ELABORADOR/ APROVADOR		
RESPONSAVEL		**DATA**
ELABORADOR	Luc Salmon	25/02/2021
APROVADOR	Henri Le Rasle	26/02/2021

Histórico de revisão

Versão	Date	Descrição
1.0	23/02/2021	Versão inicial

1 Introdução

O documento tem como objetivo apresentar o gerenciamento de criptografia.

Também responderá à questão da ISO 27001.

2 MÉTODOS DE CRIPTOGRAFIA

2.1 Certificado SSL

Os certificados do cliente podem ser

- Fornecido pelo cliente e sob sua responsabilidade
- Adquirido pela Ecritel na Global Sign com validade de 1 ano
  A organização é responsável pela vida das chaves e sua revogação
- A expiração do certificado é monitorada 24/7/365

2.2 Backup

2.2.1 Veeam

A Ecritel está usando as funcionalidades do Veeam para proteger alguns de seus backups.

Uma senha de 26 caracteres é definida para cada trabalho. A senha é armazenada no CMDB.

Veeam Backup & Replication usa um algoritmo de criptografia RSA 2048.

2.2.2 Bacula

A Ecritel está usando as funcionalidades do Bacula para proteger alguns de seus backups.

Uma senha de 16 caracteres é definida para cada trabalho.

A implementação usa AES-CBC de 128 bits, com chaves de sessão simétricas de criptografia RSA. O hash do arquivo assinado usa SHA-256.

2.3 Transferência de Dados

A transferência de dados depende dos mecanismos acima para proteger as transações.

Dependendo da classificação dos dados, diferentes medidas se aplicam.

As transferências físicas de dados usando soluções de armazenamento externo não são permitidas.

2.4 Ativos em Trânsito

Os ativos que podem sair das áreas de escritório devem cumprir as seguintes medidas:

- Nenhum armazenamento de dados local é permitido
- Bloqueio automático

A sensibilização das equipes sobre as boas práticas a respeito será realizada (para evitar o armazenamento de informações sensíveis localmente, etc ...).

3 RECOMENDAÇÕES DA ECRITEL

3.1 HTTPS

A Ecritel recomenda o uso das versões mais recentes do TLS, que agora é o TLS 1.3 para acesso HTTPS. No entanto, permitimos o uso dos seguintes protocolos:

- TLSv1.2 TLSv1.3

As seguintes cifras são permitidas:

- ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES128-GCM-SHA256: DHE-RSA-AES256-GCM-SHA384: DHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES256-SHA384: ECDHE -RSA-AES128-SHA256: ECDHE-RSA-AES256-SHA: ECDHE-RSA-AES128-SHA: DHE-RSA-AES256-SHA256: DHE-RSA-AES128-SHA256: DHE-RSA-AES256-SHA: DHE-RSA -AES128-SHA: ECDHE-RSA-DES-CBC3-SHA: EDH-RSA-DES-CBC3-SHA: AES256-GCM-SHA384: AES128-GCM-SHA256: AES256-SHA256: AES128-SHA256: AES256-SHA: AES128 -SHA: OF-CBC3-SH

Dependendo das solicitações do cliente, poderíamos restringir os protocolos e cifras permitidos para tornar o ambiente mais seguro. Isso terá que ser discutido caso a caso.

3.2 RDP

Recomendamos que nossos clientes habilitem a autenticação NLA (Network Level Authentication) para tornar a conexão RDP aos servidores mais segura.

4 Criptografia Interna

A maioria do trabalho e informações utilizadas no trabalho normal de integrantes da ecritel são armazenadas e utilizadas no ecossistema Google Drive / Google Docs. Naturalmente, são protegidos por SSL e outras técnicas de segurança que garantem sua confidencialidade, integridade, e disponibilidade. Armazenar arquivos no Drive em combinação com a proibição de mídias removíveis também elimina riscos provenientes de armazenamento local.

O armazenamento e gerenciamento de chaves de sistemas técnicos é feito usando o sistema Si da ecritel, que usa HTTPS e outros meios para garantir a segurança dos mesmos.
Os outros sistemas não necessitam de armazenamento local de chaves, então usam navegador para gerenciar contas e acessos em sistemas remotos como google drive.

A responsabilidade de manutenção e implementação das medidas criptográficas são do CTO e do Dpto. Ti.