

Política de Segurança da Informação

Documento: Política de Segurança da Informação
Versão: 4.2
Data: 08/2026
Aprovado por: Samuel Santos / CFO
Periodicidade de Revisão: Anual

CONTROLE DE VERSÃO

Versão	Data	Descrição
1.0	**06/2014**	• **Criação do Documento**
2.0	**06/2015**	• **Revisão Periódica**
3.0	**11/2024**	• **Revisão e atualização do conteúdo**
4.0	**04/2026**	• **Atualização de governança documental (inclusão de controle de versão, aprovador e periodicidade de revisão)**
4.1	**04/2026**	• **Correções de inconsistências textuais, ajustes de redação, melhoria de clareza conceitual, alinhamento com práticas de governança e atualização de terminologia**
4.2	**08/2026**	• **Inclusão de diretrizes complementares sobre monitoramento corporativo, uso de ativos, transparência no uso de ferramentas de monitoramento e ciência dos colaboradores e prestadores de serviços**

A data de criação do documento foi definida com base nos registros disponíveis mais antigos mantidos pela organização. As versões foram classificadas de acordo com a evolução e atualização do conteúdo ao longo do tempo, considerando as revisões identificadas.

ÍNDICE

CONTROLE DE VERSÃO **2**

ÍNDICE **3**

POLITICA DE SEGURANÇA DA INFORMAÇÃO **4**

1. OBJETIVO 4
1.1. ABRANGÊNCIA E VIGÊNCIA 4
1.2. ESTRUTURA ORGANIZACIONAL RESPONSÁVEL 4
2. POLITICA ITERATIVE 5
2.1. POR QUE A SEGURANÇA DA INFORMAÇÃO É NECESSÁRIA? 5
2.2. CONFIDENCIALIDADE, INTEGRIDADE E DISPONIBILIDADE 6
2.3. CICLO DE VIDA DA INFORMAÇÃO 7
2.4. CLASSIFICAÇÃO DA INFORMAÇÃO 9
2.5. INCIDENTES DE SEGURANÇA DA INFORMAÇÃO 10
2.6. GESTÃO DE RISCOS À SEGURANÇA DA INFORMAÇÃO 10
3. SANÇÕES 61
4. CICLO DE VIDA DA POLITICA 61
5. APÊNDICE A - GLOSSÁRIO 61

1. OBJETIVO

A Política de Segurança da Informação tem como objetivo estabelecer, manter e desenvolver a cultura organizacional nos conceitos de segurança da informação, além de promover a melhoria contínua das medidas de controle que resultam na redução de riscos.

Como resultado, espera-se a evolução da segurança dos sistemas, a confidencialidade, integridade e disponibilidade das informações, a continuidade dos negócios e a aderência às leis e normas vigentes, mitigando riscos que podem resultar em perda ou prejuízo, sejam de ordem financeira ou de imagem para a Iterative e seus clientes.

Este documento possui enfoque nas definições de objetivos de controles de segurança, esclarecendo as principais motivações do estabelecimento dos mesmos, porém, sem detalhar os meios técnicos específicos de implementação, os quais são tratados em normas e procedimentos complementares. Documentos adicionais, como Normas e Procedimentos deverão ser definidos e publicados, a fim de cobrir as especificidades e detalhes relacionados a cada assunto ou área relacionada.

1.1. ABRANGÊNCIA E VIGÊNCIA

Este documento é destinado a todos os colaboradores e prestadores de serviços que tenham acesso ou interação com informações e ativos de informação de propriedade ou sob posse da Iterative. A presente política entra em vigor na data da sua publicação, permanecendo vigente por tempo indeterminado, podendo ser atualizada sempre que necessário, substituindo as versões anteriores.

1.2. ESTRUTURA ORGANIZACIONAL RESPONSÁVEL

A **Diretoria da Iterative** é a responsável primária por seus ativos de informação, administra a segurança da informação de acordo com a Política de Segurança da Informação, assim como leis e regulamentações, assumindo os custos ligados a seu gerenciamento.

O **Diretor de Tecnologia da Iterative** organiza e gerencia a Segurança da Informação. Avalia a segurança nos sistemas de informação e toma as medidas necessárias a fim de manter o nível adequado de segurança, mantendo a Diretoria da empresa informada quanto à evolução dos riscos.

A **Gerência de Tecnologia da Iterative** representa localmente a diretoria e é responsável pela organização e gestão dos padrões de Segurança da Informação, opera e administra a infraestrutura de segurança de TI.

Os **Coordenadores e Líderes de Tecnologia da Iterative** são atores permanentes na aplicação dos controles de segurança da informação nas áreas de sua responsabilidade. Viabilizam e/ou implantam medidas adicionais quando da existência de riscos inaceitáveis à segurança das informações.

Os **Colaboradores** e **Prestadores de Serviços da Iterative** devem garantir a observância e conformidade à Política de Segurança da Informação.

2. POLITICA ITERATIVE

A informação é o conjunto de conhecimentos sobre algo. Como qualquer outro ativo importante de uma organização, ela é necessária para a realização dos negócios da organização e consequentemente deve ser adequadamente protegida.

Ela pode existir em diversas formas: impressa ou escrita em papel, armazenada eletronicamente, transmitida pelos correios ou meios eletrônicos, apresentada em vídeos ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é apresentada ou compartilhada, é necessário que seja devidamente protegida.

Segurança da Informação é a proteção da informação de uma vasta gama de ameaças, com o objetivo de assegurar a continuidade dos negócios, minimizar riscos, maximizar oportunidades de negócio e o retorno de investimentos.

A segurança da informação é alcançada através da implantação de um conjunto de controles, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções tecnológicas de hardware e software. Estes controles precisam ser estabelecidos, implantados, monitorados, revisados e aprimorados, para assegurar que os objetivos específicos de segurança sejam alcançados. Isso deve ser feito de forma integrada a pessoas, processos e tecnologias.

2.1. Por que a Segurança da Informação é necessária?

Uma organização é uma rede de pessoas, processos e tecnologias, que se relacionam constantemente entre si, de forma dinâmica e dependente, para que seus objetivos de negócio sejam alcançados. Estas relações dependem de informações, como alicerce de suas interações.

As organizações são expostas a diversos tipos de ameaças, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação. A interconexão de redes públicas e privadas de dados, e o compartilhamento de recursos de informação aumentam a dificuldade de se controlar os riscos.

Adicionalmente, muitos processos e sistemas de informação não foram projetados para serem seguros. O nível de segurança que pode ser alcançado somente por meios técnicos é limitado, portanto devem ser apoiados por uma gestão, procedimentos e comportamentos apropriados. Sendo assim, definir,

estabelecer, manter e aprimorar a segurança da informação são atividades necessárias para evitar riscos que podem causar prejuízos à organização, buscando a continuidade de seus negócios.

Os termos gerais de segurança da informação são os seguintes:

- Uso adequado dos ativos de informação;
- Ausência de impactos à disponibilidade da infraestrutura operacional;
- Aprimoramento do relacionamento entre entidades operacionais e colaboradores dentro da empresa;
- Inclusão de segurança no ciclo de vida de projetos e processos de negócio;
- Considerar a segurança como um processo contínuo, e não como ações isoladas;
- Responsabilização dos agentes pelas suas ações e decisões;
- Medidas de segurança devem estar em conformidade com os riscos identificados.

A presente política considera, quando aplicável, os princípios de proteção de dados pessoais previstos na legislação vigente, incluindo a Lei Geral de Proteção de Dados (LGPD)

2.2. Confidencialidade, Integridade e Disponibilidade

Todas as informações são sujeitas a três propriedades principais de segurança, que devem ser preservadas e respeitadas, como segue:

Confidencialidade: Esta propriedade visa que as informações sejam de conhecimento ou posse somente das pessoas que tenham autorização legítima de acesso. Significa proteger informações contra sua revelação para alguém não autorizado – interna ou externamente.

Consiste em proteger a informação contra leitura e/ou cópia por alguém que não tenha sido explicitamente autorizado pelo proprietário daquela informação. A informação deve ser protegida qualquer que seja a mídia que a contenha, como por exemplo, mídia impressa ou mídia digital.

Deve-se cuidar não apenas da proteção da informação como um todo, mas também de partes da informação que podem ser utilizadas para interferir sobre o todo. No caso de rede de dados, isto significa que os dados, enquanto em trânsito, não devem ser vistos, alterados, ou extraídos por pessoas não autorizadas ou capturados por dispositivos ilícitos, mesmo que parcialmente.

Integridade: Esta propriedade visa que as informações sejam mantidas íntegras, sem modificações indevidas, sejam elas acidentais ou propositais.

Consiste em proteger a informação contra modificação sem a permissão explicita do proprietário daquela informação. A modificação inclui ações como escrita, alteração de conteúdo, alteração de status, remoção e inclusão de informações. Integridade significa garantir que se o dado está lá,

então não foi corrompido, encontra-se íntegro. Isto significa que aos dados originais nada foi acrescentado, retirado ou modificado.

Disponibilidade: Esta propriedade visa que as informações estejam disponíveis e sejam acessíveis a todos os autorizados legitimamente.

Tem como objetivo a proteção dos serviços prestados pelo ativo de informação de forma que eles não sejam degradados ou se tornem indisponíveis indevidamente, assegurando às pessoas autorizadas o acesso às informações sempre que delas precisar. Isto pode ser chamado também de continuidade dos serviços.

2.3. Ciclo de Vida da Informação

O ciclo de vida da informação é baseado em três grandes etapas: nascimento, manuseio e finalização.



Figura 1 – Ciclo de vida da informação.

Cada uma dessas grandes etapas pode ser dividida em etapas menores. O nascimento é constituído pelas etapas:

Planejamento: trata da identificação dos objetivos, necessidades e atividades necessárias para a criação da informação.

Aquisição: é a ação de levantar e agregar os dados necessários à criação da informação.

Criação: é a consolidação dos dados aplicados em contexto, ou seja, os dados destinados a um propósito.

Após a criação – nascimento da informação – ela estará pronta para ser utilizada, isto é, manuseada. O manuseio pode ser representado como:

Armazenamento: o objeto literal onde estará a informação. Pode ser um armazenamento físico, lógico ou até mesmo mental.

Compartilhamento: é o ato de divulgação da informação, porém sempre com respeito à sua classificação.

Manutenção: é a alteração ou adequação da informação. Algumas informações não podem ser alteradas e este ato "cria uma nova informação".

Aplicação: é a utilização da informação. É o instante em que uma informação se torna em conhecimento.

A última etapa, a finalização, é uma ação única, porém com três alternativas:

Descarte: é o ato de desprezar a informação que está obsoleta ou que não possui mais qualquer utilidade.

Arquivamento: é o ato de deixar a informação armazenada para usos futuros ou possíveis consultas ao histórico, independente da informação ter sido utilizada (aplicada) ou não.

Destruição: é o ato de eliminar a informação independente de sua utilização e aplicação. Muitas vezes uma informação é destruída devido à sua classificação e criticidade.

O ciclo de gestão da informação pode ser visto como um processo.

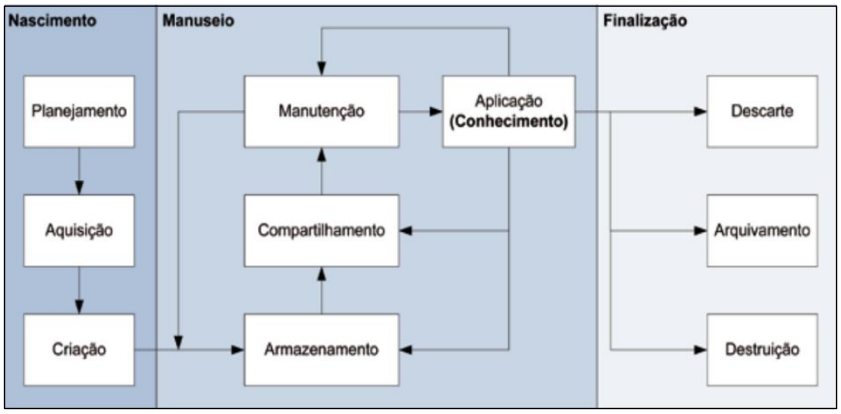


Figura 2 – processo do ciclo de vida da informação.

Nota-se por meio deste processo que a informação é criada e manuseada ciclicamente, ou seja, há um ciclo interno de armazenamento, compartilhamento e manutenção da informação e também a sua constante aplicação. Isso mostra que o conhecimento, a aplicação da informação, é dinâmico e deve ser reavaliado.

Uma aplicação (ou a falta dela) leva à finalização da informação em uma das três formas: ou descarte, ou arquivamento ou destruição. O descarte é o ignorar a informação; o arquivamento é o armazenamento de um conhecimento adquirido ou de uma informação ainda não utilizada para possível uso no futuro; e a destruição é a eliminação íntegra da informação.

Em termos físicos podemos dizer que uma correspondência recebida (informação), após lida, será jogada na lixeira (descartada), ou colocada em uma pasta ou arquivo (arquivamento), ou, por fim, triturada, picotada ou incinerada (destruída).

2.4. Classificação da Informação

Os níveis de classificação seguem uma ordem crescente de criticidade e impacto ao negócio.

Cada informação deve estar disponível para as pessoas que necessitam legitimamente de acesso, ao mesmo tempo em que há a necessidade de controles que garantam que informação não estará disponível para pessoas indevidas. A classificação das informações deve levar em conta estas premissas e principalmente os riscos de geração de impacto nos negócios pela quebra de confidencialidade das mesmas.

Os níveis de classificação determinam requisitos de controle específicos, a fim de apoiar a manutenção dos níveis de segurança necessários. Tais requisitos de controle devem ser especificados em documento de norma, com a finalidade de promover o tratamento adequado das particularidades das informações presentes nos diversos ativos de informação.

Esta classificação deve ser feita inicialmente pelo proprietário da informação, podendo ser reclassificada periodicamente, de acordo com as alterações das etapas do ciclo de vida da informação. As informações podem ser classificadas como:

Pública: O acesso a esta informação não traz riscos à empresa e pode estar acessível de forma irrestrita ao público em geral. Exemplo: Informações institucionais.

Privada: O acesso a esta informação acarreta em riscos baixos, e deve estar acessível para grupos pré-definidos. Exemplo: Procedimentos e manuais.

Sensível: O acesso a esta informação é destinado a um grupo limitado, e não deve ser divulgado a pessoas fora deste grupo. O uso ou disseminação indevida não traz danos irreparáveis, porém geram alto risco de influenciar os negócios e causar impactos à organização. Exemplo: Dados de negociações comerciais e informações de clientes.

Confidencial: O acesso a esta informação é destinado a um grupo restrito, e sua disseminação indevida pode trazer danos irreparáveis à organização. Requer medidas especiais de controle de acesso e monitoramento. Exemplo: Planos estratégicos.

2.5. Incidentes de Segurança da Informação

Um incidente de segurança da informação é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança das informações.

Exemplos de incidentes de segurança da informação são:

- Não-conformidade com políticas, normas ou procedimentos de segurança;
- Comprometimento ou ataques de negação de serviço a sistemas de informação;
- Uso ou acesso não autorizado a sistemas de informação;
- Destruição ou modificações indevidas em informações, sem o conhecimento, instruções ou consentimento prévio do proprietário ou gestor do ativo de informação;
- Uso de credenciais de acesso que não sejam de sua propriedade.

Em caso de suspeita de possíveis fragilidades ou vulnerabilidades de segurança, as mesmas não devem ser testadas por pessoal não autorizado, a fim de constatar sua existência. Testar fragilidades pode ser interpretado como um uso impróprio e também pode causar danos ao sistema de informação, resultando em responsabilidade ao indivíduo que efetuar o teste.

As possíveis fragilidades ou eventos de incidentes de segurança da informação devem ser relatados às áreas responsáveis, através dos canais apropriados definidos pela organização o mais rapidamente possível. Tais relatos devem conter todos os detalhes importantes, como por exemplo, o ativo afetado, a descrição do incidente ou das possíveis fragilidades, e quaisquer outras circunstâncias do ocorrido.

2.6. Gestão de Riscos à Segurança da Informação

As informações e os ativos de informação são sujeitas a vulnerabilidades, que se exploradas por agentes de ameaças, expõem as informações existentes, incidindo em riscos às propriedades de confidencialidade, integridade e disponibilidade das informações. Tais riscos podem gerar impactos indesejáveis à organização, devendo ser devidamente gerenciados.

O gerenciamento de riscos consiste em diversas etapas, sendo que sob os aspectos de Segurança da Informação, as mais relevantes são a **Análise de Riscos** e o **Tratamento de Riscos**.

2.6.1. Analisando os riscos de segurança da informação

As análises de riscos devem identificar, quantificar e priorizar os riscos com base nos objetivos relevantes para a organização. Os resultados orientam e determinam as ações de gestão apropriadas e as prioridades para o gerenciamento dos riscos de segurança da informação e para a implementação dos controles selecionados.

Essas análises de riscos devem ser realizadas de forma metódica, capaz de gerar resultados consistentes e coerentes com o contexto organizacional. Convém que as análises de riscos também sejam realizadas periodicamente, para contemplar as mudanças nos requisitos de segurança da informação e na situação de risco, ou seja, nos seguintes componentes:

Ameaças ou Fatores de Ameaças, que são os causadores potenciais de um incidente indesejado, que pode resultar em dano para um sistema ou organização. Os principais fatores de ameaças enfrentados pela companhia são:

a) Acidentes, tais como: Eventos ambientais (incêndio, inundação, etc.); indisponibilidade de infraestrutura de energia elétrica, telecomunicações, sistemas de informação, entre outros;

b) Erros, tais como: Falhas de desenho ou administração de infraestrutura; falhas de desenho ou implementação de softwares; falhas de utilização ou processamento de informações;

c) Atividades maliciosas, tais como: Ataques físicos (em sistemas, prédios, etc.); ataques lógicos (na infraestrutura de tecnologia da informação, sistemas de informação, etc.); abuso de privilégios, fraudes, roubo ou vazamento de informações sensíveis ou confidenciais.

Vulnerabilidades, ou fragilidades de um ativo que pode ser explorada por uma ou mais ameaças;

Ativos, sendo qualquer coisa que tenha valor para a organização;

Probabilidade, que é a capacidade e possibilidade da ocorrência dos eventos;

Impacto, resultados dos eventos.

2.6.2. Tratando os riscos de segurança da informação

Para cada um dos riscos identificados, seguindo a análise de riscos, uma decisão sobre o tratamento do risco precisa ser tomada. Possíveis opções para o tratamento do risco incluem:

Reduzir riscos, através da aplicação dos controles apropriados;

Evitar riscos, não permitindo ações que poderiam causar a ocorrência de riscos;

Transferir riscos para outras partes, por exemplo, seguradoras ou fornecedores;

Aceitar riscos, ao tomar ciência dos mesmos e sabendo que eles atendem claramente à política da organização e aos critérios e procedimentos para a aceitação de riscos;

Para aqueles riscos onde a decisão de tratamento do risco seja a de aplicar os controles apropriados, esses controles necessitam ser selecionados e implementados para atender aos requisitos identificados pela análise de riscos, a fim de assegurar que os riscos sejam reduzidos a níveis aceitáveis, levando-se em conta:

- Os requisitos e restrições de legislações e regulamentações nacionais e internacionais;
- Os objetivos organizacionais;
- Os requisitos e restrições operacionais;
- Custo de implementação e a operação em relação aos riscos que estão sendo reduzidos;

A necessidade de balancear o investimento na implementação e operação de controles, em comparação à probabilidade e potenciais impactos caso os riscos se concretizem.

É importante que seja lembrado que nenhum conjunto de controles pode conseguir a segurança completa, e que uma ação gerencial adicional deve ser implementada para monitorar, avaliar e melhorar a eficiência e eficácia dos controles de segurança da informação, para apoiar as metas da organização.

2.6.3. Níveis de Aceitação de Risco

A Iterative define que os riscos identificados devem ser avaliados com base em sua probabilidade de ocorrência e impacto potencial ao negócio, sendo classificados em níveis como baixo, médio ou alto.

A aceitação de riscos é realizada pela liderança responsável, considerando os objetivos estratégicos da organização, requisitos legais e regulatórios, e a viabilidade de mitigação. Riscos classificados como elevados devem, sempre que possível, ser tratados por meio da implementação de controles adequados, enquanto riscos de menor impacto podem ser aceitos, desde que devidamente avaliados e documentados.

2.7. Proteção de Ativos de Informação

Ativos de informação são todos os ativos que possuem informações ou dados, tais como os sistemas de informação, rede de comunicação de dados, a rede de telefonia, computadores, equipamentos e dispositivos eletrônicos, material impresso e as pessoas, com suas qualificações, habilidades e experiências.

Todos os ativos são sujeitos a vulnerabilidades, que se exploradas por agentes de ameaças, expõem as informações existentes, podendo incidir em risco de impactos negativos à empresa. Portanto, devem ser identificados, classificados, gerenciados, protegidos e monitorados.

As informações geradas, processadas, transmitidas ou acessadas nas dependências internas ou externas da companhia, são consideradas bens intangíveis, devendo ser corretamente manuseadas e utilizadas unicamente com a finalidade previamente autorizada.

2.7.1. Responsabilidades pelos Ativos de Informação

Os ativos de informação possuem diversos atores, cada qual com seus respectivos papéis e responsabilidades acerca da proteção, gestão, operação, manutenção e utilização dos ativos de informação, conforme abaixo:

Proprietário: É o principal responsável pelas informações presentes no ativo, representando e protegendo os interesses da companhia. Tem a responsabilidade de classificar as informações e definir o Gestor do ativo, que desempenhará as principais atividades no ciclo de vida das informações de sua propriedade. Deve aprovar as regras e procedimentos de gestão, acesso e uso de seus ativos de informação e patrocinar as ações de implantação dos controles necessários.

Gestor: Sob delegação do Proprietário, o Gestor do ativo de informação tem a responsabilidade de definir o nível de segurança necessário para proteger as informações e ativos sob sua gestão, conforme os objetivos de controle definidos na política corporativa de segurança da informação.

Lidera as decisões quanto às regras de gestão, acesso e uso dos ativos de informação sob sua responsabilidade, nos processos de desenvolvimento e manutenção das normas e procedimentos a serem executados pelos demais envolvidos.

Custodiante: Desempenha as funções de salvaguarda, suporte, operação e manutenção do ativo de informação. Executa tais atividades de forma a atender as regras especificadas em normas e procedimentos definidos juntamente com o Gestor do ativo, e é responsável pela documentação e implantação dos procedimentos técnicos específicos.

Registra e monitora os eventos relevantes, incluindo acessos e atividades de uso dos ativos, a fim de detectar desvios de procedimentos e prover informações para a resposta de incidentes de segurança ou posterior auditoria.

Especialista de Segurança: Acompanha os procedimentos de definição dos responsáveis de ativos de informação, orientando e apoiando o processo de tomada de decisão e documentação. Valida a aderência dos procedimentos à política corporativa de segurança da informação e promove adequações ou melhorias.

Desenvolve as normas de segurança, definindo as regras para ativos de informação que necessitem de controles específicos, juntamente com os demais envolvidos. Em caso de incidentes de segurança, organiza as ações de resposta, documenta e envolve as áreas pertinentes, a fim de promover as ações de responsabilização e melhoria contínua dos processos.

Auditor: Responsável pela avaliação periódica das atividades de gestão e operação dos ativos de informação, com o intuito de mensurar a aderência às regras definidas e eficácia dos controles implantados.

Em casos de desvio, documenta e informa as áreas pertinentes a fim de promover a melhoria contínua dos processos. Esta função é desempenhada por Controles Internos em âmbito corporativo.

Usuário: O usuário utiliza as informações dispostas nos ativos para o desempenho de suas funções e atividades nas operações de negócio da empresa. São de sua responsabilidade a ciência e conformidade às políticas, normas e procedimentos vigentes, para garantir o uso adequado dos ativos de informação.

Na ocorrência ou identificação de desvios às regras de segurança, deve comunicar seu gestor e áreas competentes a fim de possibilitar a tomada das providências necessárias e evitar danos às informações.

Inventário de Ativos: O inventário consiste em identificar, agrupar, classificar e organizar os ativos. Documentar com a finalidade de permitir a recuperação de um eventual desastre, incluindo informações como tipo do ativo, formato, localização, informações sobre cópias de segurança, informações sobre licenças e a importância do ativo para o negócio.

Trata-se de uma atividade fundamental para a correta gestão dos ativos, servindo de subsídio em diversas etapas do processo, de forma recorrente. Por isso, deve ser constantemente atualizado, de forma a refletir a situação mais atual possível dos ativos de informação da companhia.

2.8. Uso Aceitável de Ativos de Informação

Todos os ativos são de propriedade da Iterative, que os disponibiliza aos colaboradores como ferramenta de trabalho. Os equipamentos e recursos tecnológicos disponibilizados pela empresa devem ser utilizados exclusivamente para fins profissionais, relacionados às atividades da organização, sendo vedado o uso indevido ou incompatível com os objetivos de negócio. Todos os colaboradores são responsáveis pelo seu correto manuseio, devendo zelar e proteger com a finalidade de gerar benefícios à organização e, como consequência, auxiliar o cumprimento de sua missão.

O acesso aos ativos de informação deve ser realizado somente por pessoas ou entidades devidamente identificadas, autenticadas e autorizadas legitimamente. O acesso deve ser realizado através de meios reconhecidos e autorizados, protegidos contra acesso ou interferência de terceiros não autorizados, que poderiam tomar conhecimento, capturar ou se apoderar das informações acessadas.

Cada colaborador deve conhecer e cumprir a política de segurança, bem como as normas e procedimentos de segurança específicos. As normas e procedimentos de segurança são documentos que visam detalhar de forma específica as entidades responsáveis, os controles de segurança necessários e os meios de se cumprir tais controles, acerca de um ativo ou grupo de ativos de informação.

São documentos que possuem fluxos independentes de criação e atualização, mas que fazem parte da Política Corporativa de Segurança da Informação, portanto devem ser igualmente respeitados. Alguns exemplos de ativos que necessitam de cuidados especiais quanto ao seu uso são:

2.8.1. Rede Corporativa de Dados

A rede corporativa de dados é uma facilidade tecnológica privada da empresa, que permite a interconexão de sistemas de informação, computadores e outros dispositivos eletrônicos em uma rede de processamento, armazenamento e transmissão de dados. Não devem ser conectados dispositivos não homologados ou que não sejam de propriedade da empresa, salvo em caso de autorização prévia e formal.

Os arquivos armazenados em rede devem ser exclusivamente de propriedade ou posse reconhecida da empresa, respeitando os requisitos de proteção de informações a fim de impedir acesso, alteração ou destruição indevida. Da mesma forma, devem ser observadas as demais regras e leis vigentes, incluindo o código de ética e as leis governamentais, em especial as leis de direitos autorais e de propriedade intelectual.

2.8.2. Sistemas de Informação

Os sistemas de informação são ativos de informação compostos por recursos tecnológicos que processam dados de forma organizada, com o objetivo de fornecer suporte a processos da companhia. Em ambientes altamente informatizados e interconectados como o da Iterative, os sistemas de informação desempenham um papel vital na viabilização das operações de negócio.

O uso de sistemas de informação deve ser condicionado à prévia autorização, e os objetivos de uso restritos às atividades profissionais na empresa. Os limites dos níveis e permissões de acesso dos usuários devem ser respeitados, e suas senhas de acesso aos sistemas protegidas.

2.8.3. Internet e Correio Eletrônico

O acesso à Internet e sistema de Correio Eletrônico pode ser permitido, mediante autorização, para os usuários que necessitem dessas ferramentas para desenvolver suas atividades profissionais, dentre elas, pesquisa, troca de informações e análise de dados. As informações acessadas ou transmitidas pelos usuários, que representam a empresa, podem gerar altos riscos, uma vez que as leis e regulamentações governamentais são aplicáveis tanto a empresa quanto ao usuário responsável.

Ambas as ferramentas não devem ser utilizadas, em hipótese alguma, para atividades indevidas, antiéticas, proibidas ou ilegais. Além disso, deve-se evitar a cópia ou execução de arquivos oriundos destas fontes, pois são o principal meio de disseminação de vírus ou códigos maliciosos.

2.8.4. Estações de Trabalho

A estação de trabalho do usuário, assim como sua mesa ou cadeira pertence exclusivamente à empresa e deve ser tratado como um recurso precioso. Os computadores, quando conectados à rede corporativa de dados, são considerados parte integrante da mesma, sendo assim, sua utilização indevida pode apresentar riscos não somente a estação de trabalho em si, mas também à rede de dados como um todo.

Devem ser observados os requisitos de proteção de acesso físico e lógico às estações de trabalho, utilizando credenciais de acesso legítimas e bloqueando a sessão sempre que estiver ausente. Não devem ser armazenados arquivos de teor indevido ou ilegal, de qualquer natureza. No caso da existência de informações críticas aos negócios, devem ser realizadas cópias de segurança por meios apropriados, garantindo assim a salvaguarda das informações em caso de pane na estação.

2.8.5. Dispositivos Portáteis

Os dispositivos portáteis, como notebooks, aparelhos celulares, *tablets*, *pendrives* e mídias graváveis (CD, DVD, Blu-Ray, Discos Rígidos, Fitas Magnéticas e etc), devido à sua mobilidade, têm a capacidade de circular fora das dependências físicas da empresa. Por permitirem o armazenamento de informações da companhia, devem ser dotados de meios de proteção que impeçam o acesso não autorizado.

Todas as regras aplicáveis aos dispositivos dentro da empresa também são aplicáveis aos dispositivos em ambientes externos. O usuário que detém autorização de uso e posse destes ativos também tem a responsabilidade de zelar pela sua segurança física, mantendo sob sua guarda constante ou outras medidas que impeçam seu extravio, perda ou roubo. Caso ocorram, deve-se notificar o gestor e a área responsável imediatamente.

2.8.6. Impressoras

As impressoras possibilitam a transformação de uma informação do meio digital (arquivos de computador) para o meio analógico (papel). Todos os usuários devem imprimir somente as informações necessárias e recolher o material imediatamente após a impressão, evitando assim, desperdício e riscos desnecessários. No caso da impressão de informações confidenciais, deve-se utilizar senha de impressão sempre que esta facilidade estiver disponível.

2.8.7. Monitoramento e Auditoria

O monitoramento e auditoria nos ativos de informação deverão ser realizados periodicamente pelas áreas responsáveis por desempenhar estes tipos de funções. O acesso a qualquer informação deverá ser monitorado e periodicamente analisado, possibilitando assim maior eficácia na investigação de eventuais incidentes referentes à segurança da informação.

O trânsito de informações por qualquer um dos meios de comunicação também deverá ser monitorado, visando identificar o acesso não autorizado ou potencial vazamento de conteúdos restritos. Da mesma forma, os ambientes de trabalho também requerem monitoramento, pois fazem parte do ciclo de vida das informações.

A Iterative, como proprietária do *software* e *hardware,* poderá monitorar, auditar e registrar quaisquer acessos a Internet, sistemas e ativos de informação, e utilizar as informações para análises internas ou atendimento de medidas judiciais, conforme as diretrizes internas e em conformidade com os limites legais e regulatórios aplicáveis, garantindo a privacidade dos colaboradores e prestadores de serviços. Desta forma, o foco do monitoramento é mantido nas informações da organização, e não nas pessoas que as utilizam.

O monitoramento dos ativos de informação tem como finalidade a segurança da informação, proteção de ativos e gestão de riscos, sendo direcionado aos sistemas, dados e infraestrutura da organização.

Para fins de segurança da informação, proteção de ativos, gestão de riscos, continuidade operacional e atendimento a requisitos contratuais de clientes, a Iterative poderá adotar ferramentas tecnológicas de monitoramento, auditoria e gestão de acessos em equipamentos corporativos, sistemas, redes, aplicações e demais recursos tecnológicos utilizados na execução das atividades profissionais, inclusive quando utilizados em regime remoto.

Essas ferramentas poderão registrar informações relacionadas à utilização dos recursos tecnológicos, acessos realizados, disponibilidade dos sistemas, conformidade com políticas internas, integridade dos ativos e indicadores operacionais estritamente vinculados à prestação dos serviços, sempre observando os princípios da transparência, necessidade, proporcionalidade e os limites legais aplicáveis.

O monitoramento será restrito ao ambiente corporativo, aos sistemas, aplicações, acessos e equipamentos utilizados para fins profissionais, não tendo como objetivo monitorar a vida privada, comunicações pessoais ou conteúdos alheios ao contexto de trabalho.

As informações decorrentes do monitoramento serão tratadas com confidencialidade, com acesso restrito às pessoas expressamente autorizadas pela Iterative, e utilizadas exclusivamente para fins

legítimos relacionados à segurança da informação, proteção de ativos, gestão contratual, atendimento a requisitos de clientes e melhoria dos processos operacionais, sendo vedada sua divulgação ou compartilhamento indevido, ressalvadas hipóteses legais ou contratuais aplicáveis.

2.9. Controle de Acesso Lógico

Os controles de acesso lógicos são um conjunto de procedimentos e medidas com o objetivo de proteger informações tipicamente dispostas em ativos de informação tecnológicos, contra tentativas de acesso indevido feitas por entidades (pessoas, softwares ou hardwares), permitindo apenas acessos legítimos e autorizados.

Para executar essa função com critério, regras de controle de acesso devem ser definidas levando-se em consideração os conceitos presentes nesta política, em conjunto com as normas e procedimentos de segurança desenvolvidos especialmente para o ativo ou grupo de ativos de informação, caso existentes.

Através destes controles, deve ser possível determinar quais recursos podem ser acessados por quais entidades e que tipo de acesso pode ser realizado. Através de registros de auditoria e rastreabilidade, deve ser possível determinar que tipos de acesso foram realizados, por quem, quando e através de qual meio. Estes controles são implantados através de mecanismos de *Autenticação*, *Autorização* e *Auditoria*.

Autenticação: Visa garantir a correta identificação e autenticidade de uma determinada entidade que está tentando realizar acesso a um ativo de informação. Possui dois componentes principais, que atuam em conjunto, também chamados de credenciais de acesso: Conta de Acesso e Chave de Acesso.

Conta de Acesso: É o componente que identifica uma entidade perante um ativo de informação. No acesso de usuários a sistemas de informação, são utilizadas as “contas de usuários”, também chamadas de “identidades digitais”. As contas de usuários devem ser registradas de forma a garantir a unicidade e exclusividade, outorgando propriedade a uma única entidade, garantindo assim o não- repúdio quanto à responsabilidade sob a mesma.

Chave de Acesso: É o componente que certifica que a entidade realmente é quem ela diz ser, realizando sua autenticação. Da mesma forma que as contas, as chaves de acesso são componentes exclusivos e de propriedade de uma única entidade, e não devem ser compartilhadas ou reveladas a terceiros, sendo de uso e responsabilidade restrita ao proprietário da conta de acesso correspondente. As chaves de acesso podem utilizar, basicamente, três fatores de autenticação:

a) Fator “Saber”: É algo que somente a entidade sabe ou conhece. Senhas, palavras-chave ou frases secretas são exemplos deste fator de autenticação;

b) Fator "Ter": É algo que somente a entidade possui. Pode ser um componente físico, como *smartcards*, ou então um componente lógico, como um *certificado digital*;

c) Fator "Ser": É algo que somente a entidade é. Mecanismos de *biometria* como reconhecimento de Impressões digitais, íris ou de voz são comuns a este fator de autenticação.

Em casos de controle de acesso a informações classificadas como confidenciais, recomenda-se a utilização de dois fatores de autenticação de forma simultânea, a fim de efetuar um processo de autenticação forte, que apresenta um nível superior de segurança na autenticação de uma entidade.

Autorização: Consiste em controlar os diversos níveis de permissões de acesso de uma entidade a uma determinada informação. Um ativo de informação pode conter diversos tipos e classificações de informação, além de permitir diversos tipos de interação com as informações. Por exemplo, um sistema de informação pode conter um conjunto de informações classificadas como públicas, e outro conjunto classificado como sensíveis. Também pode disponibilizar diversos níveis de acesso, sendo de leitura, escrita, alteração e administração, entre outros tipos de interações possíveis.

As regras de autorização devem ser definidas com o devido envolvimento dos diversos atores responsáveis pela gestão e operação de um ativo de informação, sempre respeitando o princípio de "mínimo privilégio necessário", ou seja, atribuir o menor conjunto de permissões que são necessários para o desempenho das atividades necessárias e legítimas.

A fim de facilitar a administração de permissões, devem ser utilizados perfis de acesso, que são agrupamentos de permissões que determinam um nível de acesso. Este método permite que a administração de permissões seja realizada de forma mais eficaz.

Sempre que necessário, devem ser aplicados os conceitos de *segregação de funções*, evitando a atribuição ou acúmulo excessivo de permissões, sob os aspectos funcionais, por usuários aos sistemas de informação. Este conceito visa impossibilitar que operações indevidas possam ser realizadas pelos usuários, seja por erros operacionais ou por tentativas de atos indevidos ou fraudulentos.

Auditoria: Tem como principal objetivo garantir a capacidade de detecção de tentativas inválidas de acesso, e de fornecer rastreabilidade de um acesso que foi efetuado com sucesso, seja devido ou indevido. Devem ser utilizados métodos de registro e coleta de informações, implementados nos ativos de informação, a serem analisados periodicamente por uma área competente, que deve ser diferente da área custodiante do ativo, com permissões que permitam acesso apenas à leitura dos dados.

Os registros ou logs de auditoria devem possuir regras de armazenamento, estabelecendo requisitos de confidencialidade e retenção para que não sejam visualizados por entidades mal-intencionadas, e para garantir a capacidade de análise histórica aos eventos de acessos.

O uso de trilhas de referência (*timestamps*) deve ser considerado sempre que for necessária a análise de logs em conjunto com logs oriundos de outros sistemas, com a finalidade de possibilitar a correlação entre os registros. Outras informações mínimas a serem consideradas são *endereço IP*, conta de acesso, perfil de acesso utilizado e interação realizada.

2.10. Gestão de Acessos

Além dos componentes técnicos relacionados aos controles de acesso, é essencial que seja realizada a gestão correta de tais componentes. A estrutura organizacional e os processos de negócio da companhia são dinâmicos, portanto, as medidas de controle devem acompanhar as mudanças sempre que necessário, a fim de garantir a manutenção de sua efetividade.

Os processos de gestão de acessos devem ser definidos através de normas específicas, cobrindo os diversos eventos que disparam a necessidade de criação, alteração ou revogação de acessos, podendo ser de naturezas diversas. Alguns exemplos de eventos são:

- Eventos de Recursos Humanos: Contratação ou encerramento de contrato de colaboradores e prestadores de serviços, alteração de cargo e função, férias, licenças e mudança de local de trabalho.

- Eventos Organizacionais: Criação, substituição ou alteração de sistemas de informação, mudança de estrutura da empresa, alteração de regras de negócios e a criação de novos objetivos de negócio.

- Eventos Temporais: Encerramento de prazos pré-determinados para validade de acessos, períodos de revisão periódica de acessos.

- Eventos Não-Estruturados: Surgimento ou término “ad-hoc” de necessidade de acesso a sistemas de informação, incidentes de segurança, entre outros.

Senhas de Acesso

As senhas de acesso são os mecanismos de autenticação mais comuns no ambiente corporativo, principalmente nos sistemas de informação. Devem possuir controles de segurança específicos, como:

Requisitos de formação: Os ativos de informação que utilizem senhas para o processo de autenticação devem ser capazes de definir os requisitos mínimos de formação de senhas, como quantidade e tipos de caracteres (letras minúsculas e maiúsculas, números e caracteres especiais).

Troca da senha padrão: Softwares ou equipamentos muitas vezes possuem senhas padronizadas, definidas pelo fabricante. Tais senhas devem ser trocadas antes que informações de propriedade da empresa sejam processadas por tais ativos, evitando a exposição das mesmas.

Troca da senha inicial no primeiro acesso: As senhas iniciais, que devem ser aleatórias e não previsíveis, normalmente são definidas pelos custodiantes do ativo no momento da criação da conta de acesso. Sendo assim, quando a mesma for recebida pelo responsável, a mesma deve ser imediatamente alterada para garantir que somente ele a conheça. Idealmente, o ativo deve possuir uma função gere automaticamente a senha inicial, sem a necessidade de interação humana, ou função que obrigue a troca da senha inicial no primeiro acesso do usuário. Caso tais funções não sejam factíveis, os procedimentos de acesso devem declarar de forma explícita aos usuários a importância e sua responsabilidade sob a troca da senha inicial.

Troca periódica: Caso as senhas de acesso sejam utilizadas sem alterações por tempo prolongado, podem ser descobertas mais facilmente por terceiros, por observação, adivinhação ou tentativas seqüenciais. Para reduzir este risco, os sistemas devem possuir a capacidade de determinar o requerimento de troca periódica de forma mandatória, solicitando a alteração da senha atual ao usuário, sem permitir o uso das mesmas senhas repetidamente na definição de novas senhas.

Troca espontânea: As senhas podem ser comprometidas por inúmeras razões. Neste caso, devem ser trocadas imediatamente para evitar o uso indevido dos acessos. Para isso, os sistemas devem possuir a função de troca de senha espontânea, permitindo que o usuário responsável pela conta e senha de acesso possa alterá-la sempre que julgar necessário, sem a necessidade de intervenção por terceiros.

Redefinição administrativa de senha: As senhas podem ser esquecidas pelos usuários, e nesta situação, a mesma deve ser redefinida e encaminhada de forma segura ao usuário responsável, que deve trocá-la imediatamente, da mesma forma realizada para as senhas iniciais. A redefinição de senhas é uma atividade que deve ser realizada somente por pessoal autorizado.

Bloqueio por tentativas inválidas: Agentes maliciosos podem tentar descobrir senhas, através de tentativas sucessivas de acesso. Para limitar a capacidade da descoberta indevida de senhas, os sistemas devem possuir funções de bloqueio de conta de acesso, após uma quantidade determinada de tentativas inválidas de acesso. Neste caso, a conta pode ser desbloqueada automaticamente após um período pré-determinado ou então através de intervenção manual de desbloqueio, realizada somente por pessoal autorizado.

Armazenamento protegido: No caso senhas de usuários, as mesmas não devem ser anotadas ou gravadas em locais que podem ser vistos ou acessados por terceiros. Em sistemas de informação, as senhas devem ser armazenadas em local especialmente protegido, utilizando mecanismos que garantam que as mesmas não sejam expostas, nem mesmo aos custodiantes do sistema, normalmente utilizando métodos de *criptografia irreversível* ou similar.

Os acessos devem ser revisados periodicamente, garantindo sua adequação às funções exercidas e sendo revogados quando não mais necessários.

2.11. Segurança Física e de Ambiente

Além da segurança às informações, também é necessário prover controles adequados para prevenir danos, interferências e acessos físicos não autorizados em ambientes e ativos da companhia. O acesso físico muitas vezes permite ações que podem suprimir controles lógicos de segurança, sendo assim, o mesmo deve ser controlado de forma a compor o nível de proteção adequado para os ativos de informação em conjunto com os controles lógicos existentes.

Perímetro de Segurança Física

Devem ser definidos os perímetros de segurança física, através de barreiras como paredes, portões de entrada controlados por cartões ou balcões de recepção com recepcionistas, para proteger as áreas que contenham informações ou instalações de processamento da informação.

Tais perímetros devem ser claramente definidos, e sua localização e capacidade devem ser compatíveis com os requerimentos de segurança dos ativos contidos no interior do perímetro. Os perímetros devem ser fisicamente sólidos, ou seja, não devem ter brechas ou pontos onde poderia ocorrer facilmente uma invasão. Caso existam, medidas adicionais de vigilância devem ser adotadas a fim de atingir o nível de segurança adequado.

Mecanismos de monitoramento e detecção de intrusão devem ser instalados, operados e testados regularmente, de acordo com normas regionais, nacionais e internacionais. Câmeras, alarmes e sensores de presença são exemplos de dispositivos que podem ser utilizados com esta finalidade.

Controles de Acesso Físico

Os perímetros de segurança devem ser protegidos por controles apropriados de entrada e saída para assegurar que somente as pessoas autorizadas tenham acesso às dependências ou facilidades. Tais controles devem incluir o tratamento adequado para visitantes, que devem ser devidamente registrados e autorizados conforme as regras vigentes.

Deve ser exigido a todas as pessoas que mantenham em local visível alguma forma válida de identificação, e os possíveis desvios devem ser reportados aos responsáveis pela segurança física do local, para a tomada das medidas cabíveis.

O acesso às áreas em que são processadas ou armazenadas informações sigilosas deve ser especialmente controlado e restrito somente às pessoas autorizadas utilizando controles de autenticação forte, por exemplo, cartão de controle de acesso mais senha de acesso. Devem ser

mantidos de forma segura os registros de todos os acessos para fins de auditoria e monitoramento. As permissões de acesso a tais áreas devem ser revistas periodicamente, e revogadas sempre que possível.

Ameaças Externas e do Meio Ambiente

Devem ser projetadas e aplicadas medidas de proteção física contra incêndios, enchentes, terremotos, explosões, perturbações da ordem pública e outras formas de desastres naturais ou danos causados pelo homem. Para isso, devem ser implantadas medidas que garantam que:

Os equipamentos para contingência e backup fiquem a uma distância segura, para que não sejam danificados por um desastre que afete o local principal;

Os equipamentos apropriados de detecção e combate a incêndios sejam providenciados e posicionados corretamente;

Barreiras de proteção ou similar contra inundação ou alagamento;

Os materiais perigosos ou combustíveis sejam armazenados a uma distância segura da área de segurança;

Suprimentos em grande volume, como materiais de papelaria e insumos de escritório, não devem ser armazenados dentro de uma área segura.

Segurança de Equipamentos

Com o objetivo de impedir perdas, danos, furto ou o comprometimento de ativos e interrupção das atividades da organização, é necessário que os equipamentos sejam protegidos contra ameaças físicas e do meio ambiente.

A proteção dos equipamentos (incluindo aqueles utilizados fora do local) é necessária para reduzir o risco de acesso não autorizado às informações e para proteger contra perdas ou danos. De forma geral, devem ser observados os seguintes requerimentos de segurança física de equipamentos:

Os itens que exigem proteção especial devem ser isolados para reduzir o nível geral de proteção necessário do ambiente em que se encontra;

Os equipamentos de processamento e apresentação de informações sensíveis devem ser posicionados de forma que o ângulo de visão seja restrito, de modo a reduzir o risco de que as

informações sejam vistas por pessoal não autorizado durante a sua utilização, e seus locais de armazenagem devem ser protegidos, a fim de evitar o acesso não autorizado;

É necessário adotar controles para minimizar o risco de ameaças físicas potenciais, tais como furto, incêndio, explosivos, fumaça, água (ou falha do suprimento de água), poeira, vibração, efeitos químicos, interferência com o suprimento de energia elétrica, interferência com as comunicações, radiação eletromagnética e vandalismo;

As condições ambientais como temperatura e umidade, devem ser monitoradas para a detecção e reação às condições que possam afetar negativamente os recursos de processamento da informação;

Não é permitido comer, beber e fumar em instalações de processamento central de informação, sendo que estas práticas podem representar riscos.

Utilidades

Todas as utilidades, tais como suprimento de energia elétrica, suprimento de água, esgotos, calefação, ventilação e ar-condicionado devem ser adequados para os ativos que eles suportam, observando as regras e requisitos de proteção previamente determinados.

A fim de assegurar seu funcionamento correto e reduzir os riscos de defeitos ou interrupções do funcionamento, devem ser inspecionadas em intervalos regulares e testadas de maneira apropriada. Da mesma forma, devem ser utilizados sistemas de monitoramento e alarme para detectar falhas de funcionamento das utilidades, sempre que necessário.

Energia Elétrica: Recomenda-se o uso de *UPS* e gerador de energia elétrica emergencial, para suportar as paradas e desligamento dos equipamentos ou para manter o funcionamento contínuo dos equipamentos que suportam operações críticas dos negócios, mesmo em casos de falhas prolongadas do fornecimento público de energia elétrica. Nestes casos, devem existir planos de contingência de energia elétrica referentes às providências a serem tomadas em caso de falha do *UPS* e/ou gerador.

Além disto, deve ser considerado o uso de múltiplas fontes de energia ou de uma subestação de força separada, com o fornecimento do combustível necessário para o funcionamento do gerador, pelo tempo que for determinado. Salas de processamento central de informações e de telecomunicações, que possuem missão críticas para os negócios da companhia são exemplos onde esta abordagem se faz necessária.

Água: O suprimento de água necessita ser estável e adequado para abastecer os equipamentos de ar-condicionado e de umidificação, bem como os sistemas de extinção de incêndios (quando usados).

Falhas de funcionamento do abastecimento de água podem danificar o sistema ou impedir uma ação eficaz de extinção de incêndios.

Voz: Os serviços de voz devem ser adequados para atender às exigências legais locais relativas a comunicações de emergência, e possibilitar que as reações a incidentes sejam tomadas sempre que necessário.

2.12. Segurança em Pessoas e TPRM

As pessoas são componentes fundamentais tanto para os negócios, quanto para a segurança das informações da organização. Somente as pessoas têm a capacidade de realizar a análise crítica de situações inesperadas, e de tomar as decisões necessárias.

Portanto, são essenciais para assegurar o nível correto de proteção de informações, diante das inúmeras situações onde ela pode ser necessária. Os princípios a seguir devem ser aplicados a todos os colaboradores e prestadores de serviços da companhia, de acordo com sua área de atuação e responsabilidades:

Informar, treinar e aprimorar a conscientização de segurança de todos os tomadores de decisão e demais envolvidos sobre segurança da informação e seus riscos, que podem levar ao comprometimento das missões corporativas;

Definir normas e procedimentos de segurança específicos aos ativos de informação que processam ou armazenam informações críticas, a fim de limitar os possíveis impactos de incidentes de segurança;

Definir os papéis e responsabilidades de todos os envolvidos na gestão, operação e utilização de ativos de informação, e garantir o não-repúdio acerca das ações realizadas;

Administrar as permissões de acesso aos ativos de informações, utilizando os procedimentos disponíveis, definidos pelos gestores responsáveis;

Controlar e monitorar a correta aplicação da política, normas e procedimentos de segurança;

Envolver os gestores na aplicação dos conceitos de segurança, em seus respectivos campos de responsabilidade;

Conhecer e respeitar as políticas, normas e procedimentos, bem como as leis vigentes na organização e território nacional.

As violações à política de segurança serão tratadas através de processo disciplinar formal que visa conscientizar e responsabilizar os envolvidos. Tal processo disciplinar deve assegurar um tratamento justo e correto aos envolvidos, de forma a levar em consideração fatores como a natureza, gravidade e recorrência da violação, bem como seu impacto ou potencial impacto ao negócio. Faltas graves devem incidir em medidas proporcionalmente rígidas, visando a correta resposta às situações de incidentes de segurança.

Antes da contratação

Medidas de segurança devem ser tomadas antes da contratação, com a finalidade de assegurar que os colaboradores e prestadores de serviços entendam suas responsabilidades e estejam de acordo com os seus papéis, e reduzir o risco de roubo, fraude ou mau uso das informações. As responsabilidades pela segurança da informação devem ser atribuídas antes da contratação, de forma adequada, nas descrições de cargos e nos termos e condições de contratação.

Convém que todos os candidatos ao emprego, fornecedores e terceiros sejam adequadamente analisados, especialmente em cargos com acesso a informações sensíveis. Todos os colaboradores e prestadores de serviços, sendo usuários dos ativos de informação, devem assinar acordos sobre seus papéis e responsabilidades pela segurança da informação.

As verificações de controle de todos os candidatos a emprego, fornecedores e terceiros devem ser realizadas de acordo com as leis relevantes, regulamentações e éticas, e proporcional aos requisitos do negócio, à classificação das informações a serem acessadas e aos riscos percebidos. Convém que as verificações de controle levem em consideração todos os aspectos relevantes relacionados com a privacidade, legislação baseada na contratação e/ou proteção de dados pessoais.

Durante a contratação

Devem ser implantados e mantidos controles durante as atividades de contratação, com o objetivo de assegurar que os colaboradores e prestadores de serviços sejam conscientes das ameaças e preocupações relativas à segurança da informação, suas responsabilidades e obrigações, e estão preparados para apoiar a política de segurança da informação da organização durante os seus trabalhos normais. A contratação deve ser formalizada através de documentos apropriados, incluindo sempre que aplicável, um contrato de trabalho e termo específico de confidencialidade de informações corporativas.

Convém que um nível adequado de conscientização, educação e treinamento nos procedimentos de segurança da informação e no uso correto dos recursos de processamento da informação seja fornecido para todas as pessoas, incluindo a assinatura de termos que visam declarar compromisso, ciência e responsabilidade quanto às políticas e normas internas, bem como manutenção de confidencialidade de informações.

Sempre que forem adotadas ferramentas, procedimentos ou controles adicionais de monitoramento relacionados ao uso de ativos corporativos, ambientes tecnológicos ou requisitos específicos de clientes, os colaboradores e prestadores de serviços serão previamente cientificados quanto às regras aplicáveis, finalidade, escopo do monitoramento, responsabilidades de uso e limites de tratamento das informações.

Tal ciência poderá ocorrer por meio de cláusula contratual, aditivo, termo de responsabilidade, política interna, aceite eletrônico ou outro instrumento formal que assegure transparência e rastreabilidade.

A adoção desses instrumentos deverá assegurar a adequada transparência quanto à finalidade do monitoramento e à proteção das informações eventualmente coletadas.

Mudança ou encerramento da contratação

Com a finalidade de assegurar que os eventos de alteração de função ou encerramento de contratos sejam tratados de forma segura, devem ser definidos e mantidos procedimentos adequados, evitando situações de excesso de permissões ou retenção indevida de ativos de informação da companhia.

Mudança da contratação

Em caso de mudanças de responsabilidades ou do trabalho, tais eventos devem ser gerenciados a fim de encerrar as atribuições do trabalho anterior e devolver ativos que não sejam mais necessários, de forma programada e controlada. A alteração de uma atividade ou função deve refletir na retirada de todas as permissões de acesso que não foram aprovadas para o novo trabalho, e sejam concedidos somente os novos acessos necessários, com as devidas autorizações.

Encerramento de contratação

A comunicação de encerramento de contratação e respectivas atividades devem incluir requisitos legais e de segurança existentes. Quando apropriado, as obrigações contidas nos contratos de trabalho, acordos de confidencialidade e termos de responsabilidade devem continuar por um período adicional após o fim do trabalho do colaborador ou prestador de serviço.

Nos casos em que a pessoa que está deixando a companhia desempenhe papel relevante para as atividades que são executadas, convém que suas atribuições e conhecimentos sejam documentados e transferidos para a organização. Também convém que sejam tomadas providências para avisar às outras pessoas que fazem parte da organização, para não mais compartilhar estas informações com a pessoa que está em encerramento de contrato.

Nos casos em que o término de contrato seja por iniciativa do gestor, os funcionários ou prestadores de serviços, em determinadas situações, podem realizar tentativas de corromper informações, sabotar os recursos de processamento da informação ou coletar informações para uso futuro. Medidas apropriadas devem ser tomadas a fim de evitar tais tentativas.

Devolução de ativos

Determina-se que todos os colaboradores e prestadores de serviços devolvam todos os ativos da organização que estejam em sua posse, durante ou após o encerramento de suas atividades, do contrato. O processo de encerramento de atividades precisa ser formalizado para contemplar a devolução de quaisquer ativos da companhia, entregues ou sob posse da pessoa. Em especial,

computadores, celulares, automóveis, cartões de crédito ou benefício, cartões de acesso, cartões de identificação, documentos, *softwares* e mídias portáteis devem ser recuperados de forma adequada.

Retirada de permissões de acesso

É necessário que as permissões de acesso de todos os usuários aos ativos de informação e aos recursos de processamento da informação sejam revogadas durante ou após o encerramento de suas atividades ou contrato, impedindo a continuidade dos acessos, sejam lógicos ou físicos.

Caso a pessoa que esteja saindo tenha conhecimento de senhas de acesso que necessitem permanecer ativas, estas devem ser transferidas para um novo responsável, que deverá alterar as senhas tão logo for possível, a fim de evitar a possibilidade de uso indevido.

Em situações especiais, medidas adicionais podem ser necessárias. A identificação de tais situações depende da avaliação de fatores de risco, tais como:

a) Se o encerramento da atividade ou a mudança é iniciado pelo colaborador ou prestador de serviço, ou pelo seu gestor;

b) A razão do encerramento da atividade;

c) As responsabilidades atuais da pessoa;

d) A criticidade ou classificação de confidencialidade dos ativos atualmente acessíveis.

Comportamento de pessoas

As pessoas desempenham um papel fundamental para a segurança da informação. São as responsáveis pela gestão, uso e proteção da informação, realizam atividades e tomam decisões que permitem que as operações empresariais sejam realizadas. São de sua responsabilidade a ciência e conformidade às políticas, normas e procedimentos vigentes, para garantir o uso adequado das informações de forma a preservar os interesses da companhia.

O ambiente de trabalho pode representar um local com diversas possibilidades para a exposição indevida de informações. Portanto, os colaboradores e prestadores de serviço da Iterative devem adotar comportamentos adequados, para reduzir os riscos de acesso não autorizado, perda de informações ou danos às informações durante e fora do horário de expediente. Tais comportamentos incluem:

“Mesa Limpa” e “Tela Limpa”: O comportamento de “mesas limpas”, para os papéis e mídias de armazenamento removíveis, e “telas limpas”, para as facilidades de processamento de informações, são úteis para reduzir os riscos de acessos não autorizados, perda ou dano de informações.

O comportamento deve considerar os aspectos culturais da organização e as exposições do ambiente a que estão sujeitos. Informações deixadas sem restrição de acesso são passíveis de serem observadas ou capturadas por uma pessoa não autorizada.

Comunicação restrita com terceiros: O colaborador ou prestador de serviço deverá estar atento na comunicação com terceiros, pois podem vir a gerar para riscos que podem comprometer a imagem ou negócios da empresa, mesmo que de forma indireta ou não intencional. Pessoas mal-intencionadas podem se utilizar de métodos de engenharia social para induzir a comunicação de informações corporativas, seja através de conversas ou correspondências.

As correspondências com terceiros, em determinadas situações, pode vir a ser entendida como contrato. Toda e qualquer contratação ou alteração de contrato deve ser realizada por escrito e deve passar pelo departamento Jurídico para análise e aprovação, além de seguir os trâmites oficiais existentes.

Cuidados na divulgação de informações privilegiadas: Pessoas que tenham acesso a informações privilegiadas devem tomar todos os cuidados possíveis para não divulgar, em suas conversas ou correspondências com terceiros, informações que, quando utilizadas indevidamente, possam influenciar de forma negativa os negócios ou a imagem da companhia.

Toda solicitação de informações sigilosas deve estar acompanhada de uma justificativa legítima, e sua resposta deve ser concedida somente após análise criteriosa pelos responsáveis por tal informação.

Em caso de solicitações externas, as mesmas devem ser encaminhadas aos canais oficiais competentes, como por exemplo, a assessoria de imprensa ou departamento jurídico, especialmente caso a solicitação seja oriunda de imprensa ou órgãos públicos.

Proteção no manuseio e transporte de mídias: As mídias magnéticas possibilitam o armazenamento e transporte de grandes volumes de informações. Portanto, as seguintes salvaguardas devem ser consideradas:

a) A remoção de uma mídia deverá ocorrer apenas mediante uma autorização do responsável pelas informações contidas na mesma;

b) Em caso de transporte físico, o acondicionamento deve ser suficiente para proteger conteúdo contra acidentes ou interferências externas, que podem provocar danos;

c) Quando necessário, devem ser tomadas medidas especiais visando proteção contra modificação ou acesso não autorizado, incluindo criptografia de dados;

d) Os papéis e outras mídias que não forem Públicos devem ser armazenadas em armários trancados ou em outras formas de mobiliário adequado de segurança, especialmente fora do horário de expediente;

e) Quando for necessário imprimir documentos, utilize senha de impressão quando esta facilidade estiver disponível, ou então, retire os documentos imediatamente da impressora, minimizando sua exposição indevida.

Além dos comportamentos específicos, as pessoas da organização, tanto em ambientes internos quanto externos, devem manter um comportamento adequado no tocante às informações corporativas. Seguem as diretrizes gerais a serem aplicadas em qualquer situação:

Adote um comportamento responsável e zeloso, observando as regras existentes a fim de manter a confidencialidade, integridade e disponibilidade das informações da organização;

Ajude a promover a disseminação dos conceitos da segurança da informação, orientando e auxiliando os outros usuários;

Seja discreto em suas conversas, principalmente em locais públicos, onde a mesma pode ser ouvida facilmente por terceiros;

Não transmita qualquer mensagem abusiva, obscena, vulgar, de conteúdo difamatório, falso, impreciso, de ódio, ameaçadora ou qualquer outro material que possa violar as políticas internas ou leis públicas vigentes;

Antes de transmitir uma mensagem ou correspondência, certifique que o meio utilizado é adequado ao teor das informações, e confirme se o destinatário realmente deve receber tais informações;

Não se identifique como colaborador da empresa caso venha a publicar informações em qualquer meio, caso esta atividade não faça parte de sua atribuição profissional;

Tome cuidados especiais no uso da Internet, seja na visitação a páginas (*websites*), sistemas de comunicação instantânea (*instant messaging*), mensagens eletrônicas (*e-mail*), redes sociais (*social networks*), fóruns de discussão, *blogs* ou qualquer outro conteúdo. A Internet é o principal meio de disseminação de vírus e códigos maliciosos, e, além disso, as informações veiculadas nesta rede podem ser capturadas e utilizadas indevidamente;

Não execute arquivos anexos e não clique em quaisquer links recebidos através de mensagens eletrônicas de origem duvidosa. Consulte antes a entidade responsável pelo envio da mensagem a fim de confirmar se a mesma é legítima e de interesse;

Não empreste ou compartilhe suas credenciais (conta e senha) de acesso. Possíveis ações indevidas realizadas por terceiros serão outorgadas ao responsável pelas credenciais;

Utilize as informações corporativas somente para os fins autorizados. Na dúvida, consulte as áreas responsáveis;

Informações sensíveis ou confidenciais devem ser tratadas de forma especial, principalmente no que tange ao seu armazenamento, uso e transmissão. Observe as normas e procedimentos específicos ou consulte os responsáveis;

Computadores pessoais e outros dispositivos tecnológicos que permitam acesso à rede corporativa de dados não devem ser deixados com sessões abertas quando o usuário estiver ausente, devendo ser bloqueados sempre que não estiverem em uso;

Os usuários de computadores e dispositivos portáteis devem estar constantemente atentos à segurança física de seus equipamentos, para evitar quebra, perda ou roubo;

Caso observar sinais de riscos potenciais como fogo, fumaça, vazamentos de água ou gás, informe os responsáveis imediatamente para a tomada de ações corretivas.

2.13. Segurança na Comunicação e Operação

O gerenciamento das operações e comunicações visa padronizar formas de criação, armazenamento, transporte, acesso, recuperação e descarte da informação, de maneira a garantir o processamento seguro da mesma, mantendo as propriedades de confidencialidade, integridade e disponibilidade em níveis adequados.

Determina como devem ser tratadas as informações quando presentes em recursos do ambiente de produção, disponíveis ou acessíveis aos usuários dos ativos e sistemas de informação. Também estipula os requisitos para o planejamento e aceitação de novos sistemas a serem transacionados para a produção. Todas essas regras e requerimentos de tratamento da informação devem ter normas e procedimentos devidamente documentados, servindo como fonte de consulta para direcionar a execução de atividades corriqueiras ou emergenciais.

Procedimentos e responsabilidades operacionais

Tais procedimentos têm como objetivo a garantia da operação segura e correta dos recursos de processamento da informação. Os procedimentos e responsabilidades pela gestão e operação de todos os recursos de processamento das informações devem ser definidos, abrangendo a segregação de funções quando apropriado, para reduzir o risco de mau uso ou uso doloso dos sistemas de informação.

Documentação dos procedimentos de operação

Convém que procedimentos documentados sejam preparados para as atividades de sistemas associadas a recursos de processamento e comunicação de informações, tais como procedimentos de inicialização e desligamento de computadores, geração de cópias de segurança (*backup*), manutenção de equipamentos, tratamento de mídias, segurança e gestão do tratamento das correspondências e das salas de computadores.

Os procedimentos operacionais e os procedimentos documentados para atividades de sistemas devem ser tratados como documentos formais e suas mudanças devem ser devidamente autorizadas pelos responsáveis. Quando tecnicamente possível, convém que os sistemas de informação sejam gerenciados uniformemente, usando os mesmos procedimentos, ferramentas e utilitários.

Gestão de mudanças

Trata a necessidade de controlar as modificações nos recursos de processamento da informação e sistemas. Os sistemas operacionais, sistemas de infraestrutura de TI, aplicações de negócio e aplicativos devem ser sujeitos a rígidos controles de gestão de mudanças, incluindo itens como:

a) Identificação e registro das mudanças significativas;

b) Planejamento e testes das mudanças;

c) Avaliação de impactos potenciais de tais mudanças;

d) Procedimento formal de aprovação das mudanças propostas;

e) Comunicação dos detalhes das mudanças para todas as pessoas envolvidas;

f) Procedimentos de recuperação, incluindo procedimentos e responsabilidades pela interrupção e recuperação de mudanças em caso de insucesso ou na ocorrência de eventos inesperados.

Devem ser estabelecidos os procedimentos e responsabilidades gerenciais formais para garantir que haja um controle satisfatório de todas as mudanças no ambiente. Quando mudanças forem realizadas, é necessário manter um registro de auditoria contendo todas as informações relevantes.

Segregação de funções

Convém que funções e áreas de responsabilidade sejam segregadas para reduzir as oportunidades de uso indevido dos ativos da organização. A segregação de funções é um método para redução deste tipo de risco, seja de teor acidental ou deliberado, que possam gerar danos quaisquer.

A fim de viabilizar a segregação de funções, as áreas usuárias dos sistemas de informação devem se estruturar, através de contingente de pessoas e processos adequados, de forma a impedir o acúmulo excessivo de funções, principalmente nos casos em que tais funções sejam conflitantes quanto aos seus interesses, objetivos ou controles.

Em situações onde a segregação de funções não for possível de ser efetivada, controles compensatórios, como a monitoração das atividades, trilhas de auditoria e acompanhamento gerencial, deverão ser considerados, a fim de reduzir os riscos existentes.

Separação dos recursos de desenvolvimento, teste e de produção

Os recursos de desenvolvimento, teste e produção devem ser separados para reduzir o risco de acessos ou modificações não autorizadas aos sistemas. O nível de separação dos ambientes de produção, testes e desenvolvimento deve ser determinado conforme a criticidade dos sistemas envolvidos e as provisões cabíveis da infraestrutura tecnológica.

Quando o pessoal de desenvolvimento e teste possui acesso ao ambiente de produção e suas informações, eles podem introduzir códigos não testados e não autorizados, ou mesmo alterar os dados do sistema. Em alguns sistemas essa capacidade pode ser utilizada indevidamente, para a execução de fraudes, ou introdução de códigos maliciosos ou não testados, que podem causar sérios problemas operacionais. Da mesma forma, o acesso a informações sensíveis ou confidenciais por esta entidade gera uma exposição indevida, podendo resultar em roubo ou vazamento de tais informações.

Gerenciamento de serviços terceirizados

O objetivo do gerenciamento de serviços terceirizados é o de implementar e manter o nível apropriado de segurança da informação e de entrega em consonância com acordos ou contratos formalizados. As áreas responsáveis por serviços envolvendo prestadores de serviços devem verificar a implementação dos acordos, monitore a conformidade com tais acordos e gerencie as mudanças para garantir que os serviços entregues atendem a todos os requisitos acordados com os terceiros.

Entrega de serviços

Os controles de segurança, as definições de serviço e os níveis de entrega incluídos no acordo de entrega de serviços terceirizados devem ser implementados, executados e mantidos pelo prestador de serviços, incluindo os arranjos de segurança acordados, as definições e os aspectos de gerenciamento.

O terceiro deve manter uma capacidade de serviço suficiente, juntamente com planos viáveis projetados para garantir que os níveis de continuidade de serviços acordados sejam mantidos após falhas de serviços severas ou desastres.

No caso de acordos de terceirização, é necessário planejar as transições necessárias (de informação, recursos de processamento de informações e quaisquer outros que necessitem de movimentação) de forma que se garanta que a segurança seja mantida durante e após o período de transição.

Monitoramento e análise crítica de serviços terceirizados

Os serviços, relatórios e registros fornecidos por prestadores de serviços devem ser regularmente monitorados, analisados e auditados. A monitoração e análise crítica dos serviços terceirizados devem garantir a aderência entre os termos de segurança de informação e as condições dos acordos, e que problemas e incidentes de segurança da informação sejam gerenciados adequadamente.

A responsabilidade do gerenciamento de relacionamento com o prestador de serviço deve ser atribuída a um indivíduo designado ou equipe de gerenciamento de serviço, que devem manter suficiente controle geral e visibilidade em todos os aspectos de segurança para as informações ou para os ativos de informação acessados, processados ou gerenciados por um terceiro.

Gerenciamento de mudanças para serviços terceirizados

Convém que mudanças no provisionamento dos serviços, incluindo manutenção e melhoria da política de segurança da informação, procedimentos e controles existentes, sejam gerenciadas levando-se em conta a criticidade dos sistemas e processos de negócio envolvidos e seus riscos.

Planejamento e aceitação dos sistemas

O planejamento e a preparação prévios são requeridos para garantir a disponibilidade adequada de capacidade e recursos para entrega do desempenho desejado ao sistema. Projeções de requisitos de capacidade futura necessitam ser realizadas para reduzir o risco de sobrecarga dos sistemas. Os requisitos operacionais dos novos sistemas devem ser estabelecidos, documentados e testados antes da sua aceitação e uso em ambiente produtivo.

Gestão de capacidade

Consiste no monitoramento e medição da utilização dos recursos, para a determinação de projeções de necessidades de capacidade futura, a fim de garantir o desempenho adequado do sistema. Tais projeções devem levar em consideração os requisitos de novos negócios, sistemas e as tendências atuais e futuras de processamento de informação da organização.

Os requisitos de capacidade necessitam ser identificados para cada atividade nova ou em andamento, e as projeções dos sistemas existentes devem ser utilizadas para indicar as necessidades de melhoria dos recursos, a fim de garantir a disponibilidade e eficiência dos sistemas.

Convém que os gestores utilizem essas informações para identificar e evitar os potenciais gargalos e a dependência em pontos únicos de falha de infraestrutura ou em poucas pessoas-chave, fato que pode representar vulnerabilidades no ambiente.

Aceitação de sistemas

Os critérios de aceitação para novos sistemas, atualizações e novas versões, necessitam ser estabelecidos, incluindo a execução dos testes apropriados dos sistemas durante seu desenvolvimento e antes da sua aceitação, incluindo itens como:

a) Requisitos de desempenho e de capacidade computacional;

b) Procedimentos para recuperação de erros e de desastres;

c) Planos de contingência para situações de indisponibilidade prolongada do sistema;

d) Controles de segurança requeridos e implantados;

e) Documentações técnicas, manuais e treinamento para uso e operação, incluindo gestão de incidentes, gestão de acessos e cópias de segurança;

f) Evidências de que tenha sido considerado o impacto do novo sistema na segurança do ambiente como um todo.

Proteção contra códigos maliciosos

Precauções são requeridas para detectar e prevenir a introdução de códigos maliciosos no ambiente tecnológico da empresa. Os sistemas de informação e seus respectivos *softwares* são vulneráveis à introdução de códigos maliciosos, tais como vírus de computador, *worms* de rede, cavalos de tróia, *exploits* e bombas lógicas.

Sendo assim, é necessário que se implantem controles para prevenir, detectar e remover códigos maliciosos, e que os usuários estejam conscientes dos perigos dos mesmos, sendo ideal que a proteção contra códigos maliciosos seja baseada em *softwares* de detecção preventiva e seu devido reparo, juntamente com o controle de acesso adequado e o comportamento seguro dos usuários. As seguintes diretrizes devem ser observadas:

Instalar e atualizar regularmente *softwares* de detecção e remoção de códigos maliciosos para o exame de computadores, rede de dados e outras mídias, de forma preventiva, incluindo a verificação por códigos maliciosos antes do uso de arquivos eletrônicos transmitidos através de redes; recebidos através de correio eletrônico; descarregados a partir da Internet ou copiados de quaisquer outras mídias;

Adotar a estratégia de defesa em camadas, efetuando avaliações de segurança simultaneamente em diversos locais, como por exemplo, nos servidores de correio eletrônico, servidores de arquivos, servidores de acesso a *internet*, rede de dados, estações de trabalho e dispositivos portáteis;

Controlar o uso de software e hardware, permitindo o apenas de programas e aplicativos homologados, e computadores e outros dispositivos previamente autorizados;

Definir procedimentos de gerenciamento e respectivas responsabilidades para tratar da proteção de código malicioso nos sistemas, com o devido treinamento, reporte e instruções para a recuperação de ataques de códigos maliciosos;

Implementar procedimentos para regularmente coletar informações de inteligência de combate a códigos maliciosos e vulnerabilidades, tais como, assinaturas de listas de discussão e visitas a *sites* informativos, desde que os boletins com alertas sejam precisos e informativos.

Definir procedimentos para investigar suspeitas de códigos maliciosos, que isolem os ativos sob análise a fim de evitar a disseminação dos códigos suspeitos, bem como o envio de amostras para as entidades pertinentes efetuarem a análise especializada, e quando pertinente, desenvolverem os mecanismos de contenção e reparação a serem implantados;

Preparar planos de continuidade do negócio adequados para a recuperação em caso de ataques por códigos maliciosos, incluindo todos os procedimentos necessários para a cópia e recuperação dos dados e *softwares*;

Disseminar constantemente as boas práticas, instruções e alertas aos usuários dos sistemas de informação quanto a situações de riscos de contaminação por códigos maliciosos, como por exemplo, as mensagens eletrônicas denominadas SCAM, que tem por objetivo enganar os usuários para induzi-los a descarregar códigos maliciosos nos equipamentos da companhia.

Cópias de segurança

As cópias de segurança (*backups*) têm como principal objetivo garantir a salvaguarda das informações, com garantia de integridade e disponibilidade da informação, servindo de fonte de restauração em caso de destruição ou alteração indevida.

Procedimentos de rotina necessitam ser estabelecidos e mantidos para implementar a estratégia de geração de cópias de segurança (*backup*) e recuperação de dados (*restore*) em um tempo aceitável, sempre que necessário. Para isso, o plano de geração e recuperação das cópias de segurança deve prever, minimamente, os seguintes itens:

Respeitar os requisitos de segurança da informação e observar a criticidade da informação para a determinação dos planos de cópias de segurança, prevendo a necessidade de se apoiar a continuidade da operação e eventual recuperação de desastres da organização;

Definir e implantar o processo de geração de cópias, considerando a extensão (por exemplo, completa, incremental ou diferencial) e sua freqüência da gravação;

As cópias de segurança devem ser armazenadas em uma localidade remota, a uma distância suficiente para garantir a capacidade de restauração dos danos causados por eventual desastre ocorrido no local principal;

Determinar e cumprir o período de retenção de cópias de segurança, visando a capacidade de recuperação histórica, bem como suportar requerimentos de salvaguarda de informações, pelo período determinado pelos negócios da companhia e/ou requisitos de leis e regulamentações;

Adotar medidas apropriadas de proteção física e ambiental das informações presentes em cópias de segurança, de forma consistente com as normas aplicadas na instalação principal; As cópias de segurança das informações, os softwares de *backup* e as mídias devem ser testados regularmente, e os procedimentos de recuperação também devem ser submetidos à verificação e testes regulares, visando garantir que estes são efetivos e que podem ser concluídos dentro dos prazos definidos nos procedimentos operacionais de recuperação;

Devem ser gerados e mantidos registros completos e exatos das cópias de segurança, além de documentação apropriada sobre os procedimentos de restauração de dados;

Em situações onde a informação possui requisitos de confidencialidade, suas cópias de segurança deverão ser protegidas através de criptografia, e suas chaves de acesso devidamente protegidas.

Gerenciamento da segurança em redes

As redes de dados são os principais componentes de interconexão de dispositivos eletrônicos, desempenhando um papel fundamental no suporte aos processos de negócio, que necessitam da troca constante de informações. Por isso, constituem um ponto fundamental na infraestrutura tecnológica da empresa, sendo necessário garantir a sua devida proteção.

O gerenciamento seguro de redes, que pode ir além dos limites das dependências da organização, requer cuidadosas considerações relacionadas ao fluxo de dados, implicações legais, monitoramento e proteção. Controles adicionais podem ser necessários para proteger informações sensíveis trafegando sobre redes públicas, como a internet.

As redes necessitam ser adequadamente gerenciadas e controladas, de forma a protegê-las contra ameaças e manter a segurança de sistemas e aplicações que utilizam estas redes, incluindo a informação em trânsito. Os gestores de redes devem implementar os controles necessários para garantir a segurança da informação nestas redes e a proteção dos serviços e dispositivos a elas conectados.

As características de segurança, níveis de serviço e requisitos de gerenciamento dos serviços de rede devem ser identificados e incluídos em quaisquer acordos de serviços de rede, tanto aqueles providos internamente ou terceirizados. Neste caso, a capacidade do provedor dos serviços de rede de gerenciar os serviços acordados de maneira segura deve ser determinada e monitorada regularmente.

Serviços de rede incluem o fornecimento de conexões, serviços de rede privados, redes de valor agregado e soluções de segurança de rede gerenciadas. Estes serviços podem abranger desde o simples fornecimento de banda de rede não gerenciada até complexas ofertas de soluções de valor agregado. Em particular, os itens a seguir devem ser considerados:

A responsabilidade operacional pelas redes deve ser separada da operação dos recursos computacionais, sempre que possível e apropriado;

As responsabilidades e procedimentos sobre o gerenciamento de equipamentos de rede remotos, incluindo equipamentos em áreas de usuários ou de terceiros, devem ser estabelecidos e mantidos de forma a obedecer aos requisitos de segurança;

Controles especiais devem ser estabelecidos para proteção da confidencialidade e integridade dos dados trafegando sobre redes públicas ou sobre as redes sem fio (*wireless*) e para proteger os sistemas e aplicações a elas conectadas. Exemplos são o uso de VPN, autenticação de rede RADIUS, e a criptografia de rede wireless através de WPA/WPA2;

Controles especiais podem também ser requeridos para manter a disponibilidade dos serviços de rede e computadores conectados, como por exemplo, sistemas de detecção e prevenção de intrusão de rede (IDS/IPS) e *honeypots*;

Perímetros de segurança devem ser aplicados às redes de dados, através da utilização de mecanismos específicos, como firewalls, controle de admissão de dispositivos em rede, roteadores e redes virtuais (*VLAN*), conforme a necessidade de cada rede e de seus dispositivos;

Mecanismos apropriados de registro e monitoração devem ser aplicados para a correta operação do ambiente e manutenção de sua disponibilidade e performance, podendo ser empregados mecanismos de priorização dos tráfegos críticos de dados, através da qualidade de serviço de rede (QoS);

As atividades de gerenciamento necessitam ser coordenadas para otimizar os serviços para a organização e assegurar que os controles sejam aplicados de forma consistente sobre toda a infraestrutura de processamento da informação.

Manuseio seguro de mídias

As mídias físicas são amplamente utilizadas para armazenar informações, sendo assim faz-se necessária a prevenção contra divulgação não autorizada, modificação, remoção ou destruição aos ativos. As mídias devem ser controladas e fisicamente protegidas, através de procedimentos operacionais apropriados, visando proteger documentos, mídias magnéticas de computadores (fitas, discos), mídias removíveis, entre outras.

Gerenciamento de mídias removíveis: Devem ser estabelecidos procedimentos para o gerenciamento de mídias removíveis. Mídia removível inclui fitas, discos rígidos (HD), *pendrives*, discos removíveis, CD, DVD e mídia impressa. Tais procedimentos devem considerar a definição de quais as mídias apropriadas para cada finalidade, bem como as regras de uso incluindo seu controle de acesso, proteção contra códigos maliciosos e descarte ao término de sua utilização ou prazo de vida útil.

Descarte de mídias: As mídias devem ser descartadas de forma segura e protegida quando não forem mais necessárias, por meio de procedimentos formais. Procedimentos formais para o descarte seguro das mídias devem ser definidos para minimizar o risco de vazamento de informações sensíveis ou confidenciais a pessoas não autorizadas. Tais procedimentos devem incluir a obrigatoriedade da destruição física da mídia, ou então a inutilização completa dos dados armazenados, através de métodos que inviabilizem sua recuperação.

Procedimentos para tratamento de informação: Devem ser estabelecidos procedimentos para o processamento, armazenamento e transmissão de informações, para protegê-las contra a divulgação não autorizada ou uso indevido. Tais procedimentos devem incluir a correta classificação das informações, e a determinação e implantação das medidas de controle necessárias.

Estes procedimentos devem ser aplicados para informações em documentos, sistemas de informação, redes de computadores, computação móvel, correio eletrônico, serviços postais, uso de máquinas de fax e qualquer outro item sensível, como, por exemplo, cheques e faturas.

Segurança na transmissão de informações

A transmissão de informações é fundamental para o cumprimento dos propósitos das mesmas, porém, durante esta atividade elas são particularmente expostas, sujeitas a acesso indevido. Para evitar vazamento ou alterações indevidas, deve-se manter a segurança na troca de informações internamente à organização e com quaisquer entidades externas.

Normas e procedimentos para troca de informações

Normas e procedimentos devem ser estabelecidos para determinar os controles e métodos adequados para a troca de informações em recursos eletrônicos de comunicação, considerando os itens a seguir:

a) Devem existir procedimentos formulados e estabelecidos controles para evitar que a informação em trânsito sofra interceptação, cópia, modificação, desvio e destruição;

b) Mecanismos para detecção e proteção contra código malicioso que pode ser transmitido através do uso de recursos eletrônicos de comunicação devem ser implantados;

c) É necessária a utilização de mecanismos para proteção de informações eletrônicas sigilosas que sejam transmitidas na forma de anexos, considerando uso de senhas de acesso ou técnicas de criptografia, quando necessário;

d) Não deve ser transmitida qualquer mensagem com teor difamatório, de assédio, falsa identidade, antiético, retransmissão de "correntes" ou com conteúdos ilegais em qualquer aspecto;

e) Diretrizes de retenção e descarte para toda a correspondência devem ser adotadas, incluindo mensagens, de acordo com regulamentações e legislação locais e nacionais relevantes;

f) As pessoas não devem manter conversas confidenciais em locais públicos, escritórios abertos ou locais de reunião que não disponham de privacidade;

g) Os recursos e meios utilizados para a troca de informações devem estar de acordo com os requisitos legais pertinentes.

Acordos para a troca de informações

Devem ser estabelecidos acordos para a troca de informações e softwares entre a organização e entidades externas, principalmente no caso de informações com requisitos de confidencialidade.

Os acordos de troca de informações necessitam considerar condições de segurança das informações, incluindo o compromisso e as responsabilidades entre as partes, rastreabilidade dos eventos, padrões técnicos para a transmissão, identificação de portadores, e demais controles especiais quando necessário. Convém que os aspectos de segurança contidos nos acordos reflitam a sensibilidade das informações envolvidas.

Proteção de mensagens eletrônicas

Mensagens eletrônicas como correio eletrônico, *Eletronic Data Interchange* (EDI) e sistemas de mensagens instantâneas cumprem um papel cada vez mais importante nas comunicações do negócio.

As mensagens eletrônicas têm riscos particulares, se comparada com a comunicação em documentos impressos, pois são muito mais expostas por permitirem a disseminação e acesso de forma muito mais abrangente, além de serem sujeitos à automação de ataques técnicos.

Portanto, as informações que trafegam em mensagens eletrônicas necessitam de cuidados especiais para que sejam adequadamente protegidas, sendo necessário considerar os seguintes controles:

a) Assegurar que o conteúdo e o meio de transporte da mensagem estejam adequados;

b) Garantir a autenticidade das informações, dos remetentes e destinatários envolvidos;

c) Níveis adequados de confiabilidade e disponibilidade geral do serviço de transporte;

d) Aspectos legais, como, por exemplo, requisitos de assinaturas eletrônicas;

e) Autorização prévia das áreas responsáveis, antes do uso de serviços públicos externos, tais como sistemas de mensagens instantâneas e compartilhamento de arquivos na Internet;

f) Controles adequados de proteção de acesso, considerando autenticação e proteção por senha ou criptografia, caso a transmissão seja realizada através de redes públicas.

Segurança na integração de dados de aplicações de negócio

As aplicações de negócio são sistemas de informação que fornecem suporte direto aos processos de negócio da companhia. São responsáveis por processar os dados de entrada a fim de prover informações valiosas, gerando os dados de saída, a serem utilizadas por outras aplicações, ou por usuários no desempenho de suas funções.

Normalmente as aplicações são altamente interconectadas, a fim de refletir a mesma interconexão existente nos processos da companhia. Os dados de entrada e de saída são componentes fundamentais para o correto funcionamento das aplicações, ao mesmo tempo em que são particularmente expostos por serem constantemente transmitidos utilizando a infraestrutura de TI.

As aplicações de negócio possuem especial potencial para conter informações sigilosas, pois muitas vezes as mesmas informações essenciais às atividades internas, podendo oferecer riscos significativos à companhia caso seja utilizada indevidamente, seja pela concorrência, por sabotagem, fraudes ou erros operacionais.

Dessa forma, faz-se necessária a adoção de todas as medidas de segurança, cabíveis, de acordo com a criticidade da aplicação para o negócio e também a classificação das informações processadas. Em casos de aplicações altamente críticas, por exemplo, podem-se adotar conceitos de alta disponibilidade e contingência. Já no caso de aplicação com informações confidenciais, pode ser requerida a criptografia de dados no processo de integração, ou procedimentos mais rígidos na gestão de acessos, incluindo termos de responsabilidade para seus usuários.

Serviços de comércio eletrônico

Os serviços de comércio eletrônico consistem em sistemas informatizados que permitem que transações comerciais sejam realizadas através de computadores, criando, alterando ou redefinindo valores entre organizações, ou entre organizações e clientes, para a aquisição de bens, produtos e serviços, terminando com a liquidação financeira, que pode ser por intermédio de meios de pagamentos eletrônicos ou convencionais.

Quando os serviços de comércio eletrônico são dispostos na Internet, suas informações são particularmente expostas a sofrerem ataques, que podem resultar desde perdas financeiras até a degradação da imagem da companhia. Portanto, necessitam de medidas específicas de segurança a fim de reduzir seus riscos a níveis aceitáveis.

Tais medidas devem considerar o uso de mecanismos que garantam a autenticidade das partes envolvidas, e também a criptografia dos dados sigilosos, no armazenamento ou trânsito das informações. Por exemplo, tais funções podem ser realizadas através do uso de uma estrutura pública de certificados digitais, provendo autenticidade através de assinaturas digitais, e criptografia através de *secure sockets layer*.

Sistema de comércio eletrônico

Os sistemas que provém serviços de comércio eletrônico precisam ser protegidos de atividades maliciosas, com intenção de fraude, vantagem competitiva ou outros danos à empresa. Devem ser mantidos controles específicos de segurança, considerados os seguintes itens:

a) Garantia do nível de confiança que cada parte requer na suposta identidade de outros, como, por exemplo, por meio de mecanismos de autenticação;

b) Processo de autorização de quem pode consultar extratos, determinar preços, emitir pedidos, realizar ou alterar cadastros, emitir pedidos ou quaisquer outras transações importantes no processo comercial;

c) Requerimentos de proteção de informações privada de clientes, de forma alinhada às leis e regulamentações de privacidade de dados pessoais.

d) Garantia de que parceiros comerciais estão completamente informados de suas autorizações;

e) Requerimentos de confidencialidade, integridade e disponibilidade de informações dispostas no sistema, podendo ser públicas (como informações institucionais ou de níveis de serviço) ou não (como informações de pedidos, consultas de saldo e limites de transação);

f) Infraestrutura tecnológica que atenda aos requisitos de disponibilidade requeridos, considerando que estará potencialmente exposta a ataques de negação de serviço;

g) Mecanismos de segurança que detectem e previnam tentativas de intrusão, códigos maliciosos ou acesso não autorizado;

h) Capacidade de investigação apropriada para a verificação de informações fornecidas por clientes ou parceiros;

i) Prevenção contra perda ou duplicação de informação de transação;

j) Responsabilidades associadas com quaisquer transações fraudulentas;

Muitas das considerações acima podem ser endereçadas, por exemplo, pela aplicação de controles criptográficos. Convém que os procedimentos para comércio eletrônico entre parceiros comerciais sejam apoiados por um acordo formal que comprometa ambas as partes aos termos da transação,

incluindo detalhes de autorização. Outros acordos com fornecedores de serviços de informação e redes de valor agregado podem ser necessários.

Transações *online*

As informações envolvidas em transações *online* necessitam ser protegidas para prevenir transmissões

incompletas, erros de roteamento, alterações não autorizadas, divulgação não autorizada, duplicação ou reapresentação de mensagem não autorizada. As medidas de proteção podem prever mecanismos como:

a) Uso de assinaturas eletrônicas para as partes envolvidas na transação;

b) Validação das credenciais de usuário e outras entidades envolvidas nas transações;

c) Manter medidas de verificação dos requisitos de confidencialidade, integridade e disponibilidade em todos os componentes envolvidos nas transações, sempre que possível;

d) Criptografar o caminho de comunicação entre todas as partes envolvidas, utilizar protocolos de comunicação reconhecidamente seguros;

e) Garantir que o armazenamento dos detalhes da transação está localizado fora de qualquer ambiente publicamente acessível, e não retida e exposta em um dispositivo de armazenamento

diretamente acessível pela internet;

A extensão dos controles adotados precisará ser proporcional ao nível de risco associado a cada forma de transação *online.* Transações podem precisar estar de acordo com leis, regras e regulamentações na jurisdição em que a transação é gerada, processada, completa ou armazenada.

Informações publicamente disponíveis

Termos de uso, informações institucionais, declaração de níveis de serviço e outras informações são comumente publicadas em sistemas de comércio eletrônico, sendo disponíveis para consulta pelo público em geral. Apesar de não possuírem requisitos de confidencialidade, os conceitos de disponibilidade, e principalmente integridade são particularmente relevantes.

A perda de integridade de informações institucionais, por exemplo, podem gerar sérios danos à imagem da companhia, em casos onde as mensagens possuam teor pejorativo à instituição ou conteúdo ofensivo aos clientes ou parceiros.

Sendo assim, é necessário que a integridade das informações disponibilizadas em sistemas publicamente acessíveis seja protegida para prevenir modificações não autorizadas. Além disso, deve haver um processo formal de aprovação antes que uma informação seja publicada. Outros cuidados devem ser previstos, como:

a) Informações que sejam inseridas um sistema de publicação sejam processadas completa e corretamente em um tempo adequado;

b) Informações sensíveis sejam protegidas durante a coleta, processamento e armazenamento;c) O acesso a sistemas de publicação deve ser restrito a pessoal autorizado, por meios aprovados e em ambiente privados, dotados de medidas de proteção adequados como controle de acesso e auditoria;

d) As informações devem ser obtidas em conformidade com qualquer legislação de proteção de dados;

Cartões e Meios de Pagamentos Eletrônicos

Os cartões de pagamentos eletrônicos são instrumentos que permitem que o portador do cartão realize transações financeiras eletrônicas, para realizar pagamentos ou outras transferências de valores, nos estabelecimentos credenciados, sendo um dos componentes fundamentais dos negócios da Iterative. Um possível comprometimento de segurança dos cartões de pagamento incide diretamente em prejuízos financeiros e podem representar riscos consideráveis à imagem da companhia.

Os requerimentos de segurança da informação devem ser empregados em todo o ciclo de vida destes ativos, incluindo sua confecção, armazenamento e distribuição. O acesso físico aos cartões deve ser restrito e controlado através de medidas reforçadas, somente por pessoal autorizado.

Os dados dos cartões, quando processados ou armazenados em sistemas, devem ser especialmente protegidos, através de criptografia e/ou mascaramento de dados, a fim de minimizar riscos de perda de confidencialidade ou integridade dos dados através de acessos indevidos.

O controle de acesso aos sistemas que processam ou armazenam dados de cartões devem ser apropriados. Somente um grupo limitado de pessoas deve ter acesso a este tipo de informação, que somente podem ser concedidos após passar por processos formais de autorização e responsabilização. A relação de pessoas que possuem este tipo de permissão não deve ser de conhecimento do público em geral, a fim de evitar possível aliciamento.

O sigilo das informações deve ser estritamente mantido, portanto, tais informações não devem ser comunicadas, transmitidas, armazenadas ou processadas em meios que não sejam reconhecidamente aprovados e dotados das medidas de segurança adequadas.

Monitoramento de sistemas

Os mecanismos de segurança, além de proverem meios de evitar possíveis fraudes ou ataques à rede, também devem dispor de meios para detectar atividades não autorizadas de processamento de

informação. Sem o monitoramento nunca será possível saber como estão atuando as proteções implementadas.

Para monitorar um sistema de processamento da informação é preciso criar mecanismos de registros de acesso e falhas, a fim de identificá-los e verificar a eficácia das medidas de proteção. Através da análise de tais registros, deve-se checar a eficácia dos controles adotados e para verificar a conformidade com os requisitos de gestão, operação e utilização do sistema.

Registros de auditoria

Os registros (*logs)* de auditoria são informações geradas automaticamente por sistemas, com o intuito de prover capacidade de acompanhamento, monitoramento e análise de eventos de sistemas. Podem registrar diversos tipos de eventos específicos a cada sistema, incluindo: o processamento, armazenamento ou transporte de informações; o início, progresso e término de operações sistêmicas; e erros ou falhas do sistema.

Existem registros particularmente importantes sob os aspectos de segurança, que são os referentes às operações de administração ou operação de acessos, que registram as ações de manipulação de contas de acesso, senhas e suas permissões, bem como as operações de usuários no uso do sistema, registrando entrada ou saída (*logon* ou *logoff*), a utilização de permissões e o uso de recursos.

Os registros de auditoria devem ser armazenados em local seguro, durante o período que for necessário para suportar possíveis análises ou investigações. Sempre que necessário, os registros de auditoria devem incluir:

a) Origem do acesso: Identidade do terminal e endereço IP utilizado para originar a tentativa de acesso ao sistema; a versão e o programa utilizado para conexão; informações de sistema operacional;

b) Acessos autorizados: Identificação e conta do usuário; seus níveis de permissões, a data e o horário dos eventos-chave (incluindo *logon* e *logoff*); tipo do evento; os arquivos ou funções acessadas; os programas ou utilitários utilizados;

c) Operações privilegiadas: Uso de contas privilegiadas (ex: supervisor, *root*, administrador); inicialização e finalização do sistema; a conexão e a desconexão de dispositivos de entrada e saída; operações de integração de dados; alterações ou tentativas de alterações nos controles e parâmetros do sistema;

d) Tentativas de acesso não autorizadas, tais como: ações de usuários com falhas ou rejeitadas; ações envolvendo dados ou outros recursos com falhas ou rejeitadas; violação de políticas de acesso; bloqueio de tráfegos não autorizados em ativos de rede ou *firewalls*; alertas dos sistemas de proteção contra códigos maliciosos ou de detecção e prevenção de intrusão;

e) Alertas e falhas do sistema, tais como: alertas ou mensagens do console; registro das exceções do sistema; alarmes do gerenciamento de componentes; falhas críticas de funcionamento ou processamento de dados; falhas de processos de integração.

Monitoramento do uso do sistema

A fim de assegurar que uso do sistema está conforme os propósitos do sistema, seus requerimentos de segurança, e que os usuários estão executando somente as atividades que foram explicitamente autorizadas, faz-se necessária a condução de ações de monitoramento do seu uso. A análise crítica dos registros de auditoria deve ser realizada de forma contínua, envolve a compreensão das ameaças encontradas no sistema e a maneira pela qual elas podem existir, a fim de desenvolver controles que previnam a recorrência dos eventos de mau-funcionamento ou uso indevido.

Proteção das informações dos registros

Todos os registros de sistema precisam ser protegidos contra falsificação e acesso não autorizado, pois os dados podem ser modificados e excluídos e suas ocorrências podem causar falsa impressão de segurança ou direcionar erroneamente as possíveis análises.

Registros de administrador e operador

Os administradores e operadores de sistemas desempenham importantes funções, normalmente no papel de custodiante de ativos de informação. Os eventos relacionados ao desempenho de tais funções devem ser devidamente registrados e mantidos sob proteção. Adicionalmente, os registros de atividades dos operadores e administradores dos sistemas devem ser analisados criticamente em intervalos regulares.

Registros de falhas

Registros de falhas e erros são importantes para suportar procedimentos corretivos ou de melhoria contínua em sistemas de informação. Também podem ser indicativos de tentativas de uso indevido, como por exemplo, tentativas inválidas de *logon* ou de uso de permissões. As falhas podem impactar o desempenho do sistema. Convém que as falhas ocorridas sejam registradas e analisadas, e que sejam adotadas ações apropriadas a fim de manter a performance adequada, bem como a disponibilidade do sistema.

Sincronização dos relógios

O estabelecimento correto dos relógios dos computadores é importante para assegurar a exatidão dos registros (*logs*) de auditoria, que podem ser requeridos por investigações ou como evidências em casos legais ou disciplinares. Registros de auditoria incorretos podem causar danos à credibilidade das evidências e impedir o andamento de possíveis investigações. Convém que se levem em conta especificações locais (por exemplo, horário de verão), e que os relógios de todos os sistemas de

processamento da informação relevantes, dentro da organização ou do domínio de segurança, sejam sincronizados de acordo com uma hora oficial.

2.14. Segurança na Aquisição, Desenvolvimento e Manutenção de Sistema da informação

Garantir que a segurança é parte integrante dos processos de aquisição, desenvolvimento e manutenção de sistemas de informação é essencial para a estratégia de Segurança da Informação. Os negócios corporativos são altamente informatizados e dependentes de sistemas de informação, que necessitam ter o nível de proteção adequada para evitar riscos.

Os sistemas de informação são ativos de informação compostos por recursos tecnológicos que processam dados de forma organizada com o objetivo de fornecer suporte a processos da companhia. Incluem-se sistemas operacionais, sistemas de infraestrutura, aplicações de negócios e aplicativos.

O projeto e a implementação de sistemas de informação destinados a apoiar o processo de negócios podem ser cruciais para a segurança. Por isso, os requisitos de segurança precisam ser identificados e acordados antes do desenvolvimento e/ou implementação de sistemas de informação.

Requisitos de segurança de sistemas de informação

Devem ser definidos os requisitos para controles de segurança nas especificações de novos sistemas de informação ou melhorias em sistemas existentes. O valor para o negócio dos ativos de informação, bem como os danos potenciais que poderiam resultar de uma falha ou ausência de segurança devem refletir nos requisitos de segurança especificados.

As especificações para os requisitos de controles nos sistemas de informação necessitam considerar tanto os controles automáticos como os controles manuais a serem incorporados. As considerações de segurança devem ser aplicadas tanto quando da avaliação de sistemas desenvolvidos internamente ou adquiridos de terceiros. Tais requisitos podem ser definidos através de normas de segurança para os diversos tipos de sistemas, e em casos de maior relevância, em documentos de requerimentos de segurança específicos para uma determinada aplicação de negócio.

Controles introduzidos no estágio de projeto são significativamente mais baratos para implementar e manter do que aqueles incluídos durante ou após a implementação. Sendo assim, convém que os requisitos de sistemas para a segurança da informação, bem como os processos para implementá-la sejam integrados aos estágios iniciais dos projetos dos sistemas de informação.

Segurança de Aplicações na Internet

Parte importante dos negócios da Iterative depende de aplicações publicadas na *Internet*, disponibilizando informações para acesso de clientes e parceiros de negócios, ou então possibilitar transações comerciais. Tais aplicações possuem alto potencial de ser alvo de ataques eletrônicos, justamente pelo fato de estarem publicadas na rede mundial de computadores, possibilitando que qualquer entidade conectada a esta rede realize tentativas de acessos, sejam devidos ou indevidos.

Com o intuito de definir mais claramente os requerimentos de segurança neste tipo de aplicação, a Iterative determina as principais regras a serem seguidas no desenvolvimento, implantação ou operação deste tipo de aplicação. Segue estrutura, sendo basicamente:

a) Considere a segurança logo na iniciação do projeto;

b) Implemente controles rígidos de acesso e permissões de acesso;

c) Filtre a comunicação do ambiente externo ao ambiente interno no nível de rede e, se necessário, na aplicação;

d) Forneça trilhas de auditoria com todas as informações relevantes;

e) Não publique na Internet páginas ou funções administrativas;

f) Siga as melhores práticas de programação segura, como por exemplo, as definidas pelo *OWASP (top tem 2013)*;

g) Inclua cláusulas de segurança na contratação de provedores externos;

h) Criptografe dados sensíveis no armazenamento ou transmissão em redes públicas;

i) Esteja conforme os requerimentos do *PCI-DSS* para o armazenamento de dados de cartões de crédito;

Em adição aos pontos acima, toda aplicação exposta na Internet deve possuir descrições claras sobre seus termos de uso, privacidade de informações e segurança de dados para os usuários. Medidas especiais de segurança podem ser necessárias, como por exemplo, a restrição de acesso à aplicação por endereço IP de origem, e uso de certificados digitais para fornecer autenticidade ao serviço.

Processamento correto nas aplicações

Para se prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações, são necessários controles apropriados, que sejam incorporados no projeto das aplicações, para assegurar seu processamento correto. Esses controles devem incluir a validação dos dados de entrada, do processamento interno e dos dados de saída.

Validação de dados de entrada

Devem ser aplicadas checagens na entrada de transações de negócios, em dados (por exemplo, nomes e endereços, limites de crédito, números de referência de clientes) e em parâmetros de tabelas (por exemplo, preços de venda, taxas de conversão de moedas, tarifas de impostos).

Esses elementos são de fundamental importância para a segurança da informação, pois é sabido que a grande maioria das tragédias tem sua origem em falhas na validação inicial dos dados que possibilitam a inserção de informações que induzem os sistemas de informação a erro, quer seja pelo descuido, desconhecimento ou despreparo, ou mesmo por ações intencionais. O uso de ferramentas de automatização do processo de teste da validação dos dados de entrada e a elaboração e aperfeiçoamento constante de *checklists* é uma prática altamente recomendável.

Controle do processamento interno

É um item de controle que implica no dever de incorporar, nas aplicações, checagens de validação durante o processamento, com o objetivo de detectar qualquer corrupção de informações, por erros ou por ações deliberadas.

A possibilidade de desvio no resultado esperado de processamento de dados resulta em vulnerabilidades sistêmicas que devem ser tratadas. O resultado de um processamento interno deve ser conhecido ou esperado, e ser objeto de validação. Falhas no processamento interno das aplicações geralmente implicam diretamente em perdas de performance ou perdas financeiras para a organização, podendo chegar, em determinadas situações, a níveis inaceitáveis.

Integridade de Mensagens

Mecanismos de controle precisam ser incorporados ao sistema para assegurar que os requisitos de garantia de autenticidade e a proteção da integridade das mensagens das aplicações sejam devidamente implementados.

As mensagens das aplicações são os elementos importantes da comunicação com administradores e usuários. Da comunicação eficiente deriva boa parte da segurança da informação das organizações. Em função disso, requisitos para garantir a autenticidade e proteger a integridade das mensagens em aplicações devem ser identificados, e os controles apropriados implementados.

Validação de dados de saída

Esse item estabelece a necessidade de controles adequados de dados de saída, devendo ser validados para assegurar que o processamento das informações armazenadas está correto e é apropriado às circunstâncias. Os dados de saída de uma aplicação serão utilizados por usuários para a execução das operações de negócio, ou servirão como dados de entrada para outra aplicação ou processamento, internamente ou no ambiente externo da organização.

Controles criptográficos

A criptografia é um método de proteção de informação, visando proteger a confidencialidade, autenticidade ou a integridade das informações, através da transformação dos dados originais para um formato ilegível, de forma que possa ser decifrado somente por entidades autorizadas.

De modo geral, devem utilizar controles criptográficos, no mínimo, para proteger as partes do sistema que lidam com informações relacionadas às chaves de acessos utilizados nos processos de autenticação do mesmo. Adicionalmente, devem ser observados os requisitos de proteção inerentes à classificação das informações processadas, ou análise de riscos do sistema em si, a fim de determinar a necessidade de uso de criptografia em outros componentes ou para proteção de outros dados.

Quando necessário, devem ser desenvolvidas e implementadas normas para o uso de controles criptográficos, especificando os métodos aceitáveis e processos de implantação, incluindo os *algoritmos* de criptografia, mecanismos de *hashing* e a gestão de chaves criptográficas e certificados digitais.

Segurança dos arquivos de sistemas

Os arquivos de sistema sejam bibliotecas, rotinas ou arquivos de configuração, são alvos prediletos dos ataques intencionais, justamente por serem cruciais para garantir a disponibilidade das informações e o correto funcionamento dos sistemas de informação. Um item elementar para a segurança das informações é a garantia da segurança de arquivos de sistema, através dos controles enumerados a seguir:

Controle de softwares de sistemas

Definição de procedimentos para controlar a instalação e configuração de software de sistemas, inclusive os de infraestrutura, como os *sistemas operacionais*, *middlewares* e de *bancos de dados*. Os altos graus de dependência entre as aplicações e estes componentes, aliado ao fato de terem seu funcionamento e funcionalidades amplamente divulgados e estudados, representam um elevado grau de risco, sendo necessárias as seguintes medidas de segurança:

a) A atualização do *sistema operacional*, *bancos de dados*, *middlewares*, de aplicativos e de bibliotecas de programas seja executada somente por administradores treinados e com autorização gerencial;

b) Os sistemas tenham somente contenham código executável e aprovado, e não contenham códigos em desenvolvimento ou indevidos;

c) Sistemas e aplicativos somente sejam implementados após testes extensivos e bem-sucedidos;

d) Um sistema de controle de configuração seja utilizado para manter controle da implementação dos sistemas, assim como sua documentação;

e) Uma estratégia de retorno às condições anteriores seja disponibilizada antes que mudanças sejam implementadas nos sistemas;

f) Um registro de auditoria seja mantido para todas as atualizações dos sistemas e suas bibliotecas;

g) Versões antigas de *software* sejam arquivadas, junto com todas as informações e parâmetros requeridos, procedimentos, detalhes de configurações e *software* de suporte durante um prazo igual ao prazo de retenção dos dados.

Proteção dos dados para testes de sistema

Um importante mecanismo de controle é o que deve ser implementado visando à segurança e a confiabilidade dos dados a serem utilizados para testes dos sistemas de informação e sistemas operacionais.

Uma vez que tais dados devem refletir ao máximo possível o ambiente real de operação dos sistemas, esses dados de teste devem ser selecionados com cuidado, protegidos durante seu manuseio, obedecendo aos mesmos requisitos de segurança dos dados do ambiente de produção, e o acesso a eles controlado. Sempre que for necessário, as informações devem ser substituídas ou mascaradas durante a preparação da massa de testes, a fim de não comprometer a confidencialidade das mesmas.

Controle de códigos-fonte

O acesso, manuseio e o armazenamento desses devem estar submetidos a um rígido controle. Deve ser evitado ou limitado o acesso ao conjunto dos *códigos-fonte*, o qual deverá ocorrer apenas no momento de geração das versões executáveis para teste e entrega, em ambiente especificamente preparado para isso e, evidentemente, seguro. O uso de produtos de controle de acesso e de versão é altamente recomendável.

Segurança em processos de desenvolvimento e de suporte

Os processos de desenvolvimento e suporte a sistemas de informação trazem em si grande quantidade de riscos em potencial. Grande parte das vulnerabilidades em sistemas de informação existe em decorrência dessas etapas ou atividades. O objetivo dos controles nesse item é o de manter a segurança durante o processo de desenvolvimento e suporte dos sistemas de informação.

Procedimentos para controle de mudanças

As mudanças em sistemas de informação são eventos necessários em qualquer ambiente informatizado, porém devem ser controlados adequadamente, para garantir que os requisitos de segurança sejam preservados. Portanto, a implementação de mudanças deve ser controlada utilizando procedimentos formais de controle de mudanças.

É essencial que os procedimentos de controle de mudanças sejam documentados e reforçados com a finalidade de minimizar a corrupção dos sistemas da informação. Em casos de introdução de novos sistemas, bem como em mudanças em sistemas existentes, é requerido que se sigam processos formais de documentação, especificação, teste, controle da qualidade e gestão da implementação.

Convém que os processos incluam etapas de análise do impacto das mudanças, e que sejam obtidas a concordância e aprovação formal dos responsáveis pelas áreas impactadas, para qualquer mudança que for necessária.

Vazamento de informações

As possibilidades de vazamento de informações necessitam ser prevenidas nos sistemas de informação que lidem com informações com quaisquer níveis de sigilo. Para isso, faz-se necessária a observância dos seguintes itens:

a) Definição e especificação dos requisitos técnicos de controle de acesso, tanto para os usuários quanto para administradores do sistema, prevendo os conceitos de autenticação, autorização e auditoria;

b) Definição e especificação dos requisitos processuais de gestão de usuários e acessos;

c) Uso de criptografia sempre que necessário, para assegurar informações que necessitarem deste método de proteção;

d) Medidas de proteção que impeçam o acesso através de meios alternativos, não previstos nas *interfaces* padrão dos sistemas;

e) A utilização de sistemas e *software* reconhecidos como de alta integridade, utilizando produtos avaliados e de entidades confiáveis;

f) O monitoramento regular das atividades do pessoal e do sistema, tanto sob os aspectos de administração e operação, quanto o uso normal.

Desenvolvimento terceirizado de aplicações

Nos casos de desenvolvimento terceirizado de aplicações, deve ser definida uma área responsável para supervisionar e controlar as atividades desempenhadas por terceiros, e respectivos produtos. Os requisitos específicos de negócio, bem como de arquitetura e infraestrutura de TI devem ser exigidos e validados. Além disso, devem-se garantir os requerimentos específicos de segurança sendo minimamente:

a) Acordos de licenciamento, propriedade do código, direitos de propriedade intelectual e de confidencialidade;

b) Termos de ciência e compromisso das políticas e regras internas aplicáveis, inclusive a política corporativa de segurança da informação;

c) Certificação da qualidade e exatidão do serviço realizado;

d) Provisões para custódia no caso de falha da terceira parte;

e) Permissões de acesso para auditorias de qualidade e exatidão do serviço realizado;

f) Requisitos contratuais para a qualidade e funcionalidade da segurança do código;

g) Testes antes da implantação para detectar mau funcionamento ou presença de códigos maliciosos.

Gestão de vulnerabilidades técnicas

Convém que seja obtida informação em tempo hábil sobre vulnerabilidades técnicas dos sistemas de informação em uso, avaliada a exposição da organização a estas vulnerabilidades e tomadas as medidas apropriadas para lidar com os riscos associados.

Um inventário completo e atualizado dos ativos de informação é um pré-requisito para uma gestão efetiva de vulnerabilidades técnicas. Dentre as informações necessárias para o apoio à gestão de vulnerabilidades técnicas inclui-se o fornecedor de *software*, o número de versão, o estado atual de uso e distribuição (por exemplo, que *softwares* estão instalados e em quais sistemas) e as pessoas na organização responsáveis pelos *softwares*.

O correto funcionamento do processo de gestão de vulnerabilidades técnicas é crítico para reduzir o grau de exposição dos ativos, portanto, convém que seja medido e aprimorado regularmente. As ações apropriadas devem ser tomadas, no prazo máximo de 60 dias após disponibilização do mesmo, como resposta às potenciais vulnerabilidades técnicas identificadas, de forma que:

- Sejam estabelecidas as funções e responsabilidades associadas na gestão de vulnerabilidades técnicas, incluindo o monitoramento de vulnerabilidades, a análise de riscos de vulnerabilidades, *patches*, acompanhamento dos ativos e qualquer coordenação de responsabilidades requerida;
- Sejam definidos prazos para a reação a notificações de potenciais vulnerabilidades técnicas relevantes;
- Uma vez que uma vulnerabilidade técnica potencial tenha sido identificada, devem ser avaliados os riscos associados e as ações a serem tomadas. Tais ações podem requerer o uso de *patches* nos sistemas vulneráveis; quando não existir a disponibilidade de um *patch*, convém considerar o uso de outras medidas compensatórias;
- O tratamento de uma vulnerabilidade técnica deve ser realizado de acordo com os controles relacionados com a gestão de mudanças, e ser mantido um registro de auditoria de todos os procedimentos realizados;
- Com a finalidade de assegurar sua eficácia e a eficiência, o processo de gestão de vulnerabilidades técnicas necessita ser monitorado e avaliado regularmente.

2.15. Gestão da Continuidade de Negócio

O objetivo gestão da continuidade de negócio é o de promover condições para minimizar o impacto nos negócios da Iterative em caso de interrupções não previstas nos sistemas e processos, e proteger atividades críticas ao negócio contra os efeitos gerados por falhas críticas ou desastres.

Um plano de continuidade de negócio compreende uma série de atividades desenvolvidas para suportar o negócio em uma situação adversa, situação em que, os ativos que mantém os processos de negócio não estejam disponíveis ou aptos a sustentar o negócio. Devem-se considerar ativos de todos os tipos, inclusive:

Tecnologia da Informação: Computadores, sistemas de informação, sistemas operacionais, aplicações de negócio, aplicativos, controladoras de discos, impressoras, redes de comunicação de dados, equipamentos e a infraestrutura de TI;

Utilitários e Infraestrutura: *UPS,* geradores, ar condicionado, transportes; abastecimentos (óleo, gás, energia elétrica, água, etc.);

Provedores e Parceiros: Provedores de telefonia, suporte às redes e infraestrutura, serviços de comunicação, serviços de entrega, guarda e manuseio, suporte técnico e manutenção geral;

Recursos Humanos: Colaboradores, prestadores de serviços e outros terceiros envolvidos;

Outros: Catracas, controles de acesso, equipamentos de escritório, máquinas industriais, antenas e estações de transmissão, central telefônica.

O processo de gestão da continuidade de negócios deve ser implementado para minimizar um impacto sobre a organização e recuperar perdas de ativos da informação a um nível aceitável através da combinação de ações de prevenção e recuperação. Convém que este processo identifique os processos críticos e integre a gestão da segurança da informação com as exigências da gestão da continuidade do negócio, juntamente com quaisquer outros requisitos mandatórios da organização.

Para garantir a efetividade do processo, as conseqüências de desastres, falhas de segurança, e perda de disponibilidade de serviços devem estar sujeitas a uma análise de impacto nos negócios, e que os planos de continuidade do negócio sejam desenvolvidos e implementados para assegurar que as operações essenciais sejam recuperadas dentro da requerida escala de tempo.

Incluindo segurança da informação no processo de gestão da continuidade de negócio

O processo de gestão de continuidade deve ser desenvolvido não somente para manter a continuidade dos negócios em si, mas também deve contemplar os requisitos de segurança da informação que necessitam ser mantidos. Este processo necessita agregar os seguintes elementos-chave:

a) A responsabilidade pela coordenação do processo de gestão continuidade de negócios deve ser atribuída a um nível adequado dentro da organização.

b) Entendimento dos riscos a que a organização está exposta, no que diz respeito à sua probabilidade e impacto no tempo, incluindo a identificação e priorização dos processos críticos do negócio;

c) Entendimento do impacto que incidentes de segurança da informação provavelmente terão sobre os negócios;

d) Identificação de todos os ativos envolvidos em processos críticos de negócio;

e) Identificação, mensuração de esforços e consideração da implementação de controles preventivos e de mitigação;

f) Consideração de contratação de seguro compatível que possa ser parte integrante do processo de continuidade do negócio, bem como a parte de gestão de risco operacional;

g) Garantia da segurança de pessoal, proteção de recursos de processamento das informações e bens organizacionais;

h) Execução de testes e atualizações regulares dos planos e processos implantados;

i) A gestão da continuidade do negócio deve ser incorporada aos processos e estrutura da organização.

Cópias do plano de continuidade do negócio também devem guardadas em um ambiente remoto, a uma distância suficiente para escapar de qualquer dano de um desastre no local principal. O gestor deve garantir que as cópias dos planos de continuidade do negócio estejam atualizadas e protegidas ao menos no mesmo nível de segurança como aplicado no ambiente principal. Da mesma forma, outros materiais necessários para a execução do plano de continuidade do negócio também devem ser armazenados e protegidos em local remoto.

Estrutura do plano de continuidade do negócio

Cada plano de continuidade do negócio deve descrever o enfoque para continuidade, por exemplo, o enfoque para assegurar a disponibilidade dos sistemas de informação. Além disso, também precisa incluir o procedimento de escalonamento e as condições para sua ativação, assim como as responsabilidades individuais para execução de cada uma das atividades do plano.

Quando novos requisitos são identificados, é importante que os procedimentos de emergência relacionados sejam ajustados de forma apropriada, por exemplo, o plano de abandono ou o procedimento de recuperação. Procedimentos do programa de gestão de mudança da organização

devem ser incluídos para assegurar que os assuntos de continuidade de negócios estejam sempre direcionados adequadamente.

Os procedimentos de emergência, de recuperação e planos de reativação devem ser de responsabilidade dos gestores dos recursos de negócios ou dos processos envolvidos. Já os procedimentos de recuperação para serviços técnicos alternativos, como processamento de informação e meios de comunicação, normalmente são de responsabilidade dos responsáveis por tecnologia da informação e os provedores de serviços envolvidos.

É necessário que exista uma estrutura de planejamento que contemple os seguintes itens:

- Condições para ativação dos planos que descrevam os processos a serem seguidos antes de cada plano ser ativado;
- Procedimentos de emergência que descrevam as ações a serem tomadas após a ocorrência de um incidente que coloque em risco as operações do negócio;
- Procedimentos de contingência que descrevam as ações necessárias para a transferência das atividades essenciais do negócio ou os serviços de infraestrutura para localidades alternativas temporárias e para a reativação dos processos do negócio no prazo necessário;
- Procedimentos operacionais temporários para seguir durante a conclusão de recuperação e restauração;
- Procedimentos de recuperação que descrevam as ações a serem adotadas quando do restabelecimento das operações;
- Uma programação de manutenção que especifique quando e como o plano deverá ser testado e a forma de se proceder à manutenção deste plano;
- Atividades de treinamento, conscientização e educação com o propósito de criar o entendimento do processo de continuidade de negócios e de assegurar que os processos continuem a ser efetivo; Designação das responsabilidades individuais, descrevendo quem é responsável pela execução de que item do plano, prevendo que suplentes sejam definidos quando necessário;
- Os ativos e recursos críticos precisam estar aptos a desempenhar os procedimentos de emergência, recuperação e reativação.

Testes, manutenção e reavaliação dos planos de continuidade do negócio

Os planos de continuidade do negócio necessitam ser testados e atualizados regularmente, de forma a assegurar sua permanente atualização e efetividade. Espera-se que os testes assegurem que todos os membros da equipe de recuperação e outras pessoas relevantes estejam conscientes dos planos e de suas responsabilidades para a continuidade do negócio e a segurança da informação, e conheçam as suas atividades quando um plano for acionado.

O planejamento e a programação dos testes dos planos de continuidade de negócios indicam como e quando cada elemento do plano seja testado. Convém que os componentes isolados dos planos sejam freqüentemente testados.

Convém que os resultados dos testes sejam registrados e ações tomadas para a melhoria dos planos, onde necessário. A responsabilidade pelas análises críticas periódicas de cada parte do plano deve ser definida e estabelecida. O controle formal de mudanças assegura que os planos atualizados são distribuídos e reforçados por análises críticas periódicas do plano como um todo.

2.16. Conformidade

O conceito de conformidade determina as regras a serem cumpridas, visando evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações, obrigações contratuais e de quaisquer requisitos de segurança da informação.

O projeto, a operação, o uso e a gestão de sistemas de informação podem estar sujeitos a requisitos de segurança contratuais, regulamentares ou estatutários da Iterative em território nacional.

Os requisitos legislativos variam de país para país e também para a informação criada em um país e transmitida para outro (isto é, fluxo de dados transfronteira), sendo assim, tais situações devem ser previstas e controladas.

Identificação da legislação vigente

Convém que todos os requisitos estatutários, regulamentares e contratuais relevantes, e o enfoque da organização para atender a esses requisitos, sejam explicitamente definidos, documentados e mantidos atualizados para cada sistema de informação da organização. Os controles específicos e as responsabilidades individuais para atender a estes requisitos devem ser definidos e documentados em normas ou procedimentos específicos.

Direitos autorais e de propriedade intelectual

Convém que procedimentos apropriados sejam implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais no uso de material, em relação aos quais pode haver direitos autorais e de propriedade intelectual e sobre o uso de produtos de *software* proprietários.

Direitos de propriedade intelectual incluem direitos de *software* ou documento, direitos de projeto, marcas, patentes e licenças de códigos-fonte. Produtos de *software* proprietários são normalmente fornecidos sob um contrato de licenciamento que especifica os termos e condições da licença, por exemplo, restringe o uso dos produtos em máquinas especificadas ou limita a cópia apenas para criação de uma cópia de segurança. A questão relativa aos direitos de propriedade intelectual de *software* desenvolvido pela organização precisa ser esclarecida e controlada efetivamente.

Violações aos direitos de propriedade intelectual podem conduzir a ações legais, que por sua vez, podem envolver processos criminais. Portanto, as seguintes diretrizes devem ser consideradas para proteger qualquer material que possa ser considerado como propriedade intelectual:

a) Definir e divulgar normas de conformidade com os direitos de propriedade intelectual que defina o uso aceitável de produtos de *software* e de informações;

b) Adquirir *software* somente por meio de fontes conhecidas e de reputação, para assegurar que o

direito autoral não está sendo violado;

c) Manter de forma adequada os registros de ativos e identificar todos os ativos com requisitos de proteção de direitos de propriedade intelectual;

d) Manter provas e evidências da propriedade de licenças, discos-mestre, manuais e etc.;

e) Implementar controles para assegurar que o número máximo de usuários permitidos não excede o número de licenças adquiridas;

f) Conduzir verificações para que somente produtos de *software* autorizados e licenciados sejam

instalados;

g) Estabelecer e manter normas e procedimentos para a manutenção das condições adequadas de licenças, prevendo condições para disposição ou transferência de *software* para outros;

h) Utilizar ferramentas de auditoria de utilização de software e alocação de licenças de uso apropriadas;

i) Cumprir termos e condições para *software* e informações obtidas a partir de redes públicas;

j) Não duplicar, converter para outro formato ou extrair de registros comerciais (filme, áudio) outros que não os permitidos pela lei de direito autoral;

k) Não copiar, no todo ou em partes, livros, artigos, relatórios ou outros documentos, além daqueles permitidos pela lei de direito autoral.

Proteção de registros organizacionais

Convém que registros organizacionais importantes sejam protegidos contra perda, destruição e falsificação, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio. Alguns registros podem precisar ser retidos de forma segura para atender a tais requisitos, assim como para apoiar as atividades essenciais do negócio.

Exemplo disso são os registros que podem ser exigidos como evidência de que uma organização opera de acordo com as regras regulamentares, para assegurar a defesa adequada contra potenciais processos civis ou criminais, ou confirmar a situação financeira de uma organização perante os acionistas, partes externas e auditores.

Sendo assim, faz-se necessária a devida categorização em tipos de registros, tais como contábeis, de base de dados, de transações, de auditoria e procedimentos operacionais, que devem ser classificados conforme seusrequisitos de confidencialidade, e definindo os controles de proteção necessários, como por exemplo, o período de retenção, tipo de mídia de armazenamento, controle de acesso e salvaguarda das informações.

Para atender aos objetivos gerais de proteção dos registros organizacionais, os seguintes itens devem ser mantidos:

a) Definir diretrizes gerais para armazenamento, tratamento e disposição de registros e informações, de acordo com seu tipo e classificação de segurança;

b) Elaborar uma programação para retenção, identificando os registros essenciais e o período que cada um deve ser mantido;

c) Manter um inventário das fontes de informações-chave;

d) Implementar controles apropriados para proteger registros e informações contra perda, destruição, falsificação e acesso não autorizado.

Proteção e privacidade de dados e informações pessoais

A privacidade e proteção de dados e informações pessoais devem ser asseguradas conforme exigido nas legislações e regulamentações relevantes, e caso existente, nas cláusulas contratuais.

Devem ser consideradas informações pessoais aquelas que são de propriedade de pessoas, que possam servir para identificá-las, que possuam requerimentos legais no tratamento de sua privacidade, e que foram solicitadas pela organização para a condução de processos internos oficiais, sejam na contratação ou outros procedimentos formais.

Todas as demais informações originadas por usuários, armazenadas ou processadas nos ativos da companhia, não devem ser fruto de expectativa de privacidade, uma vez que o uso de ativos de informação da empresa deve ser restrito às atividades profissionais, podendo tais ativos ser auditados para fins e interesses da própria companhia ou órgãos externos.

Conformidade com as políticas e normas de segurança da informação

É de responsabilidade dos gestores que garantam que todos os procedimentos de segurança da informação dentro da sua área de responsabilidade estão sendo executados corretamente para atender a conformidade com as normas e políticas de segurança da informação.

Para isso, faz-se necessário que os gestores analisem criticamente, a intervalos regulares, a conformidade do processamento da informação dentro da sua área de responsabilidade com as políticas de segurança da informação, normas, procedimentos e quaisquer outros requisitos de segurança.

Se qualquer não-conformidade for encontrada como um resultado da análise crítica, é responsabilidade dos gestores:

a) Determinar as causas da não-conformidade;

b) Avaliar a necessidade de ações para assegurar que a não-conformidade não se repita;

c) Definir e implantar ação corretiva apropriada;

d) Analisar criticamente a efetividade da ação corretiva tomada.

Os resultados das análises críticas e das ações corretivas realizadas pelos gestores necessitam ser registrados e esses registros devem mantidos, de forma a possibilitar que os resultados sejam relatados para os responsáveis por auditorias ou avaliações de segurança da informação, quando que solicitado.

Todos os colaboradores e prestadores de serviços são responsáveis por garantir a ciência e conformidade às regras, políticas, normas e procedimentos existentes, em qualquer atividade que venha a realizar nas dependências internas ou externas da companhia.

Esta política e demais normas e procedimentos que suportam sua implementação estão em conformidade a

Política Internacional de Segurança da Informação e as demais políticas corporativas da Iterative.

3. SANÇÕES

O descumprimento de quaisquer dispositivos estabelecidos na presente política será tratado por sanções administrativas e/ou processos disciplinares internos da Iterative.

Em casos de faltas graves, tais sanções podem incluir a suspensão ou encerramento de contrato com o responsável. Em qualquer caso, quando aplicáveis, serão previstas ainda as penalidades descritas na legislação vigente em território nacional.

4. CICLO DE VIDA DA POLITICA

Versão Atual

Este documento encontra-se na versão 2.0, vigente até que uma nova versão seja aprovada e publicada.

Validação

A validação desta política e subsequentes atualizações são efetuadas a partir da aprovação da mesma perante o Comitê de Direção da Iterative

Distribuição

Esta política é disponibilizada na "Intranet Iterative, sendo este o meio oficial de armazenamento e disposição das políticas da companhia. Este documento também poderá ser distribuído pela Segurança da Informação da Iterative sempre que for necessário.

Atualizações

Esta política será atualizada ao menos a cada 12 meses, pela Segurança da Informação da Iterative.

5. APÊNDICE A- GLOSSÁRIO

Algoritmos: Sequência de instruções bem definidas e não ambíguas, com a finalidade específica de prover os passos necessários para realizar uma tarefa.

Ambiente ou sistema crítico: Ambiente ou sistema que trata informações essenciais para a execução da atividade fim da instituição.

Ameaça: Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

Análise de riscos: Uso sistemático de informações para identificar fontes e estimar o risco.

API (Application Programming Interface): Conjunto de retinas e padrões de programação de software.

Ativo: Qualquer coisa que tenha valor para a organização.

Auditoria: É a avaliação sistemática de uma determinada atividade, com o objetivo de determinar se a mesma está sendo desempenhada de acordo com regras pré-estabelecidas.

Autenticação: É o ato de estabelecer ou confirmar algo (ou alguém) como autêntico.

Autorização: Mecanismo responsável por garantir que apenas usuários autorizados consumam os recursos protegidos de um sistema.

Avaliação de riscos: Processo de comparar o risco estimado com critérios de risco pré-definidos para determinar a importância do risco.

Backup: Cópias de segurança de dados, gravados em dispositivos de armazenamento diferentes do original, que possam ser restaurados em caso de perda ou degradação dos dados originais.

Banco de dados: Conjunto de registros ou dados dispostos de forma regular, que possibilita a reorganização dos mesmos e produção de informação.

Blog: Website que permite a inclusão ou compartilhamento de informações, com atualizações rápidas.

Caracteres especiais: Um caractere que não é letra, número, ou o espaço. Por exemplo: !@#$%^&*_+.

Cavalo de tróia (trojan horse): Programa malicioso de quebra de segurança disfarçado como algo benigno, geralmente em arquivos anexo a e-mails.

Certificado Digital: Componente integrante de uma *PKI*, utilizado para garantir autenticação ou criptografia em sistemas,

Checklists: Listas de checagem que visam facilitar a validação de procedimentos.

Códigos-Fonte: Conjunto de códigos escritos em uma linguagem de programação, de maneira lógica, que podem ser compilados para gerarem softwares.

Colaboradores: São os funcionários efetivos ou temporários, estagiários, trainees e menores aprendizes de uma organização.

Confidencialidade: Propriedade da informação que visa que as informações sejam de conhecimento ou posse somente das pessoas que tenham autorização legítima de acesso.

Controle: Forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.

Cópia de segurança (backup): Uma cópia de um arquivo, diretório, ou volume em um dispositivo de armazenamento separado do original, com a finalidade de recuperação no caso do original ser apagado acidentalmente, estragado, ou destruído.

Criptografia: Arte de escrever em cifra, técnicas que permitem embaralhar informações.

Diretriz: Descrição que orienta o que deve ser feito e como, para se alcançarem os objetivos estabelecidos nas políticas.

Disponibilidade: Propriedade da informação que visa que as informações estejam disponíveis e sejam acessíveis a todos os autorizados legitimamente.

EDI (Eletronic Data Interchange): Troca eletrônica de informações, utilizado comente na transmissão de dados entre empresas.

Endereço IP: Código identificador de um dispositivo conectado à uma rede de dados através do protocolo de comunicação TCP/IP, protocolo utilizado amplamente nas redes corporativas e na Internet.

Estação de Trabalho: Também conhecidos como *desktop*, é um computador pessoal (PC) normalmente disposto de forma fixa a um posto de trabalho, constituído minimamente de mesa e cadeira.

E-Mail: Correio eletrônico, sistema que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação.

Exploits: Códigos de computação que visam a exploração de vulnerabilidades presentes em sistemas.

Hardware: Termo freqüentemente usado para referir às partes mecânicas e elétricas que compõem um sistema de computador. Estes dispositivos incluem o mouse, teclado, monitor, memória, entre outros.

Hashing: Método de geração de códigos, originados por algoritmos de criptografia, que visam identificar um arquivo ou informação unicamente.

Honeypot: Dispositivo computacional com mecanismos aprimorados de registro de acessos, que visa simular um ativo de alto valor para atrair possíveis intrusos de rede de dados.

IDS/IPS: Tecnologia de detecção (IDS) e prevenção (IPS) de intrusão em redes de dados ou computadores.

Instant Messaging: Sistema de troca de mensagens instantâneas em rede privada ou na Internet.

Integridade: Propriedade da informação que visa que as informações sejam mantidas íntegras, sem modificações indevidas, acidentais ou propositais.

Interface: Componentes que visam possibilitar a interconexão entre entidades distintas.

Internet: Também conhecida por *world wide web*, é um conglomerado de rede de computadores em escala mundial.

Log: informação normalmente gravada automaticamente por um sistema, com o intuito de registrar eventos importantes.

Login: Termo utilizado comumente para referir à conta de acesso de um usuário a um sistema.

Logoff: Processo de saída de um usuário de um sistema, encerrando uma sessão.

Logon: Processo de entrada de um usuário a um sistema, iniciando uma sessão.

Middleware: São sistemas que atuam nas camadas intermediárias entre o sistema operacional e as aplicações.

Online: Termo utilizado para sistemas que dispõem de informações em tempo real, pronto para receber e transmitir informações de forma instantânea.

OWASP (Open Web Application Security Project): Organização sem fins comerciais que visa aprimorar métodos de segurança em aplicações.

Patches: Códigos de correção de programas ou sistemas de computador.

PCI (Payment Cards Industry): Órgão formado por processadoras de cartão de crédito.

PCI-DSS (Data Security Standards): Norma desenvolvida pelo PCI para estabelecer requerimentos de segurança para dados do portador de cartões pagamentos eletrônicos;

Pendrive: Também conhecido como flash drive ou memory key, trata-se de um dispositivo eletrônico de pequeno porte e altamente portátil, para armazenar de arquivos de computador em memória tipo flash.

PKI (Public Key Infrastructure): Conjunto de hardware, software e métodos utilizados para viabilizar o uso seguro de certificados digitais, com o objetivo de prover autenticação, integridade ou criptografia.

Política: Intenções e diretrizes globais formalmente expressas pela direção.

Prestadores de serviços: Qualquer terceiro ou fornecedor que atuam sob contrato vigente com a empresa.

QoS (Quality of Service): Mecanismo tecnológico utilizado em redes de dados a fim de classificar e priorizar tráfego de dados por sua importância.

RADIUS (Remote Authentication Dial In User Service): É um protocolo de rede que provê funções de autenticação, autorização e auditoria.

Recursos de informação: São os recursos que processam dados ou informações (servidores, estação de trabalho, aplicativos e outro).

Recursos de processamento da informação: Qualquer sistema de informação, serviço ou infraestrutura, ou as instalações físicas que os abriguem.

Rede de dados: Computadores e periféricos, como servidores, subsistemas de discos e estações de trabalho, conectados entre si, utilizando-se de infraestrutura tecnológica física de telecomunicações.

Restore: Procedimento de recuperação de dados, a partir de cópias de segurança, para tratar uma situação de destruição ou degradação dos dados nas mídias de armazenamento originais.

Sistemas operacionais: Programa ou conjunto de programas que têm como objetivo gerenciar recursos de sistema e serve como principal interface lógica entre o usuário e o computador.

Smart Card: Cartão que possui um circuito integrado, que pode armazenar informações lógicas a serem utilizadas em processos de autenticação.

Software ou programa: Um conjunto de instruções para fazer o hardware executar alguma tarefa. Sistemas operacionais, scripts, aplicações e aplicativos são todas as formas de software.

Spam, Junk mail e Correntes: Mensagens indesejadas ou não solicitadas, geralmente contendo propaganda de cunho comercial, ou assuntos que incentivam sua redistribuição, transmitidas por e-mail ou espalhado pela rede Internet, enviadas simultaneamente para muitos usuários de e-mail.

UPS (Uninterruptible Power System): Equipamentos que armazenam energia elétrica para suportar a falta da mesma pelas provedoras públicas, alimentando os equipamentos a ele ligados.

Usuário: Pessoa que utiliza um ativo, serviço ou informação.

VLAN (Virtual Local Area Network): Tecnologia de virtualização de redes privadas, que permite a separação de uma rede privada em trechos menores, com controles associados;

VPN (Virtual Private Networks): Redes privadas virtuais, que criptografam dados para serem trafegados de forma segura em redes públicas;

Social Network: Rede social, website que permite o relacionamento de uma estrutura social composta por pessoas ou organizações, através de mensagens e outras interações diversas.

Tablets: São dispositivos computacionais portáteis em formato de prancheta, que podem ser utilizados para acessar, transmitir, processar e armazenar dados.

Time Stamp: São códigos de denotam a data e hora de um determinado evento, incluindo informações adicionais como o fuso horário e horário de verão ativado ou não.

Vírus de computador: Um programa ou pedaço de código que é introduzido em um computador, que quando executado, corrompe a operação normal do sistema, afetando os conceitos de confidencialidade, integridade ou disponibilidade das informações.

Vulnerabilidade: Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

Web Security Golden Rules: Política de segurança do Iterative, que determina requerimentos de segurança no desenvolvimento de aplicações web.

Website: Conjunto de páginas,
dispostas na internet.

Wireless: Também conhecido como Wi-Fi, termo utilizado para denominar redes de dados sem fio, que utilizam ondas de rádio para transferir dados.

Worm: Vírus de computador que copia a si mesmo, geralmente através de rede, objetivamente desgastar os recursos ou causar danos.

WPA/WPA2 (Wi-Fi Protected Access): Protocolo de redes wireless que implementa criptografia, visando aprimorar a segurança em redes sem fio.