Política de Segurança da Informação

INVESTCORP
REAL ESTATE

SUMÁRIO

Aproveite seu *e-book*

Clique em cada item do sumário para acessar o capítulo/item desejado

Clique para voltar ao sumário

Clique para voltar à página anterior

Clique para ir para a próxima página

Projeto gráfico e diagramação:
Immaginarte! /immaginartes

Foto/ Capa:
Depositphotos

Ilustrações:
Upklyak • Vectorjuice • Fullvector
Jcomp • Vectorpouch •
Macrovector • Pch.vector •
Katemangostar/ Freepik

1. Objetivo

A Política de Segurança da Informação é uma declaração formal da InvestCorp acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus funcionários.

2. Abrangência

Todos os funcionários, diretores, executivos, sócios, prestadores de serviços, consultores, auditores, temporários, fornecedores, parceiros diversos e demais contratados que estejam a serviço e disponibilizam de ativos corporativos da InvestCorp, suas Unidades, subsidiárias e/ou coligadas.

3. Missão

Garantir a integralidade, confidencialidade, legalidade e autenticidade da informação necessária para a realização dos negócios da InvestCorp.

4. Diretrizes

4.1. Diretrizes de segurança da informação

Conforme definição da norma NBR ISO/IEC 17799:2005, a informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e, consequentemente, necessita ser adequadamente protegida. A Política de Segurança da Informação objetiva proteger a informação de diversos tipos de ameaça, para garantir a continuidade dos negócios minimizando os danos maximizando o retorno dos investimentos e as oportunidades de negócio.

A Segurança da informação é aqui caracterizada pela preservação da:

a) Confidencialidade, que é a garantia de que a informação é acessível somente a pessoas com acesso autorizado.

b) Integridade, que é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

c) Disponibilidade, a Política de Segurança da Informação deve ser divulgada a todos os funcionários e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento.

Para assegurar esses três itens mencionados, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não-intencional, acidentes e outras ameaças.

É fundamental para a proteção e salvaguarda das informações que os usuários adotem a ação de Comportamento Seguro e consistente com o objetivo de proteção das infor-

mações, devendo assumir atitudes proativas e engajadas no que diz respeito à proteção das informações.

A Política de Segurança da Informação da InvestCorp é aprovada e revisada anualmente pela Diretoria Executiva.

4.2. Atribuições e responsabilidades na gestão de Segurança da Informação

4.2.1. Definição

Cabe a todos os colaboradores (funcionários, estagiários e prestadores de serviços) cumprir fielmente a Política de Segurança da Informação; buscar orientação do gestor imediato em caso de dúvidas relacionadas à Segurança da informação; proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados; assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela InvestCorp.

4.2.2. Diretorias, Gerências e Coordenações

Cabe às Diretorias, Gerências e Coordenações cumprir e fazer cumprir esta Política; assegurar que suas equipes possuam acesso e conhecimento desta Política de Segurança da Informação; e comunicar imediatamente eventuais casos de violação de segurança da informação através do canal de denúncia.

4.2.3. Área de TI e Governança Corporativa

Cabe as duas áreas propor ajustes, melhorias, aprimoramentos e modificações desta Política; convocar, coordenar, lavrar atas e prover apoio às reuniões que discutam a respeito desta Política; prover todas as informações de gestão de segurança da informação solicitadas por Gestores.

4.3. Engenharia social

Engenharia Social é um termo utilizado para representar a habilidade de enganar pessoas, visando obter informações sigilosas.

A Engenharia Social manifesta-se de diversas formas, e podemos dividi-los em dois grupos. No entanto, o grande ponto onde engenheiros sociais se baseiam é na falta de conscientização do usuário com relação à Segurança da Informação e na exploração da confiança das pessoas para a obtenção de informações sigilosas e importantes, e como uma simples informação poderia trazer prejuízo à empresa:

- Diretos: São aqueles caracterizados pelo contato direto entre o engenheiro social e a vítima através de telefonemas e até mesmo pessoalmente, pois engenheiro social nem sempre é alguém desconhecido.

- Indiretos: Caracterizam-se pela utilização de softwares ou ferramentas para invadir, como, por exemplo, vírus, cavalos de Tróia ou através de sites e e-mails falsos para assim obter informações desejadas.

4.4. Classificação da informação

É de responsabilidade do Gerente/Supervisor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com os critérios a seguir:

- Pública: É uma informação da InvestCorp ou de seus clientes com linguagem e formato dedicado à divulgação ao público em geral;

- Interna: É uma informação da InvestCorp que ela não tem interesse em divulgar, onde o acesso por parte de indivíduos externos à empresa deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem da Organização;

- Confidencial: É uma informação crítica para os negócios da InvestCorp ou de seus clientes. A divulgação não autorizada dessa informação pode causar impactos de ordem financei-

ra, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais à InvestCorp ou aos seus clientes.

- Restrita: É toda informação que pode ser acessada somente por usuários da InvestCorp explicitamente indicado pelo nome ou por área a que pertence.

5. Boas práticas

5.1. Comunicação verbal dentro e fora da empresa

- Cuidado ao tratar de assuntos da empresa dentro e fora do ambiente de trabalho em locais públicos, ou próximos a visitantes, seja ao telefone ou com algum colega, ou mesmo fornecedor.

- Evite nomes e tratativas de assuntos confidenciais, nestas situações, fora da empresa ou próximos a pessoas desconhecidas.

- Caso seja extremamente necessária a comunicação de assuntos sigilosos em ambientes públicos, ficar atento as pessoas à sua volta que poderão usar as informações com o intuito de prejudicar a imagem da empresa.

- Todo acesso às informações e aos ambientes lógicos deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas através de senhas ou outros controles de acessos.

- As estações de trabalho, incluindo equipamentos portáteis e, informações devem ser protegidos contra danos ou perdas, bem como o acesso, uso ou exposição indevidos.

- As estações de trabalho possuem códigos internos, os quais permitem que sejam identificadas na rede. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do funcionário.

- Evite utilizar o notebook em locais públicos.

- Avalie se em pequenas viagens é realmente necessário levar o notebook.

- A utilização de Notebook de terceiros é proibida, sem autorização da Diretoria e análise de TI.

5.2. Proteção de dados e prevenção de ataques

- Coletar e processar apenas os dados pessoais que são realmente necessários para atingir os objetivos do tratamento para a finalidade pretendida, minimizando a coleta de dados.

- Implementar soluções de pseudonimização, como a criptografia, para cifrar dados pessoais.

- Evitar a transferência de dados pessoais de estações de trabalho para dispositivos de armazenamento externo, como pendrives e discos rígidos externos

- manter documentos físicos que contenham dados pessoais dentro de gavetas, e não sobre as mesas;

- Formatar e sobrescrever mídias físicas que contenham dados pessoais antes de descartá-las, ou, quando não for possível a sobrescrita, destruir as mídias físicas.

- não compartilhar logins e senhas de acesso das estações de trabalho;

- bloquear os computadores quando se afastar das estações de trabalho, para evitar o acesso indevido de terceiros;

- Atualizar periodicamente todos os sistemas e aplicativos utilizados, mantendo-os em sua versão atualizada.

- Adotar e atualizar periodicamente softwares antivírus e antimalwares.

5.3. Impressões

- Documentos enviados para impressão deverão ser retirados imediatamente.

- A impressão de documentos sigilosos deve ser feita sob supervisão do responsável.

5.4. Instalação de softwares

- Qualquer software que, por necessidade do serviço, necessitar ser instalado deverá ser comunicado à Diretoria ou área

de Suporte Técnico e aprovado, para que o mesmo possa ser homologado pelos responsáveis de TI e só assim serem disponibilizados para a área requerente.

- A empresa respeita os direitos autorais dos softwares que usa e reconhece que deve pagar o justo valor por eles, não recomendando o uso de programas não licenciados nos computadores da empresa. É terminantemente proibido o uso de softwares ilegais (sem licenciamento) na InvestCorp.

- A Diretoria poderá valer-se deste instrumento para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso, em atendimento à Lei 9.609/98 (Lei do Software).

6. Diretrizes quanto ao uso da rede corporativa

- Material sexualmente explícito não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede corporativa.

- Todos os arquivos devem ser gravados na rede, pois arquivos gravados no computador (local) não possuem cópias de segurança (backup) e podem ser perdidos.

- Não é permitida a gravação de arquivos particulares (músicas, filmes, fotos, etc.) nos drivers de rede, pois ocupam espaço comum limitado do departamento.

7. Diretrizes quanto ao uso de mídias removíveis e da porta USB

- É vedado aos usuários utilizarem as mídias removíveis como meio preferencial de armazenamento de informações corporativas.

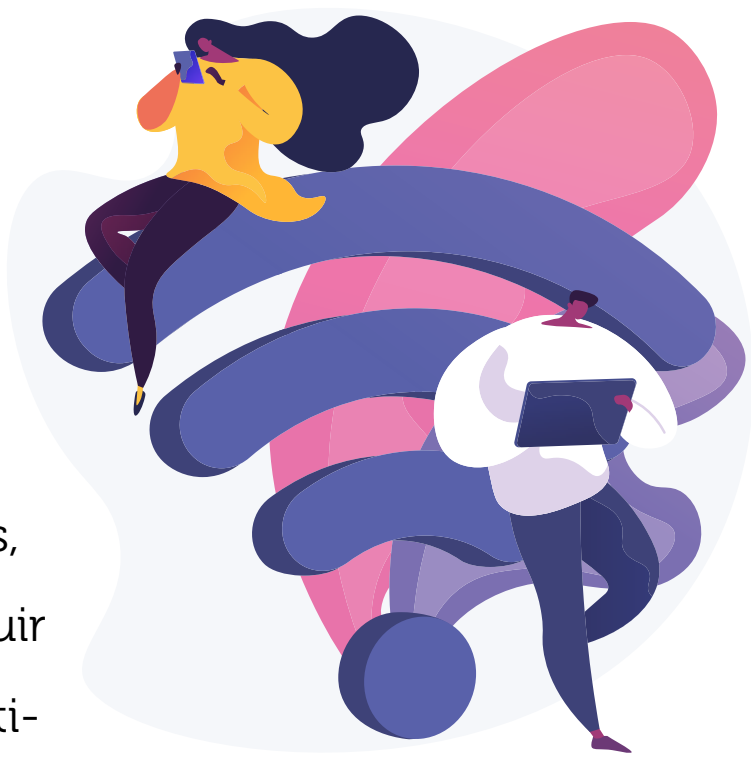
- O uso de mídias removíveis na empresa não é estimulado, devendo ser tratado como exceção à regra.

- A porta Usb é o principal ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de informações corporativas confidenciais, neste caso, os modens 3G e os pen drives merecem atenção.

- Dentro da empresa dê preferência à utilização da rede evitando a utilização de modem 3G conectado à porta Usb do notebook, pois é considerada uma forma de burlar a segurança de rede, protegida por Firewall e regras de segurança. Assim o funcionário abre a porta para acesso sem qualquer controle.

- Os usuários de mídias removíveis são diretamente responsáveis pelos riscos e impactos que o uso de tais dispositivos possa vir a causar nos ativos de informação, pois este tipo de mídia pode conter vírus e softwares maliciosos podendo danificar e corromper dados.

8. Diretrizes quanto ao uso da internet



- A Internet deve ser utilizada APENAS para fins corporativos, enriquecimento intelectual ou como ferramenta de busca de informações, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas à empresa.

- O acesso às páginas e web sites é de responsabilidade de cada usuário ficando vedado o acesso a sites com conteúdo impróprio e de relacionamentos.

- O uso da internet para assuntos pessoais deve ser restrito, sem comprometer as atividades dos usuários.

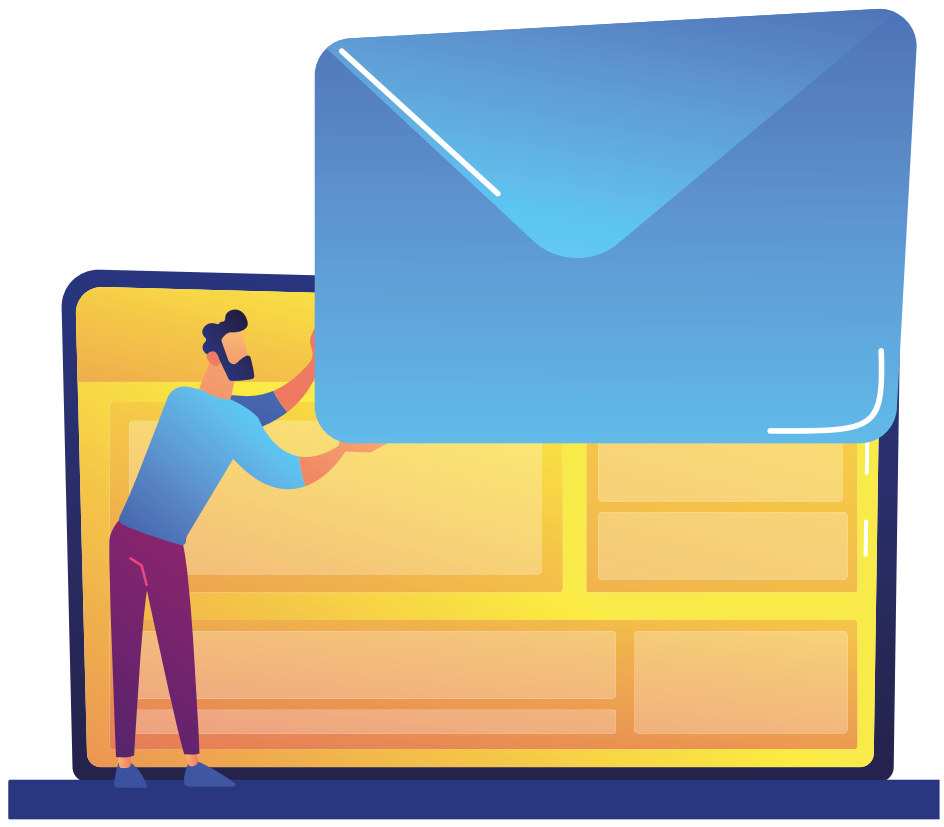
- É vedado qualquer tipo de download. Como também o upload de qualquer software licenciado à empresa ou de dados de propriedade da empresa ou de seus clientes, sem expressa autorização da Diretoria ou de TI.

- Os acessos à internet serão monitorados através de identificação e autenticação do usuário.

9. Diretrizes quanto ao uso do e-mail

- É vedado o uso de sistemas webmail externo. O uso do correio eletrônico para envio e recepção de e-mail deverá ocorrer apenas através do correio eletrônico da InvestCorp.

- É proibido o uso do Correio Eletrônico para envio de mensagens que possam comprometer a imagem da empresa perante seus clientes e a comunidade em geral e que possam causar prejuízo moral e financeiro.



- Evitar utilizar o e-mail da empresa para assuntos pessoais.

- Assegurar a propriedade de todas as mensagens geradas internamente e/ou por meio de recursos de comunicação e definir o uso desses recursos como ferramenta de comunicação e aumento de produtividade, devendo ser usado prioritariamente para atividades de negócio e podendo ser monitorado por ser propriedade da empresa e até mesmo vistoriado por direitos de verificação e auditoria.

- Não executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Exemplo de extensões que não devem ser abertas: .bat., .exe., .scr., .link e .com, ou de quaisquer outros formatos alertados.

- Não utilizar o e-mail para enviar grande quantidade de mensagens (spam) que possam comprometer a capacidade da rede, não reenviando e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/Symantec, criança desaparecida, criança doentes, materiais preconceituosos ou discriminatórios e os do tipo boatos virtuais, etc.

- A utilização do e-mail/webmail da empresa fora do horário de trabalho para posições que possuam controle/reporte de jornada deve ser aprovado pela Diretoria da empresa.

- Antivírus dos servidores e estações são atualizados automaticamente. A varredura por vírus é feita diariamente nas estações e nos servidores.

10. Diretrizes quanto ao uso da VPN

- O usuário com acesso ao VPN deve restringir o uso do acesso via VPN para as finalidades relacionadas aos negócios, devendo abster-se de usar a funcionalidade para quaisquer outras atividades.

- É vedado aos usuários do serviço compartilhar credenciais de acesso via VPN com quem quer que seja, ou de acessar ele próprio o recurso VPN e conceder o uso da sessão a quaisquer outros funcionários.

- O acesso VPN implica em riscos para a rede corporativa, uma vez que com ele é possível acessar à mesma, de forma privilegiada, a partir de qualquer ponto da internet, como se o usuário estivesse fisicamente nas instalações das empresas abrangidas neste procedimento.

- Nunca deixar sessões VPN abertas. Cada vez que o usuário deixar o seu equipamento conectado via VPN, deve executar logoff ou bloquear seu equipamento.

- Manter-se conectado à rede via acesso VPN apenas pelo tempo necessário à execução da tarefa que requereu o uso do serviço.

11. Violações da Política de Segurança da Informação e sanções

- Nos casos em que houver violação desta política, sanções administrativas e/ou legais poderão ser adotadas, sem prévio aviso, podendo culminar com o desligamento e eventuais processos, se aplicáveis.

- O funcionário infrator poderá ser notificado e a ocorrência da transgressão imediatamente comunicada ao seu gestor imediato, à diretoria correspondente e à Presidência.

12. Vigência e validade

A presente política passa a vigorar a partir da data de sua publicação, sendo válida por tempo indeterminado.

1º de dezembro de 2021.

INVESTCORP
REAL ESTATE

Av. Ibirapuera, 2144 – conjuntos 41 e 42
CEP 04028-001 – Moema – São Paulo, SP

+55 11 5055-4441

contato@InvestCorp.com.br

www.InvestCorp.com.br