Política de Controlos Criptográficos

Gabinete de Tecnologia de Informação (GTI)

Sede, Versão 1

Versão	Data da Emissão	Entrada em Vigor	Aprovado	Entidade Responsável
01	31/03/2021		Comissão Executiva (CE)	GTI

Histórico de revisões

Versão	Revisor	Revisão	Próxima revisão
1	Arson Ribisse	Classificação documental	30/04/2023

P.GTI.03_R1

INTRODUÇÃO

A presente política estabelece as directrizes para a gestão da criptografia da infra-estrutura da Indico Seguros.

a) A Unidade Orgânica responsável por esta política é a Gabinete de Tecnologias de Informação (GTI);
b) Esta política deverá ser revista anualmente para aferir a sua eficácia e a sua conformidade com as melhores práticas. Quaisquer modificações têm necessariamente que ser aprovadas pela Comissão Executiva (CE) mediante proposta do GTI;

CONTROLOS CRIPTOGRÁFICOS

Os controlos criptográficos são escolhidos e implementados de acordo com a classificação de informação e os sistemas usados para o seu manuseamento e transmissão.

A escolha dos sistemas estabelecidos já incorpora funcionalidades de criptografia forte que dão confiança na protecção da informação.

De seguida listamos os softwares utilizados com estas funcionalidade por tipo de aplicação:

- Watcguard VPN usa protocolos SSL para fornecer acesso seguro e confiável a redes e aplicativos corporativos de virtualmente qualquer local remoto conectado à Internet com autenticação de dois fatores.

- Email do Google Workspace standard é criptografado por: Criptografia de Mensagem do Office (OME)/ S/MIME (Secure/Multipurpose Internet Mail Extensions) / Gerenciamento de Direitos de Informação (IRM).

- A Microsoft Cloud fornece tecnologias do lado do serviço que criptografam os dados do cliente em repouso e em trânsito. Por exemplo, para dados de clientes em repouso, o

Microsoft Azure usa o BitLocker e o DM criptografado, e o Microsoft 365 usa BitLocker, criptografia de serviço de armazenamento do Azure, Gerenciamento de chave distribuída (DKM) e criptografia de serviço Microsoft 365. Para os dados do cliente em trânsito, o Azure, o Office 365, o suporte comercial da Microsoft, o Microsoft Dynamics 365, o Microsoft Power BI e o Visual Studio Team Services usam protocolos de transporte seguro padrão do setor, como IPsec (segurança de protocolo Internet) e TLS (Transport Layer Security), entre o Microsoft datacenters e os dispositivos de usuário e os datacenters da Microsoft.

- O site https://www.indicoseguros.co.mz/ possui comunicação encriptada por protocolo seguro SSL de 256 bits.

- Armazenamento de informação em suportes de dados como flash, pens, HDs, SSDs : BitLocker

Encriptação de ficheiros classificados para o exterior por email: Zip (ou equivalente) com password e adicionalmente criptografar o email.

A necessidade de implementação de controlos criptográficos em suporte de dados e ficheiros cabe a cada colaborador da Empresa usando como linha de orientação a necessidade de proteger a informação considerada confidencial ou restrita e o seu risco de segurança de informação.

As chaves geradas internamente são geridas como informação confidencial/uso restrito.

Sempre que algum colaborador encriptar informação classificada como confidencial ou interna na fonte deve partilhar a chave com o Gabinete de Tecnologias de Informação para este a guardar em pasta encriptada gerida por ele descrevendo a data de caducidade e o momento em que se poderá destruir.

Anualmente o Gabinete de Tecnologias de Informação revê as chaves que se encontram activas.

HISTÓRICO DO DOCUMENTO

Revisão Nº	Páginas revistas	Alterações efectuadas	Data	Validação		
				Elabobrou	Aprovação(CE)	Assinaturas
2	Não aplicável	2ª Edição	30/06/2022	GTI	Ruben Chivale Olivio Melembe Nasma Omar	DocuSigned by: BB56AA22FCF9481... DocuSigned by: B9A3310543764452... DocuSigned by: 7A41BCF05F2F42F...