ÍNDICE DE REVISÕES

REVISÃO	STATUS	DESCRIÇÃO
0	AP	Elaboração inicial do documento.
1	AP	FINALIZAÇÃO DO FLUXO

PA - PARA APROVAÇÃO	CA - CANCELADO	PR - PRELIMINAR
PI - PARA INFORMAÇÃO	AP - APROVADO	LI - LIBERADO

REVISÃO	REV. 0	REV. A	REV. B	REV. C	REV. D	REV. E	REV. F	REV. G
DATA	06/10/2022	14/10/2022						
ELABORAÇÃO	CARLOS C.	MARIANA O						
ANÁLISE CRÍTICA	MARIANA O.	MARIANA O.						
PADRONIZAÇÃO	ADRIANA S.	ADRIANA S.						
APROVAÇÃO	MARIA DELENICE	MARIA DELENICE						

SUMÁRIO

1. ATA DE APROVAÇÃO

A ata de aprovação desta política encontra-se devidamente assinada e arquivada na plataforma UniVoce, no Curso Treinamentos Corporativos – Normas e Políticas Internas, acessível a todos os colaboradores da empresa.

URL de Acesso: https://univoce.com.br/enrol/index.php?id=46

2. ABRANGÊNCIA

O documento é aplicável para clientes e colaboradores da empresa que identificarem vulnerabilidades e incidentes nos softwares da empresa ou em procedimentos internos do setor de atuação.

3. POLÍTICA

3.1 Introdução

3.1.1 Esta política está baseada em recomendações das autoridades brasileiras e internacionais relacionados ao estabelecimento de padrões internos capazes de classificar de forma eficiente as vulnerabilidades e os incidentes identificados dentro da empresa;

3.1.2 O objetivo desta política é permitir que todos os *stakeholders* envolvidos na atividade da empresa consigam identificar e classificar de forma eficiente as vulnerabilidades e os incidentes que ocorrerem internamente;

3.1.3 Todos os envolvidos nas atividades da empresa, sejam diretores, colaboradores ou clientes, estarão submetidos às regras estabelecidas nesta política.

3.2 Propósito

3.2.1 Esta política tem como propósito estabelecer diretrizes para a atuação na classificação e incidentes de vulnerabilidades dos softwares e das ferramentas utilizadas pela empresa;

3.2.2 Orientar quais devem ser as medidas adotadas, quais os tipos de classificações e quem as deve realizar;

3.2.3 Minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de clientes ou de qualquer outro impacto negativo no negócio da empresa como resultado de violações de dados.

3.3 Escopo

3.3.1 Esta política se aplica aos softwares, aplicativos, pastas e quaisquer outros procedimentos de todos os setores da empresa.

3.4 Papel do Cliente na identificação de Vulnerabilidades e Incidentes

3.4.1. O cliente terá o papel de identificar vulnerabilidades e incidentes e comunicá-los à empresa.

3.4.2. Quando uma vulnerabilidade for identificada por um cliente, o procedimento a ser seguido será:

a) O cliente que identificar alguma vulnerabilidade ou ocorrência de incidente será orientado a abrir um chamado por meio do MeuHelpdesk.

b) Os responsáveis pela gestão do MeuHelpdesk comunicarão o Intermediador de Dados sobre o ocorrido.

c) O Intermediador de Dados pessoais fará a comunicação interna com todos os responsáveis para a resolução do problema.

3.5 Classificação de Vulnerabilidades

3.5.1. A vulnerabilidade é uma condição que, quando explorada por um criminoso cibernético, pode resultar em uma violação de segurança cibernética dos sistemas computacionais ou rede de computadores e consiste na interseção de três fatores: suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha;

3.5.2. Visando documentar eventuais vulnerabilidades nos processos da empresa, registrá-los e controlá-los é importante que a empresa comece a adotar um sistema de registro e controles de vulnerabilidades. Por esse motivo, quando identificado por algum participante das operações alguma vulnerabilidade interna em seu setor, este deverá:

a) Identificar e classificar a vulnerabilidade de acordo com os critérios abaixo:

a.1. Vulnerabilidade de baixo risco

a.2. Vulnerabilidade de médio risco

a.3. Vulnerabilidade de alto risco

b) Comunicar ao Gestor de Setor sobre a vulnerabilidade identificada e sobre a classificação a ela conferida. O Gestor deverá analisar se a classificação conferida pelo colaborador foi realizada de forma correta.

c) O Gestor irá designar responsáveis por tratar da vulnerabilidade ou, caso não considere ser possível tratá-la, irá acionar o Intermediador de Dados para que realize comunicação com os demais responsáveis dentro da empresa.

d) Caso exista necessidade, serão acionados os Planos de Continuidade e Contingência para o tratamento da vulnerabilidade identificada.

e) Será papel do Gestor de Setor relatar a vulnerabilidade e a forma como ela foi tratada em documento (formulário padrão). Esse formulário deverá ser arquivado em arquivo cujo acesso seja possível todas as vezes que os interessados dentro das empresas necessitarem acessar este documento.

3.6. Classificação de incidentes

3.6.1 Esta sessão tem por objetivo detalhar os critérios de classificação dos incidentes críticos que podem ocorrer em nosso ambiente, para que possa ser dada a devida priorização do suporte para correção e restabelecimento do serviço.

3.6.2 O que é um incidente?

Podem ser considerados como incidentes interrupções não planejadas de serviços da empresa, a redução na qualidade de serviços, vazamentos de dados ou informações sobre o funcionamento da empresa ou de seus clientes e, ainda, qualquer outro acontecimento que possa causar prejuízos à empresa

3.6.3 O que é um incidente grave?

Um incidente grave é o incidente com o maior grau de impacto entre os níveis previstos. Essa classificação contribui para a priorização no tratamento de incidentes.

3.6.4 Para classificar os incidentes, os colaboradores da empresa deverão:

a) Ao identificar um incidente de dano grave ou gravíssimo, imediatamente, comunicar o Gestor de Setor.

b) Caso o Gestor de Setor faça uma análise prévia e considere o Incidente como dano grave ou gravíssimo, contactar imediatamente o Intermediador de Dados Pessoais;

c) O Intermediador de Dados Pessoais fará a comunicação do incidente aos devidos interessados, via canais de texto da ferramenta corporativa Discord, para início da solução do incidente;

d) A classificação do incidente será o último passo e será responsabilidade do Gestor de Setor classificar o incidente de acordo com as diretrizes abaixo:

- Dano mínimo
- Dano leve
- Dano médio
- Dano grave
- Dano gravíssimo

Observação: os incidentes de danos mínimos, leves e médios devem ser tratados pelo setor e registrados em formulário específico para registro de incidentes não-críticos).

3.6.5 Classificação do incidente como crítico

Para a categorização dos incidentes, será usada a matriz GUT (Gravidade, Urgência e Tendência).

A matriz GUT é uma ferramenta de priorização baseada em três critérios: gravidade, urgência e tendência. Para cada um desses critérios é atribuída uma nota — de 1 a 5 — e, ao final, esses valores são multiplicados, resultando na pontuação da GUT.

Segue abaixo uma breve explicação sobre cada critério da matriz GUT:

Gravidade – mede o impacto

O critério de gravidade leva em consideração o impacto que o incidente poderá causar na organização caso não seja solucionado logo. Então, ao analisar a gravidade você precisa se perguntar: quais efeitos a não solução desse incidente poderá causar ao longo do tempo?

Os níveis de gravidade são:

1- Dano mínimo
2- Dano leve
3- Dano médio

4- Dano grave
5- Dano gravíssimo

Urgência – mede o tempo

O critério de urgência leva em consideração o prazo disponível para realizar o suporte. Quanto menor o prazo, maior a urgência (e vice-versa). Então, ao analisar a urgência você precisa se perguntar: quanto tempo esse incidente pode esperar para ser solucionado?
Os níveis de urgência são:
1- Não há pressa
2- Pode aguardar
3- O mais cedo possível
4- Alguma urgência
5- Ação imediata

Tendência – mede a probabilidade de crescimento do problema

O critério de tendência leva em consideração a predisposição de um incidente piorar com o tempo. Esse critério existe porque um incidente pode nascer pequeno e, com o passar dos dias, se tornar uma bola de neve.
Os níveis de tendência são:
1- Não vai piorar
2- Vai piorar em longo prazo
3- Vai piorar em médio prazo
4- Vai piorar em pouco tempo
5- Vai piorar rapidamente

Resultantes da Matriz GUT (Gravidade, Urgência, Tendência)

Para efetuar o cálculo resultante das notas dadas a cada critério, basta multiplicar as notas dadas a cada um dos critérios para obter o *score* desse incidente em questão. Nesse método, o *score* mínimo que um incidente pode receber é 1 e o *score* máximo que um incidente pode receber é 125.
Ex.: Incidente #0001 que recebeu 2 para gravidade, 5 para urgência e 1 para tendência, o *score* seria de 10, pois 2 x 5 x 1 = 10.

Ranking de Priorização

Depois de calcular o score de cada incidente da lista, os incidentes foram classificados do maior para o menor score. Esta é a ordem em que os incidentes serão classificados de acordo com sua priorização.

Observação:

Como haverá casos em que um ou mais incidentes terão o mesmo *score*, no caso de ocorrer um ou mais incidentes com mesmo *score* ao mesmo tempo, ficará a cargo da diretoria ou da gerência de operações definir a priorização do atendimento de acordo com a necessidade do negócio.

3.7 Papéis e Responsabilidades

3.7.1 Colaboradores da empresa

Terão como responsabilidade identificar vulnerabilidades e incidentes e comunicar ao GESTOR DE SETOR quando for identificada uma vulnerabilidade interna no setor. Quando ocorrer a identificação de vulnerabilidade e incidente nos softwares da empresa, os colaboradores devem seguir o mesmo fluxo realizado pelo cliente, realizando inicialmente a abertura de chamados no MeuHelpDesk.

3.7.2 Gestores de Setor

Terão como responsabilidade receber os relatos dos colaboradores sobre vulnerabilidades ou incidentes identificados e tomar medidas para resolução ou comunicar o fato ao Intermediador de Dados Pessoais.

3.7.3 Intermediador de Dados Pessoais

É a pessoa designada da POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS como responsável por intermediar a relação entre a empresa e o Encarregado de Dados Pessoais Terceirizado;

Neste plano, terá o papel essencial de receber a comunicação dos GESTORES DE SETOR e comunicar aos responsáveis dentro da empresa em promover a solução da vulnerabilidade ou incidente identificado.

3.7.4 Clientes

Terão o papel de relatar vulnerabilidades e incidentes por meio de chamado no MeuHelpDesk.

3.8. Glossário - GSI/PR Nº 93

1) **Ameaça:** Conjunto de fatores externos com o potencial de causarem dano para um sistema ou organização.
2) **Análise de vulnerabilidades:** Verificação e exame técnico de vulnerabilidades, para determinar onde estão localizadas e como foram exploradas.
3) **Ativos de informação:** Meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização.
4) **Banco de Dados:** Coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam, a fim de criar algum sentido (informação) e de dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento.
5) **CVE (*Common Vulnerabilities and Expousures*):** Vulnerabilidades e Exposições Comuns.
6) **CVSS (*Common Vulnerability Scoring System*):** Sistema comum de pontuação de vulnerabilidade.
7) **Dado Pessoal Sensível:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
8) **Dado Pessoal:** informação relacionada a pessoa natural identificada ou identificável;

9) **Gestão de Vulnerabilidade:** Processo cíclico e contínuo de identificação, avaliação, documentação, gestão, comunicação e remediação de vulnerabilidades;
10) **Gestão de Mudanças nos Aspectos Relativos a Segurança da Informação:** Processo estruturado que visa aumentar a probabilidade de sucesso em mudanças, com mínimos impactos, e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação;
11) **Gestor de Segurança da Informação:** Responsável pelas ações de segurança da informação na empresa;
12) **HOST:** Um computador ou dispositivo de TI;
13) **ID CVE:** Identificação para um CVE Específico;
14) **INCIDENTE:** interrupções não planejadas de serviços da empresa, a redução na qualidade de serviços ou vazamentos de dados ou informações do funcionamento da empresa ou de seus clientes ou de clientes da empresa ou qualquer outro acontecimento que possa causar prejuízos a empresa;
15) **LOG (Registro de Auditoria):** Registro de eventos relevantes em um dispositivo ou sistema computacional;
16) **NTP:** *Network Time Protocol* ou Protocolo de Tempo Para redes. É o padrão que permite a sincronização dos relógios dos dispositivos de uma rede como servidores, estações de trabalho, roteadores e outros equipamentos à partir de referências de tempo confiáveis;
17) **Patch:** Uma parte de código adicional desenvolvido para resolver um problema ou falha em um software existente;
18) **Remediação:** O ato de corrigir uma vulnerabilidade ou eliminar uma ameaça;
19) **Risco:** No sentido amplo, trata-se da possibilidade de ocorrência de um evento que pode impactar o cumprimento dos objetivos. Pode ser mensurado em termos de impacto e de probabilidade;
20) **Risco de Segurança da Informação:** Risco potencial associado à exploração de uma ou mais vulnerabilidade de um ou mais ativos de informação, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;
21) **Segurança da Informação:** A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações da empresa.
22) **Teste de invasão:** Metodologia para testar a eficácia a resiliência de ativos através da identificação e exploração de fraquezas nos controles de segurança e da simulação das ações e objetivos de um atacante;
23) **Teste de Penetração (PenTest):** Também chamado de teste de intrusão, é fundamental para a análise de vulnerabilidade e consiste em testar todos os sistemas em busca de, além das já verificadas na fase anterior, vulnerabilidades conhecidas e disponibilizadas por especialistas ou pelas instruções detentoras dos softwares que estão sendo utilizados pelo órgão ou entidade;
24) **Violação de Dados Pessoais:** situação em que dados pessoais são processados violando um ou mais requisitos relevantes de proteção da privacidade;
25) **Vulnerabilidades:** Condição que, quando explorada por um criminoso cibernético, pode resultar em uma violação de segurança cibernética dos sistemas computacionais ou rede de computadores e consiste na interseção de três fatores: suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha.

3.9 Auditorias Internas

3.9.1 Para verificação do cumprimento das normas definidas nessa e nas demais políticas internas, será responsável o setor de Auditoria Interna, que poderá implementar rotinas, eventuais ou programadas, de auditoria.

3.9.2 Será de responsabilidade dos gestores de setor contribuir para a realização das auditorias citadas no item anterior fornecendo todos os dados necessários aos responsáveis pela sua realização.

3.10 Revisões

Esta política é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Proteção de Dados Pessoais.

3.11 Gestão da Política

3.11.1 A Política para Classificação de Vulnerabilidades e Incidentes é aprovada pela Diretoria da empresa, em conjunto com o Comitê Gestor de Proteção de Dados Pessoais.

3.11.2 Essa Política precisa estar atualizada em sua última versão na plataforma UniVoce, no Curso Treinamentos Corporativos – Normas e Políticas Internas, conforme acesso anteriormente citado.

3.12 Fluxo de Processo