Política de Segurança da Informação

Grupo Vinci

Janeiro 2019

VINCI partners

Política de Segurança da Informação
Grupo Vinci

Janeiro 2019

Índice

Política de Segurança da Informação
Grupo Vinci

Janeiro 2019

1. Objetivo

A presente política visa estabelecer as diretrizes, princípios, responsabilidades e orientações relacionadas ao tratamento das informações ao uso adequado de ativos e recursos tecnológicos pelos Colaboradores do Grupo Vinci e Terceiros e à proteção de tais ativos e recursos tecnológicos.

2. Abrangência

Para efeitos desta Política de Segurança da Informação ("Política"), "Grupo Vinci" abrange a Vinci Partners Investimentos Ltda. ("Vinci Partners"), Vinci Gestora de Recursos Ltda. ("Vinci Gestora"), Vinci Capital Gestora de Recursos Ltda. ("Vinci Capital"), Vinci Equities Gestora de Recursos Ltda. ("Vinci Equities"), Vinci Gestão de Patrimônio Ltda. ("VGP"), Vinci Real Estate Gestora de Recursos Ltda. ("Vinci Real Estate"), Vinci GGN Gestora de Recursos Ltda. ("Vinci GGN"), Vinci Infraestrutura Gestora de Recursos Ltda. ("Vinci Infraestrutura"), Vinci Assessoria Financeira Ltda ("Vinci Assessoria") e a Vinci Distribuidora de Títulos e Valores Mobiliários Ltda.

Esta Política é aplicável aos sócios, integrantes de cargos de administração ou gestão, funcionários, estagiários e demais Colaboradores, independentemente do vínculo contratual ou societário que mantenham com o Grupo Vinci ("Colaboradores"), bem como a todos os visitantes, terceiros, prestadores de serviços e partes interessadas nos negócios do Grupo Vinci ("Terceiros").

3. Diretrizes

A informação pode estar presente em diversas formas como, por exemplo, sistemas de informação, diretórios de rede, bancos de dados, mídia impressa ou eletrônica, dispositivos móveis e, até mesmo, por meio da comunicação oral.

Toda informação é um ativo de valor, devendo ser adequadamente utilizada e protegida, conforme a legislação vigente e os procedimentos internos do Grupo Vinci.

Toda informação e recurso tecnológico devem ser utilizados com o objetivo de apoiar e suportar o desempenho das atividades do Grupo Vinci. Sua utilização deve atender às políticas e procedimentos de segurança da informação.

O uso dos ativos e recursos tecnológicos, inclusive sistemas de informação e serviço de e-mail do Grupo Vinci, pode ser monitorado e os registros assim obtidos poderão ser utilizados para

avaliação de sua conformidade de uso com as atividades corporativas, podendo servir de evidência para a aplicação de medidas disciplinares, processos administrativos ou legais.

As informações geradas e recebidas devem atender às necessidades de disponibilidade, integridade, confidencialidade, autenticidade e auditoria:

- Disponibilidade: visa a garantir que todas as pessoas autorizadas obtenham acesso à informação e aos ativos correspondentes sempre que necessário;
- Integridade: visa a garantir que a informação esteja sempre completa e íntegra e que não tenha sido modificada ou destruída de maneira indevida (não autorizada ou acidental) durante o seu ciclo de vida;
- Confidencialidade: visa a garantir que a informação seja acessível somente pelas pessoas autorizadas e pelo período necessário;
- Autenticidade: visa a garantir a verificação da identidade dos usuários e à certeza de que a informação provém da origem anunciada;
- Auditoria: visa a assegurar o cumprimento da política geral de segurança da informação.

4. Atribuições e Responsabilidades

O Grupo Vinci, seus Colaboradores e Terceiros devem zelar pela manutenção da segurança das informações, aderindo aos cuidados na manutenção das mesas limpas e no tratamento das informações, independentemente da forma ou meio utilizado, inclusive oralmente.

A utilização de dispositivos móveis (smartphones, tablets, etc.) para acessar informações internas é permitida desde que a solicitação do Colaborador ou da área seja formalmente aprovada pelos procedimentos de controle vigentes.

O uso destes dispositivos móveis é restrito ao acesso de e-mails e aplicações que sejam formalmente autorizadas, nos termos dos procedimentos de controle vigentes.

A eventual utilização para fins profissionais de serviços de mensagem instantânea em smartphones pessoais (WhatsApp, etc.) deve observar o mesmo zelo e cuidado com a segurança da informação exigidos por esta política e pela relação de fidúcia existente entre as partes.

Ao utilizar recursos pessoais para fins profissionais, o Colaborador, caso solicitado, se coloca à disposição do Grupo Vinci para cooperar e fornecer informações que eventualmente sejam necessárias para a defesa e preservação dos interesses do Grupo Vinci.

4.1. Regras e Diretrizes aplicáveis à área de TI (Tecnologia da Informação)

São atribuições da área de TI relacionadas à segurança da informação:

- Manter a integridade, disponibilidade e confidencialidade dos sistemas, arquivos, informações e ativos tecnológicos do Grupo Vinci.
- Manter o controle efetivo e validado sobre as permissões de acesso concedidas a Colaboradores e terceiros.
- Assegurar que as soluções de segurança, tais como proxy, criptografia, backup, antivírus, AntiSpam, estejam operacionais e aderentes aos procedimentos internos, assim como suportando as diretrizes e objetivos listados nesta política.
- Controlar o acesso à internet em conformidade com as regras e procedimentos internos de uso da internet.
- Manter registros das atividades feitas dentro da organização por meio de: circuito fechado de televisão (CFTV), log de e-mail, acesso físico e lógico, ligações telefônicas de ramais e outras tecnologias que sejam implantadas para a coleta de registros de atividades.

4.2. Regras e Diretrizes aplicáveis aos Colaboradores

Os recursos de TI disponibilizados para os usuários têm como objetivo a realização de suas atividades profissionais no Grupo Vinci.

Os Colaboradores têm o dever de utilizar os arquivos e informações eletrônicas em conformidade com as regras e diretrizes estabelecidas nesta política e aderência aos demais procedimentos previstos no item 7 abaixo.

A proteção do recurso computacional é de responsabilidade do próprio usuário.

É de responsabilidade de cada usuário assegurar a integridade do equipamento e a confidencialidade da informação nele contida.

O usuário não deve alterar a configuração do equipamento recebido.

A gravação de informação em mídias removíveis (CDs, DVDs, *Blu Ray*, Pen Drive, etc.) é permitida somente nas condições relacionadas nos Procedimentos de Solicitação e Uso de Dispositivos de TI.

A utilização de armazenamento em nuvem (*cloud*) é permitida somente para uso corporativo por meio do parceiro credenciado informado no procedimento interno do Grupo Vinci.

É vedada a utilização de serviços de nuvem de parceiros não homologados, assim como para fins particulares.

É vedada a instalação de qualquer software/plug-in diretamente pelos Colaboradores, tais como aplicações bancárias, programas gratuitos, aplicativos terceiros de recursos para o office, Internet Explorer, Chrome, etc.

A solicitação de instalação deve ser feita exclusivamente pelo canal de TI.

É vedada a utilização de qualquer serviço de armazenamento de dados não homologado nesta política e em seus documentos de referência.

O uso de smartphones e VPN para acesso a sistemas internos deve ser solicitado individualmente por cada Colaborador à área de TI.

Os Colaboradores têm o dever de relatar prontamente à área de TI qualquer fato ou ameaça à segurança dos ativos e recursos tecnológicos do Grupo Vinci, tais como quebra da segurança, fragilidade, mau funcionamento, vírus, suspeita de intercepção de mensagens eletrônicas, de acesso indevido e desnecessário a diretórios de rede, acesso indevido à Internet e programas eventualmente instalados sem conhecimento da área de TI.

4.3. Atribuições do Departamento de Compliance relacionadas à Segurança da Informação

Sem prejuízo das demais atribuições do Departamento de Compliance estabelecidas no Manual de Compliance, são atribuições do Departamento de Compliance:

- Supervisionar, apoiar e determinar controles para que informações relativas ao negócio do Grupo Vinci sejam confiáveis e auditáveis, em conformidade com as legislações e regulamentações aplicáveis nas regiões onde existam operações da organização.
- Assegurar que o controle de acesso aos sistemas e registros do Grupo Vinci atenda às legislações e regulamentações vigentes nos territórios onde existam operações da organização.
- Assegurar que os sistemas de controle de acesso e gravações de ramais estejam íntegros e sejam corretamente controlados.
- Assegurar a aplicação de procedimentos internos para tratar de casos de vazamento de informações confidenciais, reservadas ou privilegiadas.

Cabe ao Diretor de Compliance autorizar a consulta de informações aos sistemas de controle de acesso físico.

Cabe ao Diretor de Compliance e ao CEO do Grupo Vinci autorizarem a escuta de gravações de outro usuário ou a gravação de conversas telefônicas para mídia externa, em atendimento a eventuais solicitações das autoridades competentes.

Para realização dos testes necessários à comprovação da integridade dos registros de gravação de ramais, o Head do Departamento de Compliance poderá selecionar dias e ramais aleatórios para escuta de gravações. O Departamento de Compliance é obrigado a atender os mesmos critérios de acesso das outras áreas, no entanto, é dispensada a necessidade de qualquer autorização prévia.

Em caso de vazamento de informações confidenciais, reservadas ou privilegiadas, mesmo que em razão de ação involuntária, será emitido um alerta aos Colaboradores relacionado ao vazamento de informações e o Comitê de Segurança Cibernética avaliará o impacto de tal

vazamento para Terceiros e os investidores do Grupo Vinci, bem como para as atividades que desenvolve.

5. Segurança Cibernética

O Grupo Vinci possui sistemas e procedimentos de segurança cibernética para identificação, prevenção, monitoramento e combate aos riscos e ameaças cibernéticas, conforme detalhado na Política de Segurança Cibernética, anexa a esta Política.

6. Canais Digitais para Investidores (Vinci online)

O Grupo Vinci disponibiliza aos seus investidores, senhas de acesso individuais a um canal digital disponível em seu website www.vincipartners.com, o Vinci online. Além de possibilitar a comunicação com o investidor, o acesso às informações é feito por canal criptografado e o acesso às informações armazenadas é de forma restrita.

A senha de acesso ao Vinci online é pessoal e intrasferível e não deve ser compartilhada com terceiros, sendo que as mesmas somente serão desbloqueadas mediante confirmação de dados do investidor, tais quais os dados pessoais e cadastrais fornecidos ou o histórico de operações do cliente.

O sistema Vinci online possui trilhas de auditoria para assegurar o rastreamento das operações realizadas pelos investidores, de forma a verificar:

i. A identificação do usuário;
ii. Data e horário da operação; e
iii. A identificação da operação realizada.

O período de retenção das trilhas de auditoria é de 5 (cinco) anos.

7. Treinamento e Capacitação

A área de TI, com o auxílio do Departamento de Compliance, deve estruturar programa de conscientização, educação e treinamento em Segurança da Informação direcionado para a proteção dos objetivos, boas práticas internas, conceitos e diretrizes definidas nesta política.

Sua realização deve ter periodicidade anual ou com renovação em decorrência de evento interno significativo que justifique o reforço antecipado do ciclo de conhecimento em segurança da informação.

8. Penalidades

Após a divulgação interna a todos os Colaboradores, o cumprimento desta política passa a ser formalmente mandatório. O compromisso de todos os Colaboradores é essencial para atender os objetivos de segurança dos negócios do Grupo Vinci.

O descumprimento desta política é considerado falta grave passível de punição de acordo com as sanções previstas nas disposições contratuais, procedimentos e regulamentos internos, assim como na legislação aplicável, podendo gerar, inclusive, desligamento ou demissão por justa causa do Colaborador.

9. Revisão e Atualização

A presente política será revisada em períodos não superiores a 24 (vinte e quatro) meses ou sempre que for necessário.

10. Documentos Relacionados

A presente Política contempla os seguintes anexos que regulam matérias específicas relacionadas à Segurança da Informação:

- Procedimentos de Solicitação e Uso de Dispositivos de TI;
- Procedimentos de Concessão de Acesso Lógico;
- Procedimentos de Concessão de Acesso Físico;
- Procedimentos de Concessão de Acesso Remoto;
- Procedimentos de Serviços em Nuvem;
- Procedimentos de Uso dos Sistemas de Mensageria;
- Regras e Procedimentos de Uso de Correio Eletrônico (E-mail);
- Regras e Procedimentos de Uso da Internet;
- Regras e Procedimentos de CFTV;
- Regras e Procedimentos de Gravação de Ramais;
- Política de Segurança Cibernética.

11. Referências

ISO 27001:2013 – Information technology - Security techniques - Information security management systems – Requirements

12. Glossário

AD	Active Directory – Serviço de diretórios da rede Microsoft, utilizado para autenticação e registro de usuários.
ANTISPAM	Tecnologia que observa, categoriza, filtra e elimina e-mails com conteúdo impróprio, vírus, propaganda e tipos de mensagens que não sejam autorizadas pela organização.
ANTIVÍRUS	Tecnologia que supervisiona os ativos de tecnológicos com o objetivo de identificar e remover ameaças provenientes da Internet.
ATIVO	Objeto tangível ou não que possua valor para a organização tais como equipamentos, sistemas, documentos, reputação, pessoas, etc.
BACKUP	Ação de copiar dados de um sistema ou ambiente de produção para um ambiente paralelo com o objetivo de permitir a recuperação dos dados em caso de necessidades.
CFTV	Sistema de supervisão e gravação de imagens.
CFO	Chief Financial Officer.
CONFIDENCIALIDADE	Propriedade das informações que só podem ser disponibilizadas ou divulgadas a indivíduos, grupos de trabalho ou entidades autorizadas.
CRIPTOGRAFIA	Conjunto de princípios e técnicas empregadas para cifrar a escrita com o objetivo de torná-la ininteligível para quem não tenha acesso a chave para leitura do conteúdo da informação.
DISPONIBILIDADE	Propriedade das informações estarem acessíveis e utilizáveis para uma entidade autorizada.
GOVERNANÇA	Estabelecimento de políticas e do monitoramento contínuo da sua correta aplicação.
HD	Disco rígido (hard disk) de computador.

HEAD	Chefe da área do solicitante.
INTEGRIDADE	Propriedade que assegura exatidão e integridade das informações.
ITS	IT Service Desk. Área de TI responsável por atender as solicitações de usuários.
MALWARE	Softwares (programas de computador) maliciosos, com o objetivo de roubar ou destruir dados.
NUVEM (CLOUD)	Fornecimento de recursos externos de tecnologia que possibilita o armazenamento, processamento e troca de informações por meio de recursos compartilhados. Os dados inseridos na Nuvem (Cloud) são acessíveis a dispositivos conectados à Internet que tenham usuário e senha válidos.
PLUG-IN	Componente de software que adiciona um recurso específico para um programa, sistema ou aplicação de computador existente. Exemplos de plug-ins são os aplicativos de segurança de bancos, flash, Java, Wordpress, etc.
PROXY	Tecnologia que controla e registra os acessos feitos a Internet provenientes de usuários e equipamentos.
RDP	Remote Desktop Protocol – Protocolo de acesso remoto às máquinas Windows, onde a console (desktop) da estação é transmitida remotamente.
RH	Área de Recursos Humanos.
SHARE	Diretório/folder compartilhado via rede.
TI	Área de Tecnologia da Informação.
URL	Uniform Resource Locator – Sequência de texto que especifica onde um recurso pode ser encontrado na Internet (o mesmo que “site” ou “link”). Ex: http://www.google.com
VPN	Tecnologia que cria uma conexão criptografada entre dois pontos, provendo um meio de comunicação seguro entre os ativos envolvidos na transmissão de dados.

TERMO DE COMPROMISSO

Por meio deste instrumento, eu [Nome Completo], inscrito[a] no CPF/MF sob o nº [x], declaro para os devidos fins que**:**

1. Recebi a Política de Segurança da Informação do Grupo Vinci, bem como seus anexos ("**Política de Segurança**"), cujas regras e políticas me foram previamente explicadas e em relação às quais tive a oportunidade de esclarecer todas as minhas dúvidas.

2. Li, compreendi e possuo total ciência de todas as regras, procedimentos e disposições estabelecidas na Política de Segurança e documentos relacionados, bem como me comprometo a observar integralmente todos os seus termos e obrigações.

3. Estou ciente de que a não observância da Política de Segurança poderá caracterizar falta grave, passível de punição de acordo com as sanções previstas nas disposições contratuais, procedimentos e regulamentos internos, assim como em penalizações previstas em lei, inclusive desligamento, exclusão ou demissão por justa causa.

4. Comprometo-me a informar imediatamente à área de TI, assim que tiver ciência, qualquer fato ou ameaça à segurança dos ativos e recursos tecnológicos do Grupo Vinci, nos termos da Política de Segurança.

[Rio de Janeiro ou São Paulo], [data].

_____

[Nome completo]

VINCI partners

Rio de Janeiro
55 21 2159 6000
Av. Bartolomeu Mitre, 336
Leblon - 22431-002

São Paulo
55 11 3572 3700
Av. Brigadeiro Faria Lima, 2.277
14º andar - Jd. Paulistano - 01452-000

Recife
55 81 3204 6811
Av. República do Líbano, 251 - Sala 301
Torre A - Pina - 51110-160

Nova York
1 646 559 8000
535 Madison Avenue - 37th Floor
10022 New York - NY