Política de segurança da informação e dados físicos

Versão 1.0

Setor de Tecnologia da informação do 1º Registro de Imóveis de Joinville
Titular – Bianca Castellar de Faria

SUMÁRIO

Objetivo 02

Responsabilidades 02

Definições 02

Equipamentos/Software 03

Condições Gerais 03

Referências 08

Objetivo

1. Garantir que sejam mantidos os princípios da segurança da informação – CID, confidencialidade, integridade e disponibilidade das informações coletadas e armazenadas fisicamente e digitalmente nas dependências do 1º Registro de Imóveis de Joinville em qualquer circunstância e em atendimento as legislações vigentes no país. São elas Provimento 74/2018 do CNJ, Lei 13709/2018 de Proteção de dados pessoais e a Lei 9610/1998 de propriedade intelectual. Buscar a melhoria contínua em atendimento aos requisitos aplicáveis das normas vigentes de qualidade.

Responsabilidades

1. **Setor de tecnologia interno da serventia juntamente com a empresa terceira**: Responsável em manter os dispositivos de segurança ativos e em perfeito estado de funcionamento permanentemente.
2. **Coordenação do setor administrativo:** Responsável por analisar os relatórios gerenciais da segurança de informação.
3. **Titular e controladora dos dados:** Responsável em disponibilizar os recursos necessários para manter todo ecossistema de processos em ordem.

Definições

1. **Storages de armazenamento** - Equipamento utilizado para armazenar dados e informações digitais.
2. **Storages** – Equipamento com sistema operacional dedicado a armazenamento de dados.
3. **Serventia** – Cartório 1º Registro de Imóveis de Joinville, denominado também em termos jurídicos como SERVENTIA.
4. **Client de monitoramento das estações de trabalho** – Um aplicativo da Makrolock que fica coletando os logs de monitoramento em tempo real para enviar ao servidor.

5. **WIFI Segregada –** Rede com internet separada da rede interna onde estão sendo tratadas as informações que passam pela serventia.

Equipamentos / Software

1. Estações de trabalho, Servidores físicos e virtualizados, nobreaks, gerador, Storages de armazenamento, discos externos, impressoras, scanners e fragmentadores.
2. Utilizamos softwares de backup em nuvem para maior proteção dos dados, utilizamos também, softwares que englobam todo o pacote Office do Windows, juntamente com um ERP voltado para o cartório. (Navegadores, compactadores, leitor PDF entre outros)
3. Provedor de e-Mail hospedado com a Microsoft.

Condições Gerais

1. Controle de acesso à informação

Através do serviço de domínio e usuários, são aplicadas restrições de acesso a pastas específicas com base em políticas de segurança definidas pela serventia. O acesso é amplamente permitido à maioria dos arquivos comuns, enquanto pastas sensíveis, como informações financeiras, recursos humanos, qualidade e administração, possuem limitações rigorosas de permissões, disponíveis apenas para indivíduos autorizados.

1.1 A serventia utiliza uma estrutura de acesso dividida por setores e 3 níveis de permissão distintos, conforme descrito abaixo:

1.1.1 Permissão total – administrador e titular;

1.1.2 Permissão específica/restrita – Coordenações e administrativo;

1.1.3 Permissão individual/restrita – usuários do domínio, seguindo as diretrizes estabelecidas pela POLÍTICA DE SENHAS da serventia. Essa

abordagem reforça a identificação individual em processos. No entanto, garantimos também a individualidade através de monitoramento por câmeras de vigilância.

1.1.4 A equipe é devidamente informada sobre essa exclusividade entre outras informações relevantes referente a LGPD e Segurança da Informação logo que o novo colaborador é admitido ao quadro de funcionários e recebe seus devidos treinamentos.

1.1.5 Através de um client de monitoramento instalado nas estações de trabalho, é possível monitorar e controlar as informações que estão sendo tratadas pelos usuários da rede em tempo real. No entanto, essas auditorias são executadas por demanda, quando solicitadas pelas coordenações e titular devido algum evento específico que possa ter ocorrido.

1.1.6 Todos os endpoints, desktops e notebooks são protegidos internamente pelo software de antivírus/antissequestro corporativo, firewall de rede e a VPN para possíveis e eventuais trabalhos em home office. O monitoramento e controle é feito através da própria ferramenta utilizada para mitigação das possíveis ameaças.

1.1.7 A criação de usuários novos e acessos aos endpoints e aos dados da serventia se dão somente mediante solicitação, seja verbal ou formal, da titular ou coordenações ao responsável técnico da estrutura lógica para somente assim efetuar a criação de um usuário novo e/ou a liberação de acesso a esse usuário tanto interno quanto em home office.

1.1.8 Em relação aos dispositivos externos, sejam eles móveis ou notebooks de colaboradores e visitantes, seus acessos são liberados somente via rede WIFI segregada.

1.1.9 Evidenciamos logo que o colaborador é admitido na serventia, através do PINC – Programa de inclusão de novos colaboradores como também nos treinamentos de segurança da equipe, que é terminantemente proibido o compartilhamento de informações fora dos meios de comunicação da instituição, como o WhatsApp business e dos e-mails corporativos. Podendo ocasionar em punições conforme código de ética interno da serventia.

1.1.10 Em relação ao ERP (sistema usado pelo cartório) da serventia, a desenvolvedora do ERP, mantém um serviço de auditoria interna nos processos operacionais do sistema, todo o acesso ao sistema provê um módulo completo de permissionamento conforme a necessidade de cada setor.

1.2 **Controle de acesso às dependências internas da serventia.**

Todas as 3 possíveis entradas às dependências do cartório, são controladas por acesso biométrico e câmeras devidamente sincronizadas entre si pelos servidores de horários públicos ntp.br, sendo elas de forma digital pela porta de entrada dos colaboradores (acesso biométrico) com autorização de entrada apenas nos horários de expediente devidamente configurado no grupo de permissão “Colaboradores” através do painel Control ID da IDSecure.

1.2.1 **Temporalidade das gravações de imagens.**

Considerando que o dispositivo de gravação contempla 6 discos de 6TB mais 2 discos de 8TB, sendo que as gravações estão configuradas para uma resolução de maior qualidade com 25 pontos de monitoramento, as imagens permanecem gravadas por um período de 4 meses, anterior a esse período automaticamente começam a ser sobrescritas no próprio equipamento de

gravação.

1.2.2 **Regras de acesso.**

Visto que temos imensa preocupação com a integridade física tanto dos nossos documentos e patrimônio quanto das pessoas que passam diariamente pela serventia, temos regras e critérios de QUEM? QUANDO? e ONDE? acessa, muito bem estabelecidos conforme configurado no Control ID. Bem como regra de Tela Limpa e Mesa Limpa para que não haja vazamento de informações, as telas são programadas para serem bloqueadas após um período de inatividade e os colaboradores são conscientizados sobre a importância de sempre que saírem de suas bancadas bloquearem seus acessos e resguardarem os documentos físicos de acesso indevido.

2. Estrutura física interna e contingências digitais

2.1 A titular da serventia sempre mantém os recursos disponíveis e com uma certa autonomia de decisão ao setor financeiro em relação as emergências e situações de custos aceitáveis voltados para a infraestrutura de tecnologia e equipamentos.

2.2 Toda a estrutura interna da rede, é protegida por um servidor Firewall e mecanismos de monitoramento e segurança que possibilitam um ambiente mais seguro. Porém, não descartamos o processo contínuo de conscientização da equipe em colocar como suspeito tudo que venha através de links e material duvidoso, acionando o suporte interno da serventia para que seja antes verificada a procedência.

3. Estrutura de acesso físico externo

Considerando que precisamos manter a segurança física dos documentos armazenados nos arquivos e a integridade física do patrimônio e dos colaboradores, mantemos o acesso às áreas restritas dos funcionários resguardadas por acesso

biométrico, câmeras e treinamento contínuo da equipe de como, quando e quem pode ter o acesso interno às nossas dependências.

4. Acesso de fornecedores e prestadores de serviço às dependências da serventia.

4.1 Todas as entregas e recebimentos de mercadorias são devidamente anunciadas ao administrativo por telefone ou comunicador interno, onde um colaborador responsável fica a cargo de receber a mercadoria pela porta de entrada dos colaboradores, pelo tempo necessário até conferir e liberar o fornecedor. Esse acompanhamento se dá presencial e assim permanece até a sua total saída das dependências internas do cartório. Quanto a prestadores de serviço segue também o mesmo procedimento, porém pode ocorrer pela porta de atendimento dos usuários, o prestador se identifica no balcão de triagem, onde é anunciado e um colaborador responsável pelo chamado, vai até a recepção receber e fazer o devido acompanhamento.

4.2 **Confidencialidade:**

Através das políticas de grupo do Active Directory do servidor de domínio, são efetuados bloqueios de acesso conforme já mencionado nesse documento, para que possam ser mantidas as garantias da sua confidencialidade.

5.0 Gestão contínua de vulnerabilidades.

5.1 Com as ferramentas de código aberto como o OPENVAS do Kali Linux e o GoPhishing executamos com o auxílio da D2 Tecnologia e Vortek Consultoria Digital, uma gestão contínua de vulnerabilidades, sempre atentos as possibilidades de invasão ou sequestro de dados.

5.2 Identificados possíveis pontos vulneráveis a ataques, é aberto ação corretiva no helpdesk interno onde o técnico residente executa as ações em campo, efetuado um check-up geral e aplicando os patchs necessários.

6 Referências

6.1 ISO9001:2015;

6.2 NBR 15.906:2021;

6.3 ISO 37001:2016;

6.4 ISO 37301:2021;

6.5 ISO 27001:2022;

6.6 PQTA (Programa de Qualidade Total da ANOREG).