Sumário:

Politica de Segurança da Informação

1 Objetivo:

Esta **Política de Segurança da Informação** foi estabelecida para fornecer uma política de segurança abrangente e um único conjunto de padrões de segurança aplicável a toda organização Usintek. Seu objetivo é garantir que todos os funcionários reconheçam que as informações são um ativo extremamente valioso e tomem as medidas adequadas para proteger as informações que lhes são confiadas por nossos clientes e parceiros de negócios.

2 Sumário executivo

A informação é um ativo da empresa - acionistas, analistas de mercado, clientes, concorrentes, fornecedores e funcionários estão todos tomando decisões de negócios com base nas informações. O dia a dia de todas as unidades de negócios da Usintek, está se tornando cada vez mais dependente da tecnologia da informação, para dar suporte às nossas necessidades de informação.

A tecnologia não apenas transformou nosso ambiente de negócios, mas também criou novos desafios para o gerenciamento de riscos da informação. Há agora uma aceitação generalizada de que, nesta era da informação, a segurança da informação é imprescindível, vital para o sucesso dos negócios.

A segurança da informação eficaz é essencial para manter a confiança de nossos clientes e parceiros de negócios e para permitir nosso sucesso contínuo em um mundo cada vez mais interconectado e baseado em informações. Também é uma obrigação legal proteger os dados privados de nossos clientes e funcionários e garantir sua integridade e disponibilidade em tempo hábil.

Por outro lado, as informações privadas e corporativas se tornaram um ativo valioso para nossos concorrentes e alvo de roubo por meio de programas sofisticados de inteligência.

Proteger informações é uma tarefa cada vez mais complexa. Como **Diretor**, sou responsável pela proteção de ativos de informações e apoio um programa abrangente de proteção de informações em toda a empresa.

No entanto, todos nós temos a responsabilidade de proteger as informações contra divulgação, alteração ou destruição maliciosa ou acidental.

Todos nós temos um papel a cumprir:

- Seguindo os padrões e procedimentos de segurança da informação aplicáveis a nós;
- Manter as informações que são confiadas a nós em sigilo;
- Protegendo dados privados e materiais protegidos por direitos autorais;
- Evitar ações e comportamentos que possam colocar em risco nossas redes e ativos de informação;

- Relatar qualquer suspeita de abuso ou ameaças potenciais ao nosso pessoal, redes, sistemas ou informações.

Esta Política de Segurança da Informação e seus padrões associados são a base do programa de segurança. Tenho certeza de que, juntos, protegeremos a segurança das informações da Usintek.

3 Escopo

Esta política e suas normas aplicam-se a todo e qualquer indivíduo com acesso às informações da Usintek, independentemente de seu vínculo com a instituição: dirigente, colaborador efetivo, estagiário, temporário, terceiro, parceiro, cliente e fornecedor. Também se destina a todas as informações criadas, armazenadas, processadas, transmitidas e descartadas ou ativos disponibilizados pela empresa.
As informações existem em muitas formas, pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida por correio ou por meios eletrônicos, exibida em filmes ou falada em conversas. A informação é um ativo que, como outros ativos de negócios importantes, é essencial para o negócio de uma empresa e, consequentemente, precisa ser adequadamente protegida.
As informações, os sistemas de informação e as redes que os federam enfrentam ameaças à segurança de diversas fontes, incluindo negligência, fraude assistida por computador, vazamento, espionagem, sabotagem, vandalismo, incêndio, inundação, etc. Qualquer que seja a forma da informação, ou meios pelos quais é compartilhada ou armazenada, deve sempre ser protegida de forma adequada. Essa proteção deve ser sempre proporcional ao risco ao qual as informações estão expostas.
A segurança da informação é a proteção da informação contra uma vasta gama de riscos. Inclui os seguintes serviços:

- **Confidencialidade**: serviços que garantem que a informação é observada ou divulgada apenas a quem tem a “necessidade de saber” para cumprir as suas funções ou para cumprir um pedido legal. A confidencialidade garante que a Usintek proteja as informações pessoais e privadas ao limitar estritamente quem as acessa e em que condições;
- **Integridade**: serviços que garantem que as informações sejam protegidas contra modificações não autorizadas (mantendo seu estado original), que as transações comerciais, bem como as trocas de informações dentro da empresa ou com parceiros de negócios, sejam confiáveis como precisas, completas e irrecusáveis.
- **Disponibilidade**: serviços que garantem que as informações estão disponíveis e utilizáveis quando necessário, e os sistemas que fornecem informações são confiáveis e disponíveis quando são necessários, podem resistir a ataques e se recuperar de falhas de forma adequada.
- **Responsabilidade**: serviços que garantem que as ações para acessar, alterar ou excluir informações, ou facilidades de processamento, que podem levar, ou levaram a uma violação de segurança, sejam rastreáveis a uma pessoa física ou jurídica.

A Usintek tem o compromisso de proteger de forma responsável as informações que lhe são confiadas por seus clientes e parceiros de negócios, equilibrando riscos e custos, com pleno respeito a todas às obrigações legais e à ética empresarial.

A Política de Segurança da Informação cobre todos os ativos de informação da Usintek, sejam em papel ou desmaterializados, onde quer que estejam armazenados ou em trânsito em qualquer tipo de mídia e todos os sistemas de processamento de informações.

4 Termos e Definições

Termos	Definições
Integridade	Refere-se a garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
Confidencialidade	Refere-se a garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
Disponibilidade	Refere-se a garantia de que os colaboradores e usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
Criticidade	Refere-se ao impacto que o ativo possui se não estiver em operação
Ativos de informação	Refere-se a um conjunto de conhecimento organizado e gerenciado como uma entidade única. Como qualquer outro recurso corporativo, eles têm valor financeiro — este aumenta em relação direta com o número de pessoas que são capazes de usar as informações. De forma geral, tudo o que para uma empresa for uma informação que tenha relação com o funcionamento no dia a dia, passa a ser um ativo com importância a ser protegido.

5 Acrônimos

Termos	Definições
ANPD	Autoridade Nacional de Proteção de Dados é o órgão federal responsável por fiscalizar e aplicar a LGPD, a Lei Geral da Proteção de Dados. Criada em 2018 e sancionada em 2019.
LGPD	Lei Geral de Proteção de Dados.
SDLC	Software Development Life Cycle (SDLC) – Ciclo de Vida de Desenvolvimento de Software.

GCN	Gestão de Continuidade de Negócio é um processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem.
DPI	Direito de Propriedade Intelectual é a área do Direito que, por meio de leis, garante a inventores ou responsáveis por qualquer produção do intelecto – seja nos domínios industrial, científico, literário ou artístico.

6 Regras e Responsabilidades

A Administração e Gestão da Usintek é responsável por:

- Patrocinar, Financiar e Garantir a aplicabilidade da "Política de Segurança da Informação" pelos funcionários, em total respeito a todas as leis e obrigações aplicáveis, incluindo a legislação de proteção de dados pessoais, para proteger o negócio, a reputação e interesses legítimos;
- Os gestores deverão manter postura coerente em relação à segurança da informação, servindo como modelo de conduta para os colaboradores, usuários e prestadores de serviços da Usintek.
- Os gestores deverão disseminar a cultura de cumprimento e respeito a segurança da informação, contribuindo para o entendimento desta política como fundamental para os alicerces da Usintek, preservando integridade, confidencialidade e disponibilidade.
- Garantir, com o auxílio da área de Recursos Humanos, que suas equipes estejam cientes e orientadas sobre a Política de Segurança da Informação, apoiando normas, práticas e procedimentos e a sigam no decorrer de seus trabalhos. Devem defender a segurança da informação em seu departamento, monitorar a conformidade com esta política e agir imediatamente após quaisquer relatórios ou notificações de não conformidade.

O departamento de Segurança da Informação e TI (Option Tecnologia) são responsáveis por:

- Definir e comunicar esta política dentro da organização, bem como o monitoramento e comunicação às partes interessadas sobre a conformidade da empresa;
- Implementar esta política e operações associadas;
- Estabelecer uma estrutura de Governança de Segurança da Informação, com base em uma metodologia de gerenciamento de risco, para fornecer garantia de que as estratégias de segurança da informação estão alinhadas com os objetivos de negócios, consistentes com as leis aplicáveis e resistentes a ameaças e vulnerabilidades conhecidas;
- Orçar projetos de aprimoramento de segurança, incluindo ações de preenchimento de lacunas de curto prazo para tratar de questões urgentes de segurança;

- Realizar verificações e testes regulares para obter a garantia de que os direitos de acesso, configurações e parâmetros de segurança de versão estão em conformidade com os requisitos documentados e garantir que a organização tenha a capacidade de responder e se recuperar de eventos de segurança da informação que causem interrupção ou destruição;
- Realizar auditorias regulares com o intuito de avaliar a conformidade com esta política e com os padrões e processos de segurança da informação relacionados;
- Configurar e operar as tecnologias de segurança da informação adequadas;
- Garantir que todos os procedimentos operacionais sejam documentados e executados de acordo com a orientação de implementação do padrão de segurança de informações;
- Garantir que os Planos de Recuperação de Desastres de TI sejam adequados à finalidade na estrutura geral do Gerenciamento de Continuidade de Negócios Corporativos.

O departamento de Recursos Humanos é responsável por:

- Apoiar e incutir a cultura de segurança adequada na organização, conduzindo um programa de treinamento e conscientização da Segurança da Informação;
- Por implementar os controles físicos e os requisitos de segurança para a adequada gestão de acessos predial.

Todos colaboradores, usuários e prestadores de serviços são responsáveis por:

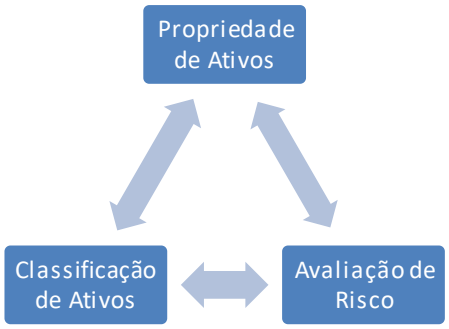
Entende-se por colaboradores, usuários e prestadores de serviços, toda e qualquer pessoa física, que exerça alguma atividade interna ou externa para Usintek.

- Seguir e cumprir esta Política de Segurança da Informação e suas definições;
- Reportar, sem exceção, quaisquer violações ou suspeita de violação e incidentes que possam infringir a Política de Segurança da Informação ou de seus padrões e práticas e procedimentos de apoio ao seu gestor ou ao responsável por segurança da informação da Usintek.
- Pelo uso das informações, redes, aplicativos, sistemas da Usintek, bem como por todas as comunicações que criem ou enviem, seja qual for o seu status de funcionário.
- Acessos indevidos e compartilhamento de informações confidenciais da empresa estão sujeitos às penalidades legais cabíveis, de acordo com o Termo de Responsabilidade assinado no momento da contratação.

7 Estratégia de gestão de riscos de informação

O gerenciamento de riscos deve orientar a estratégia de segurança da informação. Ele deve orientar e determinar as ações e prioridades de gerenciamento apropriadas para proteger contra riscos de segurança da informação identificados.

A metodologia de gestão de risco é baseada em:



7.1 Avaliação dos Riscos

A avaliação de risco é o processo para compreender e quantificar o impacto comercial de uma violação de segurança, criada por uma ameaça que explora vulnerabilidades.

Risco = ameaça x vulnerabilidade x impacto

As ameaças que enfrentamos se enquadram em três grandes categorias:

- **Ameaças acidentais:** erros humanos, negligência, falhas de processo ou sistema, desastre físico (incêndio, inundação ...), etc.;
- **Ameaças malévolas internas:** funcionários descontentes, vingança, suborno, etc.;
- **Ameaças malévolas externas:** vandalismo, desfiguração do site, inteligência do concorrente, hackers, etc.

A análise de ameaças deve levar em conta a motivação, capacidade e acessibilidade das fontes potenciais de ameaça e o catalisador potencial para determinar a probabilidade de uma ameaça específica.
Vulnerabilidades existem onde existem alguns pontos fracos em um ser humano, processo ou sistema que podem ser explorados por uma ameaça.
O impacto comercial resultante é o efeito geral que uma ameaça teria sobre nossos ativos e negócios ao explorar vulnerabilidades. Isso pode resultar em:

- Questões de pessoal;
- Perda financeira;
- Ação legal;
- Continuidade de negócios;
- Redução da confiança do cliente;
- Posição competitiva reduzida;

- Reputação.

O objetivo do gerenciamento de risco é fornecer a garantia de que o risco aos ativos e recursos de informação está sendo gerenciado de forma adequada da maneira mais econômica. As opções possíveis para gerenciamento de risco são:

- Aceitando riscos de forma consciente e objetiva (desde que satisfaçam claramente todas as obrigações legais);
- Evitar riscos, não permitindo ações que fariam com que os riscos ocorressem;
- Transferir os riscos para outras partes, por ex. seguradoras ou fornecedores;
- Implementar controles apropriados para reduzir os riscos a um nível aceitável.

7.2 Propriedades de ativos

Em nossa empresa, a Tecnologia da Informação (TI) evoluiu de uma função crítica de retaguarda para um facilitador de negócios de linha de frente mais visível. Os serviços baseados na Web e a desmaterialização de informações relacionadas nos levarão a confiar cada vez mais nas funções críticas de negócios de TI.
No entanto, as informações permanecem propriedade da empresa. A prestação de contas e a responsabilidade estão ligadas à propriedade, assim como a autoridade. É responsabilidade do proprietário da informação avaliar adequadamente a exposição ao risco de suas informações, decidir e implementar a estratégia de gerenciamento de risco apropriada para lidar com esses riscos.

Consequentemente, todos os ativos e recursos de informação devem ter um proprietário nomeado:

- Responsável pela segurança lógica e física dos ativos / recursos de informação;
- Responsável se a segurança do ativo / recurso de informações for comprometida.

7.3 Classificação de ativo

O proprietário deve garantir que todos os ativos e recursos de informação sejam classificados em termos de confidencialidade, integridade, disponibilidade e responsabilidade.
O esquema de classificação é projetado com base no impacto de uma violação do serviço de segurança relacionado.

Serviço de Segurança	Classe	Serviço de Segurança	Classe
Confidencialidade	Publica	**Disponibilidade**	Normal
	Interna		Espelhada
	Confidencial		Altamente Disponível
	Restrita		Sites Duplos
Integridade	Normal	**Responsabilidade**	Bom Ter
	Importante		Requeridas
	Altamente Importante		
Criticidade	Alta		
	Média		
	Baixa		

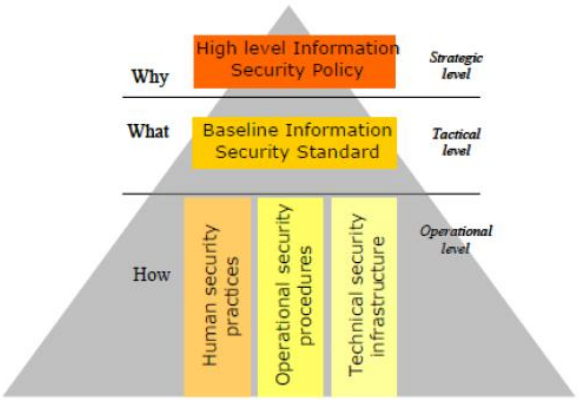
8 Sistemática de documentação de segurança

Esta Política de Segurança da Informação define **PORQUE** a segurança é importante e qual deve ser o nível geral esperado de segurança da informação. Ela especifica o lema da gestão executiva e fornece declarações de política de direção de alto nível do nível executivo. Ela representa a declaração de missão da empresa em relação à segurança da informação.

Os Padrões de Segurança da Informação definem **QUAIS** tipos de controles de segurança da informação devem ser implementados, orientam a implementação dos controles de segurança da informação e fornecem o endosso gerencial da política de segurança da informação de alto nível.

Os documentos de segurança detalhados subsequentes especificam **COMO** os controles de segurança são implementados. Eles são agrupados em três categorias:

- Práticas de segurança humana;
- Procedimentos de segurança operacional;
- Padrões técnicos de segurança.



A Usintek adotou os padrões da norma **ISO/ IEC 27001/27002 - 2013** "Código de prática para gestão de segurança da informação" como principal padrão de referência para desenvolver seu Padrão de Segurança da Informação de Base.

A implantação é acompanhada com o Sistema de Gestão de Segurança da Informação Usintek.

9 Política de segurança da informação

9.1 Organizando a segurança da informação

A prestação de contas e as responsabilidades pela segurança da informação devem ser definidas e comunicadas de forma inequívoca. Um plano estratégico de segurança da informação corporativa deve ser definido, obter suporte executivo e implementado. Recursos e orçamento adequados devem ser alocados. Um fórum de coordenação deve ser estabelecido para facilitar sua implementação, e coordenado sob a responsabilidade dos gerentes departamentais.

9.2 Gestão de ativos

Todos os ativos de informação e tecnologia da informação da Usintek devem ser claramente identificados, inventariados e ter um proprietário identificado que é responsável por sua proteção.

- Embora as responsabilidades do proprietário do ativo possam ser delegadas à pessoa mais adequada na organização, a responsabilidade final pelas ações tomadas, decisões tomadas e conformidade permanece com o proprietário do ativo;
- Um sistema de classificação de segurança deve ser implementado e usado para definir um conjunto apropriado de níveis de proteção de segurança e para comunicar aos usuários a necessidade de medidas especiais de tratamento;
- As informações confidenciais só devem ser divulgadas para funcionários autorizados ou terceiros com base na 'necessidade de saber' e após a assinatura de um **Acordo de Não Divulgação (Confidencialidade)**;
- Os equipamentos disponibilizados aos colaboradores, usuários e prestadores de serviços, são de propriedade da Usintek cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de desenvolvimento de seu trabalho, bem como cumprir as recomendações constantes nos procedimentos operacionais;
- É proibido qualquer procedimento de manutenção física ou lógica, instalação, remoção, configuração ou modificação, sem o conhecimento prévio e o acompanhamento da área de TI, ou de quem este determinar;
- Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser realizadas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor;
- Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar a área de TI;

- Os ativos da Usintek deverão ser inventariados periodicamente;
- O acesso e uso dos ativos (computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física), será através de conta individual de controle da Área de TI, com a observância:
  - Os usuários (logins) individuais de funcionários são de responsabilidade do próprio funcionário;
  - Os usuários (logins) de terceiros são de responsabilidade do gestor da área contratante;
  - O acesso aos ambientes administrativos é bloqueado para qualquer colaborador, usuário e prestador de serviço que não faça parte do grupo de colaboradores com funções administrativas.

Fica a cargo da área de TI:

- Garantir que em caso de ausência de atividade nos computadores da Usintek, a proteção de tela seja ativada;
- Garantir o bloqueio de utilização de adição de componentes do Sistema Operacional (SO), uso ferramentas de edição do Registro, alteração do nome da máquina e compartilhamento de arquivos ou pastas das máquinas para usuários comuns;
- Definir as regras formais para instalação de software e hardware em ambiente de produção;
- Garantir a disponibilização em ambiente seguro do uso, manuseio, guarda de assinatura e certificados digitais;
- Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências;
- Garantir, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa, bem como processo de exclusão de dados ou mídias das máquinas quando de utilização por um novo usuário;
- Bloquear acessos de dispositivos a rede local, tais como celulares, notebooks e instalação de impressoras externas;
- Monitorar o ambiente, gerando históricos de evidências.

9.3 Segurança de recursos humanos

A Usintek colocará em prática controles e medidas adequadas para garantir que apenas contrate e disponha de pessoas cujas atitudes e perfis sejam compatíveis com a importância que atribui à segurança da informação.

- A Usintek conduzirá um programa de conscientização de segurança para garantir que todos os funcionários estejam cientes dos riscos, políticas, práticas e contramedidas de segurança da informação;

- Todos os funcionários devem usar os sistemas de processamento de informações Usintek para fins comerciais de forma consistente com o "POL 02 - Código de Prática para o uso aceitável dos Sistemas de Processamento de Informação";
- A empresa deve finalmente garantir que, ao rescindir o emprego, contrato ou acordo, ou alterar responsabilidades ou funções, funcionários e terceiros usuários, devolvam todos os ativos e equipamentos da Usintek confiados a eles de forma controlada. E tenham todos os direitos de acesso atuais às informações e recursos de processamento de informações removidos.

9.4 Segurança Física

A Usintek irá definir, implementar e gerenciar as medidas de segurança física adequadas para proteger seus funcionários e ativos físicos.

- Edifícios que abrigam sistemas de informação devem ser adequadamente protegidos com perímetros de segurança para prevenir qualquer acesso não autorizado;
- Os controles de entrada devem garantir que apenas pessoas autorizadas tenham acesso permitido;
- Instalações de apoio de áreas seguras e salas de informática, incluindo fornecimento de eletricidade, geradores, nobreaks, aquecimento e ar-condicionado, abastecimento de água e fornecimento de telecomunicações, devem ser controlados e devem ser redundantes para evitar o risco de interrupção e consequências em equipamentos de alta disponibilidade;
- Todos os cabos devem ser colocados em bandejas de cabos e etiquetados. Os cabos de dados devem ser separados dos cabos de alimentação para evitar interferências;
- Todos os equipamentos devem ser mantidos adequadamente com suporte adequado, de acordo com as recomendações do fornecedor;
- A eliminação ou reutilização de sistemas de processamento de informações deve seguir um controle restrito para impedir o acesso de informações confidenciais por uma pessoa não autorizada;
- Uma política de mesa limpa e uma política de tela limpa “POL 02 - Código de Prática para o uso aceitável dos Sistemas de Processamento de Informação” deve ser promovida para evitar roubo oportunista ou divulgação de informações confidenciais;
- O Equipamento não supervisionado deve ser desconectado e o tempo limite da sessão implementado;
- As impressoras e fotocopiadoras usados para informações confidenciais não devem estar localizadas em áreas públicas abertas.
- Garantir o registro de novos colaboradores, usuários e prestadores de serviços junto ao RH;
- Prover acesso deles à empresa através de crachá ou biometria;
- Dar ciência aos colaboradores que todo e qualquer dispositivo de identificação pessoal não poderá ser compartilhado com outras pessoas em hipótese alguma;

- Em caso de rescisão contratual, perda ou roubo do crachá de acesso físico, cancelar o acesso o mais breve possível e formalizar. Para o caso de acesso via digital, bloquear à identificação;
- Terceiros deverão ser cadastrados nas ferramentas de segurança física do mesmo modo que colaboradores, usuários e prestadores de serviços;
- Garantir a gestão do contrato de monitoramento interno através de câmeras de segurança dispostas nas dependências mapeadas e a recuperação de imagens em caso de sinistro ou incidentes, no período disponível;
- Gerir os serviços de manutenção e testes periódicos de Nobreaks. Para o caso de testes documentar devidamente para eventuais auditorias;
- Gerir o contrato de links de comunicações, garantindo redundância entre site e provedores diferentes.

9.5 Gestão, comunicação e Operação

As instalações de comunicações e operações serão gerenciadas de acordo com as melhores práticas de mercado como ITSM (Information Technology Service Management) e da ITIL (www.itil.org).
A documentação formal da infraestrutura de TI e os procedimentos de suporte são componentes cruciais para garantir operações e comunicações perenes e seguras.

- Os procedimentos e responsabilidades operacionais devem ser documentados formalmente. Esses procedimentos devem ser classificados de acordo com o esquema de classificação, gerenciados de acordo e sujeitos ao processo de controle de mudanças;
- Deveres e responsabilidades devem ser segregados para reduzir o risco de uso não autorizado ou inadequado dos ativos da empresa. Monitoramento eficiente do uso de sistemas, usuários e operadores atividades é um controle de compensação crucial para a segregação limitada de funções e deve ser aplicado;
- As instalações de desenvolvimento e teste devem ser separadas dos sistemas de produção, para reduzir o risco de instabilidade operacional ou modificações não autorizadas;
- Os utilitários do sistema devem ser removidos por padrão de todos os sistemas de produção;
- Relacionamentos com fornecedores terceirizados contratados para fornecer serviços de TI devem ser formalmente documentados e gerenciados. Indicadores Chave de Desempenho (KPI) e Acordos de Nível de Serviço (SLA) devem ser definidos e monitorados. Devem ocorrer reuniões regulares de gerenciamento para revisar o desempenho do terceiro em relação aos SLA's e concordar com as ações corretivas/preventivas exigidas;
- A política de segurança da informação ou um resumo principal da mesma deve ser compartilhado com fornecedores e parceiros. O processo de envio da política de segurança da informação para o fornecedor é importante para garantir a segurança adequada das informações compartilhadas com os fornecedores.

- Critérios de aceitação para novos sistemas de informação, atualizações e novas versões devem ser estabelecidos. Testes adequados dos sistemas devem realizados antes da instalação em produção;
- Todos os sistemas, servidores e estações de trabalho devem estar equipados com sistemas antivírus, verificando todos os arquivos inseridos no sistema por qualquer meio (mídia removível, rede, e-mail ...). Deve haver um processo para atualizar automaticamente o arquivo de definição de vírus de acordo com a recomendação do fornecedor. O procedimento deve estar disponível para usuários remotos e em viagem. Todas as mídias removíveis devem ser verificadas em busca de vírus quando reconectadas aos sistemas de informação;
- Deve haver um padrão para definir quais provedores de código móvel, como provedores de mini aplicativos Java e ActiveX, são confiáveis e autorizados. O padrão deve ser tecnicamente aplicado em todas as estações de trabalho com verificação segura da identidade do provedor de mini aplicativos. A lista de fornecedores de mini aplicativos aprovados deve ser mantida formalmente e sujeita ao processo de gerenciamento de mudanças;
- Deve-se fazer backup das informações para garantir a disponibilidade das informações e dos sistemas de suporte. A mídia de backup deve ser protegida de acordo com os padrões de classificação de informações. A mídia de backup deve ser testada regularmente de acordo com as recomendações do fabricante. O procedimento de restauração deve ser formalmente documentado e testado. A mídia de backup deve ser etiquetada e armazenada a vários quilômetros de distância do centro operacional principal;
- Todo o tráfego da Internet deve ser filtrado pelos firewalls Usintek configurados. Modems ou outros meios de acesso à Internet, ou qualquer rede IP externa, são proibidos. Ferramentas de varredura automática devem ser usadas para detectar tais conexões IP. Modems não registrados e não autorizados devem ser removidos imediatamente;
- Todas as informações publicadas nos sites da Usintek estão sujeitas à aprovação formal da área de comunicação empresarial. Os dados do cliente coletados no site, ou por qualquer outro meio, devem estar sujeitos aos controles apropriados, de acordo com a Lei Geral de Proteção de Dados, conforme exigido pelo ANPD.

9.6 Datacenter e Backup

As instalações de comunicações e operações serão gerenciadas de acordo com as melhores práticas É de responsabilidade da Área de TI garantir que as seguintes regras se apliquem, no que diz respeito ao controle do Datacenter, sendo:

- O acesso ao Datacenter fica restrito aos colaboradores, usuários e prestadores de serviços designados e trancado por chave;
- Todo acesso ao Datacenter deverá ser registrado por nome, data e hora;
- Qualquer terceiro e/ou prestador de serviço deverá ser acompanhado por um dos colaboradores designados para administrar os processos de segurança da informação;

- O Datacenter deverá ser mantido limpo e organizado, não sendo permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável;
- A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com o preenchimento da solicitação de liberação pelo colaborador, usuário ou prestador de serviços solicitante e a autorização formal desse instrumento pelo responsável do Datacenter;
- No caso de desligamento de colaboradores, usuários ou prestadores de serviços que possuam acesso ao Datacenter, deverá ser providenciada de imediato a sua exclusão do sistema de autenticação forte e da lista de colaboradores autorizados.

É de responsabilidade da Área de IT garantir que as seguintes regras se apliquem no que diz respeito à geração de Backup dos dados da rede interna, sendo:

- Todos os backups devem ser automáticos e executados fora do horário comercial, nas chamadas "janelas de backup" – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática;
- Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não tiver mais garantia do fabricante), sugestões de melhorias, entre outros;
- Os backups ficam armazenados em nível e garantido por contrato com fornecedor representativo no mercado.

9.7 Controle de acesso

A política de controle de acesso da Usintek, que especifica os procedimentos de identificação, registro, autenticação e autorização do usuário é aplicável a todas as informações, sistemas de processamento de informações, redes e caminhos de conexão.
Todo colaborador, usuário e prestador de serviços terá acesso a login e senha individual, com alteração periódica e monitorado através de processos da área de TI. É de responsabilidade de cada colaborador a proteção e não compartilhamento de sua senha individual, ficando sujeito as penalidades administrativas e legais do seu uso indevido, de acordo com Termo de Responsabilidade assinado.

Para tanto é diretriz da política de segurança da informação os seguintes pontos:

- Uma convenção de nomenclatura de usuário padrão;
- Um procedimento de registro e cancelamento de registro do usuário, incluindo atividades de manutenção para manter os direitos e privilégios de acesso durante o ciclo de vida da conta;
- Um procedimento de autorização formal para aprovar os direitos de acesso do usuário;
- Um procedimento de autenticação;

- Os usuários são responsáveis pelo gerenciamento seguro de suas senhas. A senha é o bem mais valioso de cada usuário de TI da Usintek. Ninguém está autorizado a pedir a alguém que revele sua senha e ninguém precisa solicitá-la. Qualquer tentativa de descobrir uma senha ou qualquer divulgação de uma senha será considerada uma violação de segurança e gerenciada de acordo;
- O acesso de fornecedores e engenheiros de manutenção às portas de diagnóstico e configuração remotas do sistema deve estar sujeito à política de controle de acesso da empresa ou exceções aprovadas pela direção da Usintek. Esses controles devem ser especificados no contrato de manutenção.
- O uso do correio eletrônico é para fins corporativos e relacionados às atividades do colaborador, usuário e prestador de serviços vinculados a Usintek;
- Mensagens enviadas via correio eletrônico são criptografadas;
- Todas as mensagens transmitidas através do e-mail da Usintek possuem backup e podem ser recuperadas, com observância de prazo contratado, possibilitando o resgate do histórico total;
- Qualquer informação acessada, transmitida, recebida ou produzida na internet está sujeita a auditoria e será monitora pela Usintek e podendo ser registrada;
- Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da Usintek, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação;
- Os colaboradores, usuários e prestadores de serviços não estão autorizados a falar em nome da Usintek para qualquer dos meios de comunicação e não poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros;
- Os colaboradores, usuários e prestadores de serviços não estão autorizados a copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais;
- É proibida a divulgação e/ou o compartilhamento de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet;
- Os colaboradores, usuários e prestadores de serviços, com acesso à internet, não estão autorizados a fazer o download (baixa) de qualquer natureza. Eventual necessidade do usuário, para o desenvolvimento de suas atividades, deverá ser submetida a liberação pela Área de TI, que será feita mediante aprovação da Diretoria e instalação de antivírus nos equipamentos.

- O download e a utilização de programas de entretenimento e jogos são terminantemente proibidos;

Como regra geral, é terminantemente proibido e não será tolerado, qualquer armazenamento, distribuição, edição, impressão ou gravação, por qualquer recurso, de materiais de cunho sexual, pedofilia, racismo e/ou homofóbico, perseguição religiosa ou política, bem como degradantes em geral e/ou que de alguma forma firam as normas do Código de Conduta da Usintek.

Maiores informações também consultar “POL 02 - Código de Prática para o uso aceitável dos Sistemas de Processamento de Informação” e “POL 06 - Política de Gerenciamento de Senha”.

9.8 Sistema de informação, aquisição, desenvolvimento e manutenção

Os requisitos de segurança identificados nos estágios anteriores da fase de especificação, e introduzidos durante a fase de design de qualquer sistema de informação, reduzem significativamente o custo, o tempo de comercialização e os esforços de manutenção em comparação com a revisão da segurança durante o ciclo de vida de um sistema.

- A metodologia de aquisição e desenvolvimento de sistemas de informação deve incluir um processo formal para identificar, documentar e implementar os controles de segurança necessários. Esses controles devem ser proporcionais aos riscos identificados resultantes do processo de gestão de riscos e do esquema de classificação de ativos;
- O processamento do aplicativo deve incluir controles para garantir o processamento correto das informações, desde validação de dados de entrada, proteção de integridade de código, integridade de mensagens e verificação de saída. Esses controles devem estar alinhados com a classificação do sistema;
- As alterações no nível do sistema operacional devem ser validadas em relação aos aplicativos para garantir que não haja conflito ou instabilidade induzida;
- O desenvolvimento de software terceirizado deve estar sujeito a um Ciclo de Vida de Desenvolvimento de Software (SDLC) baseado em ITIL. A metodologia de desenvolvimento deve ser supervisionada. Os controles de segurança devem ser especificados na descrição do serviço solicitado e validados como parte do teste de aceitação;
- Um processo formal deve ser definido e responsabilidades atribuídas para monitorar vulnerabilidades, técnicas, ciclo de lançamento do fornecedor e patches / hot fixes de segurança. O processo deve identificar os critérios para instalação de correções e atualizações, levando em consideração o melhor equilíbrio entre a eficiência operacional e a mitigação de riscos de segurança;
- Os sistemas operacionais e pacotes padrão devem ser reforçados e os serviços não utilizados eliminados. O valor padrão de todos os parâmetros de segurança deve ser revisado e especificado de acordo com a classificação do sistema.

9.9 Gestão de incidentes de segurança da informação

Processos e instalações devem ser implementados para detectar desvios, agregar e correlacionar eventos anormais e fornecer relatório gerencial. Todas as falhas, detectadas por um sistema ou relatadas por um usuário, devem ser registradas e investigadas. Os registros de auditoria devem ser protegidos para, eventualmente, serem usados como evidência em caso de investigações forenses.

- Todos os funcionários e usuários terceirizados devem relatar todos os incidentes e fragilidades de segurança da informação detectados ou suspeitos ao seu gestor imediato ou ao responsável de TI;
- Deve haver um procedimento para classificar os incidentes relatados de acordo com seu impacto nos negócios para determinar a urgência de uma ação e atribuir as habilidades certas para conduzir uma investigação. O procedimento deve respeitar a regulamentação aplicável à proteção de dados privados;
- O procedimento de tratamento do incidente deve ser documentado e deve incluir, dependendo da classificação do incidente, etapas para classificação do incidente, contenção do impacto, erradicação da causa raiz, recuperação de informações e análise pós morte;
- Em caso de incidente de segurança, por exemplo, uma penetração malévola na rede, é estritamente proibido tentar “contra-atacar” para não se tornar, por sua vez, um criminoso;
- Se o incidente for suspeito de ser criminoso e exigir ações legais, possivelmente para um tribunal de justiça, as evidências do incidente devem ser protegidas.

9.10 Plano de contingência e continuidade de negócios

A Gestão de Continuidade de Negócio (GCN) permite que a empresa continue os processos de negócios essenciais em um nível aceitável, apesar de uma interrupção da função de negócios. O GCN deve garantir que todos os processos de negócios críticos, incluindo suas infraestruturas e sistemas de TI de suporte, informações, equipe, parceiros, área de trabalho, sejam identificados, inventariados e possam retomar as atividades em caso de desastre, em um tempo pré-definido e acordado por meio de alternativas possíveis em procedimentos de trabalho. O GCN deve garantir que um nível aceitável de qualidade e segurança continue a ser garantido durante a operação em condições de desastre. Deve incluir um cenário de "retorno ao normal" e deve ser validado para fornecer garantia de gerenciamento de sua resiliência.

A Usintek deve manter um Plano de Contingência vigente, documentado, divulgado e revisado anualmente. O Plano de Contingência tem como objetivo garantir a continuidade dos serviços prestados em caso de impossibilidade de acesso dos colaboradores, usuários e prestadores de serviços ao espaço físico de trabalho.

O Plano de contingência e continuidade de negócios deve cobrir os pontos abaixo:

- **Contingências de infraestruturas físicas:** assim compreendidas as situações de catástrofes naturais ou não, tais como inundações, incêndios, desabamentos e etc. que impeçam o acesso e/ou utilização das instalações da Usintek, como também danos físicos relevantes a

instalações e/ou equipamentos, intencionais ou não e ainda falhas no fornecimento de energia elétrica;

- **Contingências de infraestruturas tecnológicas:** compreendidas as situações de inacessibilidade, falha ou perda de quaisquer recursos de TI, tais como hardware, software, telecom, rede e segurança.

O Plano de contingência deve estabelecer os procedimentos a serem adotados pela Usintek e seus colaboradores, usuários e prestadores de serviços em caso de eventos relacionados a impossibilidade de acesso físico ou tecnológico, seja por eventos de greve, bloqueios de acesso ao prédio ou problemas na infraestrutura ou ainda por desastres de força maior.

9.11 Conformidade

É política da Usintek, cumprir todos os requisitos legislativos, estatutários e contratuais pertinentes aos requisitos de informação e sistemas de informação.

- A Usintek implementa a proteção de dados privados e privacidade conforme especificado pela Lei Geral Proteção de Dados (LGPD);
- A Usintek respeita os direitos de propriedade intelectual (DPI) de outras organizações e usa apenas cópias e licenças legais de software;
- Os registros da Usintek devem ser protegidos contra perda, destruição e falsificação. Eles devem ser classificados e identificados por um período de retenção do arquivo por tipo de registro.

10 Referencias de materiais utilizados

- ABNT NBR ISO/IEC 27001/27002:2013
- LGPD Lei nº 13.709, de 14 de agosto de 2018
- POL 02 - Código de Prática para o uso aceitável dos Sistemas de Processamento de Informação

Notas de Revisão

Data	Histórico	Analisado/ Aprovado:
28/03/2022	- Inclusão de documento	Vladimir Rodrigues
08/04/2022	- Revisão do documento	Fernando Deliberalli
01/02/2023	- Revisão do documento v1.2	Fernando Deliberalli
17/02/2023	- Revisão do documento v1.3	Fernando Deliberalli
13/04/2022	- Aprovação do documento	Júnior Bombana
17/01/2023	- Aprovação do documento v1.2	Júnior Bombana
22/02/2023	- Aprovação do documento v1.3	Júnior Bombana