabilidade da organização usuária notificar a administração de segurança quando um usuário deixar uma companhia. É recomendável existir um

processo estabelecido para bloquear ou excluir credenciais de acesso mediante notificação. Assim como bloquear uma credencial de acesso se não for utilizada por 3 meses e, em seguida, excluída se não for usada por 6 meses. É recomendável existir um processo estabelecido para analisar criticamente direitos de acesso de usuários pelo menos trimestralmente.

5.6.5. Gestão de Sistema

É recomendável que todas as credenciais de acesso ao Sistema ou Contas padrão que não são necessárias sejam removidas do sistema. Quando uma conta padrão de Sistema é necessária, a senha entregue pelo fornecedor **deve** ser alterada.

Instalações de teste e desenvolvimento **devem** ser segregadas de sistemas de produção ou operacionais. Maiores informações disponíveis no documento **NSI 006 - Norma de Aquisição, Desenvolvimento e Manutenção de Sistemas da Informação**.

É recomendável que os procedimentos operacionais documentados estejam disponíveis para todos os sistemas de produção, para garantir sua correta operação. Assim como as mudanças nos sistemas sejam estritamente controladas pelo uso de procedimentos documentados de controle de alteração.

É recomendável que requisitos e projeções de capacidade sejam monitorados e feitas para assegurar que processamento adequado e capacidade de armazenagem estão disponíveis quando necessário.

Gestores de Sistema **devem** assegurar que instalações apropriadas de retorno à situação anterior estejam estabelecidas para todas as alterações de sistema, de acordo com sua criticidade para o negócio.

5.6.6. Registrando, Monitorando, Relatando e Auditando

É recomendável que eventos e atividades relacionados com segurança sejam registrados conforme ocorrerem. Todos os eventos e atividades **devem** ser rastreáveis até ao usuário individual. É recomendável que gestores e administradores de sistema analisem criticamente, de forma regular, as entradas de registro de segurança, as quais são recomendáveis serem arquivadas por doze meses, para auxiliar em futuras análises críticas de auditoria.

É recomendável registrar pelo menos as seguintes atividades:

- Tentativas de autenticação de acesso malsucedidas;

- Usuários adicionados ou excluídos de um sistema;
- A atribuição e uso de privilégios especiais de sistema e utilidades de sistema;
- O uso de credenciais de Usuário ou Contas privilegiadas; e
- O uso de recursos sensíveis ou críticos (por ex. diretórios, arquivos).

É recomendável que as seguintes atividades sejam ativamente monitoradas:

- Tentativas malsucedidas de autenticação de acesso;
- O uso de credenciais ou Contas privilegiadas; e
- O uso de recursos críticos ou sensíveis (p.ex. diretórios, arquivos, programas autorizados).

É recomendável que indicações de possíveis invasões ou violações de acesso sejam investigadas e relatadas ao gestor de linha responsável. Ações corretivas imediatas **devem** ser tomadas para minimizar os riscos. É recomendável que clientes sejam informados conforme acordado no contrato com o cliente. Incidentes de segurança **devem** ser relatados usando processos padronizados.

É recomendável que auditorias regulares sejam realizadas por gestores e administradores de Sistema, para assegurar que a Confidencialidade, Integridade, Disponibilidade, Autenticidade, Legalidade e Não Repudio do Sistema estão mantidas.

5.6.7. Backup e Recuperação

Instalações adequadas de backup, de acordo com a importância e valor do sistema e dos dados, **devem** ser fornecidas para assegurar que software de sistemas, software de aplicativo e dados possam ser recuperados após uma falha de mídia ou de sistema.

É recomendável que arquivos de backup sejam armazenados em local remoto, a distância suficiente do local principal e, providos com o nível adequado de proteção física, consistente com a segurança física do local principal. É recomendável que o processo de *backup* e restauração seja testado regularmente.

5.6.8. Proteção antivírus

Todas as estações de trabalho do **DVC** (computadores desktop ou notebooks) capazes de executar o conjunto de ferramentas antivírus padrão do **DVC, devem** estar

protegidas contra vírus[1] usando este conjunto de ferramentas. Todos os servidores conectados com estações de trabalho (computadores desktop ou notebooks) ou conectados a um ambiente não-protegido **devem** executar o conjunto de ferramentas antivírus. Os arquivos de assinatura de vírus **devem** ser atualizados pelo menos uma vez por semana. É recomendável que o software de proteção antivírus seja mantido atualizado e continuamente habilitado, monitorando permanentemente quanto aos vírus e suas atividades.

Devem ser implementados em todas as máquinas no âmbito interno do **DVC** o recurso *Device Control*, que é um serviço que permite controlar o acesso aos dispositivos removíveis. A partir da configuração, **devem** ser bloqueados os dispositivos USB (*Universal Serial Bus*): todos os drivers de mídia, modens, dispositivos de fita, ***smart card***, adaptadores de rede externo, *bluetooth*, câmeras, scanners entre outros dispositivos. Caso comprovada a necessidade de tal utilização, o dispositivo poderá ser homologado e liberado. Acesso aplicado a todos os usuários, exceto colaboradores de TI. Porém dependem da aprovação de um gestor de TI.

Os usuários que utilizam recursos de *internet* **devem** ser submetidos a regras de *Web Control,* que é um serviço que permite controlar o acesso aos recursos da *Internet* em vários níveis (usuários, grupos, sites e etc.). A seguir as regras que **devem** ser consideradas:

I. **Bloqueio Padrão**: Configurado uma regra, com sites que não são permitidos dentro do **DVC**, geralmente sites mal-intencionados. Aplicado a todos usuários, exceto aos colaboradores de TI, em função de análise e investigação de riscos.

II. **Liberar Sites - Vídeos/Imagens Treinamento**: Configurado uma regra, com sites específicos que disponibilizam vídeos com fins instrutivos. Limitado a usuários específicos, após a provação do gestor da área de negócio ou diretor. No entanto, é pré-requisito a liberação técnica da TI, em função da avaliação de impacto no link de dados.

III. **Liberar Padrão - Por Conteúdo/Endereço**: Configurado uma regra, com sites específicos que são permitidos dentro do **DVC,** geralmente sites

[1] Um vírus de computador é um programa não-autorizado que se auto replica inclusive para outras redes, sistemas e ou mídias de armazenamento de dados. Outros exemplos de *softwares* maliciosos são os vermes, "*spyware"* e Cavalos de Tróia. Esta política se aplica a todos os softwares maliciosos.

governamentais, Intranet e etc. Permitido o acesso a todos os usuários que tem uma credencial de acesso na rede.

IV. **Liberar Gestores - Por Conteúdo/Todos Endereços**: Configurado uma regra, permitindo acesso a qualquer site, sem nenhuma restrição, exceto as apontadas na regra de "**Bloqueio Padrão"**. Acesso restrito a alguns grupos de usuários, tais como gestores e consultores externos. Porém, dependendo da aprovação de um gestor de TI ou diretor.

V. **Liberar Sites de Proxy - Por Conteúdo/Endereço**: Configurado uma regra, permitindo acesso a sites de proxy específicos. Acesso restrito ao grupo de usuários, gestores de TI. Porém, depende da aprovação final de um gestor de TI ou diretor.

VI. **Bloquear Sites de** Stream **- Por Conteúdo/Endereço**: Configurado uma regra, com sites de stream que não são permitidos dentro do **DVC**, geralmente sites que disponibilizam vídeos de diversas fontes. Acesso aplicado a todos os usuários, exceto aos gestores e colaboradores da TI. Porém, depende da aprovação de um gestor da TI.

VII. **Bloquear Sites Por Conteúdo/Categoria/Tipos de Arquivo**: Configurado uma regra, com categorias de conteúdo e tipos de arquivos que não são permitidos dentro do **DVC**, geralmente sites que disponibilizam conteúdo adulto, violência e etc. Acesso aplicado a todos os usuários, exceto aos gestores e colaboradores da TI. Porém, depende da aprovação de um gestor da TI.

VIII. **Bloquear Sites Por Conteúdo/Endereço**: Configurado uma regra, com sites específicos não permitidos dentro do **DVC**, geralmente sites de webmail, proxies, vídeos. Acesso aplicado a todos os usuários, exceto aos gestores e colaboradores da TI. Porém, depende da aprovação de um gestor da TI.

É recomendável que todos os arquivos em estações de trabalho do **DVC**, sistemas servidores conforme identificados acima, passem por uma varredura quanto a vírus pelo menos uma vez por semana.

Todos os novos *softwares* e arquivos de dados, especialmente se estes arquivos vêm de uma fonte desconhecida ou não-confiável (como a Internet),

dispositivos desprotegidos como mídias de armazenamento USB ou drives de discos externos, **devem** passar por varredura quanto a vírus antes de seu uso. Antes da distribuição de qualquer *software* ou arquivo de dados a um terceiro, os arquivos **devem** passar por varredura quanto a vírus.

Se um vírus for detectado e não puder ser automaticamente excluído, pelo *software* de proteção antivírus, a organização local de suporte **deve** ser imediatamente informada.

Os colaboradores do **DVC** não **devem** nunca intencionalmente escrever, gerar, propagar, executar ou tentar introduzir qualquer vírus ou outra forma de código malicioso no **DVC**, ambiente de seu cliente ou na Internet.

Os colaboradores do **DVC** usando seus sistemas de computador domésticos por justificativas de negócio **deve** estar protegido contra vírus usando software de proteção antivírus aprovado pelo **DVC** (antivírus, desktop firewall entre demais outros mecanismos de proteção). É recomendável que eles façam varredura de seus arquivos de dados antes de usar estes arquivos dentro do ambiente do **DVC** e **não devem** se conectar simultaneamente a um Terceiro Provedor de Serviço Internet. Maiores informações, estão disponíveis no documento **NSI 013 - Norma de Segurança da Internet**.

5.6.9. Computação Móvel e Teletrabalho

Os colaboradores do **DVC** são responsáveis pela proteção de seus notebooks, *tablets* e *smartphones* durante viagens. É recomendável que os *notebooks*, *tablets* e *smartphones* não sejam deixados em locais públicos. É recomendável que todos os dados de informações sensíveis do **DVC** e de seus clientes sejam criptografados nestes dispositivos. Para reduzir o risco de roubo, é recomendável que sejam utilizados cadeados de segurança sempre que os dispositivos forem “abandonados”, tanto no **DVC** quanto nas instalações de clientes, salas de reunião, hotéis ou até mesmo em casa.

É recomendável que também sejam implementadas senhas de BIOS, quando possível, para oferecer alguma proteção aos dados no caso de perda da máquina.

Os colaboradores do **DVC** trabalhando em atividades de negócio dentro ou distantes do escritório do **DVC** (por exemplo: em casa, hotel, site do cliente ou demais outras localidades) é responsável pela proteção de ativos do **DVC** (*hardware*, *software*

e informações), incluindo todos os dispositivos móveis, como notebooks, *tablets* e *smartphones*. É recomendável que tomem todas as precauções razoáveis para proteger ativos do **DVC** em conformidade com a política de segurança do **DVC** incluindo senhas de proteção dos dispositivos móveis e criptografia de informações confidenciais.

5.6.10. Confiabilidade de Estações de Trabalho

Somente as estações de trabalho do **DVC** pertencentes aos ativos do **DVC** são vistas como estações de trabalho confiáveis e podem ser usadas para qualquer tipo de atividade autorizada nas redes do **DVC** enquanto manipulam qualquer tipo de dados classificados.

Visitantes externos do **DVC** só **devem** ter acesso de modo restrito a redes do **DVC**, quando absolutamente necessário. Cada funcionário ao receber visitantes, **deve** contatar o administrador de rede local para verificar procedimentos relativos a liberação de acesso *Guest (*Visitante*)*.

Quando em viagem, fora do escritório do **DVC** os colaboradores do **DVC** são fortemente aconselhados a usar unicamente estações de trabalho de ativos do **DVC**, para manipulação de dados sob a responsabilidade do **DVC** e para conexão às redes do **DVC**. Entretanto, circunstâncias específicas podem impedir o uso de estações de trabalho pertencentes aos ativos do **DVC** quando for este o caso, as seguintes restrições **devem** ser aplicadas:

EQUIPAMENTO / AÇÕES	PC de propriedade **DVC**	PC doméstico de propriedade do funcionário[2,3]	PC do cliente alocado permanentemente ao funcionário [5,4]	PC de propriedade de terceiro [5,4]
Conectam-se a redes **DVC**	Sim	Não	Parcialmente[5]	Não
Armazenagem local de dados classificados do **DVC** ou dados do Cliente	Sim	Não	Somente dados do cliente[6]	Não
Acesso à Internet	Sim	Não	Sim	Sim

[2] **Deve** estar de acordo com as regras de segurança para estações de trabalho: Antivírus, firewall de micro, atualizações de software, etc.
[3] A referência a este tipo de uso não implica que seja prestado suporte a ele; favor consultar seu acordo de nível de serviço.
[4] **Deve** estar de acordo com as regras de segurança ou com as Regras de Segurança do Cliente.
[5] Permitido para acesso a redes de serviço relevante do cliente (Redes de serviços).
[6] Isto exclui qualquer aplicativo de e-mail de cliente para o gerenciamento de um endereço de caixa postal.

Acesso a e-mail Web	Sim	Sim	Sim	Somente ler e-mails

Tabela 1 – Descrição de Restrições

5.7. Segurança de Aplicativos e Dados

5.7.1. Aplicativos de Negócios do DVC

É recomendável que todo aplicativo de negócio crítico tenha um proprietário nomeado, os requisitos de segurança sejam determinados e documentados em um plano de segurança antes que um aplicativo seja projetado, desenvolvido ou adquirido. Assim como requisitos de segurança, com relação à confidencialidade, integridade, disponibilidade, autenticidade e não repudio sejam acordados com o proprietário. É recomendável que atenção específica seja dada às seguintes áreas de risco:

- Acesso aos aplicativos, funções e dados;
- Armazenagem de dados;
- Transporte de dados;
- Interfaces com outros aplicativos; e
- Rastreabilidade (i.e. trilhas de auditoria).

Todos os aplicativos **devem** ser testados e aceitos antes de serem levados à produção. Durante o teste de aceitação de aplicativos recém-desenvolvidos ou adquiridos é recomendável verificar se os requisitos de segurança são preenchidos. O **Departamento de Segurança da Informação deverá** assegurar que as aplicações de uso do **DVC** sejam instaladas corretamente no ambiente de produção, informando aos envolvidos sobre as regras e responsabilidades inerentes. Além disto, garantirá que os documentos e/ou procedimentos relacionados sejam sempre mantidos atualizados. Também quando aplicativos são subsequentemente corrigidos, os requisitos de segurança **devem** ser verificados. É recomendável que os aplicativos não sejam testados com dados de produção reais.

É recomendável controle estrito de acesso de todos ambientes. As aplicações desenvolvidas pelo **DVC**, **deverão** ter o acesso ao código-fonte restrito aos integrantes do projeto. Quando operacional, é recomendável que todas as medidas de segurança necessárias, manuais e automatizadas sejam cumpridas.

É recomendável que alterações afetando aplicativos sejam estritamente controladas pelo uso de procedimentos documentados de controle de alterações.

Qualquer vulnerabilidade ou evento de quebra de Segurança da Informação observado por colaboradores e terceiros **deve** ser relatado o mais rapidamente possível através do e-mail **segurançadainformacao@DVC.com.br**.

É recomendável serem considerados controles especiais, para aplicativos que iniciam processos de negócio críticos envolvendo o manuseio ou intercâmbio de informações sensíveis.

5.7.2. Aplicativos de Clientes

5.7.2.1. Requisitos de Segurança em Aplicativos de Clientes

É recomendável que os clientes sejam fortemente aconselhados a considerar com cuidado os requisitos de segurança, antes de um aplicativo ser desenvolvido, alterado ou selecionado.

É recomendável que os clientes sejam fortemente aconselhados a verificar cuidadosamente se seus requisitos de segurança são preenchidos, quando novos aplicativos são colocados em produção e alterados.

O **DVC** assegurará que fragilidades e eventos de Segurança da Informação associados com sistemas da informação, sejam comunicados ao **Departamento de Segurança da Informação** permitindo a tomada de ação corretiva em tempo hábil.

5.7.2.2. Ambientes de Desenvolvimento, Teste e Produção

É boa prática de segurança e requerimento normativo, criar diferentes ambientes para atividades durante o ciclo de vida de um aplicativo, i.e. desenvolvimento, teste e produção. **Deve** haver segregação entre estes ambientes para evitar que dados de ambientes de teste e desenvolvimento sejam usados no ambiente de produção. Dados reais de produção não **devem** ser usados para testar aplicativos em ambientes de teste. Segregação de ambientes de desenvolvimento e teste é fortemente aconselhado. É recomendável controle de acesso a todos os ambientes.

5.8. Serviços Genéricos do DVC

5.8.1. Correio Eletrônico

É recomendável que os colaboradores do **DVC** estejam cientes de que mensagens eletrônicas podem ser encaminhadas, interceptadas, impressas e armazenadas por outras pessoas. A menos que a mensagem seja criptografada, os colaboradores **devem** evitar enviar informações sensíveis via e-mail.

O emissor de uma mensagem eletrônica é considerado pessoalmente responsável por seu conteúdo. É recomendável que os colaboradores do **DVC** estejam cientes de que todas as mensagens originadas de usuários do **DVC** levam o nome do **DVC** em seu endereço de origem. É recomendável que toda mensagem seja preparada e enviada de maneira profissional seguindo todas as regras de decoro social. Da mesma forma, os colaboradores do **DVC devem** evitar enviar mensagens que podem ser consideradas inflamatórias, discriminatórias, injuriosas ou de outra forma ofensivas ou ilegais.

É recomendável que os colaboradores do **DVC** exerçam com cuidado o encaminhamento de mensagens, reconhecendo que certas informações são dirigidas a indivíduos específicos e podem não ser adequadas para distribuição geral em comunicações eletrônicas. Assim como as informações sensíveis não sejam encaminhadas a qualquer parte fora do **DVC** sem a aprovação prévia do proprietário da informação. Não é permitido encaminhamento automático de mensagens a partes fora do **DVC**.

E-mails indesejados ou "*spam"* são considerados ofensivos e e-mail contendo material ilegal, ofensivo ou malicioso é considerado intolerável.

É recomendável que ao visitar websites e tendo que preencher informações, os colaboradores tomem cuidado antes de usar o endereço de e-mail da companhia do **DVC.** Isto pode resultar em e-mail comercial indesejado e não solicitado. É recomendável que os funcionários evitem deixar seus endereços de e-mail do **DVC** se a política de privacidade do website é inexistente ou declarar que aquela informação será vendida ou compartilhada.

O **DVC** respeitará a privacidade de seus usuários de e-mail. Normalmente usuários de e-mail podem presumir que somente o destinatário lê sua correspondência eletrônica.

Entretanto, o acesso a caixas de correio eletrônico de usuários pode ser solicitado no caso de qualquer urgência comercial, incluindo atividades de investigação. Também pode ser necessário para o suporte técnico revisar o conteúdo das comunicações de membros individuais dos colaboradores durante a resolução de problema. Todos estes acessos precisam estar de acordo com a legislação local de privacidade, políticas corporativas com as devidas aprovações em alçada executiva (Recursos Humanos, Diretor da Área de Negócio e Jurídico). Maiores informações disponíveis no documento **NSI 012 - Norma de Segurança em Correio Eletrônico**.

5.8.2. Intranet do DVC

A Intranet do **DVC**, é um recurso do negócio particular e é recomendável que seja usada somente para fins de negócio. Somente os colaboradores do **DVC deveram** ter acesso autorizado.

Informações na Intranet destinam-se apenas a uso interno. É recomendável que as informações na Intranet não sejam compartilhadas com Terceiros. Os requisitos do Padrão de Classificação de Informação aplicam-se a todas as informações na Intranet. Informação “Confidencial” ou “Sensível” **deve** ser armazenada com controles eficientes de acesso e criptografia. Nenhum controle adicional é exigido ao armazenar informações “Públicas” ou “Internas”.

Não é permitido uso inadequado do sistema Intranet. Uso inadequado inclui, porém não se limita a:

- Tentativas não autorizadas de acessar informações protegidas;
- Atividades que prejudiquem o desempenho da Intranet; e
- Qualquer atividade ilegal, antiética ou qualquer outra atividade que possa afetar adversamente a companhia.

5.8.3. Extranet do DVC

Uma Extranet é um ambiente parcialmente privativo para compartilhar informações entre o **DVC** e terceiros (i.e. clientes, fornecedores). É recomendável que o proprietário da informação decida se informações “confidenciais” ou “internas” podem ser compartilhadas com terceiros usando uma Extranet. Compartilhar informações classificadas do **DVC** com uma terceira empresa exige uma avaliação de risco. Esta avaliação fornecerá os controles de segurança necessários e procedimentos a serem implementados.

É recomendável que todos os usuários sejam autenticados antes de acessar uma Extranet do **DVC**. Somente usuários autorizados terão permissão de acesso. Controles suficientes **devem** estar implantados para garantir que informações específicas não sejam compartilhadas entre empresas terceiras diferentes.

Quando uma informação é compartilhada entre o **DVC** e uma empresa terceira é recomendável que ambas assinem um **Acordo de Confidencialidade**.

5.8.4. Web Externa do DVC

É recomendável haver um processo de autorização formal antes de informações serem disponibilizadas publicamente na Internet. A integridade da informação **deve** ser protegida de modificações não autorizadas.

5.9. Gestão de Continuidade do Negócio

Cada organização do **DVC deve** avaliar os riscos para sua continuidade no negócio de um desastre potencial nas suas atividades críticas de negócio. É recomendável que sejam desenvolvidos planos de continuidade de negócio para oferecer proteção contra a perda de ativos (*hardware*, *software* e informações) ou indisponibilidade de serviços. É recomendável que estes planos assegurem que todos os desastres possíveis que apresentem riscos inaceitáveis serão adequadamente cobertos por um plano totalmente documentado e testado, de tal modo que o impacto no negócio seja minimizado e as atividades interrompidas possam ser restabelecidas o mais rápido possível.

Para assegurar que a infraestrutura do **DVC** continue a entregar serviços, gestores responsáveis por componentes da infraestrutura **devem** manter um plano de continuidade de negócio para implementação se um desastre impedir a entrega normal do serviço. Planos de continuidade de negócio **devem** ser capazes de entregar os requisitos de disponibilidade contratados aos clientes e **devem** ser testados pelo menos uma vez por ano e auditados.

O **DVC** manterá planos para Gestão da Continuidade do Negócio relativos à Segurança da Informação. Caberá ao **Departamento de Segurança da Informação**, garantir a manutenção da **Política de Gestão da Continuidade do Negócio**.

É recomendável que o planejamento de continuidade de negócios seja discutido com clientes e descrito nos contratos e Acordos de Nível de Serviço. Maiores

informações disponíveis no documento **NSI 008 - Norma de Continuidade de Negócios**.

5.10. Segurança em Cloud Computing (Nuvem)

O **DVC** manterá grande parte de seus serviços em nuvem, entre eles, máquinas virtuais, servidores, bancos de dados, entre outras tecnologias. Portanto, as seguintes práticas **devem** ser seguidas, toda vez que novos serviços de nuvem sejam contratados.

5.10.1. Acordos de Níveis de Serviço (SLA)

É necessário verificar as questões atreladas às SLA's (*Service Level Agreement*), que **devem** contemplar medidas de contingência, por exemplo, em casos de potenciais incidentes em segurança da informação, que visam assegurar a disponibilidade dos serviços do **DVC**. Tais documentos/acordos **devem** ser revisados periodicamente, em intervalos regulares, visando identificar potenciais incompatibilidades em relação ao atendimento do serviço contratado.

É recomendável que essa revisão contemple os seguintes aspectos:

- Qual tempo necessário para o reestabelecimento do serviço em casos de falhas;
- Qual plano de recuperação (backup) em caso de falha;
- Qual o tempo máximo aceitável para o negócio do **DVC** e quais as medidas **devem** ser tomadas pelo provedor para respeitar esse tempo;

5.10.2. Proteção à Dados

O provedor de serviço em nuvem **deve** assegurar os cuidados necessários em relação a privacidade e segurança dos dados dos clientes, por exemplo, estar em conformidade com a LGPD (Lei Geral de Proteção de Dados Pessoais).

Deve ser escolhido um responsável que ficará responsável pela privacidade de dados dentro do **DVC**. Este profissional deve ter o conhecimento sobre a lei, tecnologia e procedimentos utilizados no negócio da empresa.

O regulamento não considera o tratamento de dados atrelados a pessoas falecidas. Maiores informações disponíveis no documento **NSI 016 - Norma de Tratamento de Dados**.

5.10.3. Documentações de Procedimentos Operacionais

Procedimentos operacionais **devem** ser documentados e atualizados, uma vez que os sistemas/tecnologias sofrem atualizações de tempos em tempos. Essa medida tem por objetivo garantir a correta operacionalização das tecnologias mantidas em nuvem, além de assegurar que os profissionais estarão treinados para operar as máquinas virtuais, servidores, bancos de dados, entre outras tecnologias mantidas em nuvem.

5.10.4. Garantir a Conformidade em Nuvem

O **DVC deve** assegurar que todos os serviços contratados de provedores em nuvem, estão em conformidade com as leis e regulamentos de conformidade aplicáveis. Portanto, em intervalos regulares, relatórios de auditoria **devem** ser solicitados ao provedor do serviço, visando identificar potenciais aspectos de não conformidade em armazenamento, processamento e transmissão de informações.

5.11. Conformidade

5.11.1. Conformidade com a Política de Segurança

O desenho, operação e uso de cada instalação, rede, sistema, aplicativo e suas informações **devem** estar em conformidade com a Política de Segurança da Informação do **DVC**, acordos contratuais, leis relevantes e outros requisitos normativos.

Maiores informações disponíveis no documento **NSI 009 - Norma de Conformidade em Segurança**.

5.11.2. Conformidade com Políticas de Clientes

É recomendável que os colaboradores do **DVC** trabalhando em locais de clientes, esteja familiarizado e aja de acordo com as políticas de segurança, padrões e procedimentos do cliente, bem como com os equivalentes do **DVC**.

5.11.3. Conformidade com Requisitos Legais

Devem estar estabelecidos controles para assegurar conformidade com os acordos nacionais, leis e regulamentos. É recomendável que sejam aplicados controles para proteger informações pessoais, em conformidade com a legislação relevante.

O **DVC** poderá promover as medidas que julgar necessárias, inclusive judiciais, para garantir que o uso dos Recursos de Computação seja feito conforme previsto neste documento.

Aplica-se a este documento toda a legislação nacional, em especial as normas abaixo, cujo conteúdo pode ser obtido integral e gratuitamente no sítio da Presidência da República, em http://www.planalto.gov.br:

- A Constituição da República Federativa do Brasil de 1988;
- O Decreto-Lei nº. 2.848/40 (Código Penal);
- O Decreto-Lei nº. 5.452/43 (Consolidação das Leis do Trabalho – CLT);
- A Lei Federal nº. 9.279/96 (Código de Propriedade Industrial);
- A Lei Federal nº. 9.609/98 (Lei do Programa de Computador);
- A Lei Federal nº. 9.610/98 (Lei de Direitos Autorais);
- A Lei Federal nº 10.406/02 (Novo Código Civil);
- A Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais); e
- A Lei Federal nº 8.906/94 (Estatuto da Advocacia e da Ordem dos Advogados do Brasil).

5.11.4. Verificação de Conformidade

A conformidade com esta política e subsequentes padrões e procedimentos de segurança dentro de uma organização será revisada sob a responsabilidade **Departamento de Segurança da Informação**. Não conformidades serão relatadas à gestão responsável. Gestores **devem** assegurar que ações serão tomadas oportuna e adequadamente, de forma auditável, para resolver não conformidades.

5.11.5. Processo Disciplinar

É recomendável que exista um processo disciplinar formal dentro de cada grupo de serviço e organização nacional, aprovado por gestão responsável, para colaboradores do **DVC** que tenham intencionalmente violado a política, padrões e/ou procedimentos de segurança do **DVC**. No caso de uma violação da **Política de Segurança**, a gestão de linha responsável, em cooperação com o **Departamento de Recursos Humanos** dentro da Organização, país e/ou departamento de entrega de serviço pode tomar medida disciplinar. Tal medida pode variar desde advertência

verbal (com ou sem observação no arquivo pessoal) até e inclusive demissão. A gravidade do incidente orientará a severidade da medida tomada.

6. Regulamentação

Estas instruções reguladoras têm por finalidade definir as condições de uso dos recursos oferecidos pelo **DVC**, com base nos padrões e normas da família ISO 27000 e Legislação Brasileira, além das exigências nos aspectos de segurança do **DVC**.

7. Documentos Relacionados

Política ou Norma	Localização
PSI 002 - Política de Classificação da Informação	K:\Conjunto Normativo de Segurança da Informação
NSI 001 – Norma de Gestão de Ativos	K:\Conjunto Normativo de Segurança da Informação
NSI 002 - Norma de Segurança em Recursos Humanos	K:\Conjunto Normativo de Segurança da Informação
NSI 003 - Norma de Segurança Física e do Ambiente	K:\Conjunto Normativo de Segurança da Informação
NSI 004 - Norma de Gestão das Operações e Comunicações	K:\Conjunto Normativo de Segurança da Informação
NSI 005 - Norma de Controle de Acesso Lógico	K:\Conjunto Normativo de Segurança da Informação
NSI 006 - Norma de Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação	K:\Conjunto Normativo de Segurança da Informação
NSI 007 - Norma de Tratamento de Incidentes em Segurança da Informação	K:\Conjunto Normativo de Segurança da Informação
NSI 008 - Norma de Continuidade dos Negócios	K:\Conjunto Normativo de Segurança da Informação
NSI 009 - Norma de Conformidade em Segurança	K:\Conjunto Normativo de Segurança da Informação
NSI 010 - Norma de Segurança no Acesso de Usuários	K:\Conjunto Normativo de Segurança da Informação
NSI 011 - Norma de Segurança de Rede	K:\Conjunto Normativo de Segurança da Informação
NSI 012 - Norma de Segurança em Correio Eletrônico	K:\Conjunto Normativo de Segurança da Informação
NSI 013 - Norma de Segurança da Internet	K:\Conjunto Normativo de Segurança da Informação
NSI 014 – Norma de Acesso à rede Privada	K:\Conjunto Normativo de Segurança da Informação

NSI 015 – Norma de Segurança de Acesso Físico	K:\Conjunto Normativo de Segurança da Informação
NSI 016 – Norma de Tratamento de Dados	K:\Conjunto Normativo de Segurança da Informação

8. Contato, Dúvidas e Sugestões

Departamento	E-mail	Telefone
Compliance	compliance@devivocastro.com.br	+55 (11) 3048-3266
Segurança da Informação	segurancadainformacao@devivocastro.com.br	+55 (11) 3048-3266

9. Responsabilidades

Serão responsabilizados pelos seus atos e omissões não aderentes a esta política aqueles que criarem, modificarem, armazenarem e transmitirem qualquer informação pertencente ao **DVC**, sejam estes funcionários, terceiros ou clientes, por período estabelecido em contrato junto ao **Departamento Financeiro** e/ou **Departamento de Recursos Humanos**. A utilização inadequada da informação pode resultar em sanções contratuais, além de penalidades previstas por lei.

10. Aprovações

	Cargo	Nome	Data	E-mail
Revisão	Coordenadora de Contratos e de Compliance	Renata Assalim Fernandes Souza	17/11/2023	rassalim@devivocastro.com.br
Aprovador (1)	Diretor Financeiro	Tomas Neves Amado	17/11/2023	tamado@ devivocastro.com.br
Aprovador (2)	Sócio Gerente	Gustavo Lorenzi de Castro	17/11/2023	gcastro@devivocastro.com.br

11. Controle de Versões

Versão	Data	Descrição	Autor(es)
1	05//07/2019	Elaboração do Documento	Data Security e DVC
2	147/11/2023	Revisão do Documento	Compliance DVC