Política de Segurança da Informação

Conteúdo

Introdução

Definição de segurança da informação

Informação é um ativo, o qual como qualquer outro, tem valor para a organização e consequentemente necessita ser adequadamente protegido.

A informação pode ser disponibilizada de várias formas, podendo ser impressa ou escrita em papéis, armazenada eletronicamente, transmitida por correio ou por meios eletrônicos, mostrada em filmes ou apresentar-se através de conversação. Seja qual for o meio pelo qual a informação é distribuída, partilhada ou armazenada, esta sempre requer proteções apropriadas.

A segurança das informações tem a função de proteger a informação de uma série de ameaças com o objetivo de (i) zelar pela continuidade dos negócios, (ii) minimizar prejuízos e (iii) maximizar o retorno de investimentos e oportunidades de negócios. Desta forma, a segurança das informações torna-se responsável pela preservação das seguintes propriedades da informação:

a) confidencialidade: assegura que a informação permaneça acessível apenas a quem de direito;
b) integridade: protege a exatidão e a totalidade da informação e das possíveis formas de processamento desta;
c) disponibilidade: assegura que usuários autorizados tenham acesso à informação e aos ativos associados a ela quando necessário.

Para que sua atuação seja completamente eficaz, a segurança das informações depende do planejamento, análise e implementação de uma série de controles, os quais poderiam ser compostos por políticas, práticas, procedimentos, estruturas organizacionais ou mecanismos eletrônicos. Tais controles necessitam ser projetados de acordo com as necessidades das organizações no tocante à segurança.

Introdução

Definição da importância da segurança das informações

A informação, os processos que a suportam, sistemas e redes de comunicação de dados são importantíssimos ativos para os negócios de uma organização.

Confidencialidade, integridade e disponibilidade das informações são geralmente, fatores essenciais para prover às organizações vantagens competitivas, aumento do fluxo de caixa, maior lucratividade, auxílio no processo de adequação às exigências legais e de órgãos regulamentadores e suporte à sua imagem comercial.

De forma assustadoramente crescente, organizações, seus sistemas de informações e suas redes de comunicação de dados, apresentam-se diante de uma série de ameaças, dentre as quais podemos citar apenas como exemplos, fraudes eletrônicas, espionagem, sabotagem, vandalismo, fogo e inundações. Diante deste cenário, podemos afirmar que prejuízos às organizações passaram a resultar, com maior frequência e por métodos cada vez mais sofisticados, de situações diversificadas tais como a atuação de vírus de computador, "cracking" ou "hacking" dos computadores (proveniente da invasão de "crackers" ou "hackers" aos sistemas de forma não autorizada) e indisponibilidade dos sistemas.

A dependência progressiva das organizações com relação aos sistemas de informações computadorizados, as torna cada vez mais vulneráveis a ameaças. A interconexão de redes públicas e privadas e o compartilhamento de recursos aumenta consideravelmente as dificuldades de quem deseja e necessita controlar acessos ao seu ambiente computadorizado, bem como o uso de plataformas de processamento distribuído tem tornado fracos os controles de segurança centrais ora definidos.

Sistemas construídos sem contemplar na etapa de planejamento de seu projeto, preocupações e especificações voltadas à segurança das informações, requerem investimentos muito maiores das organizações para a implementação de controles, do que aqueles que já em sua estrutura contemplam controles computadorizados.

Desta forma, podemos concluir que nos parâmetros atuais, segurança das informações é vital para a continuidade dos negócios de quaisquer organizações, bem como depende de participação ativa de todos os seus funcionários em sua implementação e monitoração.

Introdução

Definição de política de segurança

É o instrumento que contém diretrizes voltadas a auxiliar a organização, no planejamento, definição e implementação de mecanismos (normas, procedimentos, padrões, controles e outros) que guiarão e suportarão as atividades relativas à segurança das informações, nas áreas de maior risco para seus processos de negócios.

A política de segurança de informações deve ser (i) definida com base nas necessidades de segurança exigidas pelos negócios da organização, (ii) documentada, (iii) adequadamente seguida por todas as pessoas envolvidas direta ou indiretamente na execução e condução dos processos de negócios da organização, (iv) revisada periodicamente visando sua adequação contínua às diversas mutações sofridas pelas necessidades da organização, (v) monitorada pelos funcionários da organização ao ponto destes serem responsáveis pelo reporte imediato e íntegro de quaisquer incidentes ocorridos. Desta forma, podemos concluir que com a implementação adequada de uma política de segurança, a organização passa a ter benefícios diversos tais como:

- Identificação da informação por seus funcionários, como um ativo significativo;
- Integração uniforme das políticas de segurança definidas com os objetivos dos negócios da organização;
- Disseminação das responsabilidades de cada funcionário com relação à preservação da integridade, confidencialidade e disponibilidade das informações;
- Maior comprometimento de sua alta gerência e de seus funcionários com relação à segurança das informações.

Introdução

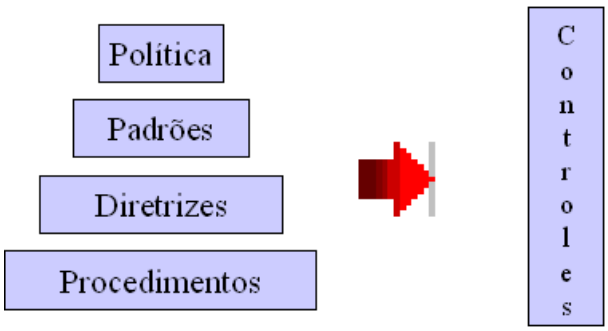
Definição de padrões, diretrizes, procedimentos, controles de segurança, dados e informações

Padrões definem o que deve ser feito. Asseguram que informações similares recebam o mesmo tipo de proteção independentemente de onde residam, com o auxílio de controles preventivos ou detectivos a serem desenhados em maior ou menor escala de rigidez, de acordo com a classificação das informações alvo de proteção.

Diretrizes definem quem será responsável e como por organizar, dirigir, controlar e executar os procedimentos voltados ao atendimento dos padrões previamente definidos.

Procedimentos definem como deveremos atender aos padrões previamente definidos. Descrevem passo a passo as ações necessárias para atingir-se o nível de segurança desejado.

Controles são mecanismos voltados à prevenção ou detecção de quaisquer ocorrências divergentes aos padrões, diretrizes e procedimentos definidos.



Dados são os elementos básicos que compõem a informação. Muitos dos dados se obtidos por pessoas não autorizadas, não representam uma grande ameaça para a Companhia. Os dados passam a ser um tanto preciosos, aos supostos atacantes que possuam um conhecimento profundo dos processos do Grupo.

Informação é o fruto do processamento dos dados, seja ele efetuado por computadores, pessoas ou processos. A informação deve ser protegida de acordo com sua classificação pois é um ativo importante do Grupo.

O documento Política de Segurança

Divulgação do documento

O documento Política de Segurança deve ser adequadamente divulgado através, (i) da entrega de cópias completas deste a todas as gerências do Grupo e a todos os membros do Comitê de Segurança, (ii) da entrega de sumário deste, contemplando apenas os aspectos julgados necessários pela VTCLOG**,** a todos os funcionários do Grupo e aos terceiros envolvidos em seus processos e (iii) do planejamento de treinamentos periódicos voltados à disseminar o conceito de segurança dentro da organização.

O processo de divulgação da Política de Segurança, deve estar de acordo com o **"Manual de Comunicação Corporativa"** do Grupo.

É necessário que todos os envolvidos na implementação da Política de Segurança, incluindo a alta gerência, funcionários e terceiros, possam entender, conscientizar-se e comprometer-se com o conteúdo da política e de seus adendos, comprovando o atendimento a estes pré-requisitos formalmente, através da assinatura de um termo de compromisso. Desta forma, o termo em questão passará a fazer parte da documentação pessoal exigida pela área de Recursos Humanos para cada funcionário, bem como dos contratos exigidos pela Companhia aos terceiros.

Manutenção do documento

Definições

Os tópicos seguintes definem os termos usados neste documento. Isto é requerido para o completo entendimento do leitor e ou pessoa a qual estará executando este procedimento. Para uma compreensão completa do processo descrito neste documento são necessários a leitura e o entendimento dos termos aqui definidos. As definições são as seguintes:

Lista de Procedimentos Ativos – Esta lista, mantida pelo gestor, age como referência das políticas de segurança da informação, e procedimentos que atualmente estão aprovados para uso na VTCLOG. Esta lista irá conter as seguintes informações:

- Nome do documento;
- Número do processo;
- Revisão atual;
- Data da revisão;
- Status do ciclo de revisão.

Documento – Política ou procedimento de segurança.

O documento Política de Segurança

Manutenção do documento

Definições

Ciclo de revisão – Ciclo de revisão se refere ao tempo pré-estabelecido para a revisão do documento (anualmente, semestralmente). Esta informação normalmente estará descrita na introdução dos procedimentos ou políticas de segurança.

Gestor – É a denominação da pessoa que, mantém um registro de todas as políticas e procedimentos existentes no processo de gerenciamento de políticas e processos. Ele gerencia as mudanças mantendo um registro das versões anteriores de políticas e procedimentos que foram aprovadas e implantadas. O gestor também é definido como o Responsável de Segurança.

Comitê de Segurança – O comitê de segurança é composto pelas pessoas que são consideradas como especialistas em um procedimento ou política. Eles estão cientes de quaisquer implicações que venham a ocorrer devido a mudanças propostas em uma política ou procedimento em particular.

Usuários – Usuários são os indivíduos que utilizam este ou outro documento para completarem as tarefas descritas nos documentos. Usuários têm o direito de propor mudanças a este ou qualquer outro documento existente dentro deste processo.

Número do processo – O número do processo é um identificador alfanumérico único, assinalado a uma mudança aprovada, ou a um documento.

Gerenciamento de Documentos

A gerência de documentos de políticas e procedimentos é requerida dentro do programa de segurança de informações para manter os documentos atualizados. As próximas seções apresentam o processo de criação, aprovação e alteração dos documentos.

1.1 Novo Documento

Os novos documentos de política dentro da VTCLOG deverão possuir um método sistemático de controle. Deverá existir um local centralizado para guarda dos documentos, para que apenas possam obter acesso a estes, pessoas devidamente autorizadas.

O catálogo de novos documentos requer a revisão e aprovação técnica e gerencial. Os itens necessários são:

1. Preenchimento do Formulário "Novo Documento"
2. Submissão do Documento com o respectivo formulário ao Gestor
3. Revisão do Gestor

O documento Política de Segurança

Manutenção do documento

Gerenciamento de Documentos

1.1 Novo Documento

4. Recebimento de número de documento pelo Gestor
5. Guarda do documento

Se o formulário estiver incompleto ou incorreto, o Gestor o devolverá à pessoa que submeteu o documento, reiniciando o processo.

1.2 Requisição de Alteração

Se um usuário considerar necessária a alteração de um procedimento ou política, ele poderá requerer a alteração do documento, através do Formulário "Pedido de Alteração".

1.2.1 Submissão do Pedido de Alteração

Os seguintes passos devem ser realizados, independente dos motivos do usuário:

1. Preencher o Formulário "Pedido de Alteração", expondo os motivos
2. Anexar as páginas da política ou procedimento afetadas, com a proposta de alteração
3. Submetê-las ao Gestor

1.2.2 Processamento da Alteração

Ao receber a solicitação, o Gestor irá:

1. Verificar o formulário
2. Retornar ao usuário em caso de erro no formulário
3. Se o formulário estiver correto, o Gestor irá fornecer um número para o processo
4. Gestor irá submeter o processo ao Comitê para aprovação.

1.3 Revisão do Pedido de Alteração

O Comitê decidirá se a solicitação procede ou não. Os passos são:

1.3.1 Aprovação

A alteração é aprovada e enviada ao Gestor para implementação.

O documento Política de Segurança

Manutenção do documento

Gerenciamento de Documentos

1.3 Revisão do Pedido de Alteração

1.3.2 Reprovação

A alteração é reprovada e repassada ao Gestor para posterior devolução ao usuário.

1.3.3 Aprovado com alterações

A alteração é aprovada com restrições. Os pedidos com as restrições são enviados ao Gestor para implementação.

1.4 Ciclo de Revisão

Cada documento possuirá uma periodicidade de revisão. Uma vez decorrido o período o documento será submetido à revisão.

1.4.1 Análise de Validade

O comitê deverá avaliar se o documento é ainda válido. Os seguintes eventos poderão ocorrer:

1. As mudanças necessárias no documento são submetidas ao Gestor para implementação
2. Se o documento não é mais válido o Comitê envia ao Gestor para arquivamento
3. Caso nenhuma mudança seja necessária o Comitê retorna ao Gestor.

1.4.2 Processo de Obsolescência

Se o documento não for mais válido ou necessário para a VTCLOG, o Comitê irá declarar que o mesmo é obsoleto e o Gestor irá retirar o documento da política de segurança.

1.4.3 Alteração de Documentos

O Comitê revisará o documento para determinar as mudanças necessárias. Se houver necessidade de mudanças o documento será enviado ao Gestor com o respectivo formulário de alteração.

O documento Política de Segurança

Termo de Compromisso de Segurança das Informações e Utilização de Ativos

A implementação de um termo de compromisso, tem por objetivo definir adequadamente os deveres e responsabilidades de cada indivíduo dentro da política corporativa.

O "Termo de Compromisso de Segurança das Informações e Utilização de Ativos" deverá ser assinado por todos os funcionários e conforme julgado necessário, também pelos prestadores de serviços da VTCLOG e deverá contemplar dentre outras, as seguintes considerações:

- Confidencialidade de códigos de identificação de usuários;
- Confidencialidade de senhas de controle de acesso;
- Confidencialidade dos dados e informações cujo acesso é permitido através de códigos de identificação de usuários e senhas de controle de acesso;
- Confidencialidade na divulgação de informações;
- Cuidados e responsabilidades quanto à utilização de ativos;
- Cuidados e responsabilidades quanto à proteção de ativos;
- Garantia da integridade, confidencialidade e disponibilidade das informações sob sua responsabilidade;
- Responsabilidade pelo entendimento, conscientização e comprometimento com o conteúdo da Política de Segurança e de seus adendos (padrões, diretrizes, normas, procedimentos e controles);
- Responsabilidade pelo reporte de quaisquer incidentes de segurança identificados;
- Medidas disciplinares voltadas ao descumprimento das condições do termo, incluindo considerações legais;
- Validade do termo.

É necessário que o processo de elaboração do termo em questão tenha o acompanhamento da área jurídica do Grupo visando a prevenção de quaisquer litígios.

Procedimentos periódicos de manutenção do termo em questão, visando sua adequação contínua às necessidades de negócio da VTCLOG**,** deverão ser considerados.

Infraestrutura de Segurança das Informações

O principal objetivo da estruturação de uma área voltada à Segurança das Informações dentro da VTCLOG é permitir a coordenação centralizada de seus aspectos, zelando pela uniformidade e consistência na implementação dos padrões, diretrizes e procedimentos ora definidos.

Fórum de gerenciamento de Segurança das Informações

Para que a Política de Segurança possa estar continuamente alinhada aos objetivos de segurança da VTCLOG, é recomendado que sejam ministrados periodicamente fóruns para tratar (i) de seu gerenciamento e (ii) do planejamento e implementação de controles de segurança, com a participação do Responsável de Segurança e do Comitê de Segurança, contemplando, entretanto não se limitando, à discussão dos seguintes aspectos:

- Revisão e aprovação da política de segurança e das responsabilidades de pessoal nela definidas;
- Monitoração de alterações significativas na política, visando novamente analisar a exposição dos ativos a ameaças;
- Revisão e monitoração dos incidentes de segurança ora identificados;
- Exposição, análise e aprovação de iniciativas visando reforçar a segurança das informações;
- Manutenção de responsabilidades sobre a Política de Segurança dentro da organização;
- Metodologias e processos utilizados (como por exemplo avaliação de riscos, critérios para classificação de ativos);
- Planejamento de programas de conscientização da função de segurança como um todo (Política de Segurança, Infraestrutura de Segurança das Informações) dentro do Grupo;
- Avaliação e manutenção dos controles existentes e planejamento da implementação de novos controles.

Infraestrutura de Segurança das Informações

Definição de responsabilidade sobre Segurança das Informações

Comitê de Segurança

Levando-se em consideração a estrutura organizacional e a cultura da VTCLOG**,** um Comitê de Segurança deve ser definido, contando com a participação de membros de sua alta administração (Gerentes e Diretores incluindo áreas de Auditoria Interna, Tecnologia da Informação e Qualidade), com a responsabilidade estratégica de definir padrões, definir diretrizes e direcionar as atividades de segurança da informação.

Suas atribuições devem incluir as seguintes funções, dentre outras:

- Condução dos fóruns de gerenciamento de Segurança das Informações;
- Definição de responsabilidades para o Responsável de Segurança;
- Identificar as áreas do Grupo que necessitem de soluções de segurança, bem como avaliar os riscos inerentes;
- Acompanhar a implementação de soluções de segurança;
- Acompanhar e auxiliar o Responsável de Segurança.

Infraestrutura de Segurança das Informações

Definição de responsabilidade sobre Segurança das Informações

Responsável de Segurança

A função de Responsável de Segurança deverá ser atribuída a um ou mais especialistas de segurança das informações visando a execução das seguintes tarefas, dentre outras:

- Participação nos fóruns de gerenciamento de Segurança das Informações;
- Identificação dos ativos do Grupo e os responsáveis por cada um;
- Criação e documentação de políticas e procedimentos de segurança para a organização;
- Condução da implementação adequada da Política de Segurança;
- Monitoração do atendimento aos padrões, diretrizes e procedimentos vigentes;
- Planejamento de formas ágeis e eficazes de se monitorar o atendimento aos padrões, diretrizes e procedimentos vigentes, como por exemplo trilhas de auditoria disponíveis em ambientes computadorizados;
- Identificação das áreas do Grupo que necessitem de soluções de segurança;
- Identificação das vulnerabilidades, dos pontos fracos existentes, dos riscos e ameaças inerentes;
- Projeção de controles que suportem os riscos e ameaças mensurados;
- Disponibilização dos recursos necessários e implementação de controles com o auxílio dos Gerentes de cada área;
- Acompanhamento da implementação de soluções de segurança;
- Atuação no processo de melhorias contínuas à segurança dentro do Grupo em conjunto com o Comitê de Segurança;
- Monitoração e análise dos incidentes de segurança ocorridos e sugestão de implementação de controles compensatórios;
- Reporte ao Comitê de Segurança, dos incidentes de segurança ocorridos e seus impactos;
- Condução de revisões periódicas de segurança a fim de garantir que a política esteja sendo adequadamente seguida;
- Avaliação do impacto de quaisquer mudanças no ambiente do Grupo (manutenção ou aquisição de ativos e contratação de novos serviços terceirizados);
- Planejamento e condução de treinamentos periódicos com o objetivo de disseminar a cultura de segurança dentro do Grupo, bem como de comunicar as atualizações eventualmente efetuadas na Política de Segurança.

Infraestrutura de Segurança das Informações

Definição de responsabilidade sobre Segurança das Informações

Responsável de Segurança

- Planejamento da continuidade dos negócios do Grupo, contemplando suas atribuições nesta área, dentre outras, as seguintes responsabilidades:

  - Definição da estratégia para a continuidade dos negócios da VTCLOG incluindo (i) avaliação dos procedimentos em vigor para continuidade dos negócios em situações emergenciais, (ii) estabelecimento de cronograma para elaboração do "Plano de Contingências e Continuidade dos Negócios" do Grupo, (iii) levantamento dos processos operacionais críticos para os negócios do Grupo e identificação de seus respectivos responsáveis, bem como indicação de seus supostos substitutos, (iv) levantamento dos sistemas computadorizados que suportam os processos críticos, (v) avaliação formal do impacto nos negócios, causado pela interrupção no fornecimento de serviços públicos, tais como, energia elétrica, comunicações, transportes, segurança e nos serviços financeiros de infraestrutura e (vi) estabelecimento de planos de análise e revisão dos procedimentos desenvolvidos;
  - Análise de riscos potenciais incluindo (i) identificação dos riscos inerentes aos processos operacionais críticos, (ii) definição de alternativas que poderiam ser implementadas em situações de contingência e (iii) avaliação do nível de impacto e das consequências para os negócios do Grupo com a ocorrência de contingências;
  - Elaboração formal do "Plano de Continuidade dos Negócios", com o auxílio de grupo de trabalho composto por membros da gerência do Grupo e do Comitê de Segurança, levando-se em consideração (i) análise de custo/benefício das alternativas de continuidade planejadas, (ii) definição de estratégias e procedimentos para retomada das operações do Grupo, (iii) estabelecimento de prazos para a implementação das alternativas planejadas e para retomada das operações a um nível satisfatório, incluindo a disponibilização dos recursos necessários para tanto, (iv) avaliação dos custos necessários para a implementação de cada alternativa, (v) avaliação das possíveis perdas do Grupo com a ocorrência de interrupção total ou parcial de seus processos críticos, (vi) definição da equipe de trabalho voltada à implementação e manutenção do "Plano de Continuidade dos Negócios" e (vii) planejamento das situações que acarretarão o acionamento do plano, bem como definição do nível de implementação deste em função de cada situação;
  - Desenvolvimento de plano de testes periódicos para as alternativas operacionais previstas no "Plano de Continuidade de Negócios";

Infraestrutura de Segurança das Informações

Definição de responsabilidade sobre Segurança das Informações

Responsável de Segurança

- Planejamento da continuidade dos negócios do Grupo, contemplando suas atribuições nesta área, dentre outras, as seguintes responsabilidades: -- continuação

  - Planejamento de atualizações ou complementações do "Plano de Continuidade de Negócios";
  - Definição de procedimentos de distribuição de cópias do "Plano de Continuidade de Negócios";
  - Definição de procedimentos para armazenamento de uma cópia do "Plano de Continuidade de Negócios" em localidade distante e independente das dependências do Grupo;
  - Definição de procedimentos de documentação das conclusões advindas de cada um dos aspectos acima mencionados, bem como de aprovação formal da documentação em questão por membros da alta administração, conforme julgado necessário.

Classificação de Ativos e Informações

Classificação e controle de ativos

Podemos dizer que um ativo, é algo que possui valor para a Companhia e, portanto, necessita de proteção. Como exemplos de ativos, podemos citar (i) *informações* contidas em arquivos e bancos de dados, documentação de sistema, manuais de usuários, material de treinamento, procedimentos de suporte e operacionais, plano de continuidade dos negócios e procedimentos de retomada das operações; (ii) *documentos* tais como contratos, demonstrações financeiras e outros contendo resultados de negócios significativos; (iii) *sistemas computadorizados* tais como aplicativos, sistemas básicos, ferramentas de desenvolvimento e utilitários; (iv) *equipamentos* tais como, computadores, equipamentos de comunicação de dados, mídias como por exemplo, fitas e discos, equipamentos de fornecimento de energia alternativa, ar-condicionado, móveis e utensílios; (v) *pessoas* tais como funcionários e clientes; (vi) *imagem e reputação do Grupo*; (vii) *serviços* tais como, computação, comunicação e fornecimento de energia.

O processo de classificação e controle de ativos visa proteger adequadamente os ativos da VTCLOG. Desta forma, todos os ativos julgados pertinentes, deverão ser formalmente inventariados, classificados, valorizados e associados aos sistemas de informação, devendo ainda, ser atribuído a cada um, um proprietário com a responsabilidade da manutenção dos controles apropriados, voltados a garantir a segurança do ativo em questão.

Classificação das informações

Visando garantir que as informações recebam um nível apropriado de proteção, estas devem (i) ser inventariadas, ou seja, devem ser definidas quais informações necessitarão ser protegidas (documentos, relatórios, telas, mídias, mensagens eletrônicas, registros de dados, arquivos de dados e outros), (ii) receber um proprietário com a incumbência de classificá-las e protegê-las e (iii) ser classificadas levando-se em consideração o grau de sensitividade, criticidade, disponibilidade e integridade exigido pelos negócios do Grupo.

As classificações e os controles voltados à proteção das informações, devem levar em consideração as necessidades do negócio em partilhar ou restringir o acesso a determinadas informações, bem como os impactos relacionados a tais necessidades. Em geral, a classificação atribuída às informações, praticamente determina como estas deverão ser manuseadas e protegidas.

As informações passíveis de proteção (documentos, relatórios, telas, mídias, mensagens eletrônicas, registros de dados, arquivos de dados e outros), devem ser rotuladas com base nos riscos oferecidos (como por exemplo Alto, Médio, Baixo, Nenhum) e em sua sensitividade (como por exemplo Extremamente Confidencial, Confidencial, Uso Interno, Uso Público), ambos voltados ao negócio. Para cada rótulo, procedimentos específicos de manuseio das informações, devem ser definidos, como por exemplo procedimentos que permitam cópia, armazenamento, transmissão por correio, transmissão por fax, transmissão por correio eletrônico, transmissão por canais de voz (telefone convencional, telefone móvel, "voice mail", máquinas que requeiram comandos de voz e outros), destruição e outros conforme julgado necessário.

Classificação de Ativos e Informações

Classificação das informações

Serão necessárias revisões periódicas das classificações atribuídas às informações, visando melhor adequar os casos onde tais classificações sejam transitórias. Como exemplo, podemos citar informações confidenciais que em determinado momento tornam-se públicas por sua própria característica e desta forma deixam de ser confidenciais.

A descrição dos rótulos baseados nos riscos oferecidos aos negócios (Alto, Médio, Baixo, Nenhum) e na sensitividade das informações (Extremamente Confidencial, Confidencial, Uso Interno, Uso Público) deverá ser formalmente definida e comunicada a todos os funcionários do Grupo para garantir a eficiência do processo de proteção das informações. Como exemplo de descrição de rótulo, podemos citar que o acesso às informações extremamente confidenciais, deve ser permitido apenas ao proprietário das informações em questão e aos membros da diretoria do Grupo e que sua divulgação acarretaria um alto risco para os negócios.

Relacionamento entre os riscos oferecidos aos negócios, sensitividade das informações e permissão de acesso às informações

Riscos aos negócios **Sensitividade das informações**	**Alto**	**Médio**	**Baixo**	**Nenhum**	**Acesso permitido**
Extremamente Confidencial	X				Proprietários (a), Presidência e Diretoria
Confidencial	X	X			Proprietários, Presidência, Diretoria e Gerência
Uso Interno		X	X		Proprietários, Presidência, Diretoria, Gerência, Áreas envolvidas no processo de geração e uso da informação
Uso Público			X	X	Todos os funcionários do Grupo e pessoas externas à Companhia

(a) Neste caso, os proprietários devem fazer parte da diretoria do Grupo.

Política de Pessoal

O objetivo principal da política de pessoal dentro de uma política de segurança corporativa é procurar reduzir os riscos advindos da ocorrência de erro humano, furto, fraudes ou uso incorreto de recursos.

Responsabilidades voltadas à segurança

As descrições dos cargos de funcionários, terceiros e prestadores de serviços devem (i) ser formalizadas e (ii) conter considerações sobre segurança, no tocante aos deveres e responsabilidades de cada funcionário sobre a implementação, monitoração e manutenção de segurança dentro do Grupo.

Segregação de funções

Segregação de funções é um método utilizado para a redução do risco da utilização incorreta de recursos de forma intencional ou acidental. Em situações onde segregar funções seja impraticável, controles compensatórios devem ser projetados, tais como monitoração de atividades, trilhas de auditoria e supervisão da gerência. É importante manter a execução de procedimentos de auditoria sempre independentes, da área onde segregar funções seja muito difícil.

Áreas que necessitem de uma única pessoa para conduzi-las, requerem que os devidos controles preventivos e detectivos de fraudes sejam desenhados e implementados. É necessário garantir que a inicialização de um evento seja separada de seu processo de autorização.

Treinamento de pessoal

Com o objetivo de manter seus funcionários e prestadores de serviços (conforme julgado necessário), adequadamente cientes e preocupados com as ameaças atualmente concorrentes à segurança das informações, a Companhia deve ministrar treinamentos regulares para disseminar a utilização adequada de facilidades de processamento de informações e a implementação de procedimentos de segurança. Desta forma os treinamentos em questão abordariam, dentre outros, aspectos tais como, (i) políticas, padrões, normas e procedimentos, diretrizes e controles em uso pela Companhia, (ii) responsabilidades internas e legais de cada elemento envolvido na Política Corporativa, (iii) utilização de sistemas computadorizados, (iv) utilização e salvaguarda de ativos em geral. O planejamento e a condução dos treinamentos em questão são de responsabilidade do Responsável de Segurança.

Política de Pessoal

Respostas a incidentes de segurança

Quaisquer incidentes de segurança (falhas de sistemas, interrupção de serviços, erros resultantes de dados incompletos ou inexatos, violações de confidencialidade e contingências dentre outros) ora detectados, devem ser imediata e formalmente reportados à área de Help Desk da VTCLOG, que será responsável por comunicá-los ao Responsável de Segurança. Este será responsável (i) pela análise dos incidentes reportados, (ii) pelo planejamento e implementação de controles preventivos e detectivos a novos incidentes de mesma natureza e (iii) pelo reporte ao Comitê de Segurança, dos incidentes de segurança ocorridos e seus impactos.

Política de “mesa limpa” e “tela limpa”

Visando a redução dos riscos de acesso não autorizado a informações, perda ou danos a informações, devem ser adotadas pelos funcionários do Grupo, as políticas que visam a inexistência de papéis e outras mídias sobre as mesas e a inexistência de informações disponíveis por muito tempo em telas de computador, durante e após o horário normal de trabalho. Desta forma, análise deve ser efetuada, para que conforme apropriado, (i) papéis e mídias utilizadas por computadores sejam armazenados em dispositivos adequadamente protegidos contra acesso, tais como armários, gavetas, cofres e outros e (ii) computadores portáteis, estações e terminais sejam bloqueados ou protegidos por senhas quando estiverem inativos ou estiverem desacompanhados de seus responsáveis.

Adicionalmente, devem ser protegidos contra acesso indevido, pontos de entrada e saída de correspondências, máquinas copiadoras e máquinas de fax. Relatórios cujas informações foram classificadas com Extremamente Confidenciais ou Confidenciais, devem ser removidos imediatamente de impressoras ou outros equipamentos.

Gerenciamento de Autorizações de Acesso

Gerenciamento de autorizações de acesso aos funcionários

Registro de usuários

Para registro de quaisquer usuários nos sistemas computadorizados do Grupo, sejam eles sistemas básicos ou aplicativos, deve ser feita uma solicitação formal à área de Tecnologia de Informática – GI da VTCLOG, estando tal solicitação, previamente aprovada pela gerência da área solicitante do cadastramento.

Devem ser mantidos registros formais de todo e qualquer funcionário cadastrado nos sistemas do Grupo.

Definição do nível de acesso a ser concedido a usuários

Como parte da solicitação de registro de usuários nos sistemas computadorizados do Grupo, deve ser formalmente e detalhadamente definido o nível de acesso a ser atribuído ao usuário em sistemas básicos, aplicativos em geral, correio eletrônico, arquivos de dados, entrando-se até mesmo no mérito de acesso a transações (leitura, gravação, execução, exclusão, criação, modificação).

Devem ser mantidos registros formais de todo e qualquer nível de acesso concedido a usuários nos sistemas do Grupo.

Utilização de grupos para definição do nível de acesso de usuários

A criação de grupos para facilitar o gerenciamento e a definição de níveis de acesso, deve levar em conta os perfis de acesso particulares definidos para cada usuário por sua gerência. Desta forma, somente deverão fazer parte do mesmo grupo e consequentemente ter o mesmo nível de acesso aos sistemas, usuários com atividades idênticas ou extremamente semelhantes em um mesmo departamento.

Devem ser mantidos registros formais de todo e qualquer nível de acesso concedido a grupos nos sistemas do Grupo, bem como dos usuários que pertençam a tais grupos.

Gerenciamento de Autorizações de Acesso

Gerenciamento de autorizações de acesso aos funcionários

Exclusão de acesso de usuários

Desligamentos de funcionários devem ser comunicados formalmente à área de Tecnologia de Informática – GI, com o máximo de antecedência à comunicação do desligamento ao funcionário, conforme consta do padrão de sistema **"Procedimentos de Segurança na Concessão e Uso de Senhas de Acesso às Redes Locais e no Desligamento / Transferência de Funcionários – 540-PS-0061-GI",** para que possam ser extintas quaisquer possibilidades de acesso aos sistemas e ativos do Grupo pelo funcionário demitido.

Juntamente com a comunicação de desligamento, a gerência responsável pelo comunicado deve definir formalmente qual é o destino desejado para os recursos utilizados pelo funcionário em questão, tais como computadores, impressoras, ramais telefônicos, caixa postal de e-mail (possível desvio para recebimento de mensagens por outro funcionário), arquivos de dados, mídias e chaves de criptografia, cartões magnéticos, chaves e "smart cards" dentre outros, conforme julgado necessário.

Devem ser mantidos registros formais de todo e qualquer comunicado de desligamento de funcionários do Grupo.

Manutenção do nível de acesso concedido a usuários

Alterações no nível de acesso concedido a usuários

Quaisquer mudanças ocorridas nas atividades desempenhadas por funcionários do Grupo, sejam elas mudança de função em uma mesma área, transferência de área, transferência de empresa, promoções, devem refletir, caso aplicável, no nível de acesso concedido a estes aos sistemas da VTCLOG. Desta forma, a gerência da área de atuação do funcionário, deve comunicar tais ocorrências formalmente à área de Tecnologia de Informática – GI.

Devem ser mantidos registros formais de toda e qualquer alteração efetuada sobre o nível de acesso concedido aos funcionários do Grupo.

Revisões do nível de acesso concedido a usuários

Devem ser efetuadas em bases semestrais, revisões do nível de acesso concedido a cada usuário nos sistemas, como um controle detectivo de quaisquer mudanças nas atividades eventualmente procedidas e não comunicadas.

Devem ser mantidos registros formais de toda e qualquer alteração efetuada sobre o nível de acesso concedido aos funcionários do Grupo.

Gerenciamento de Autorizações de Acesso

Gerenciamento de autorizações de acesso aos funcionários

Gerenciamento de contas e senhas de controle de acesso

Contas e senhas de controle de acesso são mecanismos para validar a identidade dos usuários para que estes possam obter acesso aos sistemas de informações ou serviços disponibilizados pela Companhia. A atribuição de contas e senhas deve ser controlada através de um processo formal de gerenciamento destas o qual deve contemplar:

- Assinatura de contratos que tratem da confidencialidade de contas, senhas e das informações às quais estas permitem acesso;
- Procedimentos formais para definição de senhas temporárias, como por exemplo, as utilizadas no cadastramento de usuários nos sistemas, quando do esquecimento da senha por parte do usuário ou durante o desbloqueio de usuários no sistema pelo Administrador ou cargo semelhante;
- Exigência de senha de controle de acesso a todos os usuários, para que estes possam obter acesso aos sistemas da VTCLOG**.** Casos em que seja necessário, devem ser documentados e discutidos entre o Comitê de Segurança e o Responsável de Segurança;
- Procedimentos formais que exijam a troca imediata de senhas temporárias por usuários;
- Procedimentos formais de bloqueio de contas por motivos diversos, tais como férias de funcionários, término de contratos de terceiros, término de projetos, licença maternidade, licença por doença, inatividade por tempo razoável, desligamento de funcionário e excesso de tentativas indevidas de acesso consecutivas, dentre outros;
- Existência de um número mínimo de usuários com excesso de privilégios de acesso ao sistema;
- Armazenamento seguro de senhas de controle de acesso em ambientes computadorizados;
- Procedimentos formais para trocas obrigatórias em senhas de controle de acesso em bases mensais;
- Procedimentos formais para composição obrigatória de senhas de controle de acesso com no mínimo 6 caracteres;
- Procedimentos formais para assegurar que senhas de controle de acesso sejam compostas por valores aleatórios, não facilmente decifráveis;
- Procedimentos formais visando não permitir que usuários reutilizem as últimas senhas colocadas em uso por estes;
- Não permissão de conexões concorrentes ao sistema por um mesmo usuário, devendo a Companhia documentar os casos em que este recurso seja necessário;
- Utilização em conjunto com outras tecnologias de identificação e autenticação, tais como sistemas biométricos, assinaturas digitais, "smart cards" e outros.

Gerenciamento de Autorizações de Acesso

Gerenciamento de autorizações de acesso aos funcionários

Responsabilidades dos usuários

Uso de senhas de controle de acesso por usuários

Usuários dos sistemas devem (i) manter suas senhas de controle de acesso confidenciais, (ii) evitar o registro de senhas de controle de acesso em papéis, e caso necessário, tais registros deverão ser mantidos seguros em cofres, (iii) alterar imediatamente suas senhas de controle de acesso, caso desconfiem ou tenham indícios de que estas tenham sido decifradas, (iv) utilizar-se de senhas fáceis de serem lembradas, mas não facilmente decifráveis (nomes próprios, números de telefone, nome da conta no sistema, datas de aniversário e outros), (vi) evitar compor suas senhas com caracteres idênticos repetidos, sejam eles sinais, números ou letras, (v) não reutilizar senhas antigas, (vi) alterar senhas temporárias no primeiro acesso ao sistema com tal senha, (vii) não incluir senhas em processos automáticos de acesso ao sistema, (viii) não compartilhar sua senha com outros indivíduos, nem mesmo utilizar-se da senha de outros indivíduos.

Uso de equipamentos por usuários

Usuários são responsáveis por manter seguros os equipamentos sob sua responsabilidade quando desacompanhados. Desta forma, de acordo com a disponibilidade dos recursos existentes, é necessário que (i) estações sejam bloqueadas quando não atendidas, (ii) protetores de tela sejam ativados em um tempo mínimo de inatividade e sejam protegidos por senha, (iii) sejam utilizados sistemas de controle de acesso às estações de trabalho e (iv) sessões sejam terminadas pelo usuário antes deste ausentar-se, caso não disponha dos recursos suficientes para atender os itens (i), (ii) e (iii).

Vale ressaltar que equipamentos devem ser adquiridos mediante autorização, para que sejam observados os padrões pré-definidos pela Companhia.

Gerenciamento de autorizações de acesso a terceiros

Com o objetivo de manter a segurança das facilidades de processamento de informações e dos ativos, aos quais terceiros e prestadores de serviço tenham acesso, deve ser efetuada análise de riscos sobre o nível de acesso físico e lógico concedido a terceiros e prestadores de serviços, visando a projeção de controles preventivos e detectivos, para que a Companhia possa administrar adequadamente seu risco. As responsabilidades e obrigações dos terceiros e prestadores de serviços com relação aos controles desenhados, devem ser relacionadas no contrato de terceirização ora firmado.

Gerenciamento de Autorizações de Acesso

Gerenciamento de autorizações de acesso aos funcionários

Gerenciamento de autorizações de acesso a terceiros

Os terceiros e prestadores de serviços devem ter inclusas em seus contratos, as mesmas cláusulas constantes do "Termo de Compromisso de Segurança das Informações e Utilização de Ativos", bem como cláusula voltada ao entendimento, conscientização e comprometimento com o conteúdo da Política de Segurança da VTCLOG e de seus adendos (padrões, diretrizes, normas, procedimentos e controles).

Os contratos firmados entre a VTCLOG e seus terceiros e prestadores de serviços, devem passar por revisão de sua área jurídica, visando evitar quaisquer litígios.

.

Segurança Física e Ambiental

Deverão ser implementados procedimentos e controles de segurança voltados à prevenção de acesso físico não autorizado e danos aos ativos da VTCLOG**.** Tais procedimentos e controles deverão proteger áreas tais como centros de processamento de dados, salas com equipamentos de comunicação e fornecimento de energia, dentre outras.

A segurança física deverá ser tratada com a mesma seriedade dispensada à segurança lógica. Esse esforço visa eliminar a ocorrência de roubos, danos ou mal-uso das informações pertencentes à Companhia ou sob responsabilidade da mesma, e garantir a continuidade dos negócios da VTCLOG. Medidas de segurança deverão ser consideradas nos projetos de expansão, alocação e realocação de áreas.

Áreas seguras

A segurança física pode ser implementada com sucesso, através da definição de áreas seguras, as quais podem ser definidas como locais onde estão localizados ativos importantes para a Companhia, sejam eles informações, documentos, sistemas computadorizados, equipamentos e serviços dentre outros e que necessitam de atenção especial com relação à segurança.

Na VTCLOG podem ser identificadas como áreas seguras, centros de processamento de dados, "forrós" (Centros de Distribuição), fábricas, áreas que possuam estações de trabalho e terminais e locais onde são armazenados os equipamentos de suporte e as facilidades de processamento de dados, tais como equipamentos para fornecimento de energia alternativa, suprimentos, fax e impressoras, cada uma com sua característica particular em termos de riscos para a Companhia.

Alguns aspectos devem ser levados em conta quando da construção ou escolha de áreas seguras:

- Localização reservada;
- Controles de acesso e auditoria;
- A construção deve ser fisicamente sólida, não estando sujeita a arrombamentos externos;
- Existência de equipamentos de prevenção e combate a incêndios e inundações.

Quando da mudança de localização física de uma área segura existente, os itens acima devem ser levados em consideração.

Controles de acesso físico

Deverão ser usados controles de acesso físico tais como cartões inteligentes ou magnéticos, senhas ou controles biométricos, dentre outros, para que apenas pessoal autorizado tenha acesso às áreas seguras, devendo todos os acessos ser autenticados e registrados por trilhas de auditoria.

O acesso a áreas seguras pelo pessoal técnico interno da área de Informática da VTCLOG, não necessita de autorizações prévias. Para os demais profissionais, autorizações prévias são necessárias, bem como devem ser geradas trilhas de auditoria com registros dos acessos.

Segurança Física e Ambiental

Áreas seguras

Controles de acesso físico

Visitantes ou prestadores de serviços que necessitem de acesso a uma área segura, deverão (i) ser formalmente autorizados para tanto, (ii) estar acompanhados, (ii) ser alertados dos procedimentos de segurança e de emergência da área, (iii) portar identificação visível, (iv) ter seus acessos registrados por trilha de auditoria.

Todos os funcionários devem usar de forma visível cartão de identificação e devem interpelar pessoas estranhas e ou desacompanhadas com ou sem cartão de identificação, nas áreas seguras do Grupo.

Os procedimentos e controles utilizados para controlar acessos à uma área segura, devem ser periodicamente revisados.

Proteção de escritórios, salas e facilidades

Uma área segura poder ser composta por uma ou mais salas, adequadamente protegidas. A seleção e construção de áreas seguras devem levar em consideração a possibilidade de danos pôr fogo, inundação e outros desastres naturais. Atenção também deverá ser dada a outras questões como poeira, fuligem, efeitos químicos, e interferências elétricas.

Nas áreas seguras, as seguintes medidas de proteção devem ser consideradas:

- Equipamentos e sistemas de controles de acesso, como por exemplo, dispositivos eletrônicos e biométricos, para efetuar a autorização e registro de todos os acessos efetuados às áreas seguras;
- Todas as áreas seguras devem ser discretas, não exibindo a presença de atividades de processamento de informações, dentro ou fora do prédio;
- Equipamentos de suporte como fax, impressoras e copiadoras devem estar localizadas dentro de áreas seguras, evitando assim acessos indevidos a informações;
- Portas e janelas devem permanecer trancadas quando as salas forem desocupadas. Cuidados especiais devem ser dados a janelas localizadas em áreas de fácil acesso, como por exemplo no andar térreo de um edifício;
- Sistemas de detecção de intrusos, em conformidade com os padrões da indústria devem ser adequadamente instalados em todas as portas e janelas devendo ser regularmente testados;
- Guias, catálogos, e agendas contendo informações sensíveis como nomes, números de telefone e endereços devem ser mantidos em locais seguros evitando o acesso de pessoas não autorizadas;
- Materiais perigosos e/ou combustíveis devem ser armazenados de forma adequada e o mais distante possível das áreas seguras;

Segurança Física e Ambiental

Áreas seguras

Proteção de escritórios, salas e facilidades

Nas áreas seguras, as seguintes medidas de proteção devem ser consideradas: -- continuação

- Equipamentos de segurança tais como detectores de fumaça e de combate a incêndio devem estar instalados e ativos, devendo ser regularmente testados de acordo com as especificações do fabricante;
- As áreas seguras devem estar localizadas longe de áreas públicas e de grande acesso, evitando assim o conhecimento e acesso do público;
- Deverão ser implantados equipamentos de monitoração de ambiente (câmeras de vídeo) que registrem todas as atividades efetuadas dentro de uma área segura com risco significativo para a Companhia. Os registros devem ser adequadamente armazenados por um prazo mínimo de 180 dias, permanecendo desta forma disponível para quaisquer análises.

Segurança dos equipamentos

Todos os equipamentos do Grupo, mesmo os localizados fora das áreas seguras ou utilizados fora das instalações do Grupo devem ser protegidos apropriadamente contra acessos não autorizados, perda ou dano dos dados neles armazenados, bem como contra desastres naturais como incêndios e inundações.

Localização dos equipamentos

Os equipamentos do Grupo devem ser localizados e protegidos de forma a reduzir os riscos de desastres naturais e oportunidades de acesso não autorizado. Os seguintes controles devem ser considerados:

- Os equipamentos devem estar localizados de forma a minimizar o acesso desnecessário ás áreas de trabalho;
- Facilidades que permitam o processamento e armazenamento de informações devem ser posicionadas de forma a evitar que pessoas não autorizadas possam ter acesso a estes;
- Equipamentos que requeiram proteção especial como por exemplo servidores e impressoras da diretoria, dentre outros, devem ser isolados, reduzindo-se desta forma o nível de proteção requerido para determinadas áreas;

Segurança Física e Ambiental

Segurança dos equipamentos

Localização dos equipamentos

Os seguintes controles devem ser considerados: -- continuação

- Controles devem ser adotados para minimizar o risco de ameaças potenciais como:

    a) Roubo;
    b) Incêndio;
    c) Explosivos;
    d) Fumaça;
    e) Água (Inundação ou falta de);
    f) Poeira;
    g) Efeitos químicos;
    h) Falta de energia;
    i) Radiação Eletromagnética;
    j) Outras ameaças detectadas no ambiente.

- Não é permitido comer, beber ou fumar nas proximidades dos equipamentos que processem ou armazenem informações do Grupo;
- Quando da avaliação de ameaças ambientais (incêndio, inundação) deverá ser considerado o impacto de desastres que venham a ocorrer nas vizinhanças de áreas seguras.

Suprimento de energia

Os equipamentos do Grupo devem ser protegidos contra falhas ou outras irregularidades no fornecimento de energia elétrica. Procedimentos de fornecimento alternativo de energia devem ser implementados, visando a continuidade dos negócios do Grupo.

Algumas opções para garantir a continuidade no fornecimento de energia são:

- Implementação de várias fontes de energia, evitando assim a dependência de um único ponto;
- Instalação de equipamentos de fornecimento ininterrupto de força (Uninterruptable Power Supply - UPS) com capacidade suficientemente planejada;
- Gerador de Backup.

Todos os equipamentos de processamento e armazenamento de informações devem estar conectados a equipamentos de fornecimento ininterrupto de força, garantindo assim um fluxo constante e sem anomalias de energia.

Segurança Física e Ambiental

Segurança dos equipamentos

Suprimento de energia

Planos de continuidade dos negócios devem contemplar as ações a serem tomadas em caso de falha de equipamentos de fornecimento ininterrupto de força (UPS) e de fornecimento de energia alternativa (Gerador).

Os equipamentos de fornecimento ininterrupto de força e de fornecimento de energia alternativa devem ser regularmente testados para assegurar que a capacidade especificada e o seu funcionamento estão normais.

Equipamentos de fornecimento de energia alternativa (Geradores), devem ser considerados em locais onde falhas prolongadas de energia sejam esperadas e devem ser testados regularmente de acordo com as instruções do fabricante. Deverá existir combustível suficiente para garantir o funcionamento do gerador em caso de falhas prolongadas de energia.

Luzes de emergência também devem ser consideradas para casos de falha geral de energia elétrica, equipamentos de proteção contra raios deverão ser implementados em todas as construções que contenham áreas seguras e filtros devem ser implantados em todas as linhas de comunicação externa.

Segurança do cabeamento

O cabeamento de rede e elétrico, transmitindo dados ou suportando os serviços de informação da VTCLOG deve ser protegido contra interceptações e danos. Os seguintes controles devem ser considerados com relação ao cabeamento:

- Cabos devem permanecer à medida do possível abaixo do piso ou embutido em paredes, sempre que possível, ou devem ser submetidos a medidas de proteção alternativas;
- O cabeamento de rede deve ser protegido de interceptações e danos, desta forma, exposição através de áreas públicas deve ser evitada;
- Cabos de energia e comunicação devem ser segregados para que seja evitada interferência;
- Equipamentos de comunicação (“hubs”, “switches”, repetidores) que tenham de estar localizados fora de uma área segura, deverão estar dentro de móveis trancados, resistentes a violações físicas;
- Somente os pontos de rede necessários devem estar habilitados, dependendo a habilitação de novos pontos, da autorização do responsável pela área de Tecnologia de Informática – GI. Pontos habilitados para uso temporário, devem ser desabilitados logo após o término de seu uso;
- Para sistemas extremamente sensíveis ou críticos é necessário planejar o uso de fibra ótica e a varredura do cabeamento visando a detecção de dispositivos não autorizados, sniffers ou outros coletores de pacotes de rede.

Segurança Física e Ambiental

Segurança dos equipamentos

Uso de equipamentos fora da organização

O uso de qualquer equipamento fora do perímetro do Grupo para o processamento de informações, deverá ser autorizado pela diretoria independente da propriedade do equipamento.

A segurança desses equipamentos deverá ser equivalente aos usados dentro do Grupo para o mesmo propósito, levando-se também em consideração os riscos do trabalho efetuado fora das premissas do Grupo. Equipamentos para processamento de informações incluem todas as formas de computadores portáteis, organizadores pessoais, telefones móveis e celulares, dentre outros. Os seguintes controles devem ser considerados:

- Equipamentos, documentos e mídias fora do perímetro do Grupo, não devem permanecer desacompanhados;
- Quando em viagem, computadores portáteis devem ser levados como bagagem de mão;
- As instruções do fabricante sobre a proteção dos equipamentos devem sempre ser observadas, tais como verificação de voltagem e proteção contra campos eletromagnéticos, dentre outras;
- O uso de criptografia deverá ser considerado para informações sensíveis;
- Equipamentos usados fora das premissas da organização, deverão ser apropriadamente cobertos por seguros.

Os riscos aos quais os equipamentos são expostos variam de acordo com a localidade que está sendo visitada, isso deve ser levado em conta pela avaliação de riscos que irá determinar os controles a serem utilizados para garantir a segurança das informações e equipamentos.

Remoção de ativos

Equipamentos, informações sob quaisquer formas (mídias, documentos e outras) ou sistemas computadorizados não devem ser removidos do Grupo sem a devida autorização. Deverão ser planejadas auditorias sem prévio aviso visando detectar ativos removidos sem a devida autorização.

Segurança Física e Ambiental

Segurança contra desastres naturais

Desastres naturais representam uma ameaça significativa aos negócios do Grupo, pois os equipamentos usados no processamento e armazenamento das informações têm sensibilidade a mudanças de temperatura, falhas e anomalias no fornecimento de energia elétrica, água e poeira. Essas características requerem a implantação de controles preventivos adequados para garantir a continuidade dos negócios do Grupo.

Uma análise de riscos formal deve ser efetuada, levando-se em consideração a estrutura física de cada instalação, as ameaças inerentes da região de residência da área segura, a natureza das operações de cada área segura e o número de ativos residentes, para que os controles preventivos e detectivos abaixo relacionados, possam ser adequadamente adaptados visando minimizar os riscos em questão.

Os seguintes controles devem ser implementados e devem constar como parte do Plano de Continuidade de Negócios do Grupo:

Fogo e Fumaça

- Deverão ser instalados detectores de fumaça e temperatura, bem como alarmes, nas proximidades de áreas seguras, conforme julgado necessário;
- Áreas seguras devem possuir extintores de incêndio, periodicamente revisados de acordo com as especificações do fabricante;
- Deverão ser implementadas políticas formais de proibição ao fumo em áreas seguras, principalmente próximo aos equipamentos de tecnologia;
- Deverão ser implantados sistemas automáticos de extinção de incêndio em todas as áreas seguras, conforme julgado necessário.

Variações Climáticas

- Em áreas seguras que possuam equipamentos de informática, conforme julgado necessário, deve haver mecanismos de controle de temperatura e umidade;
- Procedimentos e controles voltados à monitoração dos níveis de umidade e temperatura, devem ser implementados;
- Em áreas com exposição significativa a poeira e fuligem, filtros de ar devem ser considerados.

Água

- Em áreas seguras, proteções contra eventuais danos causados por inundações, rompimento de encanamentos ou vazamentos, devem ser consideradas, como por exemplo o uso de equipamentos de drenagem, e de sensores de água nos tetos e paredes, dentre outros.

Segurança Física e Ambiental

Segurança contra desastres naturais

Raios

- Deve ser considerada, a implantação de proteções contra raios em áreas seguras;
- Mídias magnéticas devem ser armazenadas o mais distante possível de estruturas de aço das construções, evitando assim o contato com campos magnéticos, criados quando da ocorrência de raios.

Cópias de Segurança dos Dados e Informações

O acesso às cópias de segurança deve ser controlado e restrito aos proprietários da informação armazenada. Todas as cópias de segurança deverão ser testadas periodicamente para garantir a sua integridade e conformidade com os planos de contingência do Grupo.

Geração de cópias de segurança

Cópias de segurança das informações e sistemas do Grupo, devem ser efetuadas periodicamente, desta forma procedimentos formais adequados para a geração de cópias de segurança, devem ser implantados para garantir a recuperação das informações e sistemas do Grupo, quando da ocorrência de quaisquer desastres ou problemas potenciais em mídias de armazenamento.

Deve-se determinar a periodicidade com que serão geradas as cópias de segurança, com base nos seguintes fatores, dentre outros:

- Número de usuários do sistema;
- Volume de alterações;
- Volume de transações;
- Classificação atribuída às informações, balizada nos riscos oferecidos ao negócio e em sua sensitividade;
- Profundidade do Plano de Continuidade dos Negócios do Grupo.

Adicionalmente, deve-se considerar (i) o uso de técnicas de criptografia para informações sensíveis, (ii) planejamento quanto a recursos computacionais necessários e horários para a geração das cópias de segurança para se evitar impacto significativo na performance dos equipamentos e sistemas.

Armazenamento de cópias de segurança

Cópias de segurança devem ser mantidas internamente, nas instalações do Grupo, e externamente em local distante e independente das instalações em questão, tendo ambas localidades o mesmo nível de segurança contra acessos não autorizados.

As mídias em localidades internas e externas à Companhia, devem ser mantidas em cofres à prova de fogo, os quais devem permanecer trancados e em local com acesso restrito e controlado.

O período de armazenamento das cópias deve ser determinado com base na classificação das informações nelas contidas.

Cópias de Segurança dos Dados e Informações

Verificação periódica das cópias de segurança

Cópias de segurança armazenadas internamente ou externamente à Companhia, devem ser verificadas periodicamente para certificar-se de que (i) a mídia não possua danos, (ii) a informação tenha sido armazenada corretamente, (iii) a restauração dos dados possa ser efetuada de forma integra e em conformidade com o Plano de Continuidade dos Negócios do Grupo.

Identificação das cópias de segurança

Todas as mídias contendo cópias de segurança devem ser devidamente rotuladas, facilitando sua localização quando necessário, bem como evitando que cópias sejam apagadas acidentalmente. Os rótulos devem conter, dentre outros, os seguintes dados:

- Data e hora em que as cópias foram geradas;
- Nome do operador;
- Descrição das informações contidas na mídia;
- Especificação do tipo de cópia efetuada (total, incremental ou outras);
- Data do último teste;
- Nome de quem efetuou o último teste;
- Numeração especificando a posição da mídia em um conjunto.

Segurança sobre cópias de segurança em trânsito

Cópias de segurança que necessitem ser transportadas para outros locais, apresentam-se expostas a uma gama de ameaças, tais como acessos não autorizados, danos causados às mídias e corrupção dos dados, dentre outras. Para zelar pela segurança das cópias, os seguintes controles devem ser considerados:

- A idoneidade das empresas ou pessoas que estiverem efetuando o transporte deverá ser constatada e aprovada pela Companhia;
- A embalagem contendo as mídias deverá dar mostras de violação, ser resistente a choques, ser resistente a mudanças de temperatura e deve atender às especificações do fabricante da mídia;
- Uso de criptografia;
- Uso de senhas quando da criação das cópias de segurança;
- Entregas das embalagens somente devem ser efetuadas para as pessoas responsáveis pelo recebimento, em quaisquer localidades. Para tanto deve ser criado procedimento formal para envio e recebimento de mídias a localidades externas.

Trilhas de Auditoria

Trilhas de auditoria são extremamente necessárias tendo o objetivo de se detectar a execução de atividades não autorizadas. Portanto, procedimentos formais voltados ao planejamento, geração, análise e armazenamento de trilhas de auditoria periódicos, devem ser criados.

Análise de riscos e planejamento

Visando a detecção de quaisquer atividades inadequadas, danosas ou não usuais, o uso de trilhas de auditoria faz-se necessário. Portanto, deve ser efetuado um breve processo de análise de riscos aos negócios, visando definir-se (i) quais atividades devem ser acompanhadas por trilhas de auditoria (como por exemplo, tentativas indevidas de acesso consecutivas, operações, problemas com processamento, falhas, trilhas de sistemas operacionais, trilhas de transações em aplicativos e outras), (ii) de que forma (eletronicamente ou manualmente), (iii) quais serão os mecanismos necessários para atender às necessidades de geração de trilhas de auditoria (tais como, recursos disponibilizados pelos sistemas computadorizados existentes, novas ferramentas, novos equipamentos, recursos que incrementem a capacidade dos equipamentos, dentre outros), (iv) qual a periodicidade de revisão necessária das trilhas de auditoria, (v) procedimentos para análise das trilhas de auditoria e (vi) procedimentos para armazenamento de trilhas de auditoria.

Geração de trilhas de auditoria

Com base na análise de riscos acima mencionada, trilhas de auditoria devem ser mantidas, conforme julgado necessário, sobre:

- *Eventos*, abrangendo dados tais como nomes das contas de usuários, data e hora de entrada e saída do sistema, identificação do terminal ou estação, número de tentativas de acesso válidas e inválidas aos sistemas, número de tentativas válidas e inválidas de acesso aos dados e outros recursos;
- *Uso do sistema*, contemplando o acompanhamento de operações privilegiadas tais como:
  - uso de contas com privilégios máximos de acesso aos sistemas;
  - inicialização e desligamento do sistema;
  - conexão e desconexão de dispositivos de entrada e saída de dados da rede;
- *Tentativas de acesso não autorizadas*, contemplando tentativas inválidas de acesso, violações da política de acessos e notificações para "gateways" ou "firewalls", alertas de sistema específico para detecção de intrusos;
- *Alertas do sistema ou falhas*, contemplando alertas ou mensagens da máquina "console", alertas sobre falhas nos sistemas, alarmes sobre problemas com o gerenciamento de rede, ações corretivas sobre falhas;
- *Operação do sistema*, contemplando erros do sistema e ações corretivas tomadas, manuseio de arquivos de dados, nome do operador.

Trilhas de Auditoria

Sincronização dos relógios do sistema

A sincronização dos horários nos relógios dos computadores é muito importante no processo de geração de trilhas de auditoria para garantir a precisão dos dados constantes nas trilhas em questão. Trilhas de auditoria inexatas podem atrapalhar investigações baseadas nos dados nelas contidos, bem como fazem com que sua credibilidade seja afetada. Portanto, devem ser seguidos procedimentos para manter sincronizados todos os relógios dos computadores utilizados pela Companhia.

Tráfego de Informações

Gerenciamento de redes de comunicação de dados

A gerência de redes é responsável pela disponibilidade e compartilhamento de informações do Grupo. Portanto a implantação de controles para garantir a segurança das informações compartilhadas ou armazenadas na rede, bem como dos serviços disponibilizados, deve ser de responsabilidade da gerência de redes. Os seguintes aspectos, dentre outros, devem ser considerados em redes de comunicação de dados:

- Segregação das responsabilidades operacionais sobre gerenciamento de redes e operação de computadores;
- Deverão ser estabelecidos responsabilidades e procedimentos para administração remota de quaisquer equipamentos;
- Controles devem ser implementados para garantir a confidencialidade e integridade das informações trafegadas na rede, bem como para garantir a disponibilidade dos serviços de rede e dos computadores nela conectados;
- O monitoramento da performance da rede deve ser efetuado visando a garantia da (i) qualidade e (ii) disponibilidade do serviço e a exposição de tentativas de ataques.

Redes que (i) ultrapassem os limites organizacionais, (ii) estejam interconectadas a outras Companhias ou (iii) utilizem infraestrutura pública, devem considerar a implementação dos seguintes controles, dentre outros:

- Implantação de filtros de pacotes e ou “firewalls”, visando o controle do tráfego entre as redes;
- Uso de sistemas de detecção de intrusos, visando a análise e resposta em tempo real de atividades suspeitas;
- Uso de redes privadas virtuais (“VPN’s – Virtual Private Networks”) e criptografia para garantir a integridade e confidencialidade das informações trafegadas.

Deverá ser assegurado que os controles de segurança sejam aplicados uniformemente em todas as redes do Grupo.

Tráfego de Informações

Segurança e manuseio de mídias

Segurança de mídias

Todas as mídias, sejam elas (i) eletrônicas como discos flexíveis, cartuchos e fitas, (ii) listagens de programas ou (iii) documentação em geral, pertencentes à Companhia, devem ser adequadamente protegidas, devendo o nível de proteção, ser definido em conformidade com a classificação das informações nelas armazenadas. A lista abaixo identifica algumas mídias que requerem tratamento seguro:

- Documentos em papel;
- Gravações de vozes;
- Vídeos;
- Papel carbono;
- Relatórios em papel ou eletrônicos;
- Fitas descartáveis para impressora;
- Fitas magnéticas;
- Discos e cassetes removíveis;
- Listagens de códigos fonte de programas computadorizados;
- Dados de testes efetuados em sistemas;
- Documentação de sistema.

Procedimentos adequados deverão ser estabelecidos visando a proteção contra danos, roubo, acessos não autorizados e outros riscos inerentes, às mídias de armazenamento.

Manuseio das informações armazenadas

Procedimentos para o manuseio e armazenamento das informações contidas nos diversos tipos disponíveis de mídia, devem ser estabelecidos de maneira a assegurar a proteção de tais informações. Deverá ser considerada a avaliação das informações quando da escolha de procedimentos de manuseio e armazenamento de informações. Os seguintes fatores, dentre outros, devem ser levados em consideração:

- Todas as mídias devem estar rotuladas, observando-se os padrões previamente definidos em **"Identificação das Cópias de Segurança"**;
- Definição e manutenção de registros formais de usuários autorizados a receber as mídias contendo informações;
- Revisão periódica dos registros de usuários autorizados a receber as mídias;
- Distribuição de informações restrita a um número mínimo de usuários;
- Definição de controles para assegurar a integridade das entradas de dados, visando melhor garantir a qualidade da saída do processamento dados a ser armazenada em mídias.

Tráfego de Informações

Segurança e manuseio de mídias

Manuseio das informações armazenadas

Os seguintes fatores, dentre outros, devem ser levados em consideração: -- continuação

- Proteção de dados armazenados em áreas temporárias tais como "spool", à espera de processamento;
- O armazenamento das mídias deverá ser efetuado de acordo com as especificações do fabricante da mesma, bem como devem ser observados os padrões previamente definidos no capítulo **"Armazenamento de Cópias de Segurança"**.

Destruição de mídias

Mídias devem ser devidamente descartadas quando não mais possuírem utilidade para a Companhia. O descarte das mídias deverá ser efetuado visando garantir a segurança contra acessos indevidos às informações nelas contidas. Procedimentos formais devem ser estabelecidos, considerando-se, dentre outros, os seguintes fatores:

- Mídias que contenham informações sensíveis, classificadas como "Extremamente Confidenciais", "Confidenciais" ou "Uso Interno" devem ser descartadas através de fragmentação, incineração ou trituração;
- Mídias eletrônicas defeituosas, conforme julgado necessário, devem ser desmagnetizadas;
- Arquivos em mídias eletrônicas devem ser excluídos de forma segura;
- Quando da escolha de prestadores de serviços de coleta do material descartado, observações cuidadosas devem ser efetuadas quanto à idoneidade e experiência destes.

Segurança de mídias em trânsito

As informações estão vulneráveis a acessos não autorizados, mal-uso ou corrupção durante o seu transporte físico por quaisquer meios. Desta forma, as mesmas considerações efetuadas no capítulo **"Segurança sobre cópias de segurança em trânsito"** devem ser observadas.

Tráfego de Informações

Segurança do correio eletrônico

O correio eletrônico atualmente está sendo utilizado nas Companhias em detrimento de outras tecnologias como fax, telex e cartas. O Correio eletrônico difere de outras tecnologias de comunicação de várias formas, como por exemplo, na informalidade, velocidade e vulnerabilidade a ações não autorizadas, dentre outras. Abaixo são listados alguns dos riscos de segurança apresentados na comunicação através de correio eletrônico:

- As mensagens enviadas estão passíveis de ataques tais como (i) acessos não autorizados, (ii) modificações, (iii) DoS[1] e (iv) viroses;
- Possibilidade de erros, como por exemplo, endereços incorretos;
- Impacto da mudança do meio de comunicação nos processos do Grupo, como por exemplo, o efeito da velocidade de entrega da mensagem e do envio de mensagens formais de pessoas para pessoas e não de Companhias para Companhias;
- Considerações legais, como necessidade de provas de (i) origem, (ii) envio e (iii) recebimento de mensagens;
- Possíveis implicações da publicação das listas de endereços eletrônicos do Grupo;
- Acesso remoto de usuários legítimos aos serviços de correio eletrônico.

Uma política clara e completa sobre o uso de correio eletrônico, deve ser criada, divulgada para todos os usuários e administradores da VTCLOG e o seu cumprimento deverá ser monitorado. Alguns dos aspectos os quais deverão ser considerados na elaboração da política são:

- Definição de uso do correio eletrônico como uma ferramenta de comunicação do Grupo, não devendo ser utilizada para assuntos pessoais;
- Responsabilidade do funcionário em não comprometer a empresa com as suas ações, como por exemplo, o envio de mensagens difamatórias e a efetivação de compras não autorizadas;
- Descrição e divulgação dos controles implementados contra-ataques;
- Proteção dos arquivos anexados às mensagens;
- Definição do tamanho máximo permitido para arquivos que sejam anexados a mensagens enviadas e recebidas;
- Cuidados com o tráfego de informações extremamente confidenciais, confidenciais ou para uso interno;
- Uso de criptografia para garantir a confidencialidade e integridade das informações;
- Uso de assinaturas digitais visando garantir a identidade do remetente e integridade da mensagem;
- Retenção ou destruição de mensagens de acordo com o seu conteúdo;
- Possível uso de mensagens em processos jurídicos;
- Controles para negar o recebimento de mensagens que não possam ser autenticadas;
- Medidas disciplinares para aplicação caso a política não seja atendida.

[1] O acrônimo DoS (Denial of Service) significa o ato de interromper o funcionamento de algum serviço de rede, utilizando-se de alguma falha no protocolo ou software.

Controles de Criptografia

Sistemas de criptografia devem ser utilizados em informações conforme sua classificação bem como, em áreas onde controles não garantem um nível de segurança adequada. Controles de criptografia podem ser utilizados para garantir a autenticidade de informações e mensagens e fornecer proteção para as seguintes propriedades da informação:

Confidencialidade
O uso de criptografia assegura que apenas pessoas autorizadas tenham acesso à informação criptografada. A confidencialidade é assegurada mesmo com a ocorrência de incidentes como roubos de mídias ou computadores.

Integridade
Alguns algoritmos de criptografia proveem proteções contra falsificações evitando a alteração indevida de dados. Este tipo de criptografia detecta qualquer alteração efetuada, sendo ela autorizada ou não.

Autenticidade
Técnicas de criptografia podem ser usadas para a confirmação exata de dados, como exemplo podemos citar a confirmação do remetente de uma mensagem. Desta forma, transações comerciais e legais são garantidas.

Apesar de todas os benefícios enumerados, o uso de criptografia deverá ser previamente planejado e uma estrutura de manutenção de chaves de criptografia deverá ser criada para suportar adequadamente os controles implantados.

Política para o uso de criptografia

A decisão do uso de controles de criptografia deve fazer parte de um processo de avaliação de riscos e seleção de controles para que o nível de proteção requerido por um determinado ativo de informação possa ser determinado. Esta avaliação também poderá ser usada para que seja determinado se o uso de criptografia é apropriado e qual tipo de controle deverá ser aplicado.

Deve ser desenvolvida uma política para o uso de criptografia visando proteger as informações do Grupo. Esta política visa maximizar os benefícios, minimizar os riscos apresentados pelo uso de controles de criptografia e evitar seu uso inapropriado ou incorreto. Para tanto, os seguintes tópicos deverão ser considerados:

- Diretrizes administrativas para o uso de controles de criptografia na Companhia, incluindo os princípios gerais para que as informações sejam protegidas;
- As diretrizes para administração de chaves de criptografia, incluindo métodos para efetuar a recuperação de informações criptografadas em caso de perda, comprometimento ou danos às chaves;
- Definição de cargos e responsabilidades de pessoal para a política, em seu (i) planejamento e análise de riscos, (ii) criação, (iii) implementação, (iv) divulgação, (v) manutenção e (vi) administração de chaves de criptografia;

Controles de Criptografia

Política para o uso de criptografia

- Determinação do nível apropriado de criptografia a ser aplicado nas informações;
- Padrões adotados pela Companhia para a implementação efetiva dos controles de criptografia definindo-se qual solução será usada e em quais processos.

Encriptação

Encriptação é uma técnica criptográfica que pode ser usada para proteger a confidencialidade das informações. O uso de encriptação deverá ser considerado para proteção de informações sensíveis ou críticas.

Baseado em uma avaliação de riscos, o nível de proteção requerido deverá ser identificado tendo em consideração o tipo e qualidade do algoritmo de encriptação utilizado e também o tamanho das chaves de criptografia utilizadas.

Quando da implementação da política de criptografia do Grupo, deverão ser consideradas quaisquer leis, regulamentos e restrições legais sobre o uso de técnicas de criptografia nos países em que a Companhia atua e também as questões acerca do fluxo de informações encriptadas. Consideração adicional deverá ser dada aos controles de importação e exportação de tecnologia de criptografia.

Consultorias especializadas podem ser exigidas para identificação do nível apropriado de proteção e para a seleção de produtos adequados que irão prover a proteção requerida e a implementação de um sistema seguro de gerenciamento de chaves. Adicionalmente, consultoria legal pode ser exigida para garantir o cumprimento das leis e regulamentos que se apliquem às técnicas de criptografia pretendidas pela Companhia.

Assinaturas digitais

Assinaturas digitais proveem meios para assegurar a autenticidade e integridade de documentos eletrônicos. Elas podem ser usadas, por exemplo, em comercio eletrônico aonde exista a necessidade de verificação de quem assinou um documento eletrônico e na verificação de mudanças do conteúdo de um documento que tenha sido previamente assinado.

Assinaturas digitais podem ser utilizadas em qualquer forma de documentos que possam ser processados eletronicamente, por exemplo, assinatura de pagamentos eletrônicos, transferência de fundos, contratos e acordos. Podem ser implementadas usando uma técnica de criptografia baseada em um par de chaves relacionadas, onde uma das chaves é utilizada para criar a assinatura (chave privada) e a outra para verificar a assinatura (chave pública).

Controles de Criptografia

Assinaturas digitais

Cuidados deverão ser tomados para garantir a proteção da chave privada. Esta chave deve ser mantida em segredo, pois qualquer pessoa que possua acesso a ela poderá assinar documentos eletrônicos. Adicionalmente a proteção da integridade da chave pública também é importante e é implementada através do Certificado de Chave pública.

Consideração deve ser dada para o tipo e qualidade do algoritmo de encriptação utilizado, assim como para o tamanho das chaves de criptografia. As chaves utilizadas para assinaturas digitais deverão ser diferentes das chaves de encriptação.

Deverá ser formalizada a validade legal do uso de assinaturas digitais em contratos e acordos.

Serviços de não repúdio

Serviços de não repúdio devem ser utilizados na resolução de disputas sobre a ocorrência ou não de um evento ou ação, por exemplo, uma disputa envolvendo o uso de uma assinatura digital em um contrato eletrônico ou pagamento. Elas podem ajudar a estabelecer evidências, que provem a ocorrência de um determinado evento ou ação. Estes serviços são baseados no uso de técnicas de criptografia e assinaturas digitais.

Gerenciamento das chaves de criptografia

O Gerenciamento de chaves de criptografia é essencial para o uso efetivo de técnicas de criptografia. O comprometimento ou perda de chaves de criptografia acarretará em possível perda de confidencialidade, integridade e ou disponibilidade das informações. Com isso, deverá ser implantado um sistema de gerenciamento de chaves para suportar o uso destas pela Companhia através das seguintes técnicas de criptografia:

Técnica de Chave Privada
Onde as partes envolvidas no processo de criptografia de dados compartilham a mesma chave, a qual é utilizada nos processos de encriptação e decriptação (processo inverso a encriptação, reverte as informações encriptadas ao seu formato original) das informações. Esta chave deve ser mantida em segredo pois qualquer pessoa que a possua estará habilitada para decriptar informações e introduzir informações não autorizadas.

Técnica de Chave Pública
Cada parte envolvida no processo tem em seu poder duas chaves relacionadas, a chave pública (a qual poderá ser revelada a qualquer pessoa ou organização) e a chave privada (a qual deverá permanecer em segredo). Técnicas de chave pública podem ser utilizadas para encriptação e na criação de assinaturas digitais.

Controles de Criptografia

Gerenciamento das chaves de criptografia

Todas as chaves devem ser protegidas contra modificação e as chaves privadas necessitam de proteção para que sejam mantidas em segredo. Deverá ser assegurada a proteção física de equipamentos utilizados para gerar e armazenar chaves.

Deverá existir um responsável pela manutenção do sistema de gerenciamento assim como por quaisquer incidentes que envolvam controles de criptografia.

Padrões, procedimentos e métodos

Um sistema de gerenciamento de chaves deve ser composto de um conjunto fixo de padrões, procedimentos e métodos seguros para:

- Criação de chaves para diferentes sistemas de criptografia e aplicações;
- Criação e obtenção de certificados de chave pública;
- Distribuição de chaves para usuários autorizados, incluindo procedimentos de armazenamento e ativação das chaves quando recebidas;
- Mudanças ou atualizações de chaves, incluindo regras sobre quando as chaves devem ser alteradas e como deverá ser efetuada a mudança;
- Cancelamento de chaves incluindo quando estas devem ser retiradas do sistema ou desativadas. Em caso de desligamento de um funcionário deverá ser considerada a troca das chaves e arquivamento das mesmas;
- Recuperação de chaves perdidas ou corrompidas, garantindo a recuperação das informações encriptadas;
- Armazenamento de chaves;
- Destruição de chaves;
- Geração de trilhas de auditoria.

De maneira a reduzir a probabilidade do comprometimento de chaves, deverão ser definidas datas de ativação e desativação, permitindo assim que as chaves sejam utilizadas apenas por um período limitado de tempo. Este período será dependente das circunstâncias sobre as quais o controle de criptografia está sendo utilizado e os riscos envolvidos.

Procedimentos deverão ser considerados para o tratamento de requisições legais de acesso a chaves, por exemplo, quando da necessidade de informações encriptadas em processos legais.

Adicionalmente, deverá ser considerada a proteção de chaves públicas através de certificados digitais. Os certificados digitais são produzidos de maneira a relacionar informações do Grupo ao seu par de chaves públicas e privadas, dificultando ou impossibilitando a falsificação das mesmas. Portanto é de extrema importância que o processo de criação dos certificados seja confiável e conduzido por alguém idôneo e competente para tanto.

Segurança sobre Recursos de Automação Comercial

Utilização de recursos de automação comercial

Visando (i) proteger as informações e dados manuseados por sistemas computadorizados de automação tais como editores de textos, planilhas eletrônicas, softwares gráficos e softwares de envio e recebimento de mensagens, dentre outros, bem como (ii) evitar a ocorrência de quaisquer danos aos negócios da VTCLOG, advindos do mau uso dos sistemas em questão, os seguintes aspectos devem ser observados:

- A aquisição dos recursos em questão, somente deve ser efetivada mediante autorização da área de Tecnologia de Informática – GI, visando a utilização apenas de sistemas homologados pela Companhia;
- Não devem ser utilizados através das facilidades de processamento de informações do Grupo, sistemas não licenciados;
- As aquisições e contratações de serviços relacionados com os recursos em questão, apenas devem ser efetuadas através de fornecedores de equipamentos, sistemas computadorizados e demais produtos de informática devidamente homologados pela área de Tecnologia de Informática – GI;
- Auditorias periódicas devem ser conduzidas, visando a detecção do uso de equipamentos, sistemas computadorizados e demais produtos não homologados pela Companhia.

Proteção contra vírus

Com o intuito de proteger os serviços, sistemas e informações do Grupo, devem ser utilizados sistemas de detecção, prevenção e eliminação de vírus em todas as estações de trabalho, computadores portáteis, computadores pessoais e servidores dentre outros. Adicionalmente, devem ser observados os seguintes fatores:

- Devem ser adotados procedimentos formais para obtenção de sistemas e arquivos de redes externas com o intuito de utilizá-los nos computadores do Grupo;
- Deve haver estudo para identificar a melhor alternativa preventiva de vírus nos computadores do Grupo, como por exemplo a utilização de criptografia em discos rígidos e flexíveis e a desabilitação dos acionadores de discos flexíveis, dentre outros;
- Procedimentos formais rígidos de atualização dos sistemas de detecção, prevenção e eliminação de vírus devem ser projetados.

É expressamente proibida a remoção de sistemas de detecção, prevenção e eliminação de vírus de computadores do Grupo, sem autorização das áreas de Tecnologia de Informática – GI e de Segurança. Casos em que haja necessidade devem ser documentados e aprovados formalmente.

Controle de Acesso em Redes de Comunicação

Autenticação de usuários para conexões externas

Quaisquer conexões externas devem passar por um "firewall", monitorado por sistemas automáticos de prevenção e detecção de intrusos.

Controle de acesso

Facilidades de segurança disponibilizadas por sistemas para restringir acesso a recursos computadorizados, devem ser adequadamente utilizadas, principalmente visando (i) autenticar a identidade e se necessário, a localização de cada usuário de forma segura, (ii) registrar tentativas com sucesso ou não, de obtenção de acesso ao sistema, (iii) onde apropriado, restringir tempo de conexão de usuários. Desta forma, procedimentos seguros de autenticação devem levar em consideração, dentre outros, a ativação de recursos que viabilizem os seguintes aspectos:

- Obter acesso ao sistema impreterivelmente através de uma senha de controle de acesso por quaisquer usuários;
- Mudanças imediatas de senhas temporárias por usuários;
- Bloqueio de usuários por um número máximo de três tentativas inválidas de acesso;
- Contas bloqueadas por tentativas inválidas de acesso, devem permanecer bloqueadas até que haja intervenção do administrador do sistema, bem como o contador de tentativas inválidas, não deve ser reinicializado em prazos curtos de tempo;
- Senhas de controle de acesso, devem sofrer alterações obrigatórias em bases mensais;
- Senhas de controle de acesso devem ser compostas obrigatoriamente por no mínimo 6 caracteres, não repetidos e não facilmente decifráveis;
- A usuários apenas uma conta para acesso ao sistema seja atribuída e a identificação da conta em questão, não deve ter quaisquer relações com o nível de acesso que lhe fora atribuído (como por exemplo *manager*, *supervisor*);
- Usuários não possam reutilizar permanentemente as últimas senhas colocadas em uso por estes;
- Não se deve exibir na tela dos equipamentos (i) dados sobre os sistemas ou aplicações ou (ii) mensagens de ajuda, até que a autenticação do usuário tenha sido finalizada com sucesso;
- Deve ser exibida na tela dos equipamentos, mensagem informando que o acesso aos computadores do Grupo, somente pode ser efetivado por pessoas autorizadas;
- Devem ser utilizadas técnicas de criptografia;
- Utilização em conjunto com outras tecnologias de identificação e autenticação, tais como sistemas biométricos, assinaturas digitais, "smart cards" e outros;
- Deve ser planejada a utilização de sistemas de gerenciamento de senhas de controle de acesso, caso os recursos disponibilizados pelos sistemas utilizados pela Companhia, não sejam suficientes;
- Devem ser definidos procedimentos formais voltados ao controle sobre o uso de utilitários do sistema operacional que possam de alguma forma burlar controles de acesso em vigor.

Controle de Acesso em Redes de Comunicação

Computação móvel e acesso remoto

A computação móvel (computadores portáteis, organizadores pessoais, "palmtops" e "laptops", dentre outros) e a necessidade de funcionários obterem acesso remoto a recursos e informações, introduzem novos riscos para os ativos do Grupo. A proteção requerida deverá ser planejada em função dos riscos apresentados por esses métodos específicos de trabalho.

Quando do uso de computação móvel, os riscos de se trabalhar em um ambiente desprotegido deverão ser considerados e as proteções apropriadas devem ser aplicadas. No caso de acessos remotos iniciados através de locais fixos, a Companhia deverá aplicar proteções ao local em questão, observando-se os critérios pré-definidos no capítulo **Segurança Física e Ambiental**.

Cuidados especiais deverão ser tomados para garantir que as informações da VTCLOG não sejam comprometidas pela necessidade de utilização de tecnologias de computação móvel. Procedimentos formais deverão ser adotados, com base em análise voltada a mensurar os riscos do uso da computação móvel, principalmente em ambientes desprotegidos. Os seguintes aspectos principais, dentre outros, deverão ser considerados quando da elaboração dos procedimentos em questão:

- Segurança física do local de trabalho;
- Controles de acesso;
- Controles de criptografia;
- Cópias de segurança das informações;
- Proteção contra vírus;
- Regras e instruções para a conexão de dispositivos de computação móvel às redes do Grupo;
- Definição do trabalho permitido, horas de trabalho e os controles de acesso que deverão ser aplicados aos sistemas e informações acessados;
- Instruções específicas para o uso de dispositivos de computação móvel em locais públicos, salas de reunião e outras áreas desprotegidas, localizadas fora das dependências da organização;
- Acessos que utilizem telefonia discada deverão considerar o uso de "callback" para garantir que a ligação estará sendo efetuada a partir de um local predeterminado, o que não substitui o processo de autenticação e apenas complementa o processo;
- Provisão de equipamentos adequados de comunicação, para localidades que tenham acesso a informações sensíveis e considerações sobre o uso de criptografia (Redes Privadas Virtuais e outras).
- Revisão periódica e auditoria dos procedimentos em questão.

O acesso remoto aos recursos e informações do Grupo deverá ser permitido após a completa autenticação do usuário, e mecanismos de controle de acesso devem ser aplicados. Informações sensíveis que necessitem ser acessadas remotamente poderão exigir controles adicionais como a criptografia da conexão.

Controle de Acesso em Redes de Comunicação

Computação móvel e acesso remoto

Dispositivos de computação móvel deverão ser fisicamente protegidos contra (i) roubos de equipamentos e informações, (ii) acessos não autorizados e (iii) mal-uso dos equipamentos, principalmente quando deixados em carros e outras formas de transporte, quartos, salas de conferência e quartos de hotel. Equipamentos que armazenem informações sensíveis ou críticas para os negócios não deverão ser deixados sozinhos e quando possível deverão ser trancados em cofres ou armários.

Gerenciamento de Mudanças em Sistemas Computadorizados

A estabilidade e segurança estabelecidas durante o processo de gerenciamento de mudanças em sistemas computadorizados, permitem a operação segura e correta das facilidades de processamento de informações do Grupo.

Documentação de procedimentos operacionais

Todos os procedimentos operacionais do Grupo, devem ser mantidos documentados, atualizados e periodicamente revisados visando sua melhor adequação.

Controle de alterações operacionais

Alterações, sejam elas corriqueiras ou emergenciais, em quaisquer sistemas e facilidades de processamento de informações devem ser adequadamente controladas, visando evitar a ocorrência de falhas nos sistemas e em sua segurança. Desta forma, procedimentos formais devem ser adotados para garantir que aquisições ou mudanças em equipamentos e sistemas sejam formalmente solicitadas, analisadas em termos de viabilidade econômica, aprovadas e revisadas. Com isso, faz-se necessária a utilização de mecanismos e formulários, sejam eles eletrônicos ou manuais, para registro dos processos de solicitação, análise, aprovação e revisão de tais ocorrências.

Planejamento de capacidade

A capacidade das facilidades de processamento de dados deve ser formalmente monitorada, visando um adequado planejamento dos recursos necessários para suportar as operações do Grupo. Com isso, faz-se necessária a adoção de procedimentos formais para tanto.

Planejamento e aceitação do sistema

Findo o processo de controle de alterações operacionais em sistemas, ou seja, com a solicitação de aquisição ou mudança em determinado sistema devidamente documentada, aprovada e revisada, inicia-se a fase de planejamento e aceitação do sistema.

Sistemas novos ou modificados não podem de forma alguma ser implementados em ambiente de produção, sem a execução de processos prévios de análise e aprovação formais de suas funções, por usuários e outros conforme julgado necessário. Portanto, a formalização de procedimentos nesta área é necessária, visando definir-se claramente os critérios de aceitação a serem seguidos. Tais critérios deveriam englobar dentre outras as seguintes considerações:

Gerenciamento de Mudanças em Sistemas Computadorizados

Planejamento e aceitação do sistema

- Agilidade e capacidade dos computadores necessárias aos negócios do Grupo;
- Procedimentos para recuperação, retomada do processamento e contingenciamento;
- Preparação de área específica para execução dos testes de aceitação;
- Planejamento dos controles manuais e computadorizados necessários ao processo;
- Avaliação da eficácia contínua dos controles manuais e computadorizados em vigor, diante das alterações efetuadas em sistemas existentes ou de novos sistemas;
- Especificação detalhada do roteiro de testes a ser seguido por usuários e pessoal da área de Tecnologia;
- Execução de testes visando avaliar que as alterações efetuadas em sistemas ou que o funcionamento dos novos sistemas, não afetarão a estabilidade dos demais sistemas ou facilidades de processamento de informações do Grupo;
- Utilização de mecanismos e formulários, sejam eles eletrônicos ou manuais, para registro da execução dos testes e de suas aprovações;
- Documentação das evidências de execução dos testes e de seus resultados;
- Treinamento de pessoal na operação e uso do novo sistema ou da nova versão do sistema.

Adicionalmente, deve-se manter seguros os dados existentes em massas disponibilizadas para testes, visto tratarem-se de dados do Grupo e, portanto, também necessitarem de proteção.

Gerenciamento de Mudanças em Sistemas Computadorizados

Implementação de sistemas

Findo o processo de planejamento e aceitação do sistema com resultados satisfatórios, é necessário manter documentada a etapa de implementação de sistemas novos ou de novas versões de sistemas existentes, em ambiente de produção. Desta forma, faz-se necessária a utilização de mecanismos e formulários, sejam eles eletrônicos ou manuais, para registro desta etapa para que se possa manter registrada a identificação do responsável pela implementação do sistema em ambiente produtivo, bem como a data do ocorrido.

Conforme previamente sugerido no capítulo **"Segregação de funções"**, pessoas com capacidade de construção e de modificação de sistemas, não devem possuir acesso ao ambiente de produção do Grupo, não podendo de forma alguma ser responsabilizadas por esta etapa do processo.

Metodologia de Desenvolvimento de Sistemas

Visando padronizar o desenvolvimento de quaisquer sistemas, rotinas, funções e relatórios dentre outros, devem ser observados os aspectos constantes da Metodologia de Desenvolvimento de Sistemas da VTCLOG.

Segurança da documentação dos sistemas

Procedimentos formais de atualização e revisão da documentação dos sistemas de informação do Grupo, devem ser seguidos após a implementação de sistemas novos ou de novas versões de sistemas existentes em ambiente produtivo.

Adicionalmente, por conter a documentação dos sistemas (como por exemplo, manuais de sistema, manuais de operação e manuais de usuário) informações sensíveis e confidenciais, tais como descrições de processos de aplicações, procedimentos, estrutura de dados e processos de autorização, dentre outras, deve-se mantê-la armazenada em local seguro, com acesso controlado e registrado à mesma. Desta forma, atenção especial deve ser dada à segurança de acesso à qualquer documentação eletronicamente disponível.

Gerenciamento de Mudanças em Sistemas Computadorizados

Requerimentos de segurança dos sistemas

Durante os processos de desenvolvimento de novos sistemas, funções ou rotinas, análise de riscos deve ser efetuada pela gerência usuária do sistema juntamente com o Responsável de Segurança, para que haja a definição de quais controles computadorizados (sejam eles preventivos ou detectivos, sobre entradas de dados, processamento ou saídas), deverão ser considerados durante o processo de desenvolvimento para fazer parte da estrutura do sistema, visando a sua segurança.

Antes do início de quaisquer processos de aquisição de novos sistemas, também devem ser definidos pela gerência usuária do sistema a ser adquirido, em conjunção com o Responsável de Segurança, quais controles a Companhia necessita que sejam contemplados pelo sistema, visando sua segurança.

Segurança sobre as manutenções em sistemas básicos

Procedimentos formais visando o registro das manutenções efetuadas em sistemas básicos, tais como, sistemas operacionais, sistemas de gerenciamento de bancos de dados, sistemas de gerenciamento de programas fonte, sistemas de controle de acesso e sistemas de gerenciamento de senhas de controle de acesso, dentre outros, devem ser seguidos conforme procedimentos definidos.

Política para uso de Internet

A utilização da Internet como ferramenta de trabalho e comunicação traz benefícios visíveis para a Companhia, entretanto por apresentar vários riscos aos negócios, requer a criação de uma política específica voltada a seu uso. Todos os funcionários do Grupo deverão estar cientes da política de acesso à Internet e das medidas disciplinares a serem tomadas quando da ocorrência de quaisquer infrações à mesma. A adoção de controles para o acesso, implantação de serviços e disponibilização de informações na Internet deve ser adequadamente planejada, pois visa maximizar os benefícios e minimizar os riscos apresentados.

As constantes mudanças em tecnologias utilizadas na Internet e a criação de novas formas de ataques à informação, impossibilitam a criação de uma lista definitiva de controles e exige uma revisão periódica destes. Os seguintes aspectos, dentre outros, deverão ser observados em todos as localidades que possuam acesso à ou disponibilizem serviços da Internet:

- Deverão ser geradas trilhas de auditoria de todos os acessos efetuados por funcionários, terceiros e outros usuários autorizados, a serviços disponibilizados pela Companhia, quer tenham tido sucesso ou não;
- Deverão ser implantados meios de limitação de acesso e dispositivos de detecção de intrusos em tempo real, em todas as localidades que façam uso da Internet;
- Deverão ser implantados dispositivos de controle para acessos de funcionários a serviços externos, permitindo assim que apenas serviços de interesse do Grupo estejam disponíveis;
- A conexão de usuários aos sistemas internos disponibilizados na Internet, deverá possuir os mesmos controles de autenticação e autorização existentes sobre as conexões efetuadas na rede interna do Grupo;
- Deve ser planejado o uso de criptografia para conexão a sistemas classificados como críticos ou sensíveis;
- Sistemas que disponibilizem informações públicas e de livre acesso, por exemplo, “Servidores Web e FTP”, devem ter o seu conteúdo controlado, visando a preservação da imagem do Grupo e o atendimento a quaisquer implicações legais;
- A cópia de software da Internet deverá ser controlada e estar de acordo com os acordos de licença e propriedade intelectual;
- Equipamentos que possuam acesso à Internet deverão possuir proteções contra vírus e “cavalos de tróia” (“Trojan Horses”) e os usuários deverão ser treinados e estarem cientes sobre o perigo de softwares copiados da Internet ou anexados a mensagens de correio eletrônico.

Plano de Continuidade dos Negócios

Sob responsabilidade do Responsável de Segurança do Grupo, um plano de continuidade dos negócios deverá ser formalmente criado, revisado, implementado e periodicamente testado, visando minimizar as interrupções causadas por desastres e falhas de segurança a um nível aceitável, através de uma combinação de controles de prevenção e recuperação de contingências e assegurar que os serviços do Grupo serão restaurados em tempo hábil. Estes incidentes podem ter várias causas, como por exemplo, desastres naturais, falhas de sistemas e equipamentos, acidentes e ações deliberadas.

As consequências dos desastres, falhas de segurança e serviços deverão ser formalmente analisadas e novos controles deverão ser implementados caso necessário, por conta desta avaliação.

O planejamento de continuidade dos negócios, deve cobrir dentre outros, os seguintes aspectos:

- Avaliação dos procedimentos em vigor para a continuidade dos negócios em situações de emergência;
- Definição da estratégia para a continuidade dos negócios da VTCLOG**;**
- Execução de procedimentos de análise de riscos potenciais;
- Documentação do "Plano de Continuidade dos Negócios", com o auxílio de grupo de trabalho composto por membros da gerência do Grupo e do Comitê de Segurança;
- Desenvolvimento de plano de testes periódicos para as alternativas operacionais previstas no "Plano de Continuidade de Negócios";
- Definição de procedimentos para revisão do plano;
- Avaliação formal da possibilidade de ocorrência de desastres naturais (incêndios e inundações, dentre outros) e controles utilizados para minimizar o impacto dos mesmos.

Revisões de Segurança Periódicas

Revisões periódicas sobre segurança devem ser planejadas a fim de manter-se conforto de que a segurança dos ativos do Grupo permanece razoável e inalterada, dadas as necessidades dos negócios da VTCLOG. Desta forma, revisões visando os seguintes aspectos, dentre outros, devem ser consideradas:

- Implementação adequada da Política de Segurança;
- Implementação adequada dos padrões, normas e procedimentos do Grupo, voltados a Segurança;
- Correção das vulnerabilidades apontadas através de revisões prévias;
- Detecção de novas vulnerabilidades, dado o crescente uso de novas tecnologias e a expansão de redes públicas tais como a Internet;
- Utilização de ferramentas automáticas de detecção de intrusos e vulnerabilidades;
- Revisão e manutenção das políticas, padrões, normas e procedimentos do Grupo, voltados a Segurança.

CONTATO

O Responsável de Segurança da informação é o Sr XXXXXXXX que responde pelo e-mail xxxxxxx e pelo telefone xxxxxxx.

REVISÕES

A revisão do presente documento foi efetuada no mês de novembro de 2022.