POLÍTICA DE SEGURANÇA E OPERAÇÃO DO SISTEMA DE INFORMAÇÕES

Índice

1. Âmbito

A Política de Segurança e Operação do Sistema de Informações da Inovadora Capital (SVDM), baseia-se na norma ISO/IEC 27001, através da consciencialização e definição das regras e procedimentos necessários para proteger a confidencialidade das informações.

A Política de Segurança e Operação do Sistema de Informações articula-se com um conjunto de controlos e mecanismos que garantem a integridade e segurança da estrutura de gestão de acessos na qual exista o trafego de informações e dados comuns e/ou restritos, incluindo os equipamentos que armazenam tais informações.

2. Glossário

Termos e Definições	Descrição
Activo de Informação	Qualquer componente (seja humano, tecnológico, software…) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio, onde informações são criadas, processadas, armazenadas, transmitidas ou descartadas.
Activos	É tudo aquilo de tem valor para a instituição.
Autenticação	Propriedade de um sistema que permite identificar quem pode aceder um determinado objecto (como um sistema, arquivo ou instalação) por meio da combinação correcta do nome de utilizador e sua senha de acesso.
Backup [Cópia de Segurança]	Cópia de dados de um dispositivo de armazenamento para outro, permitindo assim, que os mesmos possam ser restaurados em caso de perda dos dados originais.
Backup Completo, Full, Total ou Normal	Faz o backup na íntegra de todos arquivos e directórios seleccionados para a média de backup.
Backup Diferencial	É um backup cumulativo de todos arquivos criados ou alterados desde o último backup completo.
Backup Incremental	É feito o backup apenas dos arquivos criados ou alterados desde o último backup completo ou incremental.
Backup -Período de retenção	Tempo em que os dados ficam guardados, após este período, são descartados, libertando o espaço de armazenamento ocupado, em espaço para novos backups.
BCM [Business Continuity Management / GCN (Gestão de Continuidade de Negócio)]	Processo holístico de gestão que identifica ameaças potenciais para uma organização e os impactos para as operações de negócio que essas ameaças, caso se concretizem, podem causar, e que fornece um framework para uma construção organizacional resiliente com a capacidade para uma resposta eficaz, que salvaguarde os interesses de seus actores principais, a reputação da marca, e actividades de criação de valor.

Código-fonte	É o conjunto de palavras ou símbolos escritos de forma ordenada, contendo instruções em uma das linguagens de programação existentes, de maneira lógica. Após ser compilado, o código fonte transforma-se em software, ou seja, programas executáveis.
Confidencialidade	Propriedade da informação que garante que a mesma não estará disponível ou divulgada a indivíduos, entidades ou processos sem autorização, ou seja, é a garantia do resguardo das informações dadas pessoalmente em confiança e protecção contra a sua revelação não autorizada.
Continuidade de negócio	Capacidade estratégica e táctica da organização para planear e responder a incidentes e interrupções de negócio, com objectivo de continuar as operações de negócio num nível aceitável pré-definido.
Dados	Conjunto de valores ou ocorrências em um estado bruto com o qual são obtidas informações com o objectivo de adquirir benefícios.
Data Center	Instalação que centraliza as operações e equipamentos de TI de uma organização, bem como armazenamento, gestão e disseminação seus dados.
Disponibilidade	Propriedade que garante que a informação esteja disponível sempre que requisitada pelos utilizadores autorizados mesmo com as interrupções involuntárias de sistemas, ou seja, não intencionais.
Informação	Reunião ou conjunto de dados e conhecimentos organizados que possam constituir referências sobre um determinado acontecimento, facto ou evento. Este conhecimento pode ser registrado em forma impressa, digital, oral ou audiovisual.
Integridade	Propriedade que garante que a informação não seja adulterada falsificada ou furtada.
ISO / IEC	Comité técnico conjunto da Organização Internacional para Padronização (ISO) e da Comissão Electrotécnica Internacional (IEC), sua finalidade é desenvolver, manter e promover padrões nas áreas de tecnologia da informação (TI) e Tecnologia da Informação e Comunicação (TIC).
ISO/IEC 27001	Especifica os requisitos para estabelecer, implementar, operar, monitorar, rever, manter e melhorar um sistema de gestão de segurança da informação de acordo com as necessidades específicas de cada organização.
ISO/IEC 27002	É um padrão de segurança da informação, denominado: Técnica de segurança - Código de prática para controlos de segurança da informação. Funciona como um guia completo de implementação, em que descreve quais controlos devem ser estabelecidos e de que forma. Ela tem como base uma avaliação de riscos dos activos mais importantes da empresa.

ISO/IEC 27005	é o padrão internacional que lida com o gerenciamento de riscos de segurança da informação. A norma fornece directrizes para o gerenciamento de riscos de segurança da informação em uma empresa, apoiando particularmente os requisitos do sistema de gerenciamento de segurança da informação definido na ISO 27001.
Log / Logs	Expressão utilizada para descrever o processo de registro de eventos relevantes num sistema computacional.
MFA [Multi-Factor Authentication / Autenticação Multifactor]	É uma solução de autenticação de dois factores que fornece aos utilizadores e administradores uma segunda camada de verificação ao efectuar logon em aplicativos ou portais. O MFA possui duas ou mais maneiras de verificação de acesso, a autenticação é comprovada através de Senha, Dispositivos móveis ou factores presentes no próprio usuário como Biometria.
Política de Segurança da Informação	Conjunto de acções, técnicas e boas práticas relacionadas ao uso seguro de dados, ou seja, trata-se de um documento que determina as acções mais importantes para garantir a segurança da informação.
Programa Utilitário	É um pequeno programa que fornece uma adição aos recursos fornecidos pelo sistema operativo.
Proprietário do Activo	Indivíduo ou entidade que detém a gestão e a responsabilidade pelo controlo de todo o ciclo de vida do activo.
RTO [Recovery Time Objective]	Objectivo de tempo de recuperação, em que o banco sol pode estar sem operar enquanto se efectuam os restauros dos serviços e aplicações para a continuidade dos serviços do Banco.
SIEM [Security Information and Event Management / Gerenciamento e Correlação de Eventos de Segurança]	É uma solução de segurança e auditoria composto por componentes de monitoramento e análise de eventos.
SLA [Service Level Agreement]	Compromisso assumido por um prestador de serviços de TI perante um cliente. Este compromisso descreve o serviço de TI, os níveis de qualidade que devem ser garantidos, as responsabilidades das partes e eventuais compensações quando os níveis de qualidade não forem atingidos.
SOC [Security Operations Center / Centro de Operações de Segurança]	é um termo genérico que descreve parte ou a totalidade de uma plataforma cujo objectivo é prestar serviços de detecção e reacção a incidentes de segurança a informação.
Token	Dispositivo electrónico gerador de senhas, geralmente sem conexão física com o computador, podendo também em algumas versões, ser conectado a uma porta USB.

2. Objectivo

A Política de Segurança e Operação do Sistema de Informações tem como principal objectivo proteger as informações internas e confidenciais para a continuidade do negócio da organização, padronizando e estabelecendo requisitos mínimos de segurança. Garantir a protecção das informações entre clientes e a Inovadora Capital (SDVM) nos aspectos de confidencialidade, integridade, disponibilidade, autenticidade, não repúdio e conformidade.

3. Funções e Responsabilidades

- **Administração do Topo** – Assegurar que os objectivos da política estejam alinhados com os objectivos estratégicos da Inovadora Capital (SDVM). Aprovar a política.
- **Gabinete de Auditoria** – Baseia-se na política para testar os controlos dos processos e procedimentos inerentes a política.
- **Gabinete de Gestão de Risco** – Identificar, avaliar, controlar, mitigar e monitorar os riscos inerentes a operacionalização da política.
- **Gabinete de Compliance** – Verificar a conformidade da política com as normas vigentes no país.
- **Todas as unidades de Estrutura** – Implementação da política.

4. Comprometimento

4.1. Comprometimento dos Responsáveis Hierárquicos

- Apoiar e zelar pelo cumprimento da Política de Segurança e Operação do Sistema de Informações, servindo como modelo de conduta para os colaboradores sob a sua gestão;
- Atribuir na fase de contratação e de formalização dos contractos individuais de trabalho, prestação de serviços ou de parceria, a responsabilidade do cumprimento Política de Segurança e Operação do Sistema de Informações;
- Sensibilizar os utilizadores sobre os princípios e procedimentos de Segurança da Informação;
- Notificar imediatamente o responsável da TI, de quaisquer vulnerabilidades e ameaças na quebra de segurança;
- Adaptar os processos, procedimentos e sistemas sob sua responsabilidade para atender as Políticas de Segurança.

4.2. Comprometimento dos Utilizadores

- Respeitar as Políticas de Segurança da Informação;
- Responder pela guarda e protecção dos activos de informação colocados à sua disposição para o exercício das suas funções;
- Responder pelo uso exclusivo e intransmissível de suas senhas de acesso;
- Relatar prontamente ao responsável da TI, qualquer facto ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, presença de vírus, etc.;
- Assegurar que as informações e dados de propriedade da Inovadora Capital (SDVM), não sejam disponibilizadas a terceiros, a não ser com autorização do Conselho de Administração;
- Responder pelo prejuízo ou dano que vier a provocar a Inovadora Capital (SDVM) ou a terceiros, em decorrência da não obediência às directrizes aqui referidas.

4.3. Comprometimento do Departamento Administrativo e serviços Gerais

- Configurar os equipamentos e sistemas para cumprir os requisitos das Politicas de Segurança da Informação;
- Administrar, proteger e testar as cópias de segurança dos programas e dados críticos do negócio Inovadora Capital (SDVM);
- Gerir o descarte de informações a pedido dos utilizadores;
- Garantir que as informações nos computadores sejam removidas antes da saída ou mudança do utilizador;
- Proteger todos os activos de informação da Inovadora Capital (SDVM) contra códigos maliciosos e ou vírus;
- Garantir que processos de mudança não permitam vulnerabilidades ou fragilidades no ambiente de produção;
- Definir as regras formais para instalação de software e hardware, exigindo o seu cumprimento dentro Inovadora Capital (SDVM);
- Gerir o uso, manuseio e guarda de assinaturas e certificados digitais; Instalar sistemas de protecção, preventivos e reactivos, para garantir a segurança das informações;
- Implementar sistemas de monitorização dos componentes da rede de modos a identificar utilizadores e respectivos acessos efectuados, bem como a informação manipulada;
- Monitorizar no ambiente de TI a capacidade instalada da rede e dos equipamentos, tempo de resposta no acesso à internet e aos sistemas críticos da Inovadora Capital (SDVM), indisponibilidade aos sistemas críticos, actividade de todos os colaboradores durante os acessos às redes externas, inclusive internet.

5. Segurança da Informação

5.1. Protecção da Informação

- Toda informação relacionada às operações da Inovadora Capital (SDVM), gerada ou desenvolvida na sua unidade de estrutura, durante a execução de actividades por prestador de serviços externos constitui um activo da Inovadora Capital (SDVM), essencial à condução de negócios e em última análise, à sua existência.
- Independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada.
- O acesso, modificação, divulgação e destruição devem ser efectuados apenas sob autorização do Conselho de Administração.
- A regra é que toda informação, propriedade da Inovadora Capital (SDVM), seja protegida de riscos e ameaças que possam comprometer a **Confidencialidade, Integridade, Disponibilidade, Autenticidade, Não Repudio e Conformidade.**

5.2. Manuseio de Informações

- O manuseio de toda informação produzida na Inovadora Capital (SDVM) rege-se pela política de classificação da informação.
- Nenhuma das informações internas e confidenciais podem ser repassadas para terceiros sem consentimento por escrito do Conselho de Administração.
- Qualquer revelação das informações internas e confidenciais deverá estar de acordo com os termos e condições estabelecidos pela Inovadora Capital (SDVM).
- As cláusulas de responsabilidade e confidencialidade quanto à política e directrizes de segurança da informação visam alertar e responsabilizar de que o acesso e o manuseio da informação devem ser restringidos ao exercício da função ou processo que requer essa informação, sendo proibido o uso para qualquer outro propósito distinto do designado.

5.3. Acesso a rede e aos Sistemas de informação

- O Utilizador é totalmente responsável pela correcta posse e utilização de suas senhas e autorizações de acesso aos sistemas, bem como pelas acções decorrentes da utilização destes poderes.
- O acesso e o uso de todos os sistemas de informação, directórios de rede, bancos de dados e demais recursos devem ser restritos a pessoas explicitamente autorizadas e de acordo com a necessidade para o cumprimento de suas funções.
- Periodicamente, os acessos concedidos devem ser revistos pelo Departamento Administrativo Financeiro e Serviços Gerais.
- Não são permitidas tentativas de obter acesso não autorizado, tais como tentativas de defraudar a autenticação do utilizador ou segurança de qualquer activo de rede.
- É obrigatório a manutenção do directório pessoal e password de acesso quer seja no computador pessoal ou no servidor, evitando o acumular de ficheiros ou listagens inúteis;

- Não é permitido a exposição, armazenamento, distribuição, edição de material de natureza pornográfica, racista, xenófoba, religiosa, politica e desportiva, através do uso dos recursos informáticos da Inovadora Capital (SDVM);
- Não é permitido criar e/ou remover arquivos que venham a comprometer o desempenho e funcionamento dos sistemas.
- A pasta PÚBLICO ou similar, não deverá ser utilizada para armazenamento de ficheiros que contenham assuntos sigilosos ou de natureza sensível;
- É expressamente proibida, a cedência do utilizador e palavra passe de acesso a terceiros.
- O sistema periodicamente obriga a alteração da palavra passe do utilizador ou dos serviços aplicacionais.
- É proibido descarregar qualquer pasta e/ou ficheiro para os dispositivos móveis pessoais (Smartphones e/ou Tablet) incluindo dispositivos de armazenamento amovíveis (USB e Discos Externos) que possam colocar em causa a Confidencialidade e Integridade dos dados.

5.4. Controlos de fuga de dados

- Devem ser implementados mecanismos de controlo para prevenir a fuga de dados confidenciais da Inovadora Capital (SDVM) ou dos clientes que possam ser removidos fisicamente ou electronicamente sem autorização prévia.

5. Utilizadores de Acesso á Internet e Correio Eletônico Corporativo

- O uso e acesso do colaborador a internet e correio electrónico corporativo, deverão ser exclusivos para o uso profissional, para a execução e desempenho dos objectivos da Inovadora Capital (SDVM).
- Não é permitido a utilização dos recursos da Inovadora Capital (SDVM) para fazer a descarga (download) ou distribuição de software não licenciados;
- Não é permitido a divulgação de informações internas e confidenciais da Inovadora Capital (SDVM) em grupos de discussão, listas ou chats, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas nas políticas e procedimentos internos e/ou na forma criminal ou cível;
- Não é permitido a utilização de softwares de ponto a ponto;
- Não é permitida a utilização de aplicações de reprodução multimídia na internet.
- O acesso a internet para propósitos particulares ou estranhos a actividades Inovadora Capital (SDVM), poderá ser bloqueada, sem prévia comunicação ao colaborador, sem prejuízo das demais sanções aplicáveis.

6. Penalidades

O não cumprimento desta política constitui falta grave e o utilizador que a viole estará sujeito a acção disciplinar incluindo o despedimento e/ou processo civil e criminal.

7. Revisão e Gestão Documental

Este documento é válido desde o momento da sua aprovação, devendo ser revisto com periodicidade predefinida e quando se verifiquem alterações justificáveis para garantir que se mantenha actualizado.

O proprietário deste documento é o Departamento Administrativo Financeiro e Serviços Gerias, que deve garantir que o mesmo seja revisto pelo menos uma vez por ano.

Ao avaliar a eficácia e adequação deste documento, os seguintes critérios devem ser considerados:

- Comunicação interna na Organização;
- Formação aos utilizadores;
- Revisão e auditoria periódica da política;
- Elaboração da documentação de Procedimentos.

8. Nota de Propriedade e Distribuição

Este documento é propriedade da Inovadora Capital (SDVM), ele pode ser livremente copiado desde que sejam respeitadas as seguintes condições:

- É permitido fazer cópias inalteradas do documento completo ou em partes, contando que esta nota de distribuição seja mantida em todas as cópias, e que a distribuição não tenha fins comerciais.
- Se este documento for distribuído apenas em partes, instruções de como obtê-lo por completo devem ser incluídas.
- É vedada a distribuição de versões modificadas deste documento, bem como a comercialização de cópias, sem a permissão expressa da Inovadora Capital (SDVM).

7. Outorgamento

Elaborado por	Revisto por	Data de Aprovação
Gabinete de Controlo Interno e Auditoria	Conselho de Administração	30-08-2023