I. OBJETIVO

Estabelecer diretrizes corporativas para a segurança da Informação, as quais servirão de base para a definição de políticas, procedimentos, controles e demais padrões relacionados, a fim de manter e preservar a confidencialidade, integridade e disponibilidade da Informação e a privacidade.
A Valid se compromete a controlar e prevenir violações de segurança, além de garantir a continuidade dos negócios e atender aos requisitos legais e contratuais.

II. CAMPO DE APLICAÇÃO

É aplicável a todos os colaboradores e terceiros, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.

IV. RESPONSABILIDADES E AUTORIDADES

A política de segurança da informação da VALID é uma responsabilidade compartilhada entre todas as partes interessadas, incluindo colaboradores, acionistas, clientes, parceiros de negócios e fornecedores. Cada indivíduo deve compreender e cumprir as políticas, diretrizes e processos de gestão estabelecidos.

- A **alta direção** é responsável por avaliar e aprovar a política de segurança da informação, alocar recursos para sua implementação e manutenção, e promover a cultura de segurança da informação;

- Os **líderes** devem garantir que as políticas de segurança da informação sejam seguidas em seus departamentos, promover a cultura e gerenciar os riscos relacionados aos processos de negócios e ativos sob sua responsabilidade;

- Os **colaboradores** devem conhecer e seguir as políticas de segurança da informação, utilizar os recursos tecnológicos e as informações da VALID de forma responsável e ética, manter o sigilo das informações e proteger as informações às quais têm acesso;

- Os **terceiros** deverão ser orientados (presencial ou virtual) e seguir esta política, garantindo que os dados e/ou informações manipulados ou acessados estejam em acordo com o código de ética e compliance da empresa e tenha sua proteção e sigilo garantido;

- **Cibersegurança** é responsável por definir a política de segurança da informação, monitorar os recursos e ambientes para garantir sua proteção, gerenciar os controles, ferramentas e promover auditorias internas dos controles de segurança da informação;

Em resumo, a política de segurança da informação da VALID é um esforço conjunto de todas as partes interessadas para garantir a segurança, integridade e confidencialidade das informações. Todos têm um papel a desempenhar e são responsáveis por cumprir as políticas e procedimentos estabelecidos.

V. CONSIDERAÇÕES GERAIS/REFERÊNCIAS

REFERÊNCIAS

Os documentos referenciados abaixo complementam as diretrizes desta política.

PL 01.008 – Política de Gestão de Riscos Corporativos

PL 01.017 – Programa de Proteção de Dados

PL 01.158 – Aviso de Privacidade

PL 01.164 – Política de Security by Design

PL 01.166 – Política de Desenvolvimento Seguro – Cibersegurança

P 01.065 – Controle da Legislação Aplicável à Segurança da Informação

P 01.203 – Política de Antivírus/Malware (EDR)

P 01.206 – Política de Controle de Acesso Lógico

P 01.207 – Procedimentos para Utilização dos Recursos Computacionais

P 01.208 – Segregação de Funções

P 01.209 – Administração de VPN

P 01.210 – Manuseio e Descarte de Mídias

P 01.211 – Controle de Acesso à Rede

P 01.212 – Análise de Vulnerabilidades e Ameaças

P 01.214 – Procedimento de Segurança da Informação nos Processos de Admissão, Alteração de Função e Demissão

P 01.219 – Gerenciamento de Incidentes

P 01.234 – Inventário de Ativos de Tecnologia da Informação

P 01.235 – Gerenciamento de Problemas

P 01.324 – Gerenciamento de Backup

P 01.509 – Gerenciamento de Mudanças

P 01.575 – Norma Complementar de Gestão de Incidentes Envolvendo Dados Pessoais

MG 01.005 – Manual de Gestão de Riscos Corporativos

MG 11.004 – Manual da Segurança Patrimonial – Sorocaba

VI. TERMOS E DEFINIÇÕES

- **PSI –** Política de segurança da informação;
- **Integridade:** 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**: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;
- **NIST** – Framework de Cibersegurança: É uma guia de melhores práticas, que ajuda as organizações a fortalecerem sua postura de segurança cibernética, identificar e mitigar riscos, adotar medidas eficazes de proteção de dados e sistemas. É um padrão que deve ser analisado e adaptado de acordo com o negócio de cada empresa;
- **ISO/IEC 27001:** A norma ISO 27001 é o padrão e a referência Internacional para a gestão da Segurança da informação;
- **DPO –** Data Protection Officer ou Encarregado de Dados;
- **Informação:** toda Informação em formato verbal, eletrônico ou físico que seja de propriedade da Valid, de um parceiro comercial da Valid ou de um cliente;
- **Dado Pessoal:** qualquer Informação relativa a uma pessoa física identificada ou razoavelmente identificável e registrada em qualquer formato, como nome, endereço, número da identidade, entre outras;
- **Dado Pessoal Sensível**: qualquer Dado Pessoal que, além de identificar uma pessoa natural, também defina origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
- **Custodiante:** pessoa ou entidade que fará a custódia (proteção, uso ou guarda) do ativo de Informação;
- **Titular de Dados**: pessoa natural a quem se referem os Dados Pessoais.

V. DESCRIÇÃO DO PROCESSO

DIRETRIZES

A Valid segue os principais frameworks de segurança da informação como: ISO 27001 e o NIST de Cyber Security Framework.

1.Informação

A informação, que pode existir em diversas formas, é um ativo essencial para os negócios de uma organização e, portanto, deve ser adequadamente protegida. No ambiente de negócios interconectado, a informação está exposta a um número crescente de ameaças e vulnerabilidades, tornando a segurança da informação fundamental.

A segurança da informação é a proteção da informação contra vários tipos de ameaças para garantir a continuidade dos negócios, minimizar riscos, maximizar o retorno sobre os investimentos e as oportunidades de negócios. Ela é obtida através da adoção de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Esses controles são estabelecidos, implantados, monitorados, analisados criticamente e melhorados conforme necessário para garantir que os objetivos do negócio e da segurança sejam atendidos.

A proteção é realizada preservando a confidencialidade, integridade e disponibilidade das informações. É essencial criar políticas, procedimentos e mecanismos de controle para proteger as informações, prevenindo situações que possam prejudicar os negócios e os envolvidos, sejam colaboradores ou clientes.

Os colaboradores têm um papel fundamental nesse processo, devendo proteger as informações a que têm acesso no dia a dia e garantir a confiança em suas relações internas e externas. A informação é um recurso de valor para a organização e deve ter sua CID: confidencialidade, integridade disponibilidade garantidas. Quando a informação também é um dado pessoal, a privacidade do titular dos dados deve ser assegurada. Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pertence à organização. As exceções devem ser explícitas e formalizadas por meio de contrato entre as partes.

2.Gestor da Informação e Custodiante da Informação

A política de segurança da informação da Valid estabelece que cada informação deve ter um gestor, responsável por autorizar o acesso, definir a proteção, priorizar ações e estabelecer requisitos para os controles de segurança. Além disso, cada informação deve ter um custodiante, encarregado de gerenciar o ambiente que suporta a informação, garantindo a eficácia dos controles de segurança.

A política destaca a importância da privacidade e do sigilo, comparando a falta deles a situações desconfortáveis, como morar em uma casa de vidro ou ter informações pessoais divulgadas. A privacidade e o sigilo são essenciais para a relação de respeito com os clientes internos e externos.

A divulgação de informações confidenciais para pessoas não autorizadas pode prejudicar a empresa e o colaborador, colocando em risco a reputação e a confiança perante o público. Portanto, é crucial conscientizar todos os colaboradores sobre o sigilo e a privacidade das informações, bem como as normas e regulamentos aplicáveis ao negócio.

A política enfatiza que toda organização deve preservar a confidencialidade de suas informações para se manter viva e alcançar seus objetivos. Assim, a informação deve ser acessada e utilizada apenas por quem precisa dela para realizar suas atividades. A política também alerta sobre os riscos de divulgar muitas informações na Internet, pois isso pode expor a privacidade do indivíduo, mesmo contra sua vontade.

3.Gestor do Colaborador

A responsabilidade do gestor do colaborador é dupla:

- Para os colaboradores contratados pelo regime CLT, o gestor é a chefia imediata. Para todos os outros casos, o gestor é o responsável pela área que contratou o colaborador.
- O gestor tem o dever de assegurar que o colaborador tenha acesso ao ambiente de informação durante seu período de trabalho na Valid.

4.Controle de Acesso

O controle de acesso na Valid enfatiza que o acesso e autenticação às informações são individuais e intransferíveis. Cada colaborador tem permissão para acessar apenas as informações necessárias para o desempenho de suas funções. O acesso é rastreável e sujeito a sanções em caso de violação das políticas internas.

As senhas são uma ferramenta crucial de controle e prevenção contra o uso indevido de informações. Cada colaborador é responsável por sua senha e, consequentemente, por qualquer acesso indevido realizado em seu nome. Portanto, é essencial não compartilhar senhas, mesmo com colegas de trabalho.

Não tenha vergonha de dizer "***Não emprestarei a minha senha***!".

Para garantir a segurança, os colaboradores devem seguir várias diretrizes ao criar e gerenciar suas senhas. As senhas devem ser difíceis de decifrar, não devem ser baseadas em informações pessoais e devem ser alteradas regularmente. Além disso, é importante memorizar a senha em vez de anotá-la.

Na Valid, as senhas devem ter no mínimo 12 caracteres, incluir pelo menos uma letra maiúscula, um número e um caractere especial. Qualquer ação realizada com o login de um usuário será de sua exclusiva responsabilidade. Portanto, é crucial proteger a identidade digital e evitar o uso de senhas fracas ou de fácil dedução.

Em resumo, a política de segurança da informação da Valid enfatiza a importância do controle de acesso individualizado, a responsabilidade dos colaboradores em manter a segurança de suas senhas e a necessidade de seguir diretrizes rigorosas para a criação e gerenciamento de senhas. A empresa também fornece um link com boas práticas para a escolha, uso e armazenamento de senhas de forma segura.

O link abaixo possui boas práticas para a escolha, uso e armazenamento de senhas de forma segura.
https://cartilha.cert.br/guardiao/fasciculo-senhas-egc.pdf

5.Tela e Mesa Limpa

A Valid enfatiza a importância de um ambiente de trabalho organizado e seguro. A política de mesa e tela limpa é aplicada a todos os departamentos e colaboradores para evitar o acesso não autorizado a documentos e mídias removíveis. Os colaboradores devem manter a mesa limpa, bloquear ou desligar o computador quando não estiverem em uso, e retirar imediatamente as cópias enviadas para impressão.

Além disso, é dever dos colaboradores garantirem que todas as informações sejam armazenadas em local seguro. Isso inclui não deixar a senha anotada em locais visíveis, guardar todo material digital em local seguro e certificar-se de que o computador corporativo não armazena conteúdos pessoais ou ofensivos.

Após as reuniões, os colaboradores devem garantir que nenhuma informação seja deixada na sala, seja em papéis, quadros, lousas ou computadores compartilhados. A política visa garantir a excelência e qualidade das operações, minimizando o risco de vazamento de informações.

6.Controle de Log e Auditoria de Arquivos

A Valid monitora e grava seus ambientes, sistemas, computadores e redes, conforme as leis brasileiras, garantindo transparência aos colaboradores e terceiros. Trilhas de auditoria são mantidas para rastrear o uso normal e possíveis falhas e fraudes.

O gerenciamento dos diretórios de rede e dos limites de espaço é realizado pelo líder da área com apoio de Cibersegurança que monitora e audita todos os diretórios de rede para evitar problemas de direitos de propriedade intelectual e armazenamento indevido de conteúdos impróprios.

Os colaboradores devem evitar armazenar arquivos redundantes e conteúdo não relacionados às suas funções profissionais nos recursos da Valid.

Não é permitido o armazenamento de músicas e vídeos sem direitos autorais ou licenciamento de uso nos diretórios de rede.

As informações de negócios devem ser armazenadas apenas nos servidores de arquivos na rede da empresa, nunca em CDs, pen drives e outros dispositivos de armazenamento, para garantir a confidencialidade, integridade e disponibilidade da informação. Informações, especialmente arquivos sensíveis aos processos da Valid, não devem ser armazenadas em diretórios locais em estações de trabalho, notebooks e dispositivos móveis, que também não podem ser compartilhados.

7.Uso aceitável dos Ativos de TI

A Valid estabelece que os recursos tecnológicos da empresa devem ser usados exclusivamente para fins profissionais, éticos, seguros e legais. Os colaboradores não estão autorizados a usar esses recursos para atividades pessoais, ilícitas, imorais, antiéticas ou contrárias às políticas da empresa.

A segurança dos ativos, como desktop, notebook e celulares é essencial para proteger os dados e evitar atividades maliciosas, como disseminação de spam e propagação de códigos maliciosos. Portanto, é importante manter os ativos seguros.

Apenas os recursos de TI adquiridos, homologados, licenciados, instalados e gerenciados pelo Service Desk podem ser utilizados. A instalação, controle, movimentação e manutenção de recursos computacionais são responsabilidades da área do Service Desk. Os colaboradores não estão autorizados a realizar aquisições, instalações ou manutenções de hardware.

Todas as demandas devem ser encaminhadas ao Service Desk. Não é permitido o armazenamento de arquivos sensíveis, músicas, programas executáveis não homologados ou jogos nos equipamentos.

8.Planos de Continuidade

É essencial a existência de planos de continuidade para os sistemas e serviços que sustentam o negócio da Valid. O principal objetivo desses planos é atenuar os impactos e garantir a continuidade das operações da organização, mesmo em situações de indisponibilidade de recursos de informação.

A atualização constante desses planos é crucial e eles devem ser submetidos a testes, no mínimo, uma vez a cada 12 meses para garantir sua eficácia.

9.Ambiente de Produção

Os ambientes de produção devem ser segregados e submetidos a um controle rigoroso, assegurando um isolamento absoluto em relação a todos os outros ambientes.

Os ambientes de desenvolvimento e produção devem ser segregados e protegidos de tal maneira que todas as informações que circulam nesses segmentos sejam devidamente controladas.

As informações pessoais e os dados dos clientes que circulam nesses segmentos devem ser protegidos integralmente por meio de processos sistêmicos automatizados. Além disso, devem ser utilizadas aplicações seguras para o armazenamento dessas informações.

Sempre que possível, deve-se evitar o uso de informações de dados pessoais, nos ambientes de desenvolvimento e homologação.

10. Segregação de Função

É imperativo que o acesso à informação esteja em conformidade com as diretrizes de segregação de funções, a fim de limitar e definir claramente as autoridades de cada membro da equipe.

As diretrizes para a segregação de funções devem ser claramente estabelecidas e formalmente documentadas.

11. Gestão de Backup

A segurança da informação é uma prioridade para a Valid. Para garantir o CID = confidencialidade, integridade e disponibilidade das informações, adotamos as seguintes medidas:

• **Cópias de Segurança**: Implementamos um sistema robusto de cópias de segurança para garantir que, em caso de perda de informações, possamos atender às demandas de operação do negócio, legislação, histórico da organização e auditoria.

• **Contingência e Redundância**: Nossos processos sistêmicos e recursos tecnológicos são equipados com métodos de contingência e/ou redundância para garantir a recuperação e a resiliência da infraestrutura.

• **Direitos dos Titulares de Dados**: Estabelecemos processos e configurações que garantem o atendimento aos direitos dos Titulares de Dados previstos na legislação e mencionados no PL 01.143 Política para Atendimento de Solicitações de Titulares de Dados com relação ao backup.

• **Prevenção de Perda de Dados**: Encorajamos todos os colaboradores a adotar uma postura preventiva para evitar a perda de dados. Isso inclui a realização regular de cópias de segurança dos arquivos importantes.

• **Armazenamento de Informações**: É compromisso dos colaboradores armazenar todas as informações que interfiram no desempenho das atividades profissionais nos diretórios de rede. Não é recomendado o armazenamento de arquivos nas estações corporativas, pois podem ser submetidos a procedimentos de backup e acessados indevidamente por outros.

• **Responsabilidade sobre Arquivos Locais**: A segurança da informação não se responsabiliza por arquivos salvos em unidades locais e em dispositivos de armazenamento externo.

Lembramos a todos os colaboradores da importância de manter seus equipamentos seguros e de realizar backups regularmente. A perda de dados pode ter consequências significativas, por isso, é essencial que todos estejam cientes do valor das informações que manuseiam diariamente.

12. Gestão de Incidentes

A segurança da informação é uma prioridade em nossa organização. Para garantir o CID = confidencialidade, integridade e de nossos dados, implementamos uma política rigorosa de gestão de incidentes que é a P 01.219 Gerenciamento de Incidentes, contendo as seguintes diretrizes:

• **Comunicação de Incidentes:** Qualquer incidente que comprometa a segurança da informação deve ser prontamente comunicado aos responsáveis pelo processo de Gestão de Incidentes. Isso permite uma resposta rápida e eficaz para minimizar o impacto e prevenir futuras ocorrências;

• **Incidentes Envolvendo Dados Pessoais:** Caso o incidente envolva Dados Pessoais, é imperativo que o Encarregado de Proteção de Dados (DPO) e o departamento Jurídico sejam imediatamente notificados. Eles avaliarão os riscos associados e determinarão a necessidade de notificar os Titulares de Dados e/ou a Autoridade Nacional de Proteção de Dados Pessoais, conforme exigido pela legislação aplicável e definido na política P 01.575 Norma Complementar de Gestão de Incidentes Envolvendo Dados Pessoais;

• **Procedimento de Tratamento de Incidentes:** Nosso procedimento para o tratamento de incidentes tem como objetivo identificar os eventos ocorridos no ambiente e implementar ações corretivas adequadas. Este processo busca garantir a não recorrência de incidentes, fortalecendo assim a nossa postura de segurança;

• **Restrições ao Usuário:** É expressamente proibido ao usuário que notifica um incidente de Segurança da Informação tentar selecionar o mesmo ou explorar suas vulnerabilidades. Tal ação pode agravar o incidente e aumentar o risco para a organização.

13. Classificação da informação

Toda informação deve ser classificada pelo Gestor da Informação em relação ao seu nível de sigilo. Essa classificação deve ser aplicada em todas as fases do ciclo de vida da informação.

As informações são classificadas em três categorias, conforme documento PL 01.017 Programa de Proteção de Dados:

CLASSIFICAÇÃO	CARACTERÍSTICAS
Pública	Informações que podem ou devem ser divulgadas publicamente sem que causem algum dano à organização, incluindo partes interessadas internos e externas, público em geral e mídias sociais. Normalmente a divulgação deste tipo de informação é de responsabilidade de áreas específicas que fazem a interface com os públicos em geral, como por exemplo, as áreas de comunicação e marketing, entretanto a responsabilidade pela classificação continua sendo do proprietário ou gestor da informação. Devem ser classificadas como públicas as informações que não ferem, dentro do contexto que estão sendo compartilhadas/acessadas/utilizadas, os princípios de confidencialidade e integridade. **Exemplos:** - Comunicados ao mercado, publicidade e propaganda (somente Diretoria; Marketing e Comunicação) - Publicações na imprensa oficial (somente Relação com Investidores) - Documentos que não oferecem riscos à companhia ou não pertencentes à Valid (todos os colaboradores)
Restrita	Informações restritas que, quando divulgadas indevidamente, podem representar um impacto significante nas operações ou nos objetivos da organização. Essas informações podem ser divulgadas somente a determinados grupos, áreas ou cargos. Devem ser classificadas como restritas informações que seu conteúdo é restrito às partes interessadas e previamente autorizadas dentro do contexto e do processo que estão sendo compartilhadas/acessadas. Os princípios de confidencialidade e integridade potencialmente serão afetados em situações de compartilhamento/acesso/uso por pessoas não autorizadas. **Exemplos:** - Comunicados internos em massa; - Manuais de procedimento e políticas internas; - Demais documentos internos ou restritos a um grupo ou área específico.
Confidencial	Informações de alto nível de sensibilidade e criticidade, cuja divulgação indevida representa um sério impacto nas operações, nos objetivos da organização e aos negócios. Estas informações requerem um tratamento especial, e sua divulgação não autorizada ou acesso indevido pode gerar prejuízos financeiros, legais, normativos, contratuais ou na imagem e reputação da organização. Devem ser classificadas como confidenciais informações que seu conteúdo é exclusivo às pessoas autorizadas. Os princípios de confidencialidade e integridade serão afetados em situações de compartilhamento/acesso/uso por pessoas não autorizadas. **Exemplos:** - Informações estratégicas da Valid; - Dados pessoais e dados pessoais sensíveis (informação relacionada a pessoa natural identificada ou identificável), em adequação à Lei Geral de Proteção de Dados Pessoais (LGPD)

Os proprietários ou gestores da informação devem realizar a classificação das informações de acordo com os critérios acima definidos. As informações devem ser classificadas:

- Quando a informação é gerada ou inserida nos processos da organização;
- Quando é identificada uma informação que ainda não foi classificada;
- Quando é identificada uma informação incorretamente classificada;
- Quando ocorrer mudanças no contexto de sensibilidade das informações durante seu ciclo de vida.

Em caso de dúvidas sobre a classificação de determinada informação, deve-se recorrer ao superior imediato, proprietário da informação ou área de Segurança da Informação.

Os colaboradores da Valid têm o dever de:

- Não compartilhar as informações de nossos clientes, assim como informações confidenciais de maneira geral, exceto com os colaboradores autorizados ou que necessitem delas para a realização do seu trabalho;
- Utilizar as informações da Valid de maneira segura, não permitindo sua divulgação ou circulação descontrolada.
- Não levar documentos confidenciais da Valid para fora do ambiente de trabalho;
- Acessar apenas as informações e os recursos que tenham direito de acesso e sejam destinados ao desempenho das atividades;
- Atentar quanto aos documentos que são impressos e copiados por equipamentos de uso coletivo;
- Atuar de acordo com a Política de Segurança da Informação e procedimentos relacionados;
- Confirmar o compromisso com a Segurança da Informação por acordos de sigilo e responsabilidade;
- Além disso, é nosso dever identificar, classificar, rotular e tratar adequadamente as informações, mantendo o sigilo daquelas classificadas como confidenciais e restritas, impedindo quaisquer tipos de acesso, alteração, cópia e destruição não autorizada, assim como qualquer forma de descarte inadequado a sua classificação.

A classificação adequada da informação é essencial para a segurança da informação. É muito importante que cada colaborador tenha conhecimento sobre a classificação das informações e a utilize no dia a dia de seu trabalho. A conscientização e a adesão a essas práticas são fundamentais para garantir a segurança das informações da VALID. Em caso de dúvidas, converse com o respectivo gestor.

14. Gestão de Ativos

Os ativos de TI, tanto nos ambientes fabris quanto corporativos, são fundamentais para as operações diárias e, portanto, devem ser gerenciados com o máximo cuidado.

Os ativos de TI **deverão ser inventariados** de maneira sistemática e regular. Este inventário deve ser abrangente, incluindo todos os equipamentos, sistemas e dados relevantes. O objetivo principal do inventário é permitir a **identificação e rastreabilidade** de cada ativo.

É de suma importância a identificação precisa dos ativos, necessária para que se entenda melhor a estrutura de sua infraestrutura de TI, enquanto a rastreabilidade garante que qualquer alteração ou movimentação de ativos possa ser monitorada e registrada. Isso é essencial para manter a segurança, pois permite a detecção rápida de qualquer atividade suspeita ou não autorizada.

Além disso, o inventário de ativos deve ser mantido atualizado para refletir quaisquer mudanças, como a aquisição de novos ativos ou a desativação de ativos existentes. Isso garantirá que a organização tenha sempre uma visão clara e precisa de seus ativos de TI.

15. Auditorias

A política de segurança da informação deve ser reforçada por auditorias periódicas e sistemáticas. Essas auditorias têm como objetivo verificar se os controles de segurança da informação estão implementados e são cumpridos de maneira adequada.

A análise dos controles, incluindo a política e os procedimentos de segurança da informação, deve ser realizada de forma sistemática e periódica. Isso garante que esses controles permaneçam efetivos, pertinentes e aderentes aos requisitos do negócio. E é essencial promover auditorias internas dos controles de segurança da informação.

16. Gestão de Riscos

A política de riscos cibernéticos da organização deve contemplar um plano de tratamento abrangente para todos os riscos identificados, com classificação conforme estabelecido na PL 01.008 – Política de Gestão de Riscos Corporativos e no MG 01.005 – Manual de Gestão de Riscos Corporativos.

É obrigatório que todos os terceiros que manuseiem Dados Pessoais da Valid sejam submetidos à avaliação de riscos relacionados à segurança da informação e à privacidade. Essa avaliação deve ocorrer por meio de um Processo de Avaliação de Fornecedores rigoroso, que considere aspectos técnicos, administrativos e organizacionais, garantindo a conformidade com os requisitos de segurança e proteção de dados.

17. Conscientização e Disseminação da Segurança da Informação

Todo colaborador da Valid deve ser constantemente conscientizado sobre a importância da segurança da informação desde a sua contratação.

Os treinamentos devem abordar tópicos de Cibersegurança, Privacidade e Proteção de Dados Pessoais. É essencial esclarecer aos colaboradores, desde o início, suas responsabilidades no tratamento dos Dados Pessoais da Valid, direitos enquanto Titulares de Dados, e a necessidade de cuidados específicos ao tratar Dados Pessoais Sensíveis ou de Crianças e Adolescentes (pessoas até 18 anos).

As ações de conscientização são realizadas, no mínimo, anualmente e podem ser apresentadas através de várias formas de comunicação. Isso inclui, mas não se limita a: treinamento presencial, divulgação por e-mail, cartazes em áreas comuns, revistas eletrônicas, revistas físicas, distribuição de folders e orientação dos gestores. O objetivo dessas ações é garantir um alcance contínuo e permanente a todas as partes envolvidas.

Cada colaborador deve se manter atualizado em relação às regras de Cibersegurança e Privacidade. Em caso de dúvidas, devem buscar orientação de seu gestor, do DPO ou consultar as políticas sempre que se sentirem inseguros em situações de uso da Informação.

É fundamental conscientizar, educar e treinar os usuários nas políticas de segurança da informação, bem como no uso adequado de seus ativos.

A disseminação da cultura de Segurança da Informação é um compromisso permanente de todos.

18. Desenvolvimento Seguro

O desenvolvimento de sistemas, aplicações e serviços deve contemplar requisitos de segurança da informação desde a fase de concepção, garantindo que controles de segurança sejam incorporados em todas as etapas do ciclo de vida. A organização adota práticas de desenvolvimento seguro conforme estabelecido nos documentos P 01.068 – Desenvolvimento Seguro de Software e Sistemas e PL 01.166 – Política de Desenvolvimento Seguro - Cibersegurança, que definem critérios técnicos, responsabilidades e controles aplicáveis, incluindo revisões técnicas, testes de vulnerabilidade e segregação entre ambientes.

19. Security by Design

A aquisição, contratação e implementação de sistemas, softwares e serviços devem observar o princípio de Security by Design, assegurando que requisitos de segurança sejam analisados e aplicados desde a fase de concepção ou seleção das soluções. Todos os projetos de tecnologia devem contemplar avaliação de riscos, requisitos de conformidade e controles técnicos necessários para prevenir vulnerabilidades e reduzir riscos à segurança da informação. A organização adota como referência a PL 01.164 – Política de Security by Design, que estabelece critérios para fornecedores, desenvolvedores e áreas responsáveis na adoção de novas soluções.

20. Terceiros que fornecem serviços e/ou produtos para Valid

Parceiros e Fornecedores: Todos os terceiros que prestam serviços e/ou fornecem produtos para a Valid são obrigados a manter um padrão de controles de segurança e privacidade equivalente ao adotado pela Valid. A Valid reconhece que podem ocorrer situações de indisponibilidade com estes fornecedores e, portanto, deve implementar estratégias para minimizar o impacto dessas ocorrências.

Notificação de Incidentes: É mandatório que os fornecedores notifiquem a Valid imediatamente em caso de incidentes de segurança da informação que envolvam Dados Pessoais e/ou sistemas que processam Informações da Valid. Essas notificações devem ser feitas dentro dos prazos estabelecidos contratualmente e/ou conforme estipulado nas políticas internas da Valid.

21. Fornecedores para Informação e Recursos de Informação

Para garantir a uniformidade das informações, é essencial que a PSI seja amplamente divulgada entre todos os fornecedores da Valid. Isso assegura que a política seja rigorosamente seguida, tanto dentro quanto fora do ambiente corporativo.

Como parte fundamental de nossa política de segurança, todos os contratos de trabalho da Valid devem incluir um anexo referente ao Acordo de Confidencialidade ou à Cláusula de Confidencialidade. Essa inclusão é uma condição indispensável para que seja concedido ao fornecedor o acesso aos ativos de informação disponibilizados pela empresa.

É responsabilidade de cada fornecedor respeitar e seguir as disposições e procedimentos estabelecidos na Política de Segurança da Informação. Além disso, é necessário que cada fornecedor assine a Declaração de Conhecimento à PSI, que está contida no Guia de Boas-Vindas à PSI. Importante ressaltar que a obrigação de manter a confidencialidade das informações persiste mesmo após o encerramento do vínculo entre fornecedor e VALID, conforme estipulado em contrato.

22. Acordo de Confidencialidade

A Política de Segurança da Informação (PSI) da Valid é um conjunto de diretrizes e procedimentos destinados a garantir o CID = confidencialidade, integridade e disponibilidade das informações da empresa. A PSI é comunicada a todos os colaboradores da Valid, garantindo a uniformidade da informação e sua aplicação tanto dentro quanto fora da empresa.

Como parte essencial da PSI, todos os contratos de trabalho da Valid incluem um *Acordo de Confidencialidade* ou *Cláusula de Confidencialidade*. Este acordo é uma condição imprescindível para que seja concedido o acesso aos ativos de informação disponibilizados pela instituição.

Os colaboradores têm a responsabilidade de respeitar as disposições e procedimentos estabelecidos na PSI. Eles devem assinar a Declaração de Conhecimento à PSI, que está contida no Guia de Boas-Vindas à PSI. A confidencialidade das informações deve ser mantida pelos colaboradores, mesmo após o seu desligamento da empresa, conforme estabelecido no contrato.

Todos os colaboradores e prestadores de serviço da Valid devem atestar o conhecimento dos controles de Segurança da Informação por meio do Acordo de Sigilo e Responsabilidade. Este acordo está alinhado com as diretrizes gerais da PSI e descreve de forma sucinta as condições de utilização dos recursos de TI e das informações da Valid.

Para os colaboradores, o acordo é integrado ao contrato de trabalho. Para os prestadores de serviço, ele é integrado ao contrato de prestação de serviço. A formalização do acordo ocorre no momento da assinatura do instrumento contratual, ou posteriormente, quando novos prestadores de serviço são contratados. Todos devem assinar o acordo.

Portanto, ao receber um novo colaborador ou prestador de serviço, é necessário solicitar a assinatura do Acordo de Sigilo e Responsabilidade. Esta é uma prática fundamental para garantir a segurança das informações da Valid.

23. Pedidos de Exceção à PSI

Situações excepcionais ou impossibilidades temporárias de aderir às diretrizes estabelecidas neste documento, é necessário registrar tais ocorrências no formulário R 01.231, intitulado "*Pedido de Exceção à Política de Segurança da Informação (PSI)".* Este formulário deve ser encaminhado ao departamento de cibersegurança e passará por uma revisão anual.

O solicitante da exceção tem a responsabilidade de apresentar, com antecedência mínima de um mês ao período de revisão, provas de que a exceção ainda se mantém ativa nos ambientes designados. Caso não haja resposta do solicitante, a solicitação será encaminhada ao gestor imediato ou ao próximo nível hierárquico.

A ausência de envio das evidências necessárias dentro do prazo estipulado para a revisão resultará na suspensão do Pedido de Exceção. Neste caso, tanto o solicitante quanto o seu gestor serão devidamente informados.

24. Sanções

A Valid valoriza a segurança da informação e espera que todos os colaboradores e não colaboradores respeitem e protejam todas as informações, sejam elas físicas ou eletrônicas. A preservação da integridade, confidencialidade e proteção dos recursos e ativos de informação são de suma importância.

O não cumprimento das diretrizes estabelecidas nesta política pode resultar em sanções administrativas e/ou processos disciplinares internos. Em casos de infrações graves, as sanções podem variar desde advertências verbais ou escritas, suspensões, até demissões ou rescisões de contratos de estágio ou consultoria, dependendo da gravidade do dano. Além disso, serão aplicadas as penalidades previstas na legislação vigente em território nacional, quando aplicável.

É estritamente proibido o uso, manipulação, armazenamento, transmissão e disseminação de materiais através dos serviços disponibilizados pela Valid:

a) Conteúdo ofensivo, obsceno, pornográfico, pedófilo, abusivo, antiético, preconceituoso, discriminatório, mensagens de assédio, difamação e usurpação de identidade;

b) Propaganda com fins comerciais;
c) Vírus, correntes, spam ou qualquer programa prejudicial;
d) Material de natureza político-partidária ou sindical que promova candidatos a cargos públicos efetivos, de clubes, associações e sindicatos;
e) Material protegido por leis de propriedade intelectual, como músicas, filmes, animações e jogos.
f) Pedimos que todos ajam de maneira diligente e zelosa. O uso de informações e do patrimônio da empresa para fins particulares é proibido. Oriente seus colegas sobre os limites de uso aceitável. O desrespeito a essas regras pode levar à suspensão temporária ou definitiva do acesso à Internet e do uso do correio eletrônico, além da aplicação de penalidades conforme a gravidade da infração.

25. PRIVACIDADE

A Valid mantém firme compromisso com a conformidade às disposições da Lei Geral de Proteção de Dados Pessoais (Lei n° 13.709/18 ou "LGPD") e demais legislações aplicáveis.

Com o propósito específico de cumprir as disposições da LGPD, que estabelecem a necessidade de formalizar regras de boas práticas de governança e transparência no tratamento de Dados Pessoais e promover uma cultura organizacional, a Valid implementa a PL.01.154 Política Corporativa de Privacidade, que estabelece diretrizes claras sobre o uso adequado de dados pessoais no ambiente corporativo.

Portanto, todos os colaboradores, prestadores de serviço ou terceiros que utilizem os ativos tecnológicos fornecidos pela Valid devem observar as diretrizes de segurança da informação e privacidade presentes na referida Política ao tratar dados pessoais. Além disso, devem cumprir integralmente as disposições da LGPD, das políticas internas e demais legislações aplicáveis, garantindo a adoção de todas as medidas técnicas e administrativas eficazes e adequadas para proteger os dados pessoais contra acessos não autorizados, destruição, perda, alteração ou qualquer outra forma de tratamento inadequado ou ilícito.

A divulgação de informações confidenciais para pessoas não autorizadas prejudica a empresa e o colaborador, colocando em risco a reputação e a confiança que temos perante nossos diferentes públicos, sejam eles colaboradores, clientes, acionistas, entre outros.

É essencial a conscientização contínua de todos os colaboradores sobre o sigilo e a privacidade das informações com as quais lidamos no dia a dia. O acesso e uso de dados devem ser restritos às pessoas que efetivamente precisam dessas informações para o desempenho de suas funções, respeitando os princípios da LGPD, especialmente os da necessidade, finalidade e minimização.

Qualquer dúvida, entre em contato com a equipe de Privacidade através do e-mail: privacidade@valid.com.br.

26. DISPOSIÇÕES FINAIS

A Valid está firmemente comprometida em implementar e cumprir todos os requisitos legais e regulamentares aplicáveis ao nosso negócio.
Os controles de segurança da informação que implementamos na Valid estão alinhados com os padrões internacionais de melhores práticas de segurança da informação e estão em total conformidade com a legislação atual.
As diretrizes estabelecidas neste documento são postas em prática na Valid através de políticas e procedimentos específicos, que são obrigatórios para todos os colaboradores, independentemente de sua posição hierárquica, função na empresa ou tipo de contrato de trabalho.
A introdução de cada novo regulamento deve ser acompanhada por um procedimento de conscientização para todos os colaboradores, assim como os regulamentos que compõem a Política de Segurança da Informação.
A Valid se isenta de qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços tecnológicos concedidos aos seus colaboradores. Reservamo-nos o direito de analisar dados e evidências para obtenção de provas em processos investigatórios e adotar as medidas legais apropriadas.
É responsabilidade do usuário respeitar as disposições e procedimentos estabelecidos na Política de Segurança da Informação e assinar o *Termo de Adesão*.
O descumprimento dos requisitos estabelecidos neste regulamento resultará em violação das regras internas da empresa e sujeitará o usuário às medidas administrativas, contratuais e legais pertinentes.
Todos os regulamentos da cibersegurança devem ser revistos e atualizados pelo menos a cada 12 meses, ou sempre que um evento relevante justifique uma revisão e/ou atualização antecipada.
A equipe de cibersegurança é encarregada de manter esta política atualizada e acessível.
Se algum regulamento exigir um período de revisão menor que 12 meses, este fato deve ser explicitamente declarado no documento em questão.