Ameaças	MTD	RTO	WRT	Impacto	Valor	Importância
Ataque DDoS	4 Horas	3 Horas	2 Horas	Direto	**Medio**	3
Falha em Auditorias ou geração de Logs	5 Horas	3 Horas	2 Horas	Direto	Alto	1
Uso de Software Pirata ou Não Licenciado	6 Horas	4 Horas	2 Horas	Direto	Alto	1
Permissões Excessivas	5 Horas	3 Horas	2 Horas	Direto	Muito Alto	1

Fonte: Elaborado pelos autores (2024)

3.4 Etapa 4: Plano de Segurança de Recursos em Tecnologia da Informação

3.4.1 Proteção contra riscos ao patrimônio físico

3.4.1.1 Segurança do Perímetro da empresa

A segurança do perímetro da empresa será reforçada através de tecnologias diversas. As entradas, saídas e áreas sensíveis da empresa serão monitoradas por câmeras de vigilância e o controle de acesso será realizado por portas automatizadas e detecção de impressão digital. Alarmes e sensores de movimentos também serão acionados durante o período de inatividade da empresa para alertarem invasões noturnas.

A segurança da empresa também dependerá da segurança predial fornecida pelo edifício em que está sediada.

O procedimento de segurança mais comum para isso, além da segurança física do perímetro como muros, portões automatizados e cercas elétricas, costuma ser o controle do fluxo de pessoas realizado através da portaria de pedestres. Este controle se aplica não apenas aos visitantes e clientes, mas também aos entregadores de mercadorias.

3.4.1.2 Controle de Acesso Físico

Para ampliar a segurança ao meio físico da empresa, alguns equipamentos e processos são de extrema importância no ambiente empresarial.

- **Equipamentos de filmagem:** Câmeras capturando as imagens do ambiente ajudam a monitorar as pessoas e equipamentos no ambiente.

- **Equipamentos de biometria:** Leitores de digitais e acesso facial nos domínios da empresa são de extrema importância para garantir quem deve ou não acessar as fechadas por travas magnéticas.

- **Portaria:** Um bom profissional para cuidar do acesso à portaria é fundamental para a segurança de todo o prédio. Segurança no recebimento de mercadorias e tentativas de acesso não permitidas são bem intermediadas por uma pessoa física no local.

3.4.1.3 Proteção contra desastres

Para garantir a continuidade dos serviços prestados pela empresa mesmo após um desastre é preciso seguir algumas práticas para amenizar o dano causado por qualquer tipo de desastre, o quadro 20 lista o Plano de Continuidade de Negócios (PCN)

Quadro 20 - Proteção contra desastres

Plano de Continuidade de Negócios (PCN)	
Objetivo:	Garantir que a empresa consiga manter suas operações essenciais em funcionamento durante e após um desastre.

<table>
<tr><th colspan="2">Plano de Continuidade de Negócios (PCN)</th></tr>
<tr><td rowspan="3">Como Implementar:</td><td>➢ Identificação de Processos Críticos: Identificar quais áreas, departamentos ou sistemas são essenciais para a continuidade do negócio.
➢ Estratégias de Recuperação: Definir como esses processos serão mantidos, seja por meio de substituições temporárias, operações reduzidas ou soluções automatizadas.
➢ Treinamento e Testes: Realizar simulações regulares e treinamentos com todos os colaboradores, para que saibam como reagir em uma crise.</td></tr>
<tr><td>Ambiente físico</td></tr>
<tr><td>➢ Em cada andar da empresa vai se encontrar um profissional treinado para casos de incidentes para auxiliar e instruir todos os colaboradores a evacuarem os locais de riscos com mais segurança e agilidade.
➢ Andares equipados com extintores de incêndios e portas corta fogo na entrada de cada andar permite uma saída de segurança pelas escadas do prédio.
➢ Instruções localizadas pela empresa ajudam a manter a ordem no local, informações que à primeira vista parecem óbvias são de extrema importância serem sempre mencionadas.

Como por exemplo:
A. Não usar o elevador em suspeitas de incêndio.
B. Não fumar em locais proibidos.
C. Manter as portas cortas fogos sempre fechadas.</td></tr>
</table>

Fonte: Elaborado pelos autores (2024)

3.4.2 Proteção contra riscos aos equipamentos da empresa

3.4.2.1 Identificação e Catalogação dos dispositivos da empresa

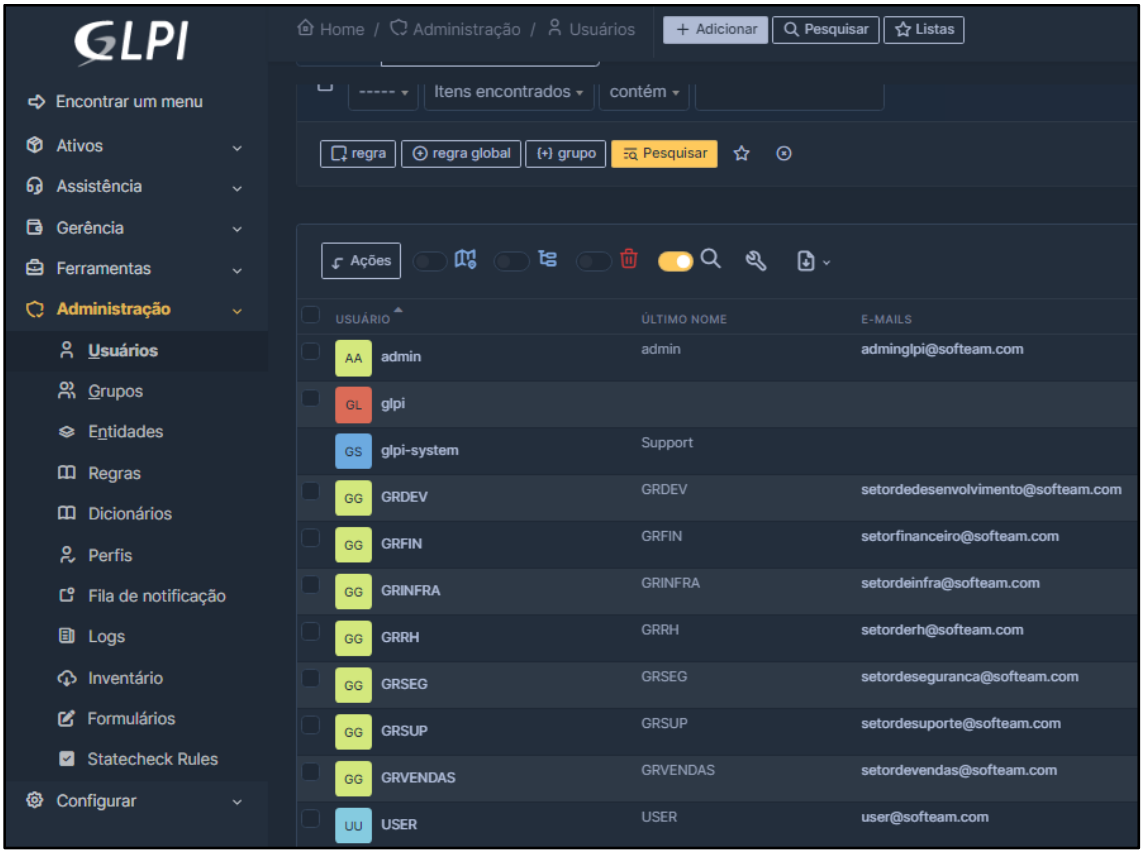
O software GLPI foi utilizado para catalogar todos os ativos da organização. Conforme ilustrado na figura 58, o dashboard exibe informações sobre os ativos da organização.

A Figura 59 ilustra usuários designados para cada departamento da empresa. *"GRDEV"*, para o departamento de desenvolvimento; *"GRFIN"*, para o departamento financeiro; *"GRINFRA"*, para a infraestrutura; *"GRRH"*, para o departamento de recursos humanos; *"GRSEG"*, para a segurança; *"GRSUP"*, para o suporte; e *"GRVENDAS"*, para o setor de vendas. e a figura 60 demonstra todos os ativos que foram adicionados à ferramenta GLPI.

Figura 58 - Captura de Tela: Dashboard (GLPI)

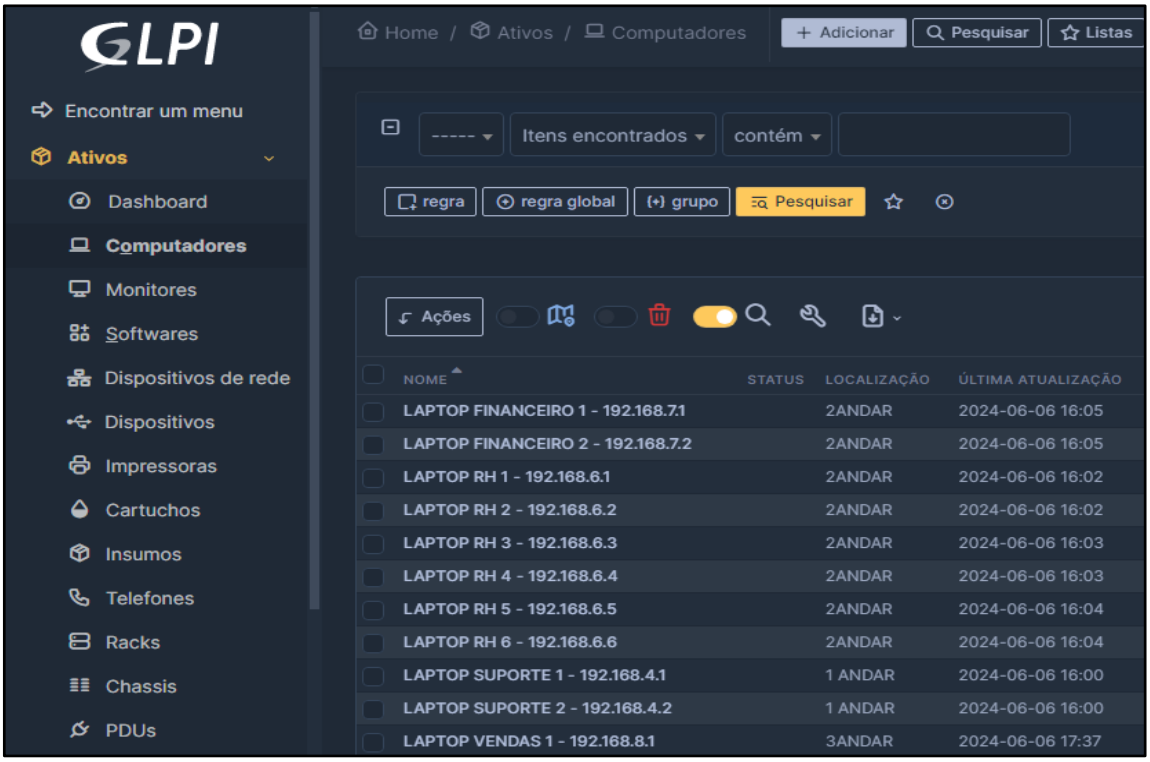
Fonte: Elaboração própria (2024).

Figura 59 - Captura de Tela: Lista de usuários (GLPI)



Fonte: Elaboração própria (2024).

Figura 60 - Captura de Tela: Gerenciamento de Computadores (GLPI)



Fonte: Elaboração própria (2024).

3.4.2.2 Manutenção preventiva e Corretiva

No setor de infraestrutura, equipes técnicas são responsáveis por garantir que a infraestrutura de Tecnologia da Informação esteja sempre em condições operacionais.

Os pedidos de manutenção são registrados através de chamados, mas também podem ser solicitados diretamente pelos usuários ao técnico responsável. O suporte e a manutenção dos equipamentos serão executados conforme as diretrizes apresentadas no quadro a seguir.

Quadro 21 - Responsáveis pela Continuidade de Negócio

Categorias	Descrições
Manutenção Preventiva:	Realizada semanalmente por setores, onde é feito uma verificação e análise do estado geral dos equipamentos.
Manutenção Corretiva:	Consiste na Correção de falhas e defeitos após sua ocorrência
Solicitação direta:	Solicitação direta solicitação direta sem um chamado formal

Fonte: Elaborado pelos autores (2024)

3.4.2.3 Segurança Física contra o roubo dos dispositivos

Quadro 22 - Segurança Física contra o roubo dos dispositivos

Categorias	Descrições
Estações de trabalho:	➢ Instalar mecanismos de segurança em todas as zonas onde equipamentos sensíveis estão guardados (como servidores), assegurando que o acesso seja restrito apenas aos funcionários autorizados. ➢ Utilizar ambientes com portas duplas (frontal e traseira) que tenham chaves distintas, que possuam chaves diferentes, caso seja necessário acesso controlado, protegendo os datacenters e cluster on-premises. ➢ Registro de acesso às estações de serviço com bloqueios, como um diário de controle ou um sistema de monitoramento de entradas e saídas. ➢ Postos de atendimento designados para cada funcionário. ➢ As salas da diretoria devem permanecer trancadas por padrão, garantindo acesso somente ao pessoal autorizado.

Categorias	Descrições
Dispositivos:	➢ Instalar travas de cabo de segurança (semelhantes aos do tipo Kensington) em notebooks ➢ Configurar a autenticação biométrica ou a autenticação de múltiplos fatores para o acesso a computadores, como uma camada adicional de segurança. ➢ Empregar programas de rastreamento e localização em notebooks corporativos para supervisão e chance de recuperação em situações de furto. ➢ Adicionar criptografia de discos como o Bitlocker, para impedir o vazamento de informações sensíveis ou críticas armazenadas nos laptops da empresa. ➢ Fortalecer as políticas de BYOD para separar os dados da empresa dos dados dos funcionários em seus telefones pessoais.
Outras Medidas:	➢ Instalar fechaduras em armários que contêm equipamentos delicados. ➢ Realizar a implementação de controle de acesso físico nas dependências, limitando a entrada a colaboradores e pessoas autorizadas com crachás magnéticos que apresentem assinaturas particulares para cada trabalhador e visitantes externos. ➢ Implementar sistemas de vigilância por câmeras em locais-chave e realizar auditorias regulares para detectar oportunidades de aprimoramento.

Fonte: Elaborado pelos autores (2024)

3.4.3 Contratação e Recursos Humanos

Quadro 23 - Contratação e Recursos Humanos

Categorias	Descrições
Processo de Seleção:	➢ Comunicar as oportunidades de forma transparente e direta, enfatizando as habilidades técnicas e comportamentais requeridas. ➢ Executar uma análise preliminar de currículos, fundamentada em experiência, educação e trajetória profissional. ➢ Realizar uma entrevista inicial para avaliar competências técnicas e harmonia cultural com o time.
Análise de Histórico e Entrevista Final:	➢ Fazer uma avaliação minuciosa do currículo profissional do candidato, examinando o rendimento em empresas passadas e quaisquer outras competências pertinentes. ➢ Para posições delicadas, levar em conta a verificação de referências para assegurar experiência e integridade. ➢ Nas entrevistas decisivas, envolver um ou mais líderes de equipe para avaliar as competências técnicas e comportamentais do postulante.
Treinamento:	➢ Oferecer um treinamento inicial obrigatório que inclua procedimentos de segurança, práticas de codificação adequadas e regras de privacidade de dados. ➢ Manter um programa de formação constante, que inclui atualizações sobre tecnologias emergentes, segurança digital e metodologias ágeis. ➢ Oferecer certificações ou cursos extras como estímulo para o crescimento profissional.
Qualificações Requeridas:	➢ Estabelecer um mínimo de competências técnicas: domínio das linguagens de programação utilizadas pela organização, frameworks e segurança de software. ➢ Preferência por qualificações e treinamentos especializados, tais como Certificações em Segurança da Informação (por exemplo, Security +, CEH), para os grupos de segurança. ➢ Valorização de competências comportamentais, tais como colaboração em grupo, ética no trabalho e solução de problemas.

Fonte: Elaborado pelos autores (2024)