



# **Tecnologia e Segurança da Informação**

**Versão: Abril/2018**

## **1. Tecnologia e Segurança da Informação**

### **1.1. Infraestrutura**

A Galt possui vários equipamentos necessários ao desempenho apropriado das suas atividades, dos quais os mais relevantes são um servidor, uma central telefônica e as estações e trabalho, tudo ligado em rede.

Além da estrutura física do escritório, a Galt tem contratados serviços de armazenamento em nuvem.

Existe uma pessoa responsável pela TI, embora os serviços mais complexos sejam realizados por uma empresa prestadora de serviços de TI, cujo contrato com a Galt inclui a assinatura de um termo de confidencialidade.

### **1.2. Manutenção do Servidor**

O servidor é responsável pela autenticação dos usuários, serviço de arquivos e banco de dados. Ele conta com a proteção de um antivírus licenciado e atualizado regularmente. A atualização / instalação de qualquer software ou serviço ocorre sempre a partir da autorização do responsável por TI, podendo haver suporte da empresa terceirizada de TI conforme necessidade.

### **1.3. Acesso à informação**

Todo o usuário ingressa na rede através de autenticação no domínio (autenticação do Windows). As permissões de cada usuário para acesso à informação são estabelecidas sempre a partir desta autenticação.

#### **1.3.1. Administrador da Rede**

O usuário administrador da Rede, cuja senha é de conhecimento apenas do responsável de TI, tem acesso a todas as informações. Institucionalmente, ele só está autorizado a acessar informações restritas se for solicitado pelo diretor de Compliance com um propósito específico.

#### **1.3.2. Pastas na Rede**

Cada usuário possui uma pasta individual no servidor. Os arquivos armazenados nesta pasta são protegidos por backup. O acesso a cada pasta é restrito ao respectivo usuário.

Existem pastas compartilhadas na rede. Cada pasta é restrita a um grupo de usuários de acordo com a sua função.

#### 1.3.3. Banco de dados

O servidor abriga um banco de dados na plataforma SQL Server, cujo acesso é feito a partir de um sistema proprietário (Galtsis). Este sistema é instalado nas estações e possui uma estrutura de permissões ajustável às necessidades de restrição de acesso a informações e funcionalidades.

#### 1.3.4. Rede para clientes

Os clientes conseguem acessar a internet via wifi, porém não têm acesso à rede corporativa por não terem autenticação no domínio da Galt.

### 1.4. Estações de Trabalho

Todas as estações de trabalho possuem antivírus atualizado. Os usuários não têm permissão de administrador das suas máquinas.

Qualquer instalação / alteração de software só pode ser feita pelo administrador da Rede e, conseqüentemente, autorizado pelo responsável de TI. Cada solicitação é analisada individualmente.

Aplicativos como o antivírus e os sistemas proprietários são atualizados automaticamente, sem a necessidade de permissão de administrador.

Sempre que necessário, a empresa terceirizada de TI é acionada para ajudar na manutenção das estações.

### 1.5. Ordens

As ordens podem ser passadas por sistema Bloomberg, telefone ou email, sendo que em todos os casos é guardada uma evidência da mesma conforme estabelecido pela regulamentação.

#### 1.5.1. Ligações Telefônicas

O escritório possui 4 linhas telefônicas. Todas as ligações são gravadas. Embora a legislação estabeleça que as ligações telefônicas devam ser armazenadas por pelo menos 5 anos, a empresa não possui rotina de descarte de ligações mais antigas.

As gravações telefônicas são armazenadas no Servidor. Seu acesso é restrito ao diretor de compliance e ao administrador da rede. O diretor de compliance recebe uma notificação automática por email sempre que uma gravação é copiada, renomeada, movida ou excluída.

#### 1.5.2. Emails

Os e-mails corporativos pertencem ao domínio da empresa (galt.com.br). As ordens passadas por email nunca são excluídas. Além da cópia local do email enviado com a ordem, também existe uma cópia no servidor de email, que é da Microsoft (Office 356) e pode ser acessada de qualquer lugar com acesso à Internet pelo usuário que enviou a ordem.

### 1.6. Contingências

#### 1.6.1. Backup

O servidor possui HD com espelhamento RAID 1 para minimizar riscos de falha. As pastas do Servidor possui backup em sombra, ferramenta do Windows que permite facilmente acessar arquivos perdidos ou versões anteriores de arquivos modificados. Esta ferramenta está configurada para realizar cópias diárias das pastas, 3 vezes ao dia.

O escritório possui um storage (HD externo com espelhamento, próprio para realizar cópias de segurança e disponibilização de arquivos). Há rotinas de backups diários e mensais no storage. As cópias diárias mantêm os arquivos dos últimos dois dias. A cópia mensal disponibiliza versões mais antigas dos arquivos.

Existe também um mecanismo de backup em nuvem, para recuperação de fora do escritório. A solução adotada para este backup é a Azure (Microsoft). Diariamente os arquivos são sincronizados com a nuvem. Esta solução mantêm cópias com as versões diárias (nos últimos 180 dias), semanais (2 anos), mensais (5 anos) e anuais (10 anos).

#### 1.6.2. Energia Elétrica

Todas as estações de trabalho são protegidas contra picos de energia por estabilizadores. Os principais equipamentos são protegidos contra picos e queda de energia por no-break. A região em que o escritório se localiza possui um histórico de disponibilidade de energia bastante estável, sendo raros os problemas com energia elétrica.

Em caso de interrupção de energia na região, as estações de trabalho param de funcionar, enquanto que o no-break mantêm os principais equipamentos funcionando

por até meia hora, tempo geralmente suficiente para o reestabelecimento da energia. Durante esse período, as ligações telefônicas continuam sendo gravadas e os e-mails corporativos podem ser acessados por dispositivos móveis pessoais.

Na hipótese de a energia não ser reestabelecida em um tempo razoável, os equipamentos principais são desligados (incluindo o Servidor e o Gravador de ligações). Nesse caso, as novas ordens devem ser dadas obrigatoriamente por email.

Se for necessário acessar arquivos da Rede na falta de luz após o desligamento do Servidor, o storage pode ser facilmente removido do escritório para um ambiente com energia elétrica. Como alternativa ao storage, existe o backup na nuvem que pode ser recuperado. Em ambos os casos, os arquivos sempre estão criptografados e é necessária a senha para acesso.

### 1.6.3. Acesso ao prédio

Em caso de impossibilidade de acesso ao prédio, é possível acesso e uso de e-mails de qualquer lugar com acesso à Internet, a partir de webmail. Em caso impossibilidade permanente de acesso ao prédio ou ao Servidor, os arquivos poderão ser recuperados a partir do backup em nuvem, realizado conforme descrito no item 1.6.1.