Política de segurança da informação

PLANO DE CONTINUIDADE DA SEGURANÇA DA INFORMAÇÃO (PCSI)

Rua Prof. José Leite e Oiticica, 530
Vila Gertrudes - 04705-080
São Paulo, SP - Brasil
T +55 (11) 4040 3514
www.cba-design.com/latam

Sumário

Rua Prof. José Leite e Oiticica, 530
Vila Gertrudes - 04705-080
São Paulo, SP - Brasil
T +55 (11) 4040 3514
www.cba-design.com/latam

1. Objetivo

Garantir a continuidade da confidencialidade, integridade e disponibilidade das informações críticas em situações de incidentes, falhas técnicas, indisponibilidades ou desastres. Este plano estabelece estratégias, responsabilidades e procedimentos para manter as operações essenciais com o menor impacto possível à segurança da informação.

2. Abrangência

Este plano aplica-se a todos os sistemas críticos, plataformas em nuvem (Microsoft 365), servidores em colocation, dados sensíveis e processos operacionais essenciais da empresa.

3. Princípios de Continuidade

Confidencialidade: Garantir que dados confidenciais não sejam acessados indevidamente durante incidentes.

Integridade: Assegurar que as informações não sejam alteradas, corrompidas ou perdidas.

Disponibilidade: Restabelecer rapidamente o acesso seguro aos dados e serviços essenciais.

4. Componentes do PCSI

4.1. Classificação dos Ativos Críticos

Ativo	Tipo	Criticidade	Responsável
Microsoft 365 (e-mails, arquivos)	Nuvem SaaS	Alta	TI
Servidor em colocation (aplicativos internos)	Infraestrutura local	Alta	TI / Fornecedor do colocation
Banco de dados de projetos	Aplicação web	Alta	Líder Técnico
SharePoint (documentos internos)	Nuvem SaaS	Média	Coordenação Administrativa

Rua Prof. José Leite e Oiticica, 530
Vila Gertrudes - 04705-080
São Paulo, SP - Brasil
T +55 (11) 4040 3514
www.cba-design.com/latam

4.2. Estratégias de Continuidade

Evento	Ação Imediata	Tempo Máximo de Restauração (RTO)	Ponto de Recuperação (RPO)
Indisponibilidade do Microsoft 365	Acionamento do suporte Microsoft / Notificação aos usuários	4 horas	1 hora
Falha no servidor em colocation	Acionar o fornecedor / Recuperar via backup	8 horas	4 horas
Perda de acesso por ataque (phishing/ransomware)	Bloqueio de contas / Contenção com SIEM	2 horas	1 hora
Falha de conexão de internet	Acionar contingência via acesso móvel / rede secundária	1 hora	Sem perda

5. Responsabilidades

Head de Projetos e Informação: Coordenação geral e aprovação das estratégias e garantir que todos os planos mantenham os princípios de segurança.

Tech support: Execução técnica dos planos de contingência e restauração.

Todos os Colaboradores: Acionar os responsáveis e seguir orientações em caso de incidente.

6. Comunicação de Incidentes

Toda interrupção significativa deve ser comunicada imediatamente ao responsável pela continuidade. Um relatório com a descrição do incidente, impacto e ações tomadas será emitido após a normalização.

7. Armazenamento e Acesso ao Plano

O PCSI está disponível em local seguro no SharePoint, acessível apenas a membros autorizados.

Cópias são mantidas offline (criptografadas) em local seguro da equipe de TI, com controle de versão.

8. Controle de alterações

Versão	Data	Quem	Anotações
2	04/02/2025	Luis Bartolomei	Aprovação
1	03/12/2024	Thiago Ramiro	Criação

Rua Prof. José Leite e Oiticica, 530
Vila Gertrudes - 04705-080
São Paulo, SP - Brasil
T +55 (11) 4040 3514
www.cba-design.com/latam