ATA DE REUNIÃO

EMPRESA	Portal Vidros	**MODALIDADE**	Remota
PROJETO	Adequação à LGPD	**DATA**	20/06/2023
TIPO DE REUNIÃO	Reunião de Alinhamento de Sprint	**N° DA ATA**	P049-06

TEMA DA REUNIÃO	Sprint 5	**MINISTRANTE**	Fábio Anjos
OBJETIVO	Relatar status das tarefas da Sprint passada e listar as tarefas dessa.	**LINK DA GRAVAÇÃO**	2.1.7. [PORTAL VIDROS] ADEQUAÇÃO LGPD (20/06/2023)

PARTICIPANTES	
Fábio Anjos - CMC Business	Karyta Lebre - Portal Vidros
Genilson Noronha - CMC Business	

PAUTA
Tarefas da Sprint 4 a serem validadas durante a reunião:
2.7.1 Assegurar que a infraestrutura de rede esteja atualizada
2.7.2 Manter uma arquitetura de rede segura
2.7.6 Assegurar que os dispositivos remotos estejam se conectando a uma infra AAA da empresa
2.7.7 Manter recursos dedicados para o administrativo
2.7.8 Estabelecer e manter um processo de configuração segura
2.7.9 Estabelecer um inventário de contas
2.7'.11 Restringir privilégios de administrador a contas dedicadas
2.7'.12 Estabelecer um inventário de contas de serviço
2.7'.13 Centralizar a gestão de contas
Tarefas pendentes da Sprint 4
2.2.1. Aditivar contratos
2.7.3 Gerenciar a rede com segurança
2.7.4 Centralizar AAA de rede
2.7.5 Usar protocolos de comunicação e gestão de rede seguros
2.7'.10 Desabilitar contas inativas
Assuntos a serem tratados
- Possibilidade de que as nossas sprints tenham períodos de 4 semanas ao invés de 2.

RELATÓRIO

A reunião iniciou no horário previsto com os partícipes: Karyta Lebre, Fábio Anjos e Genilson Noronha; e tratou da atualização dos status das tarefas da Sprint 4 e a definição das tarefas da Sprint 5.

Tarefas da Sprint 4 registradas como concluídas:
- 2.7.1 Assegurar que a infraestrutura de rede esteja atualizada
- 2.7.2 Manter uma arquitetura de rede segura
- 2.7.6 Assegurar que os dispositivos remotos estejam se conectando a uma infra AAA da empresa
- 2.7.7 Manter recursos dedicados para o administrativo
- 2.7.8 Estabelecer e manter um processo de configuração segura
- 2.7.9 Estabelecer um inventário de contas
- 2.7'.11 Restringir privilégios de administrador a contas dedicadas
- 2.7'.12 Estabelecer um inventário de contas de serviço
- 2.7'.13 Centralizar a gestão de contas

Tarefas da Sprint 4 proteladas para a Sprint 5:
- 2.2.1. Aditivar contratos
- 2.7.3 Gerenciar a rede com segurança
- 2.7.4 Centralizar AAA de rede
- 2.7.5 Usar protocolos de comunicação e gestão de rede seguros
- 2.7'.10 Desabilitar contas inativas

21 Novas tarefas foram inseridas na Sprint 5:
- 2.3.3. Criar instância de SI
- 2.3'.11 Configurar o bloqueio automático de sessão nos ativos corporativos
- 2.3'.12 Instalar e manter um software anti-malware
- 2.3'.13 Configurar atualizações automáticas anti-malware
- 2.3'.14 Desabilitar a execução automática para mídias removíveis
- 2.3'.15 Configurar a varredura anti-malware automática de mídia removivel
- 2.3'.16 Habilitar recursos anti-exploração
- 2.3'.17 Gerenciar o software anti-malware de maneira centralizada
- 2.3'.18 Usar software anti-malware baseado em comportamento

- 2.3'.18 Usar software anti-malware baseado em comportamento
- 2.3'.19 Centralizar alerta de eventos de segurança
- 2.3'.20 Ajustar limites de alerta para eventos de segurança
- 2.3'.21 Implantar uma solução de detecção de intrusão de rede
- 2.3'.22 Realizar filtragem de tráfego entre segmentos de rede
- 2.3'.23 Gerenciar controle de acesso para ativos remoto
- 2.3'.24 Coletar logs de fluxo de tráfego da rede
- 2.3'.25 Implantar solução de prevenção de intrusão baseada em host
- 2.3'.26 Implantar uma solução de prevenção de intrusão de rede
- 2.3'.27 Executar filtragem da camada de aplicação
- 2.4.3 Elaborar PSI
- 2.4'.12 Elaborar política de backup
- 2'.11.1 Elaborar plano de resposta a incidentes

Foram também esclarecidas algumas dúvidas acerca das tarefas 2.4.3 Elaborar PSI e 2.4'.12 Elaborar política de backup.

PLANO DE AÇÃO		
O QUE DEVE SER FEITO?	**RESPONSABILIDADE**	**PRAZO**
Tarefas para Sprint 5 (27)		
1.1.5 Ministrar palestra de conscientização	Fábio Anjos	20/06/2023 - 04/07/2023
2.2.1. Aditivar contratos	Karyta Lebre e Alexandre Marques	20/06/2023 - 04/07/2023
2.3.3. Criar instância de SI		
2.3'.11 Configurar o bloqueio automático de sessão nos ativos corporativos		
2.3'.12 Instalar e manter um software anti-malware		
2.3'.13 Configurar atualizações automáticas anti-malware		
2.3'.14 Desabilitar a execução automática para mídias removíveis		
2.3'.15 Configurar a varredura anti-malware automática de mídia removivel		
2.3'.16 Habilitar recursos anti-exploração		
2.3'.17 Gerenciar o software anti-malware de maneira centralizada		
2.3'.18 Usar software anti-malware baseado em comportamento		
2.3'.19 Centralizar alerta de eventos de segurança		
2.3'.20 Ajustar limites de alerta para eventos de segurança		
2.3'.21 Implantar uma solução de detecção de intrusão de rede		
2.3'.22 Realizar filtragem de tráfego entre segmentos de rede		
2.3'.23 Gerenciar controle de acesso para ativos remotos		
2.3'.24 Coletar logs de fluxo de tráfego da rede		
2.3'.25 Implantar solução de prevenção de intrusão baseada em host		
2.3'.26 Implantar uma solução de prevenção de intrusão de rede		
2.3'.27 Executar filtragem da camada de aplicação		
2.4.3 Elaborar PSI		
2.4'.12 Elaborar política de backup		
2.7.3 Gerenciar a rede com segurança		
2.7.4 Centralizar AAA de rede		
2.7.5 Usar protocolos de comunicação e gestão de rede seguros		
2.7'.10 Desabilitar contas inativas		
2'.11.1 Elaborar plano de resposta a incidentes		