A.S
ALMEIDA SANTOS
ADVOGADOS

POP – Procedimento Operacional Padrão					
Equipe: 17 TECNOLOGIA DA INFORMAÇÃO					
Atividade: GS – Gestão da Segurança					
Elaborado por:	**Aprovado por:**	**Publicado em:**	**Prox. revisão:**	**Ciclo:**	**ID:**
SJV	JR	27/05/2022	27/05/2026	Anual	17.9
Nome do arquivo: 17.09_GS - Gestao_Da_Seguranca.Docx					

A.S
ALMEIDA SANTOS
ADVOGADOS

Sumário

Objetivo

Definir as diretrizes básicas para a Gestão da Segurança, que compreendem: os processos de Administração contra acessos indevidos, contra-ataque de vírus eletrônicos e backup de segurança de toda a base de dados e arquivos da empresa.

Garantir a proteção das informações entre nossos clientes e a empresa nos aspectos de confidencialidade, integridade e disponibilidade.

Confidencialidade – As informações devem estar disponíveis apenas para pessoas autorizadas;

Integridade – Garantia de que a informação não seja adulterada falsificada ou furtada;

Disponibilidade – Garantia de que a informação esteja disponível sempre que requisitada pelos usuários autorizados mesmo com as interrupções involuntárias de sistemas, ou seja, não intencionais.

Frequência

1. Prazo para Execução

Os procedimentos são executados diariamente ou sob demanda, de acordo com as necessidades que exige as tarefas.

Confidencialidade

2. Administração da Segurança Contra Acesso Indevido

A segurança das informações é baseada na utilização de regras de Firewall (Servidor Linux) monitoração e medidas preventivas para correção de possíveis problemas e tentativas de invasão.

2.1. Controle dos Acessos Externos à Empresa

As regras de entrada de informações foram definidas de modo que todo e qualquer acesso à rede interna seja bloqueado.

Caso seja necessário habilitar algum tipo de acesso aos sistemas internos, o mesmo deverá ser solicitado à área de T.I., para liberação e implementação nas regras atuais.

À área de T.I. controla a segurança contra acessos externos indevidos através da verificação semanal em tempo real nos registros do Firewall.

2.2. Controle dos Acessos Internos

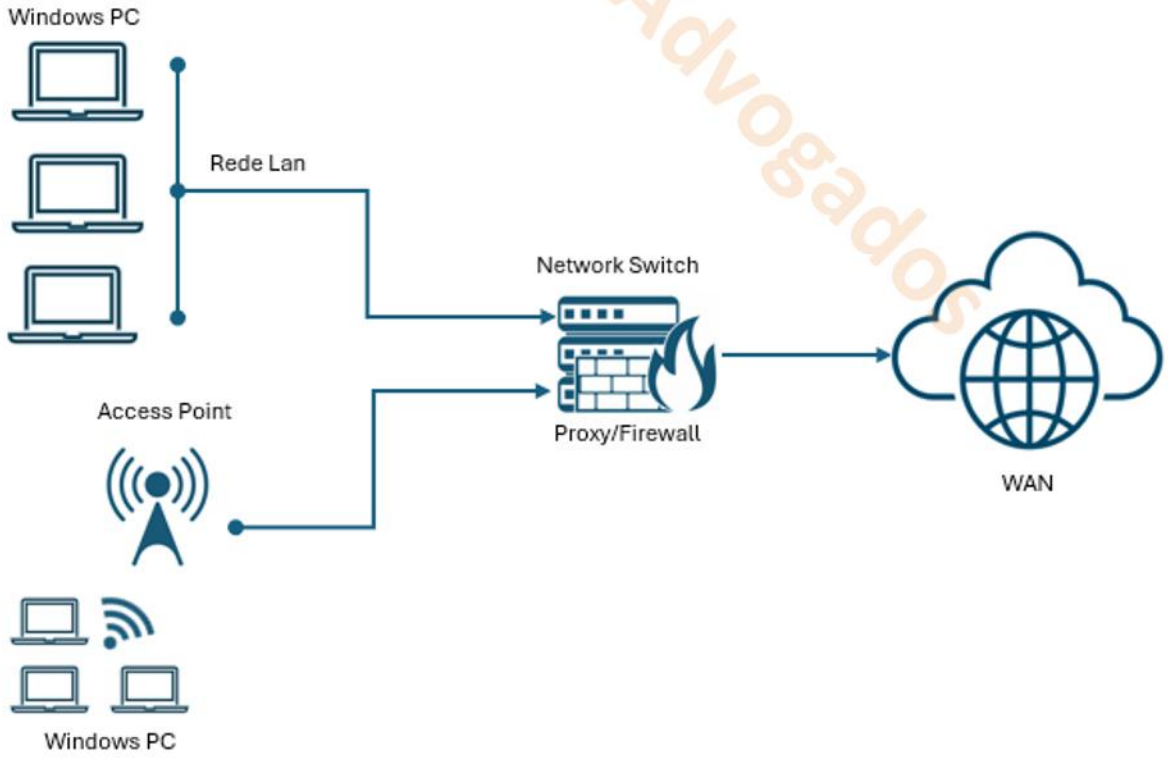
Todos os funcionários do escritório possuem usuário/senha para acessar as informações da rede local, que são configurados para acessar somente as informações necessárias para o desenvolvimento de sua rotina de trabalho. Ver Procedimento: 17.8_Gestao_da_Conectividade, item 2.1. Administração de Usuários na Rede – para maiores detalhes da criação do usuário e sua respectiva senha.

Sempre que houver a necessidade de um funcionário acessar outras informações, deve-se fazer uma solicitação através do sistema de Help Desk por seu Gestor imediato.

Quando alguma empresa terceirizada/fornecedor necessitar de acesso a alguma informação interna da **Almeida Santos Advogados**, deverá solicitar à área de T.I., que irá analisar os riscos antes de disponibilizar ou não o acesso.

2.3. Controle dos Acessos a Internet

O acesso à Internet é controlado por um servidor Proxy (Sistema BSD), sempre que houver necessidade de acesso a algum site o usuário deverá solicitar ao seu Gestor Imediato que avaliará e constatando a necessidade, enviará uma solicitação através do sistema de Help Desk para T.I. seguir com a liberação, aos terceiros/fornecedores deverá ser solicitado à área de T.I., que irá analisar os riscos e disponibilizar o acesso necessários



3. Administração da Segurança Contra-ataque de Vírus

3.1. Rede Local

O software de Antivírus, de um fornecedor específico, está instalado em um servidor (padrão Microsoft) e todos os micros são instalados e atualizados a partir deste servidor, tornando-se clientes, onde recebem todas as atualizações da lista de vírus automaticamente.

A atualização é feita automaticamente pelo servidor, através do link, diretamente na página do fornecedor.

Anualmente, os fornecedores de solução antivírus poderão ser revistos, através de nova homologação do software.

Integridade

4. Backup

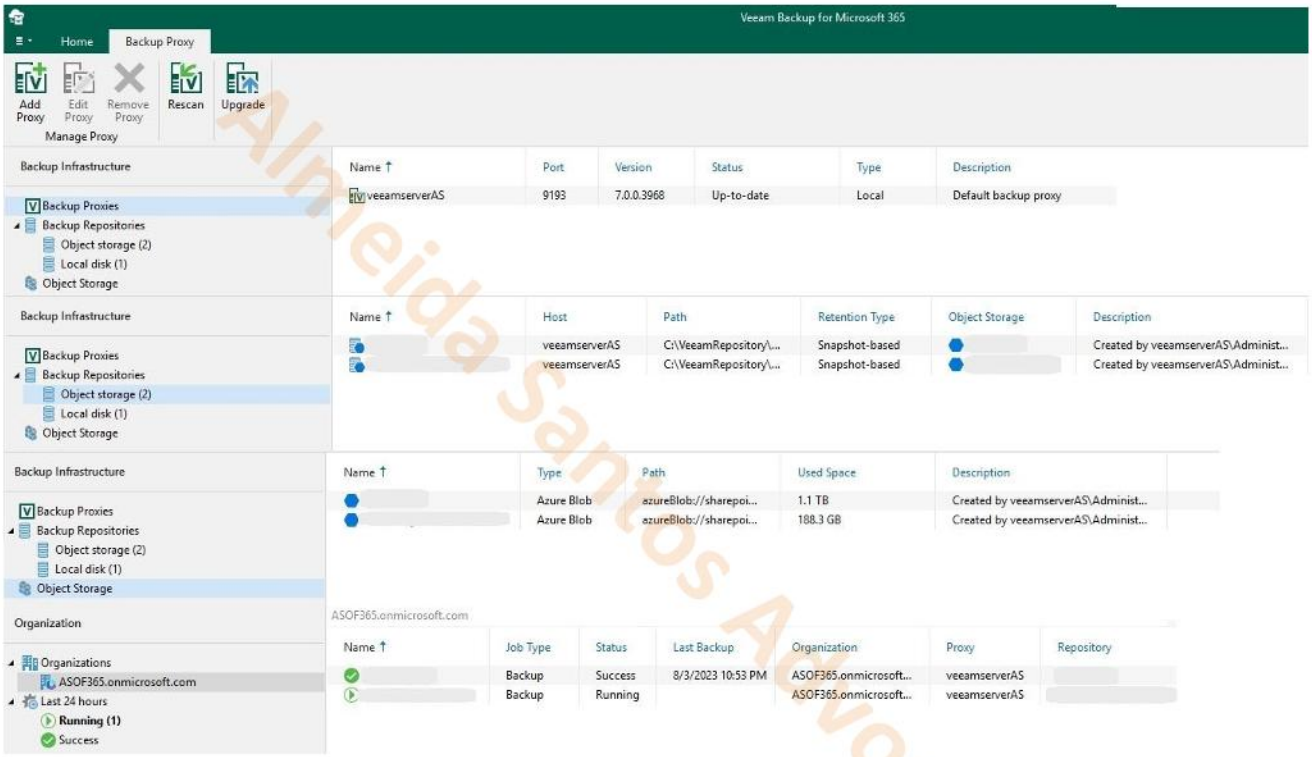
4.1. Backup de Arquivos - Microsoft

Para Microsoft Office SharePoint Online, o tempo de retenção é de 93 dias. Ele começa quando o arquivo é excluido de seu local original. Quando é excluído o item entra na lixeira do conjunto de sites. Ele permanece lá pelo restante dos 93 dias e, em seguida, é excluído permanentemente.

Se excluído da Lixeira ascidentalmente, existe a Lixeira de Segunda Estágio onde é possível recuperar o arquivo deletado.

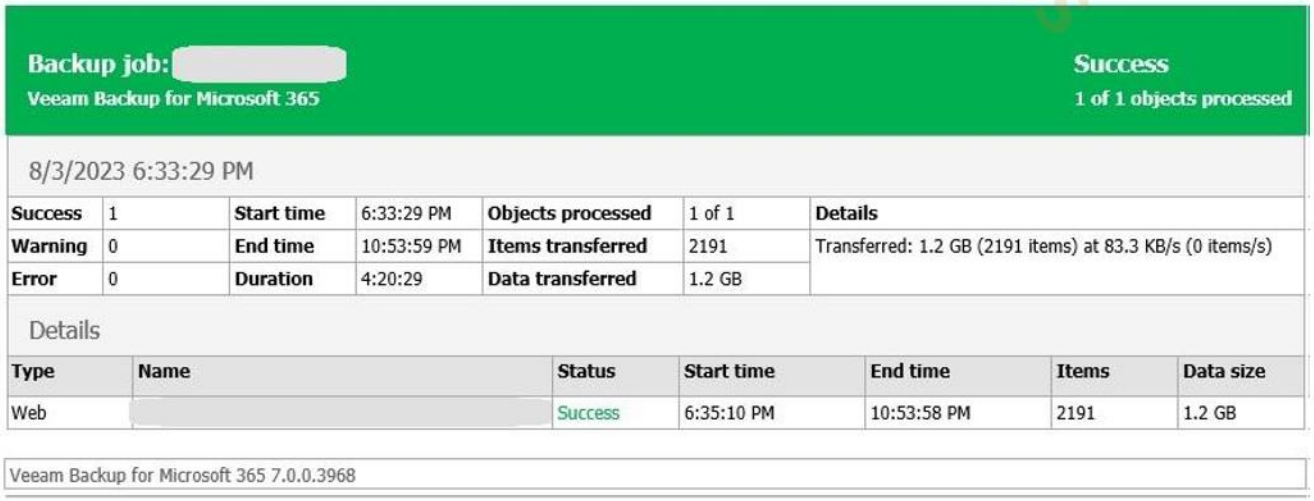
4.2. Backup de Arquivos - Veem

Todas as informações da empresa possuem cópias de segurança, que são gravadas em um ambiente fora da Microsoft, é utilizado um software de terceiro - Veem para excução deste procedimento.



JOB - Diário

Disparo automático na finalização do processo ao e-mail do TI.



Backup job: [redacted]
Veeam Backup for Microsoft 365

Success
1 of 1 objects processed

8/3/2023 6:33:29 PM

Success	1	**Start time**	6:33:29 PM	**Objects processed**	1 of 1	**Details**
Warning	0	**End time**	10:53:59 PM	**Items transferred**	2191	Transferred: 1.2 GB (2191 items) at 83.3 KB/s (0 items/s)
Error	0	**Duration**	4:20:29	**Data transferred**	1.2 GB	

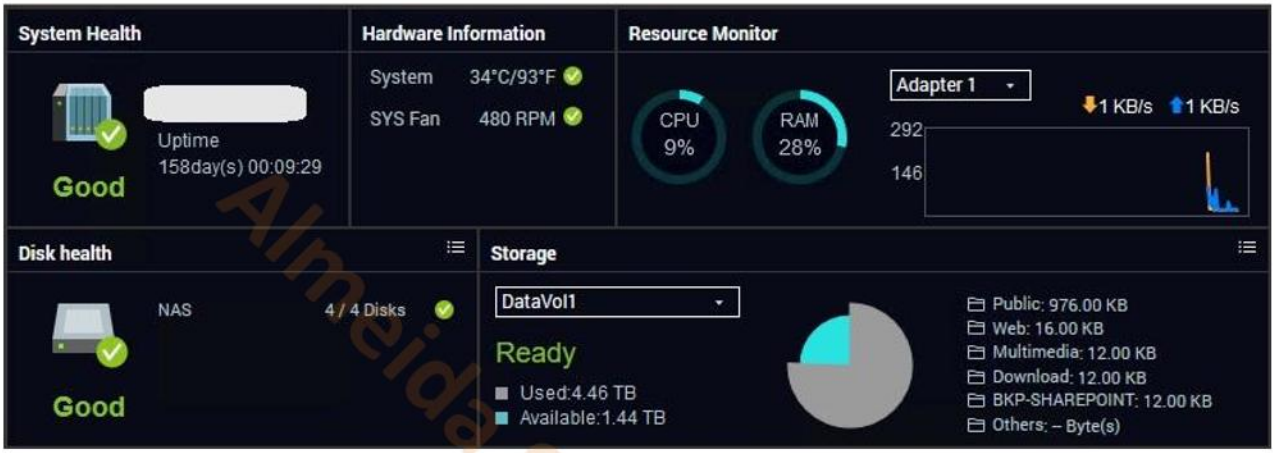
Details

Type	Name	Status	Start time	End time	Items	Data size
Web	[redacted]	Success	6:35:10 PM	10:53:58 PM	2191	1.2 GB

Veeam Backup for Microsoft 365 7.0.0.3968

4.3. Backup de Arquivos - NAS

Estamos configurando como uma terceira opção e contingência um Backup do tipo NAS.



5. Estrutura dos Servidores

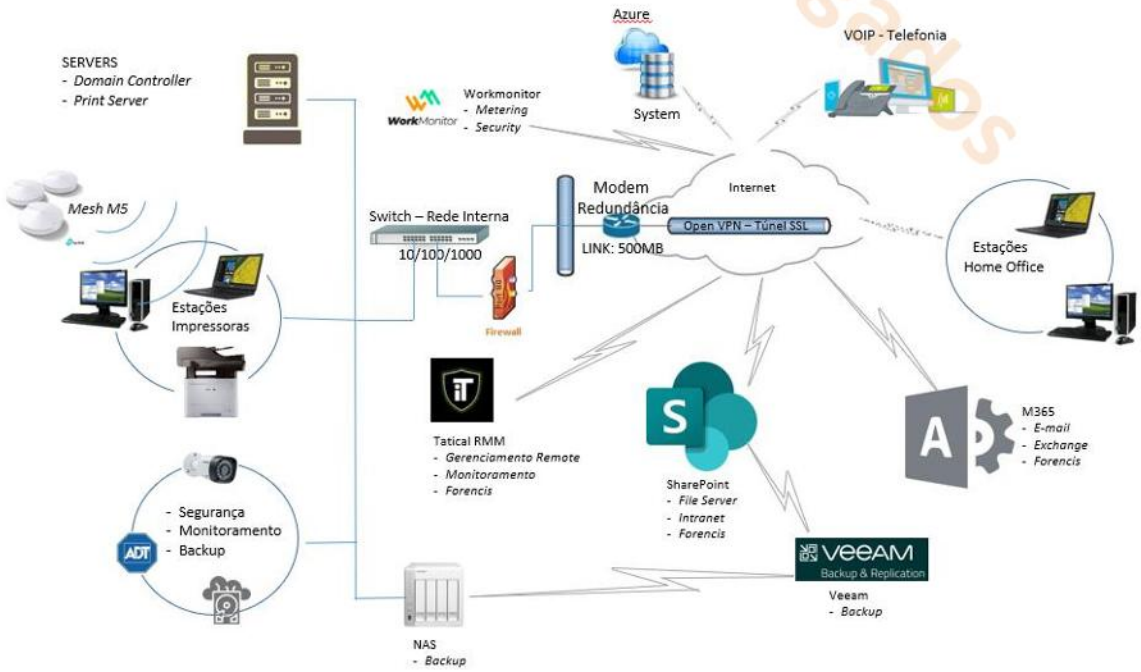
5.1. Rede Interna

Na Rede Interna é configurado o servidor para Autenticação a Rede em sincronismo com Azure AD

As máquinas autenticando na rede interna seguem as GPO´s configuradas no ambiente

As contas de e-mail seguem as GPO´s configuradas no M365 Defender

Topologia de Rede – Global



6. Segurança

6.1. Aplicação Web

Sites Almeida Santos, aplicações web, configuração de header.

Diretivas do apache:

```
Header set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"
```

Diretivas de trecho de código do Apache disponíveis:

6.2. Patching – Atualização dos Sistemas e Aplicações

Script para atualização automatizada dos S.O.

TRMM (Win):Updates

Ensure all services with startup type Automatic are running

Power - Restart or Shutdown PC

Windows 10 Upgrade

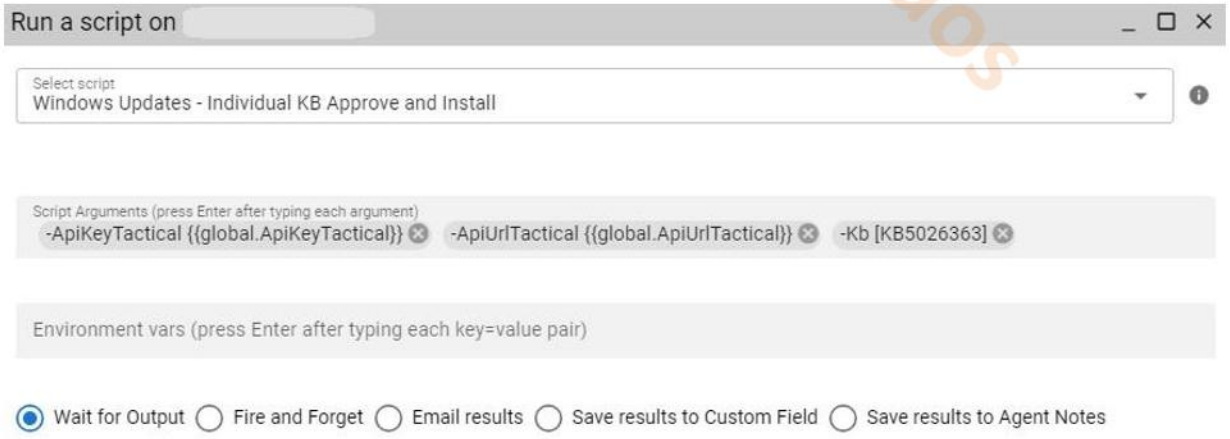
Windows 11 Upgrade Block

Windows 11 Upgrade capable check

Windows Update - Re-enable Microsoft managed Windows Update

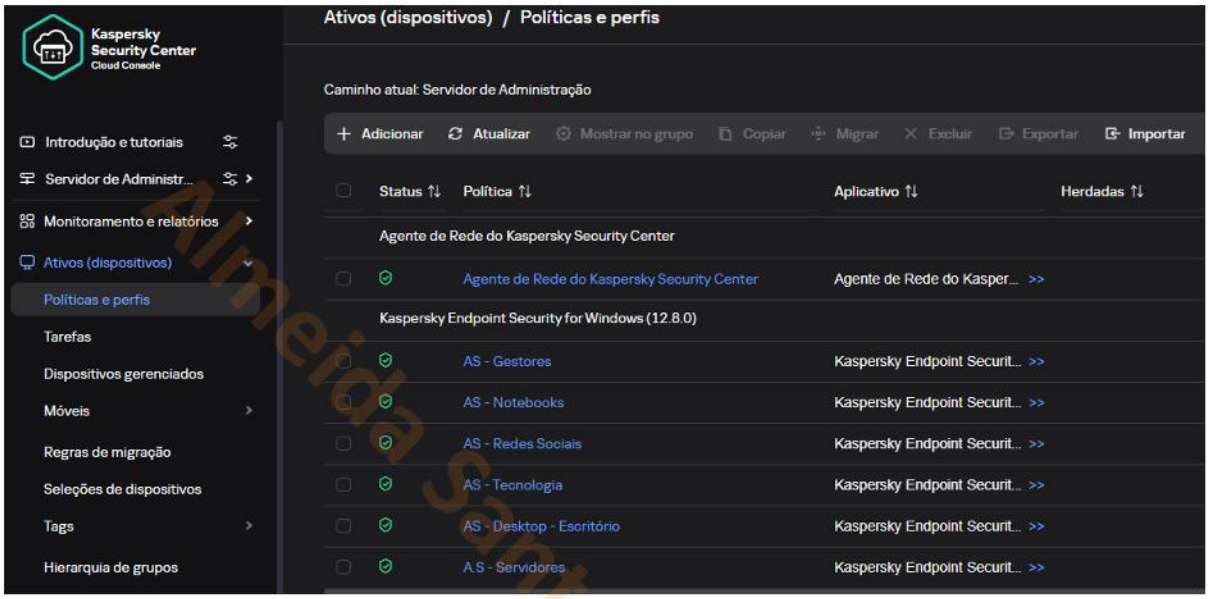
Windows Update - Reset

Windows Updates - Individual KB Approve and Install



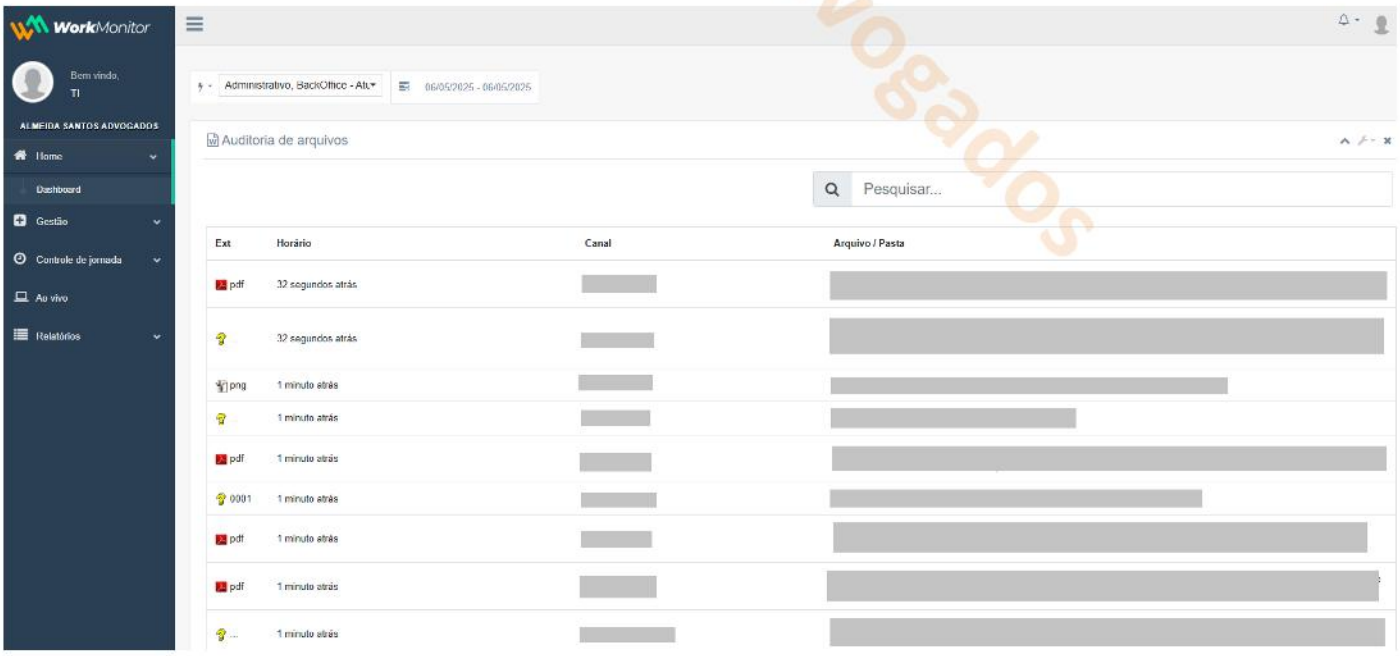
6.3. Controle de Acesso ao código fonte de programas

KSC - Cloud Console - GPO



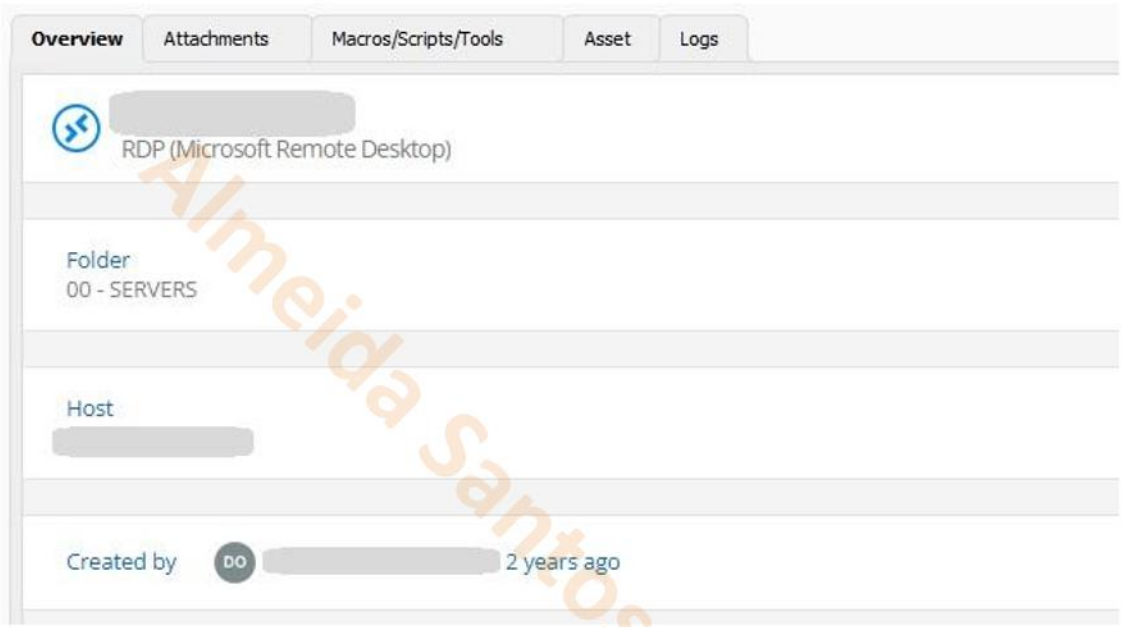
6.4. Rastreabilidade dos arquivos

Workmonitor – Registro de rastreabilidade dos arquivos



6.5. Ambiente Teste

Temos um servidor "terceiro" em nosso ambiente onde é feito os testes necessários para melhoria no ambiente, atualizações, monitoramento.



Disponibilidade

7. Restauração

7.1. Restauração de Backup

Qualquer solicitação de restauração de backup é feita através do sistema Help Desk.

Diariamente são feitos testes de integridade do Backup, este teste é feito automaticamente através do próprio sistema ao finalizar emitindo um resultado. Detectando-se algum problema o sistema envia um alerta para o e-mail da T.I

7.2. Disaster Recover

Os servidores possuem recurso de Disaster Recover, que consiste na restauração rápida do servidor (a partir de discos gerados pelo agente específico do software de backup), sem a necessidade de uma nova instalação completa.

8. Gerador/Nobreak

8.1. Gerador

A empresa possui 01 Gerador com capacidade para atender todas os servidores e pontos de eletrica de todo escritório.

Caso ocorra a queda de energia na região o sistema suporta todo ambiente mantendo os servidores e computadores ligados.

Na Sala dos servidores mantemos 02 (dois) Nobreak com autonomia de 50min, tempo suficiente para subida do gerador que leva 01min para dar carga.

9. Servidor de Autenticação a Rede

9.1. Servidor AD

A empresa possui 03 servidores de Autenticação a rede interna.

02 – Servidores com DFS ativo

01 – Servidor com Active Directory, podendo ser conectado ao NAS que passará a servir como file server da rede se necessário.

Ponto de Atenção

A monitoração das unidades e servidores de Backup será feita através de software específico, onde o mesmo emitirá alertas através de SMS e E-mail ao Gestor de TI e Técnicos para tomarem as medidas necessárias para o restabelecimento dos serviços.

Controle de Atualização

Versão	Data	Alterações
01	27/05/2022	Versão Inicial
02	27/05/2025	Versão Final