«Manual do SGSI»

PUB-PR17 - Versão 1.0

FRANÇA | EUA | CANADÁ | **BRASIL** | CHINA | HONG KONG | RÚSSIA

Status do Documento

Status	Data	Autor
Responsavel	09/06/2020	Luc Salmon
Validado por	15/07/2020	Frederic Hediard

Histórico de Mudanças

Versão	Data	ítem	Mudanças	Autor
1.0	25/05/2021	-	Criação	Luc Salmon

SUMARIO

1 Geral

Objetivo

O objetivo do documento é definir o perímetro, ou seja, as atividades a que se aplica o SGSI, e como será gerido o sistema em si.

Resumo da empresa

A Ecritel é uma provedora de serviços de hospedagem e terceirização de internet para empresas. A Ecritel possui experiência reconhecida com 10 anos de experiência em TI em serviços de hospedagem gerenciada no Brasil.

A Ecritel oferece serviços de alto valor agregado adaptados às necessidades do cliente por meio da rápida integração das tecnologias mais inovadoras: serviços de hospedagem gerenciada em nuvem pública, privada ou híbrida e aceleração de conteúdo.

A Ecritel também oferece todos os serviços vinculados à missão de provedores de serviços de hospedagem. Inclui, sem limitação, a monitorização, o backup e o plano de continuidade e recuperação do serviço, com um serviço 24/7.

Entendendo o ambiente da organização

A gestão da Ecritel está empenhada em configurar o SGSI, que inclui, mas não se limita a:

- Desenvolvimento de ofertas comerciais Ecritel 27001 com base nas expectativas do cliente
- Ao nomear um LSO para configurar o Sistema de Gestão de Segurança da Informação (ISMS), a Política de Segurança do Sistema de Informação (SGSI) e as várias políticas de segurança
- Promover boas práticas de qualidade e segurança por meio da certificação: ISO 27001 sobre segurança
- Avaliar periodicamente o sistema de gestão de segurança no comitê de governança
- Por carta de compromisso da administração.
- Nomeando os drivers do processo de segurança.

2 Referencias Normativas

ISO 27001:2013
INT-PL01- Política do sistema de segurança da informação
INT-PR01- Procedimento de Recursos Humanos
INT-PR04- Procedimento Interno de Continuação de Negócios
INT-PR06- Procedimento de Não Conformidade e Ação Corretiva
INT-PR08- Procedimento de Criação e Classificação de Documentos
INT-PR15- Auditoria Interna
INT-PR19- Procedimento de Análise de Riscos e Oportunidades

3 Termos e definições

Referência e terminologia

Ativo	Qualquer recurso ou capacidade. Os ativos de um provedor de serviços incluem qualquer coisa que possa contribuir para a entrega de um serviço. Os ativos podem ser de um dos seguintes tipos: gestão, organização, processo, conhecimento, pessoas, informações, aplicativos, infraestrutura ou capital financeiro.
Backup	(Desenho de Serviço da ITIL) (Operação de Serviço da ITIL) Cópia de dados para proteção contra perda de integridade ou disponibilidade do original.
Plano de Continuidade de Negocios (BCP)	(Desenho de Serviço da ITIL) Um plano que define as etapas necessárias para restaurar os processos de negócios após uma interrupção. O plano também identifica os gatilhos para invocação, pessoas a serem envolvidas, comunicações, etc. Os planos de continuidade de serviço de TI formam uma parte significativa dos planos de continuidade de negócios.
Cliente	Cliente da ECRITEL
CEO	Chief Executive Officer (Diretor Executivo)
CTO	Chief Technology Officer (Diretor Técnico)
Ecritel	Ecritel Brasil - São Paulo
SGSI	Sistema de Gestao de Seguranca da Informacao
LSO	Local Security Officer (Responsável pelo SGSI)

4 Contexto da Organização

4.1 Entendendo a Organização e seu Contexto

Para ter um contexto da organização é feito um levantamento das questões externas e internas relevantes, e utilizamos uma análise SWOT, esta sistemática está descrita **SEN-F44- Planejamento Estratégico**.

4.2 Entendendo as necessidades e as expectativas das partes interessadas

As necessidades e as expectativas das partes interessadas são levantadas e descritas no **SEN-F44- Planejamento Estratégico**.

4.3 Escopo

Hospedagem de e-commerce e aceleração de conteúdo a nuvem gerenciada, backups e plano de recuperação de desastres na Ecritel do Brasil, Rua Abacai 60, 04570-030, SP-SP/BR.

5 Liderança

5.1 Liderança e Comprometimento

A alta direção mostra sua liderança e comprometimento em relação ao sistema de segurança da informação através da definição da política e seus objetivos de segurança da informação garantindo que seus processos possuam a integração com requisitos de SI, prover os recursos necessários, acompanhando e assegurando que os processos alcançam os resultados pretendidos, orientando e apoiando as pessoas que contribuam com a eficácia do SI, e apoiando os papéis relevantes a demonstrar sua liderança.
Tais assuntos são tratados e evidenciados nos documentos/registros: **INT-F59- Carta de Comprometimento da Alta Direção, SEN-F44-Planejamento Estratégico, INT-PR04- Procedimento Interno de Continuação de Negócios, INT-F43- Análise crítica da Direção, INT-PL01- Politica do sistema de segurança da informação, INT-F45- Plano de Objetivos e Metas.**

5.2 Política

O objetivo principal da Alta Direção é garantir a satisfação das partes interessadas e a melhoria contínua do Sistema de Gestão de SI, bem como do seu negócio. A política de SI é uma contribuição indispensável para a representação dos seus objetivos e apresentação do rumo que direciona o empreendimento a atender o Sistema de Gestão SI.
De acordo com o contexto e a visão das partes interessadas, a Política de gestão SI da ECRITEL foi estabelecida e está evidenciada no documento **INT-PL01- Politica do sistema de segurança da informação**.

A divulgação da Política do SGSI será realizada formalmente em treinamentos programados de acordo com a necessidade identificada com base nos resultados de auditorias internas e externas, revisão da Política do SGSI e admissão de colaboradores, considerando o cronograma de treinamentos **INT-F36- PLANO DE TREINAMENTO**.
Além disso, estará disponível no website da ECRITEL, seu controle de revisões e atualizações será realizado através da lista mestra de documentos. A verificação do entendimento será avaliada nos treinamentos e auditorias internas em questionários, treinamentos, auditorias internas na verificação dos itens 5.2 e 7.3, da ISO 27001:2013.

5.3 Autoridades, responsabilidades e papéis organizacionais

Os papéis, responsabilidade e autoridades da organização referentes ao atendimento de cada atividade do SGSI do empreendimento estão definidos nos procedimentos documentados, com abordagem do que fazer, como fazer e quem faz. Estas abordagens são realizadas por tipo de função, de acordo com as atribuições e responsabilidades da **INT-F39- Descrição de Cargos** e do **INT-PL01- Politica do sistema de segurança da informação**.

6 Planejamento

6.1.1 Gerenciamento de riscos

Para projetar seu sistema de gestão de segurança, a Ecritel considerou as expectativas e as necessidades das partes interessadas. Para atingir os objetivos, a Ecritel realizou uma análise de risco **INT-F11- Análise de Riscos Oportunidades e Mudanças.**

6.1.2 Avaliação de riscos de segurança da informação

Para avaliar e gerenciar os riscos, a Ecritel criou o **INT-PR19- Procedimento de Análise de Riscos**. Neste procedimento está descrita a metodologia de avaliação dos riscos, juntamente com os processos, ativos, e responsáveis relacionados.

6.1.3 Tratamento de riscos de segurança da informação.

Para os riscos que requerem ações, o objetivo é reduzir o resultado da gravidade ou probabilidade de ocorrência desse risco, reduzindo qualquer um desses fatores e, assim, mitigando o dano potencial.
Os resultados podem ser reavaliados, e novos riscos também podem ser adicionados durante esta revisão.
Uma nota é atribuída a cada risco listado na análise de risco. Esta nota é baseada no fator entre a gravidade e a ocorrência.
A Ecritel elaborou uma declaração de aplicabilidade e contém os controles necessários e as justificativas para as exclusões do anexo A da norma 27001:2013, essa declaração se encontra no formulário **INT-F28- SoA_Brasil**.

6.2 Objetivo de segurança da informação e planos para alcançá-los

Para efetivar a Política do SGSI, a Alta Direção definiu os objetivos, mensuráveis e adequados aos processos da ECRITEL, conforme definido no formulário **INT-F45- PLANO DE OBJETIVOS E METAS**. Os objetivos do SGSI relacionados têm a finalidade de servir de

indicadores de medição dos monitoramentos dos processos implantados no empreendimento gerando dados para realização da análise crítica pela Alta Direção, onde os objetivos são quantitativamente e qualitativamente definidos.

Quando algum objetivo não for alcançado, será atribuída ação de correção e/ou corretiva, além de ação de melhoria do SGSI, conforme necessário. Tais dados terão seu desempenho analisado e apresentados para análise crítica à Alta Direção.

Os resultados de monitoramento do desempenho e a geração de gráficos indicadores serão a forma de demonstrar se as ações definidas no planejamento das ações para alcançar objetivos do SGSI, alcançam de fato aos resultados planejados.

A Alta Direção tem a responsabilidade de assegurar que os processos integrantes do Sistema de Gestão SI da ECRITEL, são analisados e monitorados periodicamente, visando verificar a sua eficiência e eficácia.

7 Apoio

7.1 Recursos

A ECRITEL proverá recursos necessários para implementar e manter o Sistema de Gestão SI, visando a melhoria contínua de sua eficácia, bem como o aumento do desempenho. A Alta Direção gerenciará os investimentos a partir da identificação de melhorias e investimentos do empreendimento, de acordo com as necessidades do empreendimento e recomendações do CEO. Estes assuntos serão discutidos nas reuniões de análise crítica da Alta Direção realizadas anualmente ou sempre que se julgar pertinente para alinhar o **SEN-F44-Planejamento Estratégico**.

7.2 Competência

As competências necessárias para colaboradores são ditadas pela **INT-F39- Descrição de Cargos**.
O **INT-PR01-Procedimento de Recursos Humanos** contêm a metodologia de contratação de novos integrantes que gera evidências das competências dos mesmos.

7.3 Concienteização

Todos os colaboradores possuem treinamento sobre a segurança e as mudanças no SGSI. Estes treinamentos visam informar os membros da equipe e lembrá-los da importância do acompanhamento do SGSI, da melhoria contínua, e de todas as regras e normas de segurança. Treinamentos são administrados conforme **INT-F36- PLANO DE TREINAMENTO**.
Juntamente aos treinamentos, também tem e-mails regulares de conscientização que são enviados periodicamente para todos os integrantes. Estes e-mails tem como objetivo lembrar

a equipe de regras, normas e riscos que podem ocorrer no dia-a-dia. Um guia de tópicos e mensagens **INT-F47- Plano de Conscientização** foi criado para facilitar esta atividade.

7.4 Comunicação

A comunicação interna e externa tem como objetivo assegurar a conformidade do 7.4 Sistema de Gestão SI pelo fluxo adequado de informações, definido no **INT-F56- Plano de Comunicação**.

7.5.1 Informação documentada

O objetivo da documentação do SGSI, da ECRITEL, é garantir o cumprimento dos requisitos exigidos pela ISO 27001:2013, a fim de assegurar a implementação eficaz dos seus processos, considerando:

- Política e Objetivos;
- Manual do Sistema de Gestão;
- Procedimentos documentados, incluindo os requeridos pela norma;
- Instruções de trabalho, onde necessário;
- Documentos de fontes externas, Métodos, Especificações, Normas, Decretos, Leis, Portarias, conforme aplicável;
- Controles e registros;
- Outros documentos que se façam necessários.

7.5.2 Criando e atualizando Informação Documentada

A informação documentada segue os requisitos de Identificação, Descrição, Formato, Análise crítica, nomenclatura e aprovação conforme o **INT-PR08-Procedimento de Criação e Classificação de Documentos.** Este procedimento é utilizado para criar e atualizar as informações documentadas da empresa de uma forma padronizada e segura.

7.5.3 Controle da Informação Documentada

A informação documentada inclui Formulários, Procedimentos, Políticas e Manuais que são controlados pela **INT-F41-Lista de Informação Documentada**. Esta lista é usada para assegurar que as informações estão adequadamente protegidas, disponíveis, e prontas para uso. Esta lista também contém as seguintes informações sobre cada item: distribuição/acesso, recuperação, dono, armazenagem e preservação, controle de versionamento, e retenção.

8 Operação

8.1 Planejamento operacional e controle

A Ecritel planejou e implementou controles para os seus processos conforme o anexo A da norma 27001. Estes controles passaram por uma análise de riscos e oportunidades conforme descritos no item 6.1 deste manual a fim de implementar as ações determinadas e também foi implementado planos para alcançar os objetivos conforme o requisito 6.2

As mudanças planejadas são controladas e as mudanças não previstas são analisadas criticamente no formulário **INT-F11-Análise de Riscos Oportunidades e Mudanças** e ações são tomadas para mitigar efeitos adversos conforme o necessário.

8.2 & 8.3 Avaliação de riscos de segurança da informação & Tratamento de riscos de segurança da informação

A Ecritel realiza avaliações de risco anualmente, quando mudanças significativas ocorrem ou são propostas.

A Ecritel implementou o plano de tratamento de riscos conforme o procedimento **INT-PR19-Procedimento de Análise de Riscos e Oportunidades** e é evidenciado no formulário **INT-F11-Análise de Riscos Oportunidades e Mudanças.**

9 Avaliação do Desempenho

9.1 Monitoramento, medição, análise e avaliação

A ECRITEL definirá, planejará e implementará medições, monitoramentos, análises e melhorias para assegurar que o seu SGSI, processos e serviços estejam em conformidade com as especificações aplicáveis, tendo como objetivo a satisfação das partes interessadas.

Desta forma, a Alta Direção estabelecerá a periodicidade, os objetivos e a forma de monitoramento e medição da eficácia dos processos que formam o SGSI, bem como as ferramentas a serem utilizadas, incluindo aplicação de ferramentas estatísticas adequadas a cada processo, de acordo com o apresentado neste Manual do SGSI, realizará análise crítica quanto aos resultados apresentados. A metodologia aplicada para a medição e monitoramento do SGSI seguirá a utilização de ferramentas estatísticas, onde a medição e o monitoramento do SGSI ocorrerão de acordo com a frequência determinada na verificação dos objetivos de cada processo abordados no plano de objetivos e metas.

9.2 Auditoria interna

Auditoria interna é uma ferramenta usada para se assegurar que o SGSI está sendo seguido e sendo efetivo. Auditoria interna é agendada conforme **INT-F35- PROGRAMA DE**

AUDITORIA, e segue o **INT-F32- Plano de Auditoria** que determina quem estará auditando o que. As auditorias seguem o processo **INT-PR15- AUDITORIA INTERNA** que descreve como a mesma será conduzida. Os resultados de cada auditoria são relatados em um **INT-F34-Relatório de Auditoria** que é preenchido a cada auditoria.

9.3 Análise crítica pela direção

A alta direção se reúne anualmente para analisar criticamente o sistema de gestão da segurança da informação da organização e avaliar sua contínua adequação, pertinência e eficácia. Usando o formulário **INT-F43- Análise crítica da Direção** como um guia de assuntos a serem abordados.

10 Melhoria

10.1 Não conformidade e ação corretiva

A sistemática para tratar as não conformidades e ação corretiva está definida no procedimento **INT-PR06- Procedimento de Não Conformidade e Acao Corretiva**.

As não conformidades são registradas no formulário **INT-F10- Registro de não Conformidade** onde o preenchimento de todos os campos garante o seguinte:

- Dados sobre a não conformidade
- Uma ação foi tomada para reagir a não conformidade
- A mesma foi avaliada criticamente para encontrar a causa raiz
- Se necessário ações a mais foram tomadas para evitar recorrência
- Análise da eficácia das ações em tratar a não conformidade

O controle do status das ações são controlados e acompanhados no formulário **INT-F31-Acompanhamento de não conformidades e ação corretiva**. O mesmo facilita o gerenciamento e acompanhamento de cada item, e facilita sua apresentação.

10.2 Melhoria contínua

A Ecritel continuamente melhora a pertinência, adequação, e a eficácia do sistema de gestão da informação usando o conjunto de medidas relatadas neste documento.