A. OBJETIVO

A Política Corporativa de Segurança da Informação (PSI) manifesta os requisitos e diretrizes das Empresas para segurança e controle de seu negócio, ativos e informações em meio físico ou digital. Objetiva proteger e assegurar a integridade, confidencialidade e disponibilidade das informações conforme riscos identificados e analisados, requisitos legais ou regulatórios, normas e melhores práticas de mercado disponíveis para este fim. Estabelece controles mínimos e necessários ao bom desempenho do Sistema de Gestão de Segurança da Informação (SGSI), conforme diretrizes da norma ISO/IEC 27001:2022. Também esclarece as responsabilidades das audiências para adesão desta Política, bem como as diretrizes a serem consideradas por estas para preservar e proteger as informações e respectivos ativos que as tratam.

B. ABRANGÊNCIA

Esta política aplica-se a VALEINVEST Participações e Investimentos LTDA e suas controladas, incluindo a empresa AGL Adquirência Ltda. As empresas controladas pela VALEINVEST são; (i) SERVNET Instituição de Pagamento Ltda, (ii) FINFLEX Instituição de Pagamento Ltda; (iii) TRIVALE Instituição de Pagamento Ltda e (iv) VLB Meios de Pagamento Ltda.

C. VIGÊNCIA

Esta política entra em vigor na data de sua publicação, sendo revisada anualmente, ou sempre que se fizer necessário.

D. DEFINIÇÕES

a) **Acesso Remoto** – Acesso no qual o usuário utiliza-se de algum mecanismo, rede ou ligação telefônica para obter acesso a um sistema fisicamente localizado em outro local.
b) **Antivírus –** Programa ou Software utilizado para detectar, anular e eliminar vírus e outros tipos de códigos maliciosos de um dispositivo.
c) **Ataque** - Tentativa, bem ou malsucedida, de acesso ou uso não autorizado a um programa ou computador. Também são considerados ataques, tentativas de negação de serviço.
d) **Backup** - Processo que objetiva manter as informações a salvo de problemas nos meios de armazenamento através de uma cópia de segurança que pode ser restaurada caso haja necessidade.
e) **Código malicioso** - Termo genérico que se refere a todos os tipos de programa que executam ações maliciosas em um computador. Exemplos de códigos maliciosos são os vírus, worms, bots, cavalos de Tróia, rootkits e etc.
f) **Criptografia** - Ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas. É usada, dentre outras finalidades para autenticar a identidade de usuários; autenticar transações bancárias; proteger a integridade de transferências eletrônicas de fundos, e proteger o sigilo de comunicações pessoais e comerciais.
g) **Dados do titular do cartão:** dados que compõem as informações de um cartão de pagamento, tais como: Número do cartão ou PAN, nome do titular do cartão, data de

vencimento, código de serviço, dados em tarja magnética ou equivalente em chip, código de verificação, PINS.

h) **DPO** – Data Protection Officer ou Encarregado de Dados
i) **E-mail ou Endereço Eletrônico** - É um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação.
j) **Estação de trabalho** - Nome genérico dado a computadores, no meio corporativo também conhecido como Desktop
k) **Firewall** - Dispositivo constituído pela combinação de software e hardware, utilizado para dividir e controlar o acesso entre redes de computadores.
l) **Freeware** - Software de livre distribuição, não é necessário que sejam adquiridas para habilitar sua utilização.
m) **FTP - File Transfer Protocol** é um protocolo de transferência de arquivos muito utilizado na Internet.
n) **Hardware** - Parte física do computador, equipamento de rede e outros.
o) **IA Generativa** - As inteligências artificiais generativas têm a capacidade de criar novas informações a partir de conjuntos de dados pré-existentes. Essas IAs são "ensinadas" a partir de grandes bases de dados com a intenção de que sejam capazes de adquirir o padrão de construção desses dados. Com essa compreensão adquirida, se tornam capazes de gerar novos dados, semelhantes aos dados utilizados para ensinar a IA, mas que podem ser únicos e originais.
p) **Invasão -** Ataque bem-sucedido que resulte no acesso, manipulação ou destruição de informações em um computador.
q) **Log -** Registro de atividades gerado por programas de computador. No caso de logs relativos a incidentes de segurança, eles normalmente são gerados por firewall ou por IDS.
r) **Logon/Login –** Processo no qual o usuário valida suas credenciais para um sistema através da informação de sua identificação e senha.
s) **Malware -** Do Inglês Malicious software (software malicioso).
t) **Mídia Removível** - É qualquer meio de armazenamento móvel, exemplos: CD's, DVD`s, ZipDrives, PenDrives, fitas magnéticas e outros.
u) **PAN (Personal Account Number):** número do cartão de pagamento.
v) **PIN (Personal Identification Number):** senha do cartão de pagamento.
w) **PSI** – Política de Segurança da Informação.
x) **Ransomware** – Software nocivo que restringe o acesso ao sistema infectado por meio de codificação das informações (criptografia) onde poderá ser exigido pagamento de resgate para recuperação das informações originais ou evitar vazamento das informações.
y) **Senha** - Conjunto de caracteres, de conhecimento único do usuário, utilizado no processo de verificação de sua identidade, assegurando que ele é realmente quem diz ser.
z) **Servidor** - Sistema de computação que fornece serviços a uma rede de computadores.
aa) **Software** - Um programa de computador é composto por uma sequência de instruções, que é interpretada e executada por um processador ou por uma máquina virtual.
bb) **Spam** - Termo usado para se referir aos e-mails não solicitados.
cc) **Syslog** - é um padrão criado pela IETF para a transmissão de mensagens de log em redes IP. O termo é geralmente usado para identificar tanto o protocolo de rede quanto para a aplicação ou biblioteca de envio de mensagens no protocolo syslog.

dd) **Vírus** - Programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando.
ee) **VPN** - Virtual Private Network é uma rede que provê uma conexão remota de forma segura.
ff) **Vulnerabilidade** - Falha no projeto, implementação ou configuração de um software ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador.
gg) **Worms** (Vermes) - Programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador.

E. REGULAÇÕES, LEIS E NORMAS APLICÁVEIS

a) ISO/IEC 27001:2022 - *Information security, cybersecurity, and privacy protection — Information security management systems — Requirements*
b) ABNT NBR ISO/IEC 27002:2022 – *Segurança da informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação*.
c) Lei Geral de Proteção de Dados Pessoais (LGPD) 13.709/2018.
d) Resolução BCB n° 85 de 8/4/2021.
e) Resolução CMN nº 4.893 de 26/02/2021.

F. REFERÊNCIAS

a) Código de Conduta e Ética.
b) Política de Privacidade e Proteção de Dados Pessoais.
c) Política para Classificação da Informação.
d) Programa de Conscientização de Segurança da Informação.
e) Procedimento de Controle de Acesso Lógico.
f) Procedimento de Controle de Acesso Remoto.
g) Política de Armazenamento, Transmissão e Descarte de Dados.
h) Procedimento de Malware e AntiSpam.
i) Procedimento de Gerenciamento de Chaves Criptográficas.
j) Procedimento de Backup e Restore.
k) Procedimento de Desenvolvimento Seguro.
l) Procedimento de Gerenciamento de Mudança.

1. INSTRUÇÕES GERAIS

A Tecnologia da Informação (TI), seus recursos e informações são imprescindíveis para o negócio das Empresas. Portanto, é premente assegurar a proteção destes ativos através da gestão contínua de Segurança da Informação (SI).

2. AUDITORIA, SANÇÕES E PUNIÇÕES

As Empresas reservam para si o direito de monitorar e manter registros de todos os tipos de acesso aos seus sistemas, redes e informações. Incluindo-se o uso particular (pessoal) através destes recursos, quando da existência de informações e/ou evidências de atos ilícitos ou conduta inadequada. Estes registros também podem ser utilizados para análises estatísticas visando a boa prestação de serviços e para verificação em casos relacionados a incidentes de segurança.

Auditorias internas podem ser executadas sem aviso prévio pela área de TI ou empresa especializada para a verificação do atendimento das considerações que compõem e suportam esta Política.

As infrações a esta política são elegíveis aplicação de medidas disciplinares, tais como, advertência verbal, advertência escrita, suspensão, e, quando for o caso, o término do contrato por justa causa, quando incorrer em qualquer das hipóteses contidas no Art. 482 da Consolidação da Leis do Trabalho (CLT).

3. DÚVIDAS, SUGESTÕES E EXCEÇÕES

A área de TI é responsável pelo esclarecimento de dúvidas, recepção e tratativa de sugestões relativas a esta política. Dúvidas, sugestões e relatos de incidentes devem ser enviados para o endereço security@valecard.com.br.

Exceções a esta política devem ser apresentadas a gerência imediata do colaborador, a qual deverá submetê-las a Diretoria de Cibersegurança, onde serão discutidas e avaliadas. Caso necessário, a exceção será submetida para apreciação da alta direção das *Empresas*.

Todas as exceções devem ser devidamente registradas e documentadas de forma a propiciar a evolução futura desta Política.

4. GERENCIAMENTO DE RISCO DE SEGURANÇA

O Gerenciamento de Riscos de Segurança da Informação é de responsabilidade da Diretoria de Cibersegurança. Essa diretriz visa gerenciar riscos de segurança relacionados a mudanças de sistemas de informações internos ou terceirizados bem como à continuidade dos serviços prestados, e deve estar na matriz de riscos com suas respectivas classificações, tratamentos e acompanhamentos, conforme Política de Riscos Operacionais.

É responsabilidade da Diretoria de Cibersegurança manter e gerenciar um programa de gestão de vulnerabilidades de acordo com as melhores práticas de mercado e alinhado a gestão de risco de SI das *Empresas*.

É responsabilidade da Diretoria TI avaliar, manter e disponibilizar contingência de recursos críticos para a continuidade do negócio bem como aqueles necessários a continuidade da gestão de SI na ocorrência de eventos adversos.

Servidores, equipamentos de rede e segurança críticos ao negócio devem ser adquiridos e implementados com capacidade própria de contingência tais como fonte redundante, placas de rede alternativas, memória com correção de erros, processadores duplos, placas controladoras e sistemas em alta disponibilidade. No caso da contratação de serviços de infraestrutura de TI em nuvem, os mesmos requisitos são aplicáveis. A arquitetura de processamento para serviços críticos deve ser analisada e validada quanto aos requisitos de contingência e continuidade.

5. SEGURANÇA RELACIONADA A RECURSOS HUMANOS

Conforme especifica o Programa de Conscientização de Segurança da Informação, a área de Recursos Humanos deve:

a) Analisar adequadamente os candidatos a emprego, especialmente em cargos ou serviços com acesso a informações confidenciais.
b) Divulgar esta política a todos os colaboradores, terceiros, prestadores de serviços, parceiros, fornecedores.
c) Garantir que todos os colaboradores entrantes recebam a PSI e o Código de Conduta e Ética e deem ciência ao termo de conduta ética.
d) Estabelecer planos de treinamento e conscientização periódicos e garantir a ciência e aderência dos funcionários e terceiros.
e) Verificar as regras do Procedimento de Controle de Acesso Lógico quanto à bloqueios de acesso por demissão, afastamento e outros, bem como a revisão das permissões após mudança de função e outras diretrizes;
f) Assegurar que os Funcionários, Terceiros, Parceiros e Fornecedores entendam seus papéis e responsabilidades, antes, durante e no encerramento ou mudança de contrato visando reduzir riscos de roubo, fraude e mal-uso dos recursos das empresas.
g) Garantir a devolução dos ativos das empresas no encerramento do contrato.
h) Aplicar as medidas disciplinares formais vigentes quando necessário, garantindo inclusive, dissuasão para que novas violações não ocorram.

6. GOVERNANÇA E TECNOLOGIA

Todos os departamentos das *Empresas* devem inteirar-se sobre melhores práticas de gestão de TI (ITIL, COBIT, SGSI, entre outras) e suportar a área de Tecnologia da Informação (TI) com informações necessárias ao bom desempenho dos processos de gestão.

É responsabilidade da Diretoria de TI estruturar, manter, executar e divulgar processos e procedimentos de gestão de desempenho, capacidade, monitoramento, operação da segurança da informação, requisição de serviços, operação de TI, gestão de mudanças, incidentes e problemas. Devendo apresentar indicadores de acompanhamento mensalmente e planos de correção de rumo no caso de desvios. Os processos e procedimentos devem ser revisados anualmente.

É responsabilidade da Diretoria de TI realizar a gestão de riscos de ambiente e de processos relacionados à Segurança da Informação, visando mitigar a ocorrência de incidentes de disponibilidade e capacidade dos serviços de TI para serviços internos ou terceirizados.

A área de TI deve garantir que recursos de hardware e software, para suportar serviços críticos, em especial aqueles direcionados aos clientes das *Empresas*, tenham características básicas de contingência e redundância tais como:

- Fontes redundantes de energia, interfaces de rede múltiplas e conectadas em portas de rede alternativas;
- Processo de cópia de segurança (backup) estruturado, implantado e monitorado;
- Processo de gestão de falhas e desempenho estruturado, implantado e monitorado.

Bem como garantir a existência de documentação da topologia e inventário de serviços críticos estruturada, implantada, monitorada, atualizada e divulgada para áreas das Empresas que requisitem e tenham estas informações como parte integrantes e necessárias para sua operação.

Equipamentos, que armazenam e processam informações das *Empresas*, devem estar acondicionados em ambiente com controle de acesso físico, energia estabilizada e condições de climatização adequadas aos requisitos técnicos de cada equipamento. Estes ambientes devem ser devidamente gerenciados, monitorados e eventos que extrapolem condições mínimas ou requisitos críticos de operação devem ser tratados como incidentes de disponibilidade, registrados e acompanhados pela área de TI. É responsabilidade da área de TI garantir as condições ambientais e físicas para o acondicionamento dos equipamentos e informações.

Todas as alterações de configuração na infraestrutura de TI, segurança da informação e sistemas críticos das *Empresas* devem ser registradas e aprovadas através de processo específico para Gestão de Mudanças. Gestão de Mudanças que envolva o tratamento de dados pessoais deve ter os riscos e impactos para a governança de dados avaliados e comunicados ao Encarregado de Dados para as possíveis providências. A gestão de mudanças na infraestrutura de TI e sistemas críticos devem ter os riscos e impactos para o Plano de Continuidade de Negócio (PCN) das Empresas avaliados e comunicados ao Gestor do PCN para as devidas providências. É responsabilidade da Diretoria de TI garantir o processo de gestão de mudanças conforme requisitos desta Política e melhores práticas.

O processo de gestão de mudanças deve assegurar no mínimo que os riscos operacionais foram identificados, que o processo de retomada/recuperação em caso de problemas existe e está validado pelos responsáveis pela gestão de mudança.

Todas as alterações de configuração na rede e sistemas críticos das *Empresas* requerem obrigatoriamente a realização de cópia de segurança das configurações antes e após a realização das mudanças. A equipe responsável pelas alterações também é responsável pela realização, classificação e armazenamento das cópias de segurança.

Mudanças emergenciais devem ser registradas, aprovadas e validadas após a sua execução em prazo mínimo possível.

Mudanças envolvendo infraestrutura e serviços críticos de terceiros (fornecedores) devem ser registradas conforme processo específico para Gestão de Mudanças.

7. GESTÃO DE ATIVOS

Assegurar que os ativos da informação sob a responsabilidade das empresas, de seus clientes, não clientes, fornecedores e parceiros, sejam utilizados de forma ética e legal, garantindo também o cumprimento das normas internas das empresas.

- Devem ser protegidos de acessos indevidos e ter documentação atualizada com seus referidos planos de manutenção.
- Os ativos de Hardware e Software devem estar devidamente legalizados dentro da empresa e devem possuir versões com suporte ativo, mesmo os recursos freeware utilizados.
- Ao usuário não deve ser liberado a permissão de alteração na configuração de sua estação de trabalho, bem como instalação de softwares e aplicativos.

7.1 Gestão de Ativos e Proprietários

Um inventário de ativos associados com informações deve ser criado e (pelo menos) um proprietário será atribuído a cada ativo.

a) O inventário deve estar sempre atualizado com informações concisas e fidedignas.
b) Os casos de depreciação ou inutilização deverão ser registrados e informados para a contabilidade para baixa deles no patrimônio e para ativos com informações, deve ser feito um backup e garantido a exclusão dos dados.

7.2 Uso e Manuseio

Regras de boas práticas e respeito do uso e manuseio de ativos deverão ser formalizadas e implementadas de forma a orientar o usuário e dar ciência de sua responsabilidade quanto ao uso bem como para neutralizar qualquer divulgação não autorizada, modificação, remoção ou destruição de todo ou parte das informações.

a) O Proprietário do ativo é o responsável pela salvaguarda e zelo deste.
b) O usuário é responsável pela segurança da informação e zelo do ativo, bem como o uso de boa-fé.

7.3 Mídias Removíveis

Produtos de gravação digital devem ter seu uso estritamente profissional e no final do seu ciclo de vida ou quando da sua inutilização, devem ter um procedimento específico e seguro de destruição.

a) As entradas USB e todos os recursos de gravação das estações de trabalho devem ser desativados.
b) Exceções para utilização desses recursos deverão ser previamente solicitadas para a Área de Segurança da Informação que irá analisar a viabilidade da liberação.

8. CLASSIFICAÇÃO DA INFORMAÇÃO

A classificação da informação consiste na definição de níveis de proteção que os dados devem receber considerando requisitos legais, regulatórios, do negócio e possíveis ameaças a sua segurança. A classificação é determinante para orientar como cada informação será tratada e protegida seguindo critérios de confidencialidade, disponibilidade e integridade.

As entidades jurídicas (empresas) são proprietárias legais das informações contidas nos sistemas de informação, sob seus controles e/ou administração e se reservam o direito de acesso, uso, monitoramento, compartilhamento e poder de decisão sobre estas informações observando os preceitos legais e, em especial, a LGPD 13.709/2018.

Todos os documentos normativos do legado intelectual da empresa assim como todo o escopo do Sistema de Gestão de Segurança da Informação, ou seja, todos os tipos de informações, independente do formato (documentos em papel ou eletrônico, aplicativos e banco de dados, e-mails e outros formatos), devem ser identificados e classificados adequadamente.

A Classificação da Informação é orientada e descrita pela Política Corporativa para Classificação da Informação.

É responsabilidade da Diretoria de Tecnologia da Informação garantir que a especificação funcional de novos sistemas contratados internamente ou externamente contenha requisitos e diretrizes para a pseudoanonimização de dados pessoais na sua exibição e armazenamento de acordo com a classificação da informação.

É responsabilidade da Diretoria de Cibersegurança definir, implementar e manter controles preventivos para evitar ou coibir o vazamento de dados tratados pelas *Empresas* em especial os dados pessoais definidos pela LGPD 13.709/2018. Os controles, independentemente de onde sejam tratadas as informações, se localmente *(on premises*) ou nuvem; devem considerar a classificação da informação e sensibilidade desta para geração de alarmes, bloqueios automáticos do vazamento e detecção de possíveis incidentes.

É responsabilidade da Gerência de Segurança da Informação manter processo e procedimento revisado anualmente para exercício do controle de prevenção a vazamento de dados.

9. RECURSOS DA TECNOLOGIA DA INFORMAÇÃO

O recurso computacional, seja de mesa, portátil ou fixo, disponibilizado para uso do funcionário ou fornecedor deve ser tratado como de propriedade e sob responsabilidade das Empresas.

Entenda-se por recurso computacional qualquer um ou conjunto dos itens: (i) computador de mesa, (ii) computador portátil e (iii) os acessórios: bolsa de transporte, mouse e teclado, headset; (iv) sistemas, (v) aplicativos, (vi) servidores, (vii) comutadores de rede, (viii) pontos de acesso sem fio, (ix) telefones, (x) equipamentos de vídeo ou conferência via Web, entre outros; devidamente adquiridos, contratados e licenciados.

Entenda-se por estação de trabalho o computador de mesa ou computador portátil (notebook), tablet e smartphone disponibilizado ao usuário. É responsabilidade da área de TI gerenciar e manter controle de acesso e recolha de recursos computacionais disponibilizados aos usuários. Estações de trabalho devem estar associadas aos domínios e grupos de trabalho disponibilizados pela área de TI.

O usuário é o gestor do recurso computacional e deve garantir a sua integridade, perfeito funcionamento e confidencialidade das informações nele contidas. O uso do recurso está condicionado as atividades e funções atribuídas por contrato de trabalho ou de serviços no caso de recursos disponibilizados a fornecedores.

É vedado ao usuário a instalação e/ou uso de software não homologado. É responsabilidade da área de TI gerenciar a homologação de software padrão das *Empresas*, bem como gerenciar as licenças de uso, e homologação de novas versões. Também deve monitorar o uso de software não homologado considerando obrigatoriamente o registro e tratamento de incidentes de segurança da informação quando da detecção deste uso.

É vedado ao funcionário o uso de estação de trabalho (ou recurso computacional) de sua propriedade, comportamento conhecido como *BYOD* (traga seu próprio equipamento).

O uso de recursos computacionais é condicionado as restrições de propriedade intelectual e de uso legal estabelecidas por seus fabricantes ou fornecedores, incluindo-se aqueles produzidos ou criados *pelas Empresas*, não sendo permitido aos usuários o uso destes inadequadamente e/ou emprego de técnicas que possam comprometer estas restrições. É responsabilidade da área de TI monitorar o emprego de técnicas ou software para engenharia reversa e uso indevido de recursos computacionais. O uso indevido deverá ser tratado como incidente de segurança da informação conforme processo e procedimento para gestão de incidentes das *Empresas*.

Os usuários devem comunicar ao Departamento de Tecnologia da Informação das Empresas, qualquer evidência de violação das normas para uso de recurso computacional, não podendo acobertar, esconder ou ajudar a esconder violações de terceiros.

9.1 Software

O uso de software é regulamentado por legislação específica e qualquer ato que a contrarie deve ser considerado e registrado como um Incidente de Segurança.

a) É proibido a instalação de software não licenciado;
b) As empresas do Grupo devem garantir a aquisição de licenças de softwares necessários para a execução das atividades dos usuários;
c) A Área de Infraestrutura de TI deve criar um inventário de softwares e mantê-lo atualizado para fins de controle de licenças;
d) Softwares de livre distribuição (freeware), não podem ser utilizados em equipamentos das empresas sem a devida homologação previa da equipe de Segurança da Informação;
e) É vedado ao usuário, a instalação e/ou remoção de softwares nos equipamentos do grupo, salvo, através de autorização formal da equipe de Segurança da Informação;
f) Todos os programas de software e documentos criados ou providos pelos colaboradores, em benefício de qualquer empresa do grupo são considerados de propriedade do grupo.
g) Sistemas que tratam informações sensíveis ao negócio e ou aqueles utilizados para prover acesso remoto ao ambiente devem prover mecanismos de geração de logs de acesso e trilha de auditoria visando a rastreabilidade de eventos. É responsabilidade da área de TI

garantir a geração de logs em sistemas desenvolvidos internamente ou contratados de fornecedores.

9.2 Hardware

Todos os recursos eletrônicos físicos internos ou externos que fazem o computador funcionar, são considerados Hardwares.

a) A área de infraestrutura deve criar e manter atualizado um inventário de Hardware.
b) Equipamentos de rede e estações de trabalho devem ser identificados fisicamente através de rótulos ou etiquetas que permitam determinar o proprietário.
c) É vedado a utilização de estações de trabalho que não estejam associadas a algum domínio de responsabilidade do grupo, exceções deverão ser previamente aprovadas pela equipe de Segurança da Informação.
d) Colaboradores/Terceiros não devem utilizar computadores e periféricos pessoais nas redes do grupo, salvo com autorização prévia da equipe de Segurança da Informação.
e) Todos os servidores, estações de trabalho e equipamentos de rede do grupo devem obrigatoriamente apresentar aviso de advertência (banner) no processo de Logon/Login para reiterar a propriedade do grupo e uso somente por pessoas autorizadas.
f) Os servidores e equipamentos de rede críticos devem estar alocados em ambiente fisicamente protegido com controle de acesso, com condições de temperatura e umidade adequada. Para sites remotos, onde não exista infraestrutura física adequada é necessário considerar o uso de cofres e racks com controles de acesso.
g) Manutenções e intervenções realizadas por terceiros nos equipamentos de rede e servidores requer acompanhamento obrigatório por pessoal especializado das empresas que forem necessárias e, processos de Gestão de Mudanças devem ser devidamente formalizados.

9.3 Aquisição de Software, Hardware e Contratação de Serviços de Processamento e Armazenamento de Dados e Computação em Nuvem

Todos os tipos de aquisição relacionados à Tecnologia devem seguir as diretrizes da Política de Compras e Política Conheça Seu Fornecedor e exigências da Resolução nº 85 do Banco Central do Brasil, observando-se principalmente, mas não se limitando a:

a) Real necessidade do produto ou serviço a ser adquirido;
b) Previamente à contratação deverá ser considerado a criticidade do serviço e a sensibilidade dos dados e das informações que serão processados, armazenados e gerenciados pelo contratado;
c) Para serviços de processamento e armazenamento de dados e computação em nuvem, deve-se garantir que a empresa contratada possui processos internos de segurança de informação bem como seu software seja desenvolvido de forma segura e traz risco mínimo ou controlado contra ataques e invasões e controles que mitiguem eventuais vulnerabilidades, seja na execução de aplicativos por meio da internet, ou até mesmo na execução em ambiente implantando internamente e/ou na disponibilização de novas versões de softwares.

d) Para serviços de processamento e armazenamento de dados e computação em nuvem, deve-se garantir previamente a contratação a análise de riscos de segurança da informação conforme procedimento "Análise de Riscos de SI – Fornecedores em Nuvem". A análise de riscos deve ser revisada anualmente de acordo com a criticidade do serviço e sensibilidade das informações processadas.

10. CONTROLE SOBRE ACESSO AOS SISTEMAS DE INFORMAÇÃO

Os Acessos aos sistemas devem cumprir as seguintes diretrizes:

10.1 Informações de Controle

a) A concessão de acesso deve seguir os critérios de menor privilégio na permissão de acesso para os sistemas de informação utilizados e internet.
b) É vedado o uso de contas genéricas. Em casos de exceção a área de Segurança da Informação deverá ser previamente consultada para validação e definido processo de dupla custódia.
c) Os acessos não podem ser "cumulativos", ou seja, numa mudança de função, promoção, mudança de área ou afins, os acessos devem ser revistos e readequados de acordo com a nova função.
d) Os acessos de todos os usuários devem ser revisados anualmente.
e) É proibido a cessão, empréstimo e/ou compartilhamento da identificação de usuário e senha associada a qualquer tipo de acesso às informações, sistemas e equipamentos.
f) Nenhum Sistema da empresa poderá ser acessado através de login e senha comum a todos, mesmo que seja para consulta. Cada usuário deverá ter acesso com seu respectivo login e senha e qualquer ação dentro do sistema deverá gerar log de evento.

10.2 Gerenciamento de Autenticação

a) Identificação exclusiva para os usuários (única, pessoal e intransferível). Deve-se impedir os acessos simultâneos pelo mesmo usuário (multi-login).
b) Os usuários estão sujeitos às técnicas de autenticação que permitam validar a identidade do usuário de Rede.
c) As tentativas de acesso não autorizadas devem ser monitoradas.
d) Todos os acessos críticos ao ambiente computacional do Grupo, deverão ser rastreáveis (logs de eventos).
e) Deve-se assegurar a troca da senha de acesso periodicamente e não pode haver repetição de senhas antigas mantidas em histórico definido.
f) As senhas iniciais de acesso fornecidas aos usuários devem estar auto expiradas, exigindo a sua troca na primeira utilização.
g) Senhas "default" de produtos ou aplicativos adquiridos devem ser alteradas imediatamente após sua ativação.
h) Deve haver um processo de bloqueio automático de identificação de usuário por inatividade e após número máximo de dias inativo essa identificação deve ser desativada.
i) Sessões inativas devem ser automaticamente bloqueadas e sua liberação deve exigir senha.
j) Em situação de tentativas repetidas de acesso sem sucesso, a identificação de acesso do usuário deve ser bloqueada.
k) A área de Infraestrutura de TI deve garantir a configuração do ambiente assegurando os critérios de segurança relevantes para regras de senhas, regras de concessão de acesso, regras da rede para navegação na internet, regras de utilização dos equipamentos e

softwares, assim como regras de domínio para assegurar a proteção contra alterações das configurações das estações de trabalho previamente definidas.

l) Quando o usuário identificar utilização suspeita ou indevida de sua senha, esta deverá ser alterada imediatamente e a situação deve ser tratada como um "incidente de segurança" sendo dever do funcionário comunicar para seu gestor imediato e para a área de Segurança da Informação.

m) As senhas cadastradas devem possuir, sempre que possível, os seguintes requisitos:
- 14 caracteres, letras maiúsculas e minúsculas, números e caracteres especiais.
- A política de configuração de senhas deve considerar histórico de controle de não repetição das últimas 10 senhas.
- Expiração das senhas de forma automática a cada 60 dias.
- Requisitos de complexidade automaticamente ativados.
- Possibilidade de reversão de criptografia desabilitada.
- Bloqueio automática após 05 tentativas informado a senha incorreta e por no mínimo 05 minutos.]
- Inserção no processo de autenticação de mecanismos de múltiplo fator de verificação (MFA).

No caso de impossibilidade de implementação dos controles mínimos é necessário avaliar os riscos associados ao sistema e informações tratadas e prover mecanismos de contorno para estes riscos.

11.ACESSO REMOTO

O acesso remoto aos recursos de TI das *Empresas* deve ser provido por meio de canal criptografado e terá privilégios diferenciados do acesso local de acordo com o perfil de acesso, com os serviços solicitados e riscos previamente avaliados. Todo acesso remoto deve ser monitorado e registrado em logs da plataforma utilizada para as conexões via VPN.

O acesso remoto deve ser formalmente solicitado e aprovado de acordo com os requisitos do negócio. Deve-se adotar recursos de Segurança para acessos ao ambiente do Grupo realizados externamente (fora da rede corporativa) com conexão via Rede Privada Virtual (VPN).

Acessos às estações de trabalho para fins de controle e manutenção devem ser realizados via software RDM (Remote Desktop Manager) formalmente homologado pela área de Segurança da Informação. Os acessos para manutenção e atendimento de requisições de serviço devem ser previamente registrados. Não deve haver acesso remoto pela equipe de Service Desk a estação de trabalho do colaborador sem registro prévio da requisição. Todo acesso deve ser monitorado e registrado em logs da plataforma RDM.

12.ACESSO A SERVIDORES E BANCO DE DADOS

O acesso aos servidores e aos bancos de dados só pode ser realizado por pessoal autorizado e deverá ser monitorado, com a devida autorização do Diretor de Segurança Cibernética. As incursões devem estar associadas formalmente a uma requisição de serviço, configuração, incidente ou gestão de mudança. A não observância deste requisito constitui falha grave a esta Política.

Qualquer inclusão, exclusão e alteração importante em ambiente de servidores ou em tabelas de banco, deverá ser realizado através de ferramenta de gestão de acessos que faz a gravação da ação com o devido registro na trilha de auditoria (*log*).

13.INTERNET, E-MAIL, REDES SOCIAIS E IA GENERATIVA

13.1 Internet

O acesso à internet é centralizado e deve possuir mecanismos de filtragem (firewall) de forma a negar o acesso à sites impróprios e vulneráveis.

Os usuários terão acesso à internet, porém, deverão ser criados perfis de internet que adequem a permissão de acesso de acordo com o cargo e área, sendo esse acesso restrito e alinhado com as necessidades para a execução das atividades diárias.

Não é permitido o compartilhamento das informações pertencentes ou custodiadas pelo grupo em sites que provêm serviço de guarda e compartilhamento de documentos (*file sharing*).

Informações sensíveis e críticas, inclusive senhas, números de cartões, dados pessoais ou sensíveis, não devem ser transmitidas através da internet.

13.2 E-mail

O Correio Eletrônico (E-mail) corporativo é disponibilizado para todos os usuários da empresa sob os seguintes critérios:

a) As comunicações internas devem ser feitas através do e-mail corporativo.
b) As assinaturas de E-mail devem seguir formato padrão.
c) Contas pessoais de E-mail não podem ser utilizadas para envio e recebimento de informações.
d) É dado o direito às empresas para registro de uso do E-mail e monitoramento para buscas de atividades ilícitas, estatísticas e possíveis fraudes.
e) O Serviço de E-mail não deve ser utilizado para armazenamento de informações importantes do negócio.
f) É proibido o envio do PAN (número do cartão) ou de qualquer informação relacionada aos dados de portador do cartão em texto claro por E-mail.
g) Deve-se ter cuidado especial no recebimento de E-mails de origens desconhecidas.
h) A equipe de Infraestrutura em conjunto com a equipe de Segurança da Informação são responsáveis por criar regras de monitoramento e bloqueio de mensagens maliciosas, spam, malware e outras ameaças potenciais.

13.3 Redes Sociais

O acesso à Redes Sociais é restrito às áreas que dependem deste para a execução de suas atividades.

Os colaboradores “autorizados” a utilizar Redes Sociais devem ter especial atenção e assegurar que NÃO representam as *Empresas* em assembleias de discussão, fóruns públicos e redes sociais, salvo com autorização previa ou função expressamente atribuída.

Para funções que não tenham associação com Redes Sociais, o acesso é automaticamente coibido. As exceções deverão ser analisadas e tratadas diretamente com a área de Segurança da Informação.

13.4 Inteligência Artificial Generativa

O acesso a serviços de IA Generativas é restrito às áreas que dependem deste para a execução de suas atividades.

Os colaboradores "autorizados" a utilizar IA Generativa devem ter especial atenção e NÃO carregar dados de clientes, dados pessoais e dados das *Empresas* nestas plataformas. Mecanismos de anonimização e pseudoanonimização devem ser utilizados para garantir a proteção das informações.

Para funções que não tenham associação com IA Generativa, o acesso é automaticamente coibido. As exceções deverão ser analisadas e tratadas diretamente com a área de Segurança da Informação.

14.CRIPTOGRAFIA

A criptografia deve ser utilizada sob certas condições, a fim de garantir confidencialidade, autenticidade e integridade das informações, dessa forma deve-se:

a) Aplicar o uso de criptografia nas comunicações e transferências de informações entre o Grupo e instituições financeiras, parceiros e fornecedores estratégicos.
b) As bases de dados contendo informações de cartões e senhas de clientes, devem estar criptografadas e com o controle adequado das chaves de criptografia seguindo as diretrizes do Procedimento de Gerenciamento de Chaves Criptográficas.
c) Estações de Trabalho que contenham informações sensíveis armazenadas, deverão ter seus discos criptografados.
d) Dados e informações definidos como sensíveis e confidenciais, deverão ser criptografados quando estiverem trafegando fora do ambiente físico da empresa.
e) Mídias com informações confidenciais devem ter seu conteúdo criptografado antes do transporte externo.

15.SEGURANÇA DAS COMUNICAÇÕES

As regras de segurança da Rede de Tecnologia da Informação, definem os requisitos de confiança e troca e são projetadas para limitar os riscos de intrusão ou acesso não autorizado aos sistemas de informação do grupo.

15.1 Segurança da Rede

A equipe de infraestrutura deve produzir um DAT – Documento de Arquitetura Técnica – a fim de documentar tudo que precisa ser feito para atingir os objetivos de segurança da rede aplicáveis nas arquiteturas operacionais, funcionais, de aplicativos e técnicas. Isso inclui a criação de um diagrama detalhado da arquitetura de rede (contemplando protocolos, matriz de fluxo, recursos ativos e passivos de proteção, configurações) e deve ser mantido atualizado e disponível apenas para pessoal autorizado.

A rede deve ser segmentada como medida estratégica de proteção contra ataques cibernéticos aos dados corporativos. A estruturação da Rede é feita em diferentes áreas de confiança, por isso a segmentação deve permitir a divisão da rede em subseções para que seja possível controlar a concessão de acessos aos usuários de acordo com suas necessidades no trabalho seguindo o princípio de que "tudo que não seja expressamente permitido, é proibido".

Os fluxos de interconexão devem ser protegidos e qualquer novo acesso de entrada ou saída ao IS, das empresas, assim como qualquer interconexão entre diferentes redes internas ou externas (com fio e sem fio) devem cumprir as regras definidas no Padrão de interconexão ISS do grupo.

Os acessos remotos devem garantir a autenticação do usuário e a confidencialidade dos dados (criptografia).

Todos os equipamentos da rede necessários para as atividades comerciais das empresas devem ser supervisionados e monitorados conforme procedimento para monitoramento de ativos críticos.

A administração do uso de credenciais privilegiadas é de responsabilidade da Diretoria de Tecnologia da Informação. O impacto do risco de uso indevido destas credenciais deve ser avaliado pela Gerência de Segurança da Informação. É obrigatório o registro de eventos em log para todas as autenticações com credenciais privilegiadas, com sucesso ou erro. Eventos de login com erro acima de 05 (cinco) tentativas devem ter a credencial automaticamente bloqueada que só deverá ser desbloqueada pelo administrador competente. Eventos de login com erro para credenciais privilegiadas devem ser monitorados e tratados com celeridade e atenção.

O registro de eventos dos sistemas e equipamentos críticos do Grupo deve ser realizado e tratado de forma centralizada (Syslog). É responsabilidade da Diretoria de Tecnologia da Informação manter processo para este controle, desenvolvimento, monitoramento e ações preventivas concernentes a correlação de eventos de segurança da informação por meio da aplicação de tecnologia para SIEM (Security Information and Event Management).

15.2 Transferência das Informações

Sobre o acesso à Internet a partir dos equipamentos do Grupo devem ser centralizadas e incluir mecanismos de filtragem.

Consultas a sites externos e trocas de e-mail devem ocorrer por meio de um gateway seguro, com mecanismos de filtro incorporados a fim de combater spam, códigos maliciosos e trocas de informações indevidas.

Dispositivos removíveis devem possuir sistemas de proteção que garantam a confidencialidade, integridade e disponibilidade dos dados, seguindo as premissas do item **13.3.**

A transferência de informação via internet deve ser realizada por meio de protocolos seguros como HTTPS, SFTP e similares. É responsabilidade da área de Segurança da Informação garantir o uso de chaves criptográficas de tamanho superior a 1024 bits.

16.SEGURANÇA OPERACIONAL

16.1 *Malware, Ransomware e Spam*

Toda estação de trabalho e servidor deve possuir software EDR *(Endpoint Detection Response*) ou XDR (*Extended Detection Response*) instalado e atualizado automaticamente. É responsabilidade da área de TI assegurar o processo de controle de malware nas *Empresas* para mitigar riscos associados a infecção por *malware*, Spam e *ransomware*.

É responsabilidade do colaborador comunicar a área de TI comportamento anômalo possivelmente associado a malware em suas estações de trabalho.

O uso de dispositivos do tipo “mídia removível” (*pen drives*) deve ser previamente autorizado formalmente e controles de segurança da informação devem ser empregados pela área de TI coibindo o uso não autorizado.

16.2 *Backup* e Contingência

Todas as informações críticas de negócio das empresas devem possuir cópia de segurança (*backup*). A equipe de Infraestrutura deve seguir as diretrizes do Procedimento de *Backup* e *Restore* que contém requisitos detalhados inerentes ao processo.

a) É responsabilidade da equipe de Infraestrutura providenciar recursos físicos e lógicos para armazenamento e restauração das cópias de segurança.
b) Os processos de backup assim como os de testes restauração das informações críticas armazenadas é de responsabilidade da equipe de infraestrutura.
c) Diretórios denominados como “COMUM” ou “PÚBLICO”, não devem ser utilizados para armazenamento de arquivos que contém informações sensíveis, devendo estes serem utilizados para armazenamento de informações de interesse geral. Diretório “Publico” deverá conter rotina que apague automaticamente informações contidas nesse local.

16.3 Gerenciamento de Vulnerabilidades

Objetiva evitar qualquer falha exposta que possa impactar os sistemas de informação do Grupo.

a) A equipe de Segurança da Informação deverá desenvolver e aplicar procedimentos de detecção de vulnerabilidades nos diferentes componentes dos sistemas de informação (*Hardware e Software*).
b) As auditorias com o objetivo de identificar as possíveis vulnerabilidades deverão ser programadas periodicamente.
c) Quando uma vulnerabilidade é identificada, deve-se aplicar um plano de ação, sendo que as vulnerabilidades caracterizadas como “críticas” deverão ser tratadas imediatamente.

d) A análise e exploração de vulnerabilidades (*Pentest*) para sistemas críticos expostos na internet deverá ser realizada em intervalos regulares, objetivando a identificação de possíveis vulnerabilidades e correção destas. É responsabilidade da alta direção o provisionamento de recursos financeiros para esta análise e sua execução pela Diretoria de Cibersegurança.

16.4 Gestão de Mudanças

Todas as alterações de configuração na infraestrutura de TI, segurança da informação e sistemas do Grupo, devem obrigatoriamente requerer o registro e a aprovação de mudança através de processo específico.

O processo de gestão de mudança deve assegurar no mínimo que os riscos operacionais foram identificados e que o processo de retomada/recuperação (*rollback)* existe e está validado, seguindo as diretrizes específicas do Procedimento de Gerenciamento de Mudança.

As alterações e configurações críticas da rede e de sistemas devem obrigatoriamente passar pela análise da equipe de Segurança da Informação de forma a identificar possíveis vulnerabilidades ou comprometimento da integridade, confidencialidade e disponibilidade das informações.

A mudança **não** poderá ocorrer sem registro e prévio alinhamento com as áreas interessadas e registro de demanda de RDM.

Mudanças realizadas por fornecedores em ativos críticos para o negócio devem ser registradas internamente e acompanhadas com o devido rigor e processo estabelecido no Procedimento de Gestão de Mudanças.

Os riscos e impactos das mudanças devem ser previamente avaliados e documentados. Mudanças que impactam na governança de privacidade e continuidade do negócio devem ser comunicadas as áreas responsáveis onde ações devem ser estabelecidas e acompanhadas para mitigar possíveis riscos.

16.5 Registro de Eventos e Notificações e Resposta a Incidentes

As regras de segurança para o gerenciamento de registros devem ser estabelecidas e implementadas com a finalidade de gravação de eventos e a capacidade de geração de evidências.

a) A equipe de infraestrutura deve criar processos de identificação, avaliação, comunicação e acompanhamento dos riscos de segurança da informação em novos projetos, mudanças críticas ou demandas eventuais, bem como assegurar que fragilidades e eventos de segurança sejam comunicados, de forma que a tomada de ação corretiva ocorra em tempo hábil.
b) O objetivo da gestão de incidentes, é limitar o impacto dos incidentes de segurança em sistemas de informação e restaurar o serviço afetado dentro de um prazo aceitável.
c) Deve-se determinar os papéis e responsabilidades na gestão de incidentes de segurança.
d) Os incidentes deverão ser classificados de acordo com o seu tipo e nível de gravidade.
e) As pessoas apropriadas deverão ser comunicadas dentro do prazo exigido pela lei e regulamentos em vigor.

f) Os colaboradores devem informar aos seus gestores e à área de Segurança da Informação qualquer incidente de segurança que tiverem conhecimento.
g) Definir responsabilidade para o tratamento de incidentes e formalização do procedimento.

17.SEGURANÇA CIBERNÉTICA

Serviços críticos e essências aos negócios das *Empresas* devem ser protegidos para evitar ou mitigar ataques cibernéticos de interrupção de serviços tais como DDoS (Ataques de Interrupção de Serviços Distribuídos), *ransomware*, envenenamento de DNS, divulgação de dados pessoais e outros. É responsabilidade da área de Segurança da Informação determinar as possíveis ameaças, definir e adotar medidas de proteção tais como a contratação de links seguros, serviços de gestão de conteúdo e outros.

É responsabilidade Gerência de Segurança da Informação planejar e executar exercícios anuais considerando ataques cibernéticos. Tais exercícios devem considerar manual próprio de testes e melhores práticas para sua execução e documentação. Os resultados devem ser comunicados e apresentados formalmente para a alta direção.

18.INTEGRAÇÃO DE SEGURANÇA DA INFORMAÇÃO EM NOVOS PROJETOS E DESENVOLVIMENTOS

Ao longo de cada projeto desde sua concepção até a sua entrega devem ser consideradas as regras de segurança necessárias para a criação de um produto seguro.

a) Os requisitos de segurança devem ser identificados na fase de definição de requisitos de um projeto, devendo refletir o valor para o negócio e os danos potenciais que poderiam resultar em uma falha ou ausência de segurança.
b) Os acessos aos arquivos de sistemas e aos programas de código fonte deve ser controlado.
c) Os novos sistemas devem ser implantados em produção somente após passarem por testes de homologação pelas áreas responsáveis e após a aprovação do requisitante, incluídos nesse caso, sistemas, aplicativos e estações de trabalho.

É responsabilidade da Diretoria de Tecnologia da Informação garantir que código desenvolvido internamente ou fornecido por terceiros seja analisado quanto a presença de vulnerabilidades que possam impactar a segurança da informação do Grupo. O código não poderá ser utilizado em produção sem a correção das vulnerabilidades e aprovação formal interna para liberação em produção.

A segregação dos ambientes de desenvolvimento, homologação, testes e produção é obrigatória. A Área de Segurança da Informação deverá ser o guardião deste requisito.

É responsabilidade da Área de Segurança da Informação garantir que credenciais de acesso para aplicações, APIs e serviços Web sejam gerenciadas por meio de cofre de senhas e utilizem padrão de autenticação forte em conjunto com senhas de vida única (OTP - *One Time Password*) ou senhas

de vida única com tempo de expiração (TOTP - *Time-based One Time Password*). É vedado o uso e armazenamento de senhas em texto plano no código fonte.

19. ASPECTOS DA SEGURANÇA DA INFORMAÇÃO NA GESTÃO DE CONTINUIDADE DE NEGÓCIO

Para assegurar a continuidade das linhas críticas de negócio por intermédio de planos de contingência equipamentos que processam e armazenam as informações devem possuir recursos para alta disponibilidade, redundância de fonte de energia, proteção de memória e cópia de segurança (backup) salvaguardados. É responsabilidade da Diretoria de Tecnologia garantir estes recursos.

Deve ser estabelecido e gerenciado um Plano de Continuidade de Negócios (PCN) para os serviços críticos de negócio do Grupo. É responsabilidade da alta direção prover os recursos para a manutenção do PCN.

20. PADRÕES E MELHORES PRÁTICAS DA INDÚSTRIA

Como parte das atividades o grupo pode manusear, armazenar ou transferir informações sensíveis de cartão de pagamento como:

- O nome do titular do cartão
- O número da conta principal (PAN)
- A data de expiração

Para garantir a máxima mitigação de risco de comprometimento dos dados sensíveis, o Grupo deve cumprir os seguintes requisitos:

a) Aplicar o truncamento do PAN quando os dados sensíveis forem processados, transmitidos ou armazenados fora dos sistemas autorizados.
b) Bloquear acesso não autorizado às informações sensíveis.
c) Utilizar criptografia de ponta a ponta no canal de troca de dados.
d) Proteger aplicativos de cartões de pagamento.
e) Garantir o vigor de todos os Controles, Políticas, Procedimentos e Processos necessários para a proteção dos dados e segurança da informação.

21. SEGURANÇA FÍSICA E AMBIENTAL

21.1 Segurança Física e Ambiental

A segurança física deve contemplar mecanismos de proteção que abrangem desde o perímetro externo até o espaço interno de trabalho, prevenindo o acesso físico não autorizado, danos, furtos e interferências com as instalações e informações críticas da empresa.

a) Definir, controlar e monitorar os perímetros de segurança física das instalações das empresas, garantindo não haver brechas nem pontos sensíveis para invasões.
b) Apenas funcionários podem ter acesso as dependências das empresas, devendo estes portar crachá de identificação.
c) Visitante deve ter registro na portaria e prévia autorização do gestor que vai recebê-lo.

d) As portas de acesso a áreas críticas devem ser controladas e monitoradas, permitindo acesso apenas de pessoal autorizado.
e) Equipamentos críticos e de alto valor, deverão ser mantidos em salas protegidas contra furtos, danos, roubos e intempéries, e os acessos físico e lógico devem ser controlados e monitorados.
f) Deve haver monitoramento de câmeras nas dependências das empresas, onde for necessário.
g) Os equipamentos críticos devem ser protegidos e monitorados contra a falta de energia elétrica e outras interrupções causadas por falhas de outros recursos (água, ar-condicionado etc.).
h) Os equipamentos devem receber manutenção nos intervalos recomendados pelos fornecedores e de acordo com as suas especificações.
i) Cabeamento de energia e de telecomunicação que transportam dados ou dão suporte aos serviços de informação devem ser protegidos contra interceptação ou danos.
j) Deve-se implementar medidas de proteção contra danos causados por incêndios, distúrbios civis e outras formas de desastres naturais ou de origem humana.

21.2 Mesa Limpa

Refere-se à Mesa, Tela, Impressora e Lixo Limpos;

a) Ao se ausentar, o funcionário deve bloquear sua estação de trabalho, evitando, desta maneira, o acesso por pessoas não autorizadas. E não deixar sobre a mesa de trabalho impressos, anotações, agendas e cadernos.
b) É recomendado que ao término do expediente, o usuário desligue sua estação de trabalho.
c) É imperativo manter documentos impressos e dispositivos de armazenamento devidamente protegidos, não deixando estes materiais na impressora ou na lixeira. Devem ser guardados em armários com chaves, descartados em lixos protegidos ou triturados;
d) Todo e qualquer documento legal deve ser arquivado no CEDOC seguindo os procedimentos da Política de Gestão Documental.

22.CONFORMIDADE, PRIVACIDADE E PROTEÇÃO DE DADOS

A conformidade com requisitos legais e contratuais é responsabilidade de todos os colaboradores das Empresas. Os gestores devem identificar e observar a legislação aplicável às *Empresas*, garantindo a adequação contratual e observância das diretrizes de Segurança da Informação desta Política.

Em especial os requisitos da Lei Geral de Proteção de Dados (LGPD 13.709/2018) devem ser observados por todos os colaboradores visando preservar a privacidade do Titular dos Dados pessoais. Informações de Identificação Pessoal ou Dados Pessoais incluem qualquer informação que possa ser associada ou rastreada a qualquer indivíduo, incluindo o nome, endereço, número de telefone, endereço de e-mail, informações de cartão de crédito, número de CPF, RG, sexo, preferências religiosas, partidárias ou outras informações factuais específicas semelhantes, independentemente da mídia na qual tais informações são armazenadas (por exemplo, em papel ou eletronicamente) incluem as informações que são geradas, coletadas, armazenadas ou obtidas como parte do exercício da

função do colaborador no Contrato de Trabalho e negócios das *Empresas*, incluindo dados transacionais e outros referentes aos clientes.

O colaborador cumprirá todas as leis e regulamentos aplicáveis de privacidade (LGPD 13.709/2018) e outras leis relacionadas à proteção, coleta, uso e distribuição de Informações Pessoais Identificáveis. Em nenhum caso, o funcionário poderá vender ou transferir informações pessoalmente identificáveis a terceiros, ou fornecer acesso a elas sem a autorização formal e prévia. Todos os dados e informações serão tratados conforme especificações e regras estabelecidas na Política de Privacidade e Proteção de Dados.

A confidencialidade e sigilo de Dados Pessoais devem ser observados, preservados e garantidos por todos os colaboradores das Empresas. A área de TI é responsável por propiciar mecanismos de proteção condizentes com a criticidade da informação e requerer estes aspectos de provedores de serviços e sistemas. Suspeitas de violação de Dados Pessoais devem ser comunicadas ao superior imediato e/ou envio de e-mail para security@valecard.com.br; dpo@valecard.com.br.

Relações contratuais com diretrizes de Segurança da Informação inferiores às contidas nesta Política devem ser evitadas e caso não haja opção, devem ser analisadas quanto ao risco e aprovadas formalmente pelo Departamento Jurídico.

Os gestores da organização devem observar e garantir direitos de propriedade intelectual de terceiros e das *Empresas*.

Enquanto durar a relação contratual, as patentes, invenções, direitos autorais, ou outras propriedades intelectuais tais como: estudos, projetos, relatórios e demais dados desenvolvidos pelo colaborador são de direito exclusivo das *Empresas* que poderá registrá-los nos órgãos competentes e utilizá-los ou cedê-los sem qualquer restrição ou custo adicional.

A análise crítica e independente do processo de gestão de Segurança da Informação deve ser realizada pelo menos uma vez ao ano através da contratação de auditoria externa. A Diretoria de Cibersegurança é responsável pela garantia de isenção neste processo devendo acompanhar e zelar pela execução das correções de acordo com o risco para o negócio.

Qualquer eventualidade e/ou incidente associado a privacidade ou tratamento de dados pessoais deverá ser comunicado ao Encarregado de Dados e a equipe de Segurança da Informação para que as medidas de correção imediatas sejam aplicadas conforme a referida Política de Privacidade e Proteção de Dados.

23.CRIPTOGRAFIA

Criptografia é a ciência ou arte de escrever mensagens em forma cifrada (codificada). É usada, dentre outras finalidades para: autenticar a identidade de usuários; autenticar transações bancárias; proteger a integridade de transferências eletrônicas de fundos; proteger o sigilo de comunicações pessoais e comerciais.

É responsabilidade da Área de Segurança da Informação a avaliação, indicação e implementação de técnicas para criptografia das informações do Grupo de acordo com a sensibilidade e classificação da informação no armazenamento e transporte desta.

É responsabilidade da Área de Segurança da Informação a gestão de chaves e certificados criptográficos mantendo estrito controle, processo e procedimento para esta gestão. Incidentes envolvendo a quebra, vazamento ou corrompimento de tais chaves devem ser comunicados imediatamente a alta direção.

Por padrão (default) o transporte de informações do Grupo via Internet deve empregar protocolos seguros como HTTPS, SSH, IPSec e SFTP entre outros com chaves criptográficas ou certificados de no mínimo 1056 Bits.

Todos os recursos computacionais portáteis devem ter implementados pela Área de Infraestrutura de TI, no seu processo de concessão ao usuário, mecanismo de criptografia automatizado para armazenamento seguro das informações no disco local e controle para que o disco não possa ser reconstruído (ativado) em outra máquina diferente da original disponibilizada ao colaborador.

As comunicações e transferências de informações entre o Grupo, clientes, outras instituições financeiras, parceiros e fornecedores estratégicos devem ser realizadas através de redes privadas (VPN) utilizando-se de esquemas criptográficos previamente avaliados e aprovados pela Área de Segurança da Informação.

Por padrão (default) as bases de dados contendo senhas devem estar criptografadas e o com respectivo controle adequado das chaves utilizadas para este controle.

24.PAPÉIS E RESPONSABILIDADES

Os papéis e responsabilidades estabelecidos nesta política, devem familiarizar-se, aderir e praticar as diretrizes contidas na PSI, bem como procedimentos e padrões relacionados à Segurança da Informação. As informações resultantes das atividades comerciais das *Empresas*, principalmente aquelas que envolvam o tratamento de dados pessoais devem garantir adequação a Lei Geral de Proteção de Dados (13.709/2018). Portanto, todos os agentes de tratamento têm a obrigação de tratar estas informações como sigilosas, sob pena de sansões, punições, processos cíveis e criminais no rigor da lei.

24.1 Conselho de Administração

a) Deliberar sobre as diretrizes e alterações nesta política; e
b) Apreciar o relatório anual de resposta a incidentes e plano de ação.
c) Supervisionar, manter e garantir recursos para a composição e garantir eficácia dos processos e controles inerentes ao SGSI.
d) Garantir orçamento adequado, pessoal capacitado, emprego de ferramentas e serviços de Segurança da Informação condizentes com os riscos identificados e agenda de treinamentos especializados.

24.2 Diretoria Executiva

a) Deliberar sobre as diretrizes e alterações nesta política;
b) Apreciar o relatório anual de resposta a incidentes e plano de ação;
c) Submeter ao Conselho de Administração a Política de Segurança da Informação; e
d) Submeter ao Conselho de Administração o relatório anual de resposta a incidentes e plano de ação.

24.3 Auditoria Interna

a) Realizar auditoria anual nos processos de segurança da informação, bem como em contratos de parceiros e contratação de fornecedores de soluções de armazenamento em nuvem.

24.4 Diretoria de Segurança Cibernética

a) Estabelecer as diretrizes para o bom andamento da governança de Segurança da Informação;
b) Garantir a aderência de todas as áreas/departamentos das *Empresas* às regras estabelecidas esta Política, por meio da avaliação e publicação periódica de indicadores;
c) Submeter à Diretoria Executiva, bem como ao Conselho de Administração os indicadores de ocorrências de incidentes e plano de ação para correções;
d) Elaborar relatório anual sobre a implementação do plano de ação e de resposta a incidentes, com data base de 31 de dezembro; e
e) Submeter o relatório anual de resposta a incidentes e plano de ação à Diretoria Executiva e Conselho de Administração.

24.5 Área de Tecnologia da Informação

a) Operacionalizar, realizar manutenção dos serviços de segurança e gerenciamento de incidentes de segurança da informação;
b) Auxiliar as demais áreas das Empresas no suporte e nas soluções de segurança de forma corporativa, cabendo ao Gerente de cada área de negócios identificar as irregularidades e falhas de SI em seus processos, reportando-as ao Gestor da área de SI.

24.6 Área Jurídica

a) Garantir que contratos ou termos de confidencialidade com clientes, fornecedores, prestadores de serviços e parceiros de negócio possuam cláusulas de Segurança da Informação que assegurem a proteção das informações e recursos de TI das Empresas.

24.7 Área de Recursos Humanos

a) Informar sobre os requisitos de Segurança da Informação aos possíveis candidatos a vagas de emprego das Empresas; e
b) Apoiar e garantir os processos de educação e conscientização em Segurança da Informação durante o ciclo de vida do funcionário nas Empresas, sem prejuízo de que sejam informados regularmente ou quando houver qualquer alteração na Política Corporativa da Segurança da Informação.

GRC-009 PO Segurança da Informação_v08_vf.pdf

Documento número #947e1a2f-e75e-4552-95b5-873db2eae16e

Hash do documento original (SHA256): 32a32ef7ec6aaf057d3eb11f21e4858fc9df81495b8243fe5179272ee2046728

Assinaturas

Luiz Antonio Abreu
CPF: 539.307.976-15
Assinou como administrador em 30 out 2023 às 13:19:07

Alan Avila
CPF: 094.416.996-16
Assinou como gestor em 30 out 2023 às 08:50:48

Thallyta Loureto de Freitas
CPF: 014.046.906-03
Assinou em 30 out 2023 às 08:55:06

Caio Augusto Faria Pajaro
CPF: 086.668.356-99
Assinou como presidente em 31 out 2023 às 13:32:47

Simonio Freita da Silva
CPF: 004.991.726-98
Assinou como administrador em 30 out 2023 às 09:30:30

Marcelo Henrique de Souza Padua
CPF: 565.672.606-10
Assinou como gestor em 30 out 2023 às 12:35:29

Log

30 out 2023, 08:43:42	Operador com email thallyta.carvalho@valecard.com.br na Conta d901cdfc-a751-4d51-acfb-ad0e4c721c7e criou este documento número 947e1a2f-e75e-4552-95b5-873db2eae16e. Data limite para assinatura do documento: 06 de novembro de 2023 (08:37). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.

30 out 2023, 08:43:43 Operador com email thallyta.carvalho@valecard.com.br na Conta d901cdfc-a751-4d51-acfb-ad0e4c721c7e adicionou à Lista de Assinatura: luiz.abreu@valecard.com.br para assinar como administrador, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Luiz Antonio Abreu.

30 out 2023, 08:43:43 Operador com email thallyta.carvalho@valecard.com.br na Conta d901cdfc-a751-4d51-acfb-ad0e4c721c7e adicionou à Lista de Assinatura: alan.avila@tuttoinvest.com para assinar como gestor, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Alan Avila.

30 out 2023, 08:43:43 Operador com email thallyta.carvalho@valecard.com.br na Conta d901cdfc-a751-4d51-acfb-ad0e4c721c7e adicionou à Lista de Assinatura: thallyta.carvalho@valecard.com.br para assinar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Thallyta Loureto de Freitas.

30 out 2023, 08:43:43 Operador com email thallyta.carvalho@valecard.com.br na Conta d901cdfc-a751-4d51-acfb-ad0e4c721c7e adicionou à Lista de Assinatura: caio.pajaro@agilli.com.br para assinar como presidente, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Caio Augusto Faria Pajaro.

30 out 2023, 08:43:43 Operador com email thallyta.carvalho@valecard.com.br na Conta d901cdfc-a751-4d51-acfb-ad0e4c721c7e adicionou à Lista de Assinatura: simonio.silva@cscresult.com.br para assinar como administrador, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Simonio Freita da Silva e CPF 004.991.726-98.

30 out 2023, 08:43:43 Operador com email thallyta.carvalho@valecard.com.br na Conta d901cdfc-a751-4d51-acfb-ad0e4c721c7e adicionou à Lista de Assinatura: marcelo.padua@valecard.com.br para assinar como gestor, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Marcelo Henrique de Souza Padua.

30 out 2023, 08:50:48 Alan Avila assinou como gestor. Pontos de autenticação: Token via E-mail alan.avila@tuttoinvest.com. CPF informado: 094.416.996-16. IP: 8.242.2.2. Localização compartilhada pelo dispositivo eletrônico: latitude -18.927109 e longitude -48.3001233. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.644.0 disponibilizado em https://app.clicksign.com.

30 out 2023, 08:55:06 Thallyta Loureto de Freitas assinou. Pontos de autenticação: Token via E-mail thallyta.carvalho@valecard.com.br. CPF informado: 014.046.906-03. IP: 200.243.224.146. Componente de assinatura versão 1.644.0 disponibilizado em https://app.clicksign.com.

30 out 2023, 09:30:30 Simonio Freita da Silva assinou como administrador. Pontos de autenticação: Token via E-mail simonio.silva@cscresult.com.br. CPF informado: 004.991.726-98. IP: 200.170.138.209. Localização compartilhada pelo dispositivo eletrônico: latitude -18.8968357 e longitude -48.2819087. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.644.0 disponibilizado em https://app.clicksign.com.

30 out 2023, 12:35:29 Marcelo Henrique de Souza Padua assinou como gestor. Pontos de autenticação: Token via E-mail marcelo.padua@valecard.com.br. CPF informado: 565.672.606-10. IP: 200.170.138.209. Localização compartilhada pelo dispositivo eletrônico: latitude -18.9273173 e longitude -48.2999476. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.645.0 disponibilizado em https://app.clicksign.com.

30 out 2023, 13:19:07	Luiz Antonio Abreu assinou como administrador. Pontos de autenticação: Token via E-mail luiz.abreu@valecard.com.br. CPF informado: 539.307.976-15. IP: 8.242.2.2. Localização compartilhada pelo dispositivo eletrônico: latitude -18.92750198517274 e longitude -48.30001376955321. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.645.0 disponibilizado em https://app.clicksign.com.
31 out 2023, 13:32:48	Caio Augusto Faria Pajaro assinou como presidente. Pontos de autenticação: Token via E-mail caio.pajaro@agilli.com.br. CPF informado: 086.668.356-99. IP: 191.31.226.57. Componente de assinatura versão 1.646.0 disponibilizado em https://app.clicksign.com.
31 out 2023, 13:32:48	Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 947e1a2f-e75e-4552-95b5-873db2eae16e.