| 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 objetivo deste documento é descrever as regras para a criação e manutenção de acessos, a fim de regular o acesso a áreas físicas e lógicas, informações proprietárias e compartilhadas.

# 2. Escopo

As informações cobertas por esta política incluem, mas não se limitam a, informações, sistemas, locais de trabalho, redes, etc...

# 3. Controle de Acesso Físico

## Área Segura

Existe uma área segura para áreas técnicas e de estoque, com acesso restrito controlado por sensores de biometria. O acesso de trabalho a esta área é restrita para membros da equipe técnica, Ti, ISMS, e alta direção.

## Contrôles de Acesso

Funcionários da Ecritel podem acessar o escritório 24/7/365.

O acesso ao edifício é controlado via uma senha numérica, que é atualizada a cada 6 meses.

O andar superior pertencente à Ecritel, e as áreas internas de acesso restrito terão seu acesso controlado por um sensor biométrico.

Se algum visitante ver o código da porta de entrada no edifício, você deverá comunicar o Dpto. Ti de modo a alterar o código e o cartão através de email ou Slack.
Também existe um sistema de alarme de intrusão, e a área de entregas fica no exterior do escritório.

## 4. Contrôle de Visitantes

Visitantes não poderão ter acesso a instalação desacompanhados. Cada visitante será registrado no logbook, com nome, ID, razão da visita e nome do contato na Ecritel pelo Dpto. RH no **INT-F06- FORMULADO DE ACESSO NA ECT**, e deverá ter um membro dos funcionários presente durante a visita.

Dependendo da natureza do visitante pode ser requerida assinatura de um NDA pelo RH usando formulário **INT-F08-Termo de Confidencialidade ou o F09** para PJ.

# 5. Controle de Acesso virtual

### 5.1 - Administração de Acessos

Acessos são gerados e mantidos pelo Depto. de Ti na "**INT-F26-IT9-Lista Mestra de Controle de Acesso**", a pedido do Depto. RH ou do CEO/CTO. Contas e direitos de usuários são inicialmente alocados na hora da contratação baseado em perfil do cargo e/ou requisições de trabalho. Mudanças futuras nas contas existentes são feitas a pedido para o depto. Ti, precisando das autorizações mencionadas anteriormente.
Usuários são dados os mínimos privilégios possíveis para fazer o que precisam, seja em termos de acesso a informações ou acesso a configurações das máquinas/sistemas.
Pedidos de Acesso podem ser feitos apenas por gerentes de Dpto, através de um Email para o Dpto. Ti.
Eventos Significativos a ver com acessos são registrados pelo Dpto. Ti com o preenchimento de um "**INT-F10- Registro de Incidente de Segurança**".

# 6. Controle de Acesso a Informação documentada

O SGSI deverá controlar a distribuição e adequação para uso, proteção (Contra perda de confidencialidade, uso impróprio ou perda de integridade) acesso, recuperação e uso, armazenagem e preservação, preservação da legibilidade, controle de alteração, retenção e disposição.

Este controle é realizado através da **INT-F26-IT9-Lista Mestra de Controle de Acesso**.

# 7. Revogação de Acesso

A Revogação de Acessos é feita pelo Dpto. de Ti a pedido por email ou slack dos Gestores de Dpto. ou do RH. A Revogação de Acessos deve ser feita com antecedência de eventos significativos como o aviso de desligamento ou mudança de cargo de integrantes.

## 8.Segurança do Edifício

O Edifício segue as normas de segurança dos bombeiros para proteção contra fogo. Os telhados são mantidos contra vazamentos de água, e no caso de algum inesperado a equipe é treinada para trabalhar de casa. O escritório não contém equipamento cuja perda causaria grandes danos às atividades da Ecritel e seus clientes.

## 9.Auditoria periodica do Ti

A auditoria de Controle de Acesso é realizada semestralmente pelo Departamento de Ti, sendo escolhido aleatoriamente 50% dos usuários em cada semestre, ou seja, ao decorrer de um ano é verificado 100% dos usuários.

Esta auditoria é realizada com o intuito de verificar se os usuários contém acessos indevidos ou antigos que já deveriam ter sido revogados.

A evidência desta auditoria é realizada através do formulário "**INT-F63-IT9-Auditoria da Lista Mestra de Controle de Acesso**".