DECLARAÇÃO DE CONTINUIDADE

Visão Geral de Segurança e Continuidade de Negócios

Julho 2022 | Versão 7.3

Í N D I C E

AVISO GERAL

Este documento está sujeito ao controle de governança do Sistema de Gestão de Segurança da Informação (SGSI). As seguintes diretrizes se aplicam a este documento:

- Este documento é controlado como parte da garantia de qualidade do departamento de Segurança da Informação;
- Nenhuma alteração neste documento é permitida sem a aprovação formal do proprietário do documento;
- Este documento é confidencial, controlado quanto suas versões e revisado regularmente;
- Quaisquer dúvidas sobre este documento devem ser encaminhadas ao responsável;
- A distribuição, as modificações e o acesso devem ser avaliados com base na classificação de informações do TMF Group;
- A versão deste documento pode ser encontrada na página inicial;
- Os detalhes da revisão são descritos abaixo;
- Este documento pode estar disponível em vários idiomas; entretanto, a versão em inglês prevalecerá.

CLASSIFICAÇÃO
Public

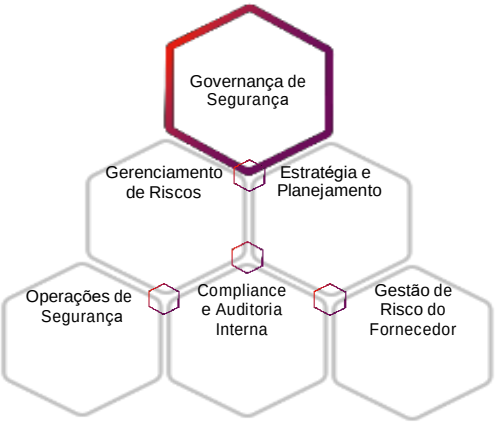
PARTES INTERESSADAS	
Proprietário	Departamento de Segurança da Informação
Titular	Chief Security & Resilience Officer (CSRO)
Aprovado por	Risk and Compliance Committee (RCC)
Patrocinador	Chief Operations & Technology Officer

REVISÃO	
Periodicidade	Anual
Última revisão	22 Junho 2022
Status	Final
Data de aprovação	1 de Julho de 2022
Data de vigência	1 de Julho de 2022

PONTOS DE CONTATO	
Contato	Departamento de Segurança da Informação
Detalhes	Entre em contato com a equipe via security@tmf-group.com

1 . GOVERNANÇA, RISCO E COMPLIANCE

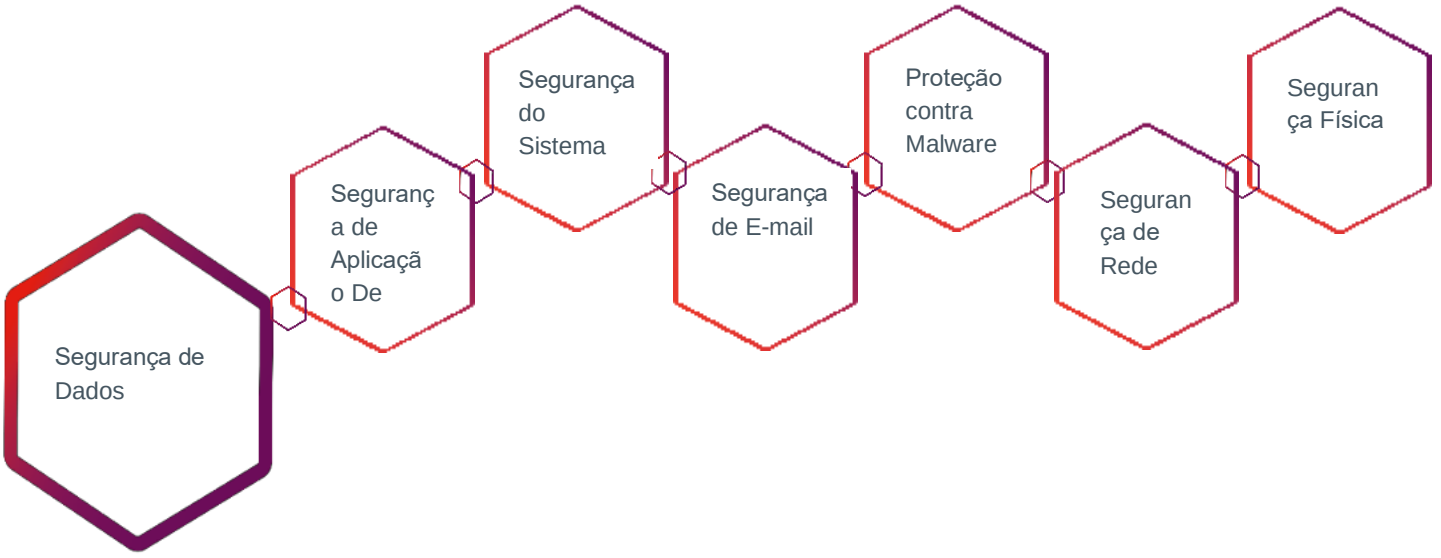
A TMF Group entende a importância e a sensibilidade dos serviços que oferece aos seus clientes em todo o mundo. Dispomos de uma estrutura de garantia de segurança robusta que combina pessoas, processos e tecnologia de ponta para garantir uma operação segura e em compliance.



GOVERNANÇA	O Comitê Executivo (Executive Committee - ExCo - gestão sênior) da TMF é, em última instância, responsável pela Segurança da Informação na TMF Group. O ExCo estabelece as políticas de Segurança da Informação, define os objetivos de segurança e fornece diretrizes e orientações estratégicas para todos os aspectos relacionados à segurança da organização. O Departamento de Segurança da Informação, liderado pelo Chief Security and Resilience Officer (CSRO), é responsável pela implantação, manutenção, monitoramento e revisão do Sistema de Gerenciamento da Segurança da Informação (SGSI), baseado na norma ISO 27001.
PLANEJAMENTO	Seguimos uma abordagem baseada em riscos para a Segurança da Informação. Os riscos externos e internos são avaliados e analisados periodicamente. O departamento de Segurança da Informação elabora planos e processos detalhados para atingir os objetivos de segurança estabelecidos. Como parte da Technical Design Authority (TDA), o Time de Segurança da Informação analisa o projeto de segurança para todas as iniciativas de tecnologia, métricas e Indicadores-Chave de Desempenho (Key Performance Indicators - KPIs) para processos críticos
OPERAÇÕES	As Operações de Segurança se concentram em proteger nossos dados e rede, mantendo o compliance com as exigências legais, regulamentares e contratuais e monitorando os riscos de prestadores de serviços terceirizados. Um Centro de Operações de Segurança de última geração monitora 24 horas por dia a rede da TMF Group para detectar e responder a incidentes de segurança cibernética. Vulnerabilidades no cenário de tecnologia corporativa são identificadas e corrigidas regularmente. Um programa de compliance global, alinhado à norma ISO 27001, monitora e mantém o compliance de segurança de escritórios e datacenters da TMF. Um programa de Auditoria Interna independente atua como a terceira linha de defesa.

2. ABORDAGEM DETALHADA DE DEFESA

No mais alto nível de segurança, a TMF Group elaborou uma estrutura de gestão de segurança e uma série de políticas, normas, processos e guias, incluindo, mas não se limitando somente a, uma Política de Gerenciamento de Continuidade de Negócios e uma Política de Segurança da Informação. A Política de Segurança da Informação da TMF Group está alinhada às exigências da norma ISO27001. Estas políticas, , normas, processos e guias são disponibilizadas a todos os colaboradores por meio da Intranet da empresa. Um programa de Conscientização de Segurança do Grupo é implementado para abordar o treinamento anual sobre a conscientização de políticas para todos os colaboradores. Todas as políticas são revisadas, pelo menos, uma vez ao ano.



A TMF Group utiliza uma abordagem de segurança em várias camadas envolvendo segurança de dados, segurança de aplicações, segurança do sistema, controles de acesso à rede, monitoramento e relatórios de incidentes, segurança física e ambiental e controles de disponibilidade de serviço.

2.1 Segurança de Dados

Os controles de segurança e proteção de dados da TMF Group se concentram no acesso dos colaboradores aos sistemas que hospedam os dados do cliente, compliance regulatório e funções do usuário.

2.1.1 Classificação dos Dados

Para compreender a sensibilidade das informações, a TMF Group definiu um padrão para tratar os dados entre as categorias Público, Interno, Confidencial e Restrito. Melhorar o entendimento sobre o tipo de documentação leva a uma maior conscientização dos potenciais riscos associados a classes de informação específicas..

2.1.2 Dados em Repouso

‘Dados em repouso’ são protegidos por meio de restrições aos direitos de acesso, conforme descrito na seção 2.1.4 “Acesso à informação”. Os dados são protegidos por meio de controle de acesso adequado e segregação lógica.

2.1.3 Dados em trânsito

‘Dados em trânsito’ são criptografados pela Internet. Várias tecnologias utilizadas neste processo são descritas neste documento. Para envios por e-mail, elas são descritas na seção 2.4. Para acesso do cliente, consulte a seção 2.1.5.

2.1.4 Criptografia

A TMF Group usará criptografia de nível AES-256 ou superior, quando a criptografia é necessária. Os dados são criptografados em repouso quando são móveis, como quando armazenados em laptops, backups e quaisquer mídias removíveis que armazenem dados de clientes. Deve-se notar que nem todos os dados em repouso são criptografados, de modo que este processo se aplica, no mínimo, em situações de dados em repouso quando armazenados em laptops, backups e quaisquer mídias removíveis que armazenem dados de clientes. Pode não ser possível criptografar dados em repouso devido a limitações relacionadas à compatibilidade ou interoperabilidade do aplicativo.

2.1.5 Acesso à informação

O acesso a qualquer informação é concedido com base no princípio de ‘Menor Privilégio’. As aprovações para acesso são fornecidas pela administração e devem ser documentadas.

A TMF não processará, transferirá, modificará, emendará ou alterará os Dados Pessoais ou divulgará ou permitirá a divulgação dos Dados Pessoais a terceiros, exceto:

- conforme necessário para processar Dados Pessoais para fornecer os Serviços e/ou de outra forma de acordo com as instruções documentadas do Cliente, ou
- conforme necessário para cumprir as Leis de Proteção de Dados ou outras leis às quais a TMF esteja sujeita, caso em que a TMF deverá (na medida permitida por lei) informar o Cliente sobre essa exigência legal antes de processar os Dados Pessoais.

O acesso às informações deve ser consistente com a Política de Proteção de Dados Pessoais da TMF Group.

2.1.6 Acesso do cliente

As transferências de arquivos em massa podem ser necessárias entre a TMF Group e seus clientes. A TMF Group oferece um serviço adicional para fornecer compartilhamento seguro de arquivos por meio do TMF Group ShareFile, uma solução comercial que usa criptografia avançada.

2.1.7 Acesso remoto

O acesso remoto exige autenticação de multi fatores, geralmente composto pelo ID do usuário, senha e um certificado ou outro fator como Senha Descartável (One Time Password - OTP). O acesso remoto ocorre por meio de um VPN ou por tecnologias de acesso remoto

2.1.8 Dispositivos móveis e *home office*

Todos os notebooks são criptografados com AES 256. O Software de Gerenciamento de Dispositivos Móveis (MAM) foi implementado para proteger os dados nos celulares incluindo recursos de limpeza remota. A Autenticação Multifatorial (MFA) é necessária em telefones celulares

2.1.9 Autenticação

A autenticação baseia-se em uma combinação de ID de usuário/senha. As senhas devem atender a exigências de complexidade que exigem um número mínimo de caracteres e devem conter caracteres alfanuméricos e especiais. A alteração da senha em intervalos predefinidos e o histórico da senha também são obrigatórios. A TMF Group possui um padrão de segurança de senha formalmente documentado, revisado anualmente.
As contas administrativas seguem a mesma política de senha das contas normais, mas exigem uma senha com maiores exigências de complexidade. Há um número limitado de administradores de sistema em posse dos detalhes das contas administrativas. O acesso de administrador é revisado periodicamente.

2.1.10 Eliminação de dados

Todas as informações passam por um ciclo de vida. No final deste ciclo, os dados subjacentes são destruídos. Especialmente no armazenamento digital, os dados aparentemente descartados ainda podem ser acessados por meio de tecnologias semiavançadas. Para evitar a divulgação de informações desta maneira, a TMF Group definiu processos rígidos de eliminação de dados e mídias.

2.2 Segurança de Aplicação

Varreduras periódicas de vulnerabilidade e são baseadas nas 10 principais vulnerabilidades do OWASP, e testes de invasão são realizados e corrigidos de forma adequada.

2.3 Segurança do Sistema

Os computadores e servidores da TMF Group são protegidos por um processo de mapeamento das ameaças (hardening), avaliações de vulnerabilidade e processos de gerenciamento de patches. As políticas de segurança baseadas nas práticas líderes do setor são aplicadas de forma centralizada. Os acessos e registros de auditoria são monitorados.

2.3.1 Gerenciamento de mudanças

A TMF Group constituiu um Conselho Consultivo de Mudanças (Change Advisory Board - CAB). Todas as mudanças de tecnologia devem ser aprovadas pelo CAB. Um registro é mantido para todas as mudanças. O CAB inclui representação da equipe de Segurança da Informação, para garantir que os aspectos de segurança da informação sejam revisados antes da implementação de qualquer mudança. A TMF Group segue as melhores práticas da ITILv3 para seus processos de gerenciamento de mudanças de TI.

2.3.2 Gerenciamento de *patches*

Os *patches* de segurança são revisados e testados. Os *patches* são aplicados aos sistemas após o teste e as devidas aprovações de acordo com o processo. A TMF Group implantou uma ferramenta para aplicar *patches* em suas estações de trabalho e servidores. O processo de gerenciamento de *patches* atende aos requisitos para distribuição de *patches* críticos conforme a necessidade, como resultado de avisos de segurança específicos.

2.3.3 Gerenciamento de *patches*

A TMF mantém os padrões de mapeamento de ameaças para as principais tecnologias que são utilizadas em seu ambiente tecnológico.

2.4 Segurança de E-mail

Todos os e-mails recebidos e enviados são roteados por meio de um gateway de e-mail seguro que oferece proteção contra malware, spam, phishing e spoofing. A TMF Group habilitou o TLS (Transport Layer Security) em seu gateway de e-mail para criptografá-los durante o trânsito. O TLS forçado está disponível sempre que suportado pelos clientes.

2.5 Antivírus e Proteção contra Malware

Os servidores e estações de trabalho são protegidos por software de detecção e resposta de endpoint de última geração.

2.6 Segurança de Rede

A TMF Group implementa as melhores práticas da indústria no projeto e configuração de sua rede e utiliza os melhores equipamentos de rede da indústria para fornecer uma plataforma segura e confiável.
As redes da TMF Group são protegidas por diferentes camadas de firewall.
A proteção do perímetro é revisada continuamente para garantir que as violações sejam altamente improváveis. Varreduras de vulnerabilidade trimestrais do perímetro da rede são conduzidas e acionadas conforme necessário

2.7 Segurança Física

Todos os servidores implantados em data centers estratégicos estão alojados em salas resistentes ao fogo. Os escritórios estão equipados com sistemas de climatização, sistemas de alerta e detecção precoce e equipamentos de extinção de incêndios adequados. Além disso, as áreas críticas, como a sala do servidor e as entradas principais, são protegidas por um sistema de controle de acesso utilizando cartões de aproximação. Equipamentos de Circuito Fechado de Televisão (CFTV) monitoram estas áreas 24 horas por dia, 7 dias por semana. Os escritórios contam com alarmes de intrusão instalados ou guardas de plantão fora do horário de expediente para detectar/prevenir o acesso não autorizado às instalações.

3. CONSCIENTIZAÇÃO

3.1 Programa de conscientização

A TMF Group incentiva seus colaboradores a se manterem informados por meio da intranet da organização. Todos os colaboradores devem cumprir um programa anual de treinamento de conscientização sobre segurança. Notificações especiais por e-mail e pela intranet garantem que todos os colaboradores sejam informados das mudanças nas situações de segurança e de alto risco. Os colaboradores são orientados de acordo com Código de Conduta da TMF Group, Manuais do Colaborador, Sessões de Indução e Programas Mandatórios de Treinamento desde o início de seu vínculo empregatício.

4. AUDITORIAS DE SEGURANÇA

4.1 Avaliações de Vulnerabilidade

A TMF Group realiza varreduras de vulnerabilidade internas e externas trimestralmente. Os resultados das varreduras são agrupados em um relatório interno. As ações e justificativas das vulnerabilidades potenciais são registradas e a correção é feita com base na importância.

4.2 Testes de Invasão

Os testes anuais de invasão em todos os IPs públicos e aplicações direcionadas à internet são conduzidos por uma empresa terceirizada independente.

4.3 Monitoramento de Segurança

A TMF Group dispõe de um serviço de monitoramento 24 horas por dia que coleta e analisa os registros de eventos do ambiente de TI da TMF Group. A TMF Group implantou ferramentas de última geração para monitoramento de segurança. Os incidentes identificados pelo Centro de Operações de Segurança Global (Global Security Operations Centre - GSOC) são tratados de acordo com o processo de resposta a incidentes de segurança definidos.

4.4 Auditorias Internas e Externas

Auditorias internas e externas são realizadas, pelo menos, anualmente, abrangendo Segurança da Informação com base na norma ISO 27001.

5. SEGURANÇA DE RECURSOS HUMANOS

As pessoas geralmente são o elo mais fraco da cadeia de segurança. Segue abaixo um resumo das medidas tomadas no TMF Group para manter os funcionários comprometidos com a segurança.

ANTES DA CONTRATAÇÃO	Os colaboradores em potencial são avaliados antes de sua contratação, por meio de verificações de antecedentes e verificações de recomendação, na medida permitida por lei em cada país.
INTEGRAÇÃO	Colaboradores e contratados recebem um briefing de conscientização de Segurança da Informação no momento de sua integração
TREINAMENTOS DE CONSCIENTIZAÇÃO	Os treinamentos de conscientização sobre Segurança da Informação estão alinhados aos nossos valores. Um treinamento periódico é fornecido à equipe sobre aspectos comportamentais de segurança, como classificação e manuseio de informações, política de organização de mesa e organização de tela, segurança de senha, etiqueta de segurança ao utilizar o e-mail e a Internet, ataques de malware e phishing, engenharia social, relatórios de incidentes de segurança, etc.
CAMPANHAS DE CONSCIENTIZAÇÃO	Para sustentar os níveis de conscientização e comportamento da equipe, são realizadas campanhas periódicas de conscientização e roadshows.

5.1 Admissão de Colaboradores

A TMF Group está comprometida em contratar e atrair os melhores talentos para a organização e espera que os funcionários atinjam altos padrões de conduta e comportamento. Todos os colaboradores da TMF Group precisam realizar uma verificação de antecedentes como parte do processo de integração de novos contratados. Os funcionários também podem solicitados a realizar verificações adicionais conforme e quando necessário. Todas as verificações de antecedentes serão realizadas de acordo com a lei e a legislação local.

5.2 Desligamento de Colaboradores

Quando os colaboradores deixam a organização, todos os direitos de acesso concedidos anteriormente são imediata e devidamente revogados, garantindo que o acesso às informações comerciais seja protegido.

6. CONTINUIDADE DOS NEGÓCIOS

A Continuidade dos Negócios é uma das principais prioridades da TMF Group, e a diretoria da TMF Group apoia a necessidade de medidas robustas de Continuidade dos Negócios para o benefício dos colaboradores, partes interessadas e clientes. Como a maioria das informações dentro da TMF Group é processada digitalmente, as medidas de continuidade concentram-se nessa área.

6.1 Resiliência

A TMF Group utiliza vários data centers comerciais espalhados geograficamente, onde todas as aplicações críticas são hospedadas. Toda a conectividade entre os data centers é redundante para garantir quase 100% de tempo de atividade.

Todos os componentes críticos de rede são redundantes internamente (fontes de alimentação duplas, interfaces de rede duplas etc.). Os equipamentos críticos são conectados aos nobreaks que são regularmente testados e atualizados.

6.2 Backups

A TMF Group faz backups diários de todos os seus dados. Os backups diários são mantidos por quatro semanas. Os backups semanais e anuais estão vigentes. Os backups anuais são mantidos por um período máximo conforme permitido legalmente na legislação local. Para garantir que os backups estejam sempre disponíveis, as gravações de backup são criptografadas e armazenadas em empresas de armazenamento profissionais certificadas, especializadas em armazenamento de gravações (sempre que possível).

6.3 Acessibilidade

A TMF Group utiliza uma solução de rede robusta e segura para fornecer conectividade. Esta solução permite que todos os escritórios se comuniquem entre si e, quando necessário e autorizado. Para fins de continuidade, esta solução oferece a TMF Group a oportunidade de atender seus clientes de qualquer outro local do mundo.

Além disso, a organização possui uma solução segura de acesso remoto. Esta solução de acesso remoto permite que os colaboradores acessem seu ambiente de trabalho de praticamente qualquer local do mundo. O ambiente é criptografado, e o acesso é baseado em uma autenticação multifatorial.

6.4 Retenção

A TMF Group tem a obrigação de disponibilizar os dados, de acordo com os requisitos legais locais. Na maioria dos casos, esta obrigação mantém-se vigente mesmo após a conclusão do serviço prestado ao cliente. A TMF Group garante que todos os dados sejam retidos, desde que seja legalmente exigido pela legislação local.

6.5 Saúde e Segurança

Como a responsabilidade corporativa é um valor fundamental da TMF Group, a organização se preocupa com o bem-estar, a saúde e a segurança de seus colaboradores, clientes e visitantes em seus escritórios.

O gerenciamento de Saúde e Segurança também é considerado parte integrante do gerenciamento de risco total da TMF Group. Por esses motivos, Saúde e Segurança são prioridades fundamentais para a organização.

7. BENCHMARKS DA INDÚSTRIA

Estamos constantemente nos comparando com os processos líderes da indústria.

CERTIFICAÇÃO ISO27001	AUDITORIA ISAE 3402 SOC 1 TIPO 2	CLASSIFICAÇÃO DE SEGURANÇA DA BITSIGHT
Todos os nossos escritórios estão alinhados à norma, com mais de 100 escritórios certificados de acordo com ela.	A TMF Group implementou um programa de auditoria ISAE 3402 SOC 1 Tipo 2 na maioria dos escritórios, para garantir uma validação independente de nossos controles e processos de TI, e para ajudar clientes a atenderem às regulamentações e exigências de compliance.	A Classificação de Segurança BitSight é um benchmarking independente do desempenho de segurança cibernética de uma organização, avaliando interfaces externas e seu desempenho de segurança. A TMF Group utiliza a classificação BitSight para avaliar sua conduta de segurança cibernética alinhada às práticas da indústria.

DEFINIÇÕES E ABREVIATURAS

TERMO	DEFINIÇÃO
CAB	Conselho Consultivo de Mudanças
CISO	Diretor de Segurança da Informação
ExCo	Comitê Executivo
GSOC	Centro de Operações de Segurança Global
RH	Recursos Humanos
SGSI	Sistema de Gerenciamento de Segurança da Informação
KPI(s)	Indicadores-Chave de Performance
MAM	Gerenciamento de Dispositivos Móveis
MFA	Autenticação Multifatorial
OTP	Senha Descartável
TDA	Autoridade de Design Técnico
TLS	Transport Layer Security, ou protocolo de Segurança da Camada de Transporte

REFERENCIA A DOCUMENTOS ASSOCIADIOS

POLÍTICA DE CONTINUIDADE DE NEGÓCIOS	
Política de Continuidade de Negócios	Biblioteca de Políticas da TMF Group
Código de Conduta	Biblioteca de Políticas da TMF Group
Estabelecimento do SGSI	Biblioteca de Políticas da TMF Group
Política de Segurança da Informação	Biblioteca de Políticas da TMF Group

HISTÓRICO DE REVISÕES E REGISTROS

VERSÃO	DATA	AUTOR	DETALHES
1	12/08/2010	Michiel Benda	Elaboração do documento
2	30/11/2010	Michiel Benda	Adições
3	30/08/2011	Michiel Benda	Adições
4	17/03/2013	Michiel Benda	Versão baseada na fusão
	21/02/2014	Michiel Benda	Pequena reformulação, nenhuma nova versão aplicada.
5	05/03/2015	Michiel Benda	Atualização para refletir a melhoria na segurança de TI e conformidade com ISO
6	20/06/2017	David Holman	Revisão pós-reestruturação
6.1	22/06/2017	Mark Belgrove	Pequenas alterações nos requisitos de comprimento/complexidade da senha
6.2	19/07/2017	Mark Belgrove	Risco adicionado à estrutura da organização
6.3	09/2018	Devender Kumar	Estrutura da organização atualizada 9.3 Auditorias Internas e Externas incluídas
7.0	13/09/2019	Devender Kumar	Estrutura do documento e gráficos revisados; sem maiores alterações
7.1	19/07/2020	Nitin Dhande	Adição das seções 2.1.1, 2.1.10 e 2.3.3
7.2	09/12/2021	Anuj Tewari	Revisão com os RSOs e CISO, alterações nos itens 2.1.4, 2.3.3, 5.1, 6.4 e pequenas modificações
7.3	01-07-2022	Anuj Tewari	Revisão anual com pequenas alterações em 2.1.4; 2.1.5 2.1.9 e 4.4, 6.3.