PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS (PUC MINAS)

Política de Segurança

Manufatura de Eletrônicos

Unitech Industries

Participantes: Gregory Stevão Amilar Costa, João Pedro Reis Martins, Nicolas Cleiton Basilio Viana, Vitor Luz de Sales

Orientador: Prof. Alexandre Teixeira

Uma política de segurança de modelo é um conjunto de diretrizes e práticas que visa proteger e gerenciar os recursos de uma organização, incluindo informações, ativos e tecnologias, e garantir a integridade, confidencialidade e disponibilidade desses recursos. Aqui está um exemplo de uma política de segurança de modelo:

1. Introdução

1.1. Objetivo

Esta política tem como objetivo estabelecer diretrizes e requisitos que garantam a segurança da informação na Unitech Industries, assegurando a proteção dos ativos corporativos e mantendo a Confidencialidade, Integridade e Disponibilidade (CID). Além disso, define controles e medidas adicionais necessários para mitigar riscos, padronizar procedimentos e apoiar a continuidade das operações.

1.2. Escopo

Esta política se aplica a todos os funcionários, contratados, fornecedores e parceiros que lidam com informações, sistemas, dispositivos ou qualquer recurso tecnológico da Unitech Industries. Abrange todas as unidades (Matriz, Fábrica e Centros de Distribuição), bem como o ambiente em nuvem configurado na AWS.

2. Princípios de Segurança (Tríade CID)

2.1. Confidencialidade

Assegurar que as informações sejam acessadas apenas por pessoas autorizadas e devidamente autenticadas. Para isso, devem ser aplicadas práticas como a classificação das informações (Pública, Interna, Confidencial e Restrita), o uso de criptografia, além da restrição de acesso baseada no princípio do menor privilégio. O compartilhamento de credenciais e senhas é proibido.

2.2. Integridade

Garantir que as informações estejam corretas, completas e não tenham sido alteradas de forma não autorizada. Isso envolve procedimentos como controle de versões, trilhas de auditoria em sistemas críticos e aplicação formal de processos de gestão de mudanças antes de qualquer alteração em sistemas, dados ou infraestrutura. Backups devem ser testados periodicamente para garantir sua integridade.

2.3. Disponibilidade

Assegurar que os sistemas, informações e recursos de TI estejam acessíveis sempre que necessário. Para isso, devem ser implementados backups automáticos, redundância de links e equipamentos críticos, políticas de continuidade, além de soluções de energia (UPS e geradores) que reduzam riscos de interrupção.

3. Gerenciamento de Acesso

3.1. Controle de Acesso

O controle de acesso deve ser implementado por meio do Active Directory (AD), segregado por unidades como Matriz, Fábrica e Centros de Distribuição, com criação e remoção de contas exclusivamente via requisições formais. Contas inativas por mais de 30 dias devem ser desabilitadas automaticamente, e o acesso remoto deve ocorrer apenas por meio de VPN corporativa com autenticação reforçada.

3.2. Autenticação

O uso de senhas fortes é obrigatório, seguindo os padrões: mínimo de 10 caracteres, combinação de maiúsculas, minúsculas, números e caracteres especiais. As senhas devem ser trocadas a cada 90 dias, e após cinco tentativas incorretas a conta deve ser bloqueada temporariamente. A autenticação multifator deve ser utilizada nos sistemas críticos e no acesso ao ambiente de nuvem.

3.3. Autorização

Os usuários devem possuir apenas as permissões necessárias ao desempenho de suas funções, garantindo o princípio do menor privilégio (Need-to-Know), com permissões organizadas por meio de GPOs e OUs no AD segmentadas por unidade (Matriz, Fábrica e CDs). Revisões periódicas (trimestrais) devem ser realizadas para verificar e ajustar acessos. Também devem ser aplicadas políticas que restrinjam o uso de dispositivos externos, instalação de softwares e configurações de firewall local por GPO.

4. Segurança Física e Ambiental

4.1. Proteção de instalações

Devem ser implementadas medidas de segurança para proteger as unidades da organização contra acessos indevidos, interferências externas, danos físicos e interrupções operacionais. Entre essas medidas, incluem-se:

- Vigilância presencial e remota
    - Utilização de câmeras de CFTV com gravação contínua em pontos estratégicos (portarias, corredores, áreas externas, salas técnicas e acessos restritos
    - Monitoramento em tempo real na sala de controle ou por empresa terceirizada especializada
    - Retenção mínima de 30 dias das gravações, com acesso restrito apenas a equipe autorizada.

- Controle perimetral
    - Cercamento físico das áreas externas com grades, muros ou alambrados adequados ao nível de risco da unidade
    - Instalação de sensores de movimento e alarmes perimetrais conectados ao sistema de vigilância
    - Iluminação reforçada em áreas externas, especialmente em estacionamentos, acessos de carga/descarga e pontos de baixa visibilidade.

- Portarias e controle de entrada
    - Presença de equipe de portaria (própria ou terceirizada) treinada em verificação de identidade, registro e autorização de entrada
    - Torniquetes, cancelas ou portas com controle eletrônico para garantir que o acesso seja realizado de forma individual e registrada.

- Identificação obrigatória de visitantes
    - Registro formal de visitantes em sistema ou livro de acesso (incluindo nome, documento, empresa, motivo da visita e responsável interno
    - Emissão de crachás de visitante com designação de acesso limitado e validade exclusiva para o dia/horário da visita
    - Acompanhamento obrigatório por um funcionário autorizado durante toda a permanência do visitante nas dependências internas.

- Proteção de áreas críticas
    - Salas de servidores, racks, datacenters ou armários de telecom devem permanecer trancados e equipados com sistemas de controle de acesso físico (crachá, fechadura eletrônica ou biometria
    - Instalação de sensores de abertura não autorizada e alarmes conectados ao sistema de segurança.

- Procedimentos para entrada de veículos e cargas
    - Controle de acesso de veículos com registro de placas e autorização prévia quando aplicável
    - Inspeção visual de cargas, entregas e materiais antes de adentrarem a área interna, especialmente em Centros de Distribuição.

- Gestão de chaves e permissões
    - Chaves físicas devem ser inventariadas, numeradas e armazenadas em local seguro
    - Em caso de troca de funcionários ou perda de chaves, deve-se revogar imediatamente o acesso e, se necessário, realizar troca das fechaduras.

- Prevenção contra danos físicos e incidentes
    - Instalação de estruturas de proteção contra quedas, impactos e infiltrações em áreas que armazenam equipamentos sensíveis
    - Inspeções periódicas das condições físicas das instalações, assegurando que portas, janelas, fechaduras, alarmes e câmeras estejam funcionando adequadamente.

4.2. Controle de acesso físico

Áreas críticas, como salas de servidores e racks, devem possuir controle de acesso reforçado, utilizando crachás, fechaduras eletrônicas e registro permanente de entradas e saídas. O acesso deve ser restrito a pessoal autorizado e suas permissões revisadas regularmente.

4.3. Segurança ambiental

Devem ser adotados sistemas de detecção de fumaça, alarme e combate a incêndios, além de monitoração constante da temperatura e umidade. No-breaks e geradores devem garantir o funcionamento dos principais serviços durante falhas de energia, e o cabeamento deve ser mantido conforme padrões de organização.

5. Segurança de Redes e Comunicações

5.1. Proteção de redes

Implementar controles de segurança para proteger as redes da organização (interligadas por Roteadores Cisco 4331 e Switches Cisco Catalyst 2950T) contra ameaças externas e internas. Isso inclui a segmentação da rede por unidade (Matriz: 192.168.1.0/24; Fábrica: 192.168.2.0/24; CD's: 192.168.3.0/24 e 192.168.4.0/24). O ambiente de nuvem (AWS VPC) deve ser protegido por Grupos de Segurança e Network Access Control Lists (NACLs) com regras bem definidas.

5.2. Monitoramento e detecção de intrusões

Ferramentas como Zabbix devem monitorar continuamente servidores, VMs e dispositivos de rede, utilizando protocolos seguros como SNMP. Alertas devem ser gerados automaticamente em caso de anomalias. Os logs de firewall, servidores e Active Directory devem ser reunidos em um mecanismo centralizado (SIEM) para análise de eventos.

6. Gestão de Incidentes de Segurança

6.1. Resposta a incidentes

Deve existir um Plano de Resposta a Incidentes (PRI) documentado, contendo processos claros e padronizados para identificar, registrar, tratar e solucionar eventos de segurança da informação. O PRI deve incluir:

A. Classificação dos incidentes

O plano deve definir níveis de severidade para orientar a resposta:

- Nível 1 – Baixo impacto:
  Incidentes sem impacto operacional significativo, como tentativas de login sem sucesso, e-mails suspeitos bloqueados pelo filtro ou falhas isoladas em dispositivos.

- Nível 2 – Médio impacto:
  Incidentes que podem comprometer dados internos, serviços específicos ou usuários, como infecção por malware em uma estação, acesso indevido a pastas compartilhadas, falhas de configuração ou interrupções temporárias de algum serviço não crítico.

- Nível 3 – Alto impacto / Crítico:
  Incidentes que comprometem a confidencialidade, integridade ou disponibilidade de sistemas essenciais, incluindo:

    - Ransomware
    - Vazamento de dados (LGPD)
    - Violação de credenciais privilegiadas
    - Indisponibilidade prolongada de sistemas críticos
    - Intrusão confirmada na rede ou infraestrutura de TI

A severidade determina prazos, responsáveis e prioridade de resposta.

B. Responsáveis e papéis no PRI

O plano deve especificar os responsáveis pela gestão de incidentes:

- Equipe de Segurança da Informação (ESI): coordena o tratamento, classifica o incidente, conduz análises e orienta a contenção
- Equipe de TI: executa ações técnicas (bloquear acessos, isolar máquinas, restaurar backups
- Gestores das áreas afetadas**:** oferecem informações, validam decisões e comunicam impactos à operação
- Equipe Jurídica/Compliance: avalia obrigações legais, especialmente em casos de vazamento de dados (LGPD)
- Diretoria: aciona o comitê de crise em situações críticas e aprova decisões estratégicas
- Comitê de resposta (quando necessário): grupo multidisciplinar ativado para incidentes severos.

C. Formas de comunicação

O PRI deve estabelecer canais e procedimentos formais de comunicação:

- Canal interno exclusivo para reporte (e-mail, sistema, telefone de plantão
- Registro obrigatório do incidente em ferramenta apropriada (ex.: GLPI, OTRS, Service Desk
- Comunicação imediata da equipe de TI para a equipe de Segurança da Informação ao identificar eventos suspeitos
- Avisos formais à diretoria em caso de incidentes de alto impacto
- Comunicação externa, quando necessária, envolvendo
    - autoridades competentes (ex.: ANPD em casos de LGPD)
    - fornecedores críticos (ex.: suporte de firewall, AWS)
- **Relatórios pós-incidente** enviados às áreas envolvidas.

D. Etapas do tratamento de incidentes

O PRI deve seguir um fluxo estruturado, composto pelas seguintes etapas:

1. Identificação

Detecção do incidente por usuários, sistemas de monitoramento (Zabbix, SIEM), logs ou alertas de segurança.
Nesta fase, registrar: data/hora, local, dispositivo, usuário envolvido e descrição do evento.

2. Análise e classificação

Avaliação inicial pela equipe de Segurança da Informação para determinar:

- tipo do incidente;
- impacto potencial;
- severidade;
- necessidade de acionar responsáveis adicionais.

3. Contenção

Ação imediata para impedir o avanço do incidente. Pode incluir:

- isolamento de máquinas comprometidas;
- bloqueio temporário de contas;
- segmentação de rede;
- desativação de serviços suspeitos;
- bloqueio de tráfego malicioso no firewall.;

A contenção pode ser **curto prazo** (emergencial) ou **longo prazo** (ação para prevenir recorrência enquanto o problema é analisado).

4. Erradicação

Ações para remover completamente a causa raiz do incidente, como:

- remoção de malware;
- aplicação de patches de segurança;
- correção de vulnerabilidades;
- redefinição de credenciais e chaves;
- limpeza de arquivos ou serviços comprometidos.

5. Recuperação

Restauração dos sistemas ao funcionamento normal, garantindo que o incidente não reapareça.
Inclui:

- restauração de backups confiáveis;
- validação de integridade dos dados
- monitoramento reforçado após a liberação
- validação com áreas de negócio.

6. Encerramento e lições aprendidas

Após o incidente, deve ser criado um relatório contendo:

- descrição detalhada;
- ações executadas;
- impactos observados;
- falhas nos controles;
- recomendações de melhoria;
- prazos para implementação de correções.

Esse relatório deve ser armazenado para auditorias futuras e utilizado para melhorar os processos de resposta.

E. Testes e validações

Para garantir a eficácia do PRI, devem ser realizados:

- Simulados anuais de incidentes, cobrindo diferentes cenários (ransomware, interrupção de serviços, falha de backup, vazamento de dados).
- **Testes de comunicação**, verificando tempo de resposta das equipes.
- **Avaliações pós-teste**, documentando pontos fortes e lacunas no processo.
- **Atualizações do PRI**, refletindo melhorias identificadas nos simulados.

F. Documentação e armazenamento

Todos os incidentes, ações e decisões devem ser registrados e armazenados por no mínimo **24 meses**, garantindo rastreabilidade, auditoria e conformidade legal.

6.2. Relatórios de incidentes

Todos os funcionários devem comunicar imediatamente qualquer incidente, suspeita ou irregularidade relacionada à segurança da informação utilizando exclusivamente os meios formais definidos pela organização.

A comunicação deve ocorrer preferencialmente por e-mail institucional destinado ao reporte de incidentes ou pelo sistema corporativo de chamados, que permite registro estruturado e anexação de evidências.

Em situações de urgência, é permitido o uso do telefone corporativo de contingência ou de canal interno de comunicação rápida, desde que o incidente seja posteriormente formalizado nos meios oficiais. Incidentes classificados como de maior impacto devem ser comunicados à direção de forma ágil, por e-mail ou contato direto, assegurando registro adequado. Todos os registros e comunicações devem permanecer armazenados por pelo menos 24 meses em repositório seguro.

7. Conscientização e Treinamento em Segurança

7.1. Programa de conscientização

A organização deve implementar um programa contínuo de conscientização em segurança da informação, proporcionando campanhas internas, materiais educativos e comunicações sobre riscos, golpes e práticas adequadas.

7.2. Treinamento em segurança

Treinamentos sobre boas práticas, proteção de dados, uso seguro de dispositivos, prevenção contra phishing e demais ameaças devem ser oferecidos regularmente, incluindo a realização de simulações de ataques para avaliação e melhoria do comportamento dos usuários.

8. Avaliação e Melhoria Contínua

8.1. Auditorias de segurança

Devem ser realizadas auditorias de segurança de forma periódica para verificar a conformidade dos controles implementados, identificar desvios, avaliar a eficácia dos mecanismos de proteção e confirmar se os procedimentos adotados estão alinhados às diretrizes da PSI e às normas aplicáveis.

Essas auditorias podem incluir revisões documentais, entrevistas, inspeções técnicas, testes de conformidade e avaliações automatizadas. Além disso, testes de penetração internos e externos devem ser executados regularmente,

a fim de simular ataques reais e identificar vulnerabilidades técnicas que possam ser exploradas. Os resultados devem ser documentados, analisados e utilizados como base para ações corretivas e melhorias contínuas.

8.2. Revisão de políticas e procedimentos

A Política de Segurança da Informação e seus procedimentos associados devem ser revisados de maneira sistemática para garantir que permaneçam atualizados diante de mudanças tecnológicas, evolução das ameaças, alterações regulatórias e necessidades operacionais da organização.

Essa revisão deve ocorrer ao menos uma vez por ano ou sempre que houver uma modificação significativa na infraestrutura, no modelo de negócios ou nos requisitos legais. O processo de revisão deve incluir avaliação crítica do conteúdo atual, análise de falhas identificadas em auditorias e incidentes anteriores, além de consulta às áreas envolvidas para validar a aplicabilidade e eficácia das diretrizes vigentes.

8.3. Análise de riscos

A organização deve manter um processo contínuo de análise de riscos voltado para identificar, avaliar e priorizar ameaças e vulnerabilidades que possam afetar os ativos de informação.

Essa análise deve considerar fatores como probabilidade de ocorrência, impacto potencial e eficácia dos controles existentes. Com base nos resultados, devem ser definidas ações de mitigação compatíveis com o apetite de risco da instituição, incluindo implementação de novos controles, reforço de medidas existentes ou revisão de processos operacionais. Esse ciclo deve ser renovado periodicamente e sempre que houver mudanças relevantes na infraestrutura, nos serviços prestados ou no ambiente regulatório.

8.4. Medição de desempenho

Devem ser utilizadas métricas e Indicadores-Chave de Desempenho (KPIs) para avaliar a eficiência dos controles de segurança e acompanhar a evolução do programa de Segurança da Informação ao longo do tempo. Esses indicadores podem incluir tempo médio de resposta a incidentes, taxa de resolução, número de vulnerabilidades críticas corrigidas dentro do prazo, adesão aos treinamentos de segurança, disponibilidade dos sistemas e demais métricas relevantes para o ambiente corporativo. Os resultados devem ser analisados periodicamente e reportados à direção, servindo de base para ajustes estratégicos, priorização de investimentos e ações de melhoria contínua.

9. Conformidade Legal e Regulatória

9.1. Conformidade com leis e regulamentações

Todas as práticas relacionadas à segurança da informação devem estar estritamente alinhadas às leis, normas e regulamentações aplicáveis, incluindo a Lei Geral de Proteção de Dados (LGPD) e demais legislações setoriais pertinentes às atividades da organização. Isso exige que os processos internos considerem princípios como necessidade, finalidade, minimização de dados, transparência e proteção dos titulares.

Devem ser mantidos mecanismos de controle que assegurem o tratamento adequado das informações pessoais, incluindo registro de operações, avaliação de impacto à privacidade quando necessário e adoção de salvaguardas técnicas e administrativas adequadas. Além disso, a organização deve acompanhar atualizações regulatórias e decisões de autoridades competentes, garantindo que as políticas internas sejam atualizadas sempre que houver mudanças relevantes no cenário legal.

9.2. Gerenciamento de vulnerabilidades e patches

A organização deve manter um processo formal de gerenciamento de vulnerabilidades que permita identificar, classificar, corrigir e monitorar falhas presentes em sistemas operacionais, aplicações, dispositivos de rede e ambientes em nuvem.

Ferramentas especializadas devem ser utilizadas para realizar varreduras periódicas, fornecendo visibilidade contínua do estado de segurança da infraestrutura. As correções (patches) devem ser aplicadas de maneira estruturada e dentro de prazos compatíveis com o nível de criticidade da vulnerabilidade, reduzindo a exposição a ataques e riscos de exploração. As janelas de manutenção devem ser planejadas para minimizar impacto em operações críticas, e registros das ações devem ser mantidos para fins de auditoria e conformidade.

10. Responsabilidades

10.1. Direção

A direção tem responsabilidade direta pelo apoio institucional à Política de Segurança da Informação, assegurando que os recursos humanos, financeiros e tecnológicos necessários sejam disponibilizados. Também é responsável por promover uma cultura organizacional orientada à segurança, definindo expectativas claras, validando prioridades estratégicas e integrando a gestão de riscos ao processo decisório.

A direção deve acompanhar os resultados das auditorias, métricas e análises de riscos, garantindo que as ações corretivas sejam implementadas com a devida urgência e que a PSI permaneça alinhada aos objetivos gerais do negócio.

10.2. Equipe de segurança da informação

A equipe de segurança da informação é responsável pela implementação e manutenção dos controles definidos pela PSI, atuando na supervisão contínua do ambiente tecnológico, na análise de vulnerabilidades, no monitoramento de incidentes e na execução de ações de contenção, mitigação e melhoria. Deve realizar auditorias internas, manter a documentação atualizada, orientar outras áreas quanto às melhores práticas e assegurar o cumprimento das normas internas. A equipe também deve apoiar treinamentos, coordenar testes de incidentes, validar a eficácia dos controles e atuar como ponto central para questões relacionadas à segurança.

10.3. Funcionários

Todos os funcionários têm a responsabilidade de seguir rigorosamente as diretrizes estabelecidas pela PSI e de adotar práticas seguras em suas atividades diárias. Isso inclui o uso adequado dos recursos corporativos, a proteção de informações sensíveis, o cumprimento das regras de controle de acesso e a participação nos treinamentos de conscientização. Também é responsabilidade dos funcionários reportar imediatamente qualquer comportamento suspeito, falha operacional, incidente ou irregularidade, contribuindo para a preservação da segurança organizacional. O comprometimento diário de cada colaborador é essencial para reduzir riscos e manter a integridade do ambiente de TI.

Esta política de segurança de modelo abrange todos os aspectos importantes para garantir a integridade, confidencialidade e disponibilidade dos recursos e informações da organização.