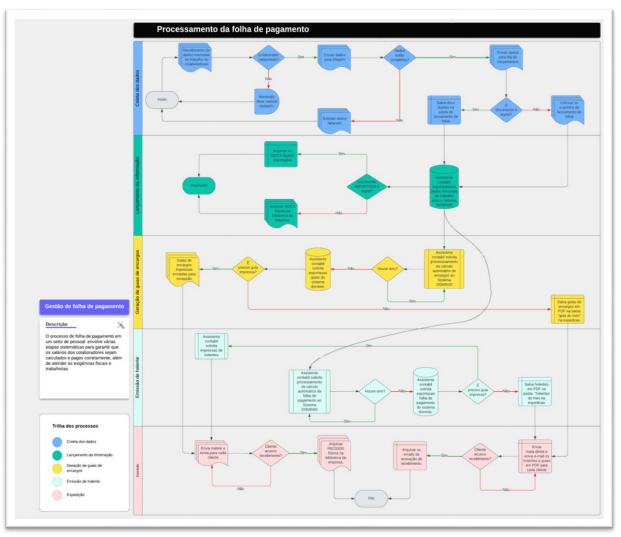


Etapa 2 – Projeto Fundamentos de Sistemas.

Equipe de trabalho

- Alex Chang 856950
- Ana Clara Flaustino Ribeiro 875365
- Emmanuel Teixeira Peixoto 875955
- Jorbralyson Freire 872630
- Mariza Santos da Silva 874807
- Pedro Henrique de Freitas Santos 877752

1. Escolher 1 processo de negócio entre os que foram identificados na etapa 1 e detalhá-lo usando uma ferramenta de construção de fluxograma.



2. Identificar os componentes suscetíveis a eventos de segurança da informação que fazem parte do processo de negócio escolhido vistos no MF de Fundamentos de Segurança.

- Recebimento de dados mensais de trabalho de colaboradores
- Triagem de completudes dos dados
- Envio dos dados recebidos para fila de lançamentos
- Salva os dados digitais recebidos na pasta de "lançamento de folha"
- Colocar os dados físicos recebidos no escaninho do setor lançamento de folha
- Assistente contábil importa/insere dados mensais de trabalho para o sistema DOMINIO
- Arquivar os DOCS digitais recebidos e processados
- Arquivar DOCS físicos recebidos e processados na biblioteca da empresa.
- Assistente contábil solicita processamento de cálculo automático de encargos ao Sistema DOMINIO.
- Salva guias de encargos do mês, em PDF, na pasta "guia do mês" na expedição
- Assistente contábil solicita processamento de cálculo automático da folha de pagamento ao Sistema DOMINIO
- Assistente contábil solicita exportação folha de pagamento do sistema DOMINIO
- Assistente contábil solicita impressão de holerites
- Salva holerites do mês, em PDF, na pasta "holerites do mês" na expedição
- Envia malote com as guias impressas para cada cliente
- Arquivar RECIBOS físicas na biblioteca da empresa.
- Envia mala-direta e envia e-mail os holerites e guias em PDF para cada cliente

3. Mapear itens relacionados à TI invisível na organização.

Setor	Item de TI não catalogado	Proprietário	Usuários		- Risco		Obs.
Todos	Whatsapp web	Colaboradores	Colaboradores	-	Violação de confidencialidade.	-	Aplicar o uso do WhatsApp Empresarial como o único meio autorizado de comunicação com os clientes. Deixar claro que o uso fora das normas constitui uma violação grave das políticas da empresa e pode resultar em responsabilização.

Todos	Google driver	Colaboradores	Colaboradores	- Perda de controle sobre a informação	-	Aplicar o uso de um google drive empresarial como o único meio autorizado de comunicação com os clientes. Deixar claro que o uso fora das normas constitui uma violação grave das políticas da empresa e pode resultar em responsabilização.
-------	---------------	---------------	---------------	----------------------------------------------	---	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

4. Identificar dispositivos pessoais utilizados na organização.

Setor	Dispositivo	Proprietário	Usuários	Risco	Obs.
Todos	Smartphones pessoais	Colaboradores	Colaboradores	- Violação de confidencialidade.	 Ter ambientes demarcados proibindo ou permitindo o uso de aparelhos celulares pessoais. Deixar claro que o uso em locais não permitidos constitui uma violação grave das políticas da empresa e pode resultar em responsabilização.

5. Identificar riscos de segurança física e lógica discutidos no MF de Fundamentos de Segurança da Informação e encontrados no contexto organizacional estudado.

Ativo	Ameaça	Vulnerabilidade
Estações de trabalho	 Vazamento de informação; Perdas financeiras; Usuários com contas de acesso de administrador. 	 Porta USB liberada; Software não licenciado; Perdas de dados e paradas dos processos da empresa.
Servidor	Paradas por falhas da fonte de energia.	Sem redundância de fonte de energia.
Servidor de arquivos	 Vazamento de informação 	Controle de acesso funcionando sem compartimentação da informação.
Gateway da rede	Ataques hackers	Ausência de firewall.
Sala da biblioteca	Incêndio; Acesso por pessoal não autorizado.	 Ausência de extintor de incêndio. Sem controle de acesso a sala.
Sala do servidor	1. Temperatura	Ausência de controle de temperatura

Ī	Infraestrutura da Rede	1.	Cabos passando por áreas	1.	Possibilidades de acesso indiscriminado a rede.
	Local		externas sem proteção.		
Ī	switch	1.	Paradas por falhas da fonte de	1.	Sem redundância de fonte de energia.
			energia.		

6. Elaborar uma Política de Segurança da informação para a organização estudada e baseada em modelo disponibilizado em material de apoio da etapa 2.

Política apresentado no documento anexo de acordo com modelo disposto da etapa 2.