Resumo da Política de Segurança Cibernética, Processamento e Armazenamento de Dados da Parmetal DTVM.

Publicado em 30 de novembro de 2020
Válida até 31 de dezembro de 2021

01. Objetivos deste Resumo da Política de Segurança Cibernética, Processamento e Armazenamento de Dados da Parmetal DTVM.

- Divulgar os princípios, as diretrizes e a postura ética e estratégica da **Parmetal DTVM** sobre Segurança Cibernética, Processamento e Armazenamento de Dados, Informações e Guarda e Recuperação de Documentos, incluindo:

    - A confidencialidade;
    - A integridade;
    - A disponibilidade de dados, informações e documentos;
    - O tempo de resposta dos sistemas de informação utilizados (próprios e de terceiros).

- Aumentar a resiliência da **Parmetal DTVM** à ataques cibernéticos e a incidentes relacionados à Tecnologia da Informação e Segurança da Informação;

- Declarar os princípios e diretrizes da **Parmetal DTVM** para definição de:

    - Procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes, compatíveis com os utilizados pela **Parmetal DTVM,** a serem adotados por empresas prestadoras de serviços a terceiros e fornecedores, que manuseiem dados, informações e documentos sensíveis ou que sejam relevantes para a condução das atividades operacionais e administrativas da **Parmetal DTVM.**

- Garantir o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes (internos e os ocorridos em empresas prestadoras de serviços a terceiros), para as atividades da **Parmetal DTVM,** referentes à segurança cibernética e processamento e armazenamento de dados, informações e documentos;

- Fazer com que todos os requerimentos legais, infralegais e as diretrizes internas da **Parmetal DTVM** relacionadas à segurança cibernética e processamento e armazenamento de dados, informações e documentos sejam cumpridos;

- Informar qual a postura esperada de funcionários, colaboradores e fornecedores ao tomar conhecimento de um incidente relacionado com segurança cibernética e processamento e armazenamento de dados, informações e documentos;

- Declarar os esforços da **Parmetal DTVM** para:

    - Prevenir, detectar e reduzir a sua vulnerabilidade a incidentes e em atender seus objetivos em segurança cibernética e em processamento e armazenamento de dados, informações e documentos, incluindo:

        - A Identificação;
        - A validação;
        - A autenticação;
        - A Criptografia.
        - A Prevenção e a detecção de intrusão;
        - A Prevenção de vazamento de Informações;
        - Os testes periódicos e varreduras para a detecção de vulnerabilidades relacionados com segurança cibernética e em processamento e armazenamento de dados, informações e documentos;
        - A Proteção contra softwares maliciosos;
        - O estabelecimento de mecanismos de rastreabilidade;
        - Os controles de acesso e de segmentação da rede de computadores; e

- A manutenção de cópias de segurança dos dados e das informações.

- Disseminar uma cultura organizacional referente a segurança cibernética e processamento e armazenamento de dados, informações e documentos, que inclui:

  - A prestação de informações a clientes e usuários de produtos e serviços sobre as precauções na utilização de produtos e serviços financeiros;
  - O compromisso da alta administração da **Parmetal DTVM** com a melhoria contínua dos procedimentos relacionados com segurança cibernética e processamento e armazenamento de dados, informações e documentos;
  - A disposição da **Parmetal DTVM** em compartilhar as informações sobre os incidentes relevantes relacionados com segurança cibernética e processamento e armazenamento de dados e informações.

- Fazer com que todos os mecanismos de monitoração e controle referentes à segurança cibernética e ao processamento e armazenamento de dados (incluindo os voltados para a rastreabilidade da informação), informações e documentos, existam e sejam efetivos e testados, inclusive no desenvolvimento e implementação de soluções de tecnologia da informação e na adoção de novas tecnologias;

- Garantir que a alta administração da **Parmetal DTVM** tenha a correta e tempestiva informação sobre a exposição a riscos e incidentes relacionados com segurança cibernética e processamento e armazenamento de dados, informações e documentos e os incidentes ocorridos;

02. Declaração Institucional

Esta Política explicita os princípios de governança e padrões da **Parmetal DTVM** para:

- Segurança Cibernética;
- Segurança de Tecnologia da Informação (TI);
- Segurança da Informação;
- Processamento e Armazenamento de Dados e de Informações; e
- Guarda e Recuperação de Documentos.

A **Parmetal DTVM**:

- Está empenhada em conhecer, registrar e eliminar ou minimizar todos as vulnerabilidades referentes às suas atividades cibernéticas e de Processamento e Armazenamento de Dados e de Informações, e de Guarda e Recuperação de Documentos aos quais está exposta;

- Não pode permitir que, por desconhecimento, omissão, negligência, culpa ou dolo dos seus funcionários e colaboradores, prestadores de serviços terceirizados e fornecedores; os seus clientes, os usuários de seus produtos e serviços, os seus parceiros e a própria **Parmetal DTVM,** venham:

  - A ser expostos a vulnerabilidades que a **Parmetal DTVM** desconheça ou que não deseja incorrer;
  - Incorrer em vulnerabilidades para as quais a **Parmetal DTVM** não tenha se preparado adequadamente;
  - Expor seus quotistas, administradores, clientes, parceiros, fornecedores, funcionários e colaboradores a qualquer tipo de vulnerabilidade que não tenham sido avaliados e formalmente assumidos.

- Não pode permitir que, por desinformação, os seus clientes e os seus usuários de produtos e serviços sejam inadvertidamente expostos a vulnerabilidades que não devem incorrer;

- Busca oferecer a todos os seus funcionários e colaboradores uma cultura organizacional que enfatize a importância da:

    - Segurança Cibernética.
    - Segurança de Tecnologia da Informação; e da
    - Segurança da Informação.

- Procura manter seus funcionários, colaboradores, prestadores de serviços a terceiros e fornecedores informados sobre suas políticas e estratégias para a Segurança Cibernética, para o Processamento e Armazenamento de Dados e de Informações, e para a Guarda e Recuperação de Documentos; mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações.

03. A Segurança Cibernética

O Professor Doutor Anthony Stafford Beer (1926/2002) considera "**Cibernética**" como "O estudo dos fluxos de informação que rodeiam um sistema".

Segurança Cibernética pode ser definida como o conjunto de meios e tecnologias que visam proteger, de danos e intrusão ilícita, programas, computadores, redes e dados no momento do fluxo de informações, e busca assegurar:

- A **Confidencialidade**.

  Nenhum acesso a serviço, recurso ou informação deve ser provido a sistemas ou utilizadores que não sejam autorizados.

- A **Integridade**.

  Serviços, recursos, dados e informações não podem ser processados (criados, modificados, transportados, eliminados) e armazenados (guardados, recuperados e destruídos) por partes não autorizadas.

  A integridade depende da confidencialidade.

- A **Disponibilidade**.

  Sistemas ou utilizadores autorizados devem ter o acesso garantido a um determinado serviço, recurso, dado ou informação, e garantido o seu poder de processar e armazenar a informação.

  E:

    - Principalmente para instituições financeiras; a disponibilidade quando são necessárias (tempo de resposta), e

    - A capacidade de extrair as informações de dados.

Considerando a definição acima, "**Segurança Cibernética**" envolve tanto as atividades relacionadas com o **Ciberespaço** e o **Processamento em Nuvem**, quanto aquelas atividades que ocorrem em redes fechadas e mesmo em equipamentos de tecnologia da informação de uso individual ("end-user" ou não, móvel ou não) conectados ou não em redes fechadas ou públicas.

É um assunto da área de Tecnologia da Informação e da Área de Gerenciamento de Riscos.

Esta **Política de Segurança Cibernética e Processamento e Armazenamento de Dados,** da **Parmetal DTVM** determina requerimentos que devem ser cumpridos por todos seus:

- Funcionários;
- Colaboradores;
- Prestadores de Serviços Terceirizados contratados, e
- Fornecedores e Prestadores de Serviços Terceirizados que de alguma forma tratam dados e informações de propriedade ou em poder da **Parmetal DTVM.**

  Relacionamentos com Prestadores de Serviços terceirizados e Fornecedores são tratados na "Política de Relacionamento com Fornecedores e Prestadores de Serviços Terceirizados" da **Parmetal DTVM.**

E se aplica a;

Sistemas e dados embarcados em soluções proprietárias de equipamentos, desenvolvidas e/ou sustentadas pela própria **Parmetal DTVM** ou por terceiros.

3.1. Ciberespaço.

Ciberespaço foi definido por Pierre Lévy em 1.999, como "o espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores".

Trata-se de um novo meio de comunicação estruturado, onde:

- Sistemas podem se comunicar com sistemas, com ou sem a presença ou intervenção humana; e

- O local geográfico do comando e execução do sistema deixa de ser o local geográfico da localização dos dados que a suporta.

Isto engloba a internet e de TODAS as redes de comunicação públicas e privadas, de propriedade de instituição ou de terceiros, que suportam as atividades de negócio e as atividades administrativas da instituição.

3.2. Processamento em Nuvem

Processamento em Nuvem depende do **Ciberespaço** e é definido no Artigo 13 da Resolução 4.658, como:

A disponibilidade, sob demanda e de maneira virtual, de ao menos uma das seguintes atividades:

- Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela instituição ou por ela adquiridos;

- Implantação ou execução de aplicativos desenvolvidos ou adquiridos, utilizando recursos computacionais de terceiros; ou

- Execução de aplicativos por meio da internet.

04. Segurança da Tecnologia da Informação (TI)

Tecnologia de Informação (TI) pode ser definido como o conjunto de todas as atividades e soluções providas por recursos de computação e comunicação que viabilizam a produção, o armazenamento, a transmissão, o acesso, a segurança e o uso das informações.

É um assunto de responsabilidade da área administrativa das instituições.

Envolve:

- Equipamentos físicos e seus sistemas operacionais (computadores, periféricos, modens, roteadores, notebooks, celulares inteligentes, equipamentos de guarda de dados externos, pen-drivers, qualquer equipamento independente de guarda de dados e outros equipamentos físicos);
- A infraestrutura necessária ao seu funcionamento, disponibilidade e proteção física (local físico, controle de acesso físico, energia, periféricos, contingências);
- Os sistemas necessários ao seu funcionamento (desenvolvidos e adquiridos);
- Os recursos de comunicação necessários ao seu funcionamento (Servidores, Provedores);
- Os dados e informações necessárias ao seu funcionamento (Banco de Dados, Data Centers);
- As atividades e processos necessários ao seu funcionamento (de TI, de Usuários, de proteção); e
- Os recursos humanos necessários ao seu funcionamento e sustentação (Operação, Suporte, Gestão, Proteção, Disponibilidade).

Segurança de Tecnologia da Informação tem por objeto a correta disponibilidade dos recursos de computação e comunicação.

05. Segurança da Informação

Dado e Informação

Dados e Informações são o alicerce para a construção do conhecimento.

Sem dados e informações o conhecimento é impossível e sem o conhecimento, a sabedoria (e qualquer gestão) também é impossível.

Dado não possui significado relevante e não conduz a nenhuma compreensão.

Representa algo que não tem sentido a princípio.
Portanto, não tem valor algum para embasar conclusões, muito menos respaldar decisões.

Informação é a ordenação e organização dos dados de forma a transmitir significado e compreensão dentro de um determinado contexto.

Informação é o conjunto e a consolidação dos dados para fundamentar o conhecimento.

Exemplo:

As palavras:

- Natural;
- Pessoa;
- Câmbio; e
- Operação.

Isoladamente NÃO têm significado e NÃO conduzem a nenhuma conclusão.

Mas organizadas e consolidadas em “Operação de Câmbio de Pessoa Natural” nos fornece uma informação.

Desde que saibamos a língua portuguesa – falada atualmente no Brasil - e saibamos o contexto no qual a frase se insere.

- "Operação de Pessoa Natural" tem significados diferentes entre o contexto das instituições financeiras e o contexto médico/cirúrgico.

- "Câmbio" têm significados diferentes no contexto de instituições financeiras e no contexto automotivo.

Menor significado a frase terá se os conceitos estiverem codificados, como:

- Pessoa Natural = "1" e Pessoa Jurídica = "2"
- Operação Comercial = "1" e Operação de Câmbio = "2".

O que nos daria a frase "2 de 1".

Menor significado ainda se a frase estiver criptografada, como "3#x@pto"

Quanto mais nos distanciamos dos dados, maior é a abstração e mais próximo ficamos da informação, do conhecimento e da capacidade de gestão (sabedoria).

Segurança da Informação, apesar de muitas vezes ser confundida com a **Segurança da Tecnologia da Informação**, tem por objeto a proteção de dados e a garantia de extração da informação dos dados.

É um assunto de responsabilidade de Gestores de Informação, que é uma especialidade de profissionais de Tecnologia da Informação e de Gerenciamento de Riscos.
Nem todas as informações têm a mesma importância.

Quanto maior for a criticidade da informação e maior a sua sensibilidade, mais efetivos e consequentemente mais complexos e caros deverão ser os meios empregados para a sua segurança.

Boa parte dos dados são digitais sem nunca originalmente, ter feito parte de qualquer documento físico que está ou esteve em poder da **Parmetal DTVM**.

TODOS os dados, de qualquer informação, estão armazenados em alguma mídia física que se encontra em algum lugar.

Portanto, os objetivos da **Segurança da Informação,** são:

- A proteção dos dados onde quer que se encontrem;
- A capacidade de extrair as informações dos dados, qualquer que seja a forma em que estejam armazenados; e
- A proteção dos documentos físicos e das mídias físicas que contenham dados digitais (equipamentos), qualquer que seja a forma em que estejam armazenados.

06. O Objeto da Segurança da Informação e da Segurança Cibernética.

Como vimos, uma informação é um conjunto de dados organizados e consolidados.

Mas o que importa são os conjuntos de informações que suportam os processos de negócios (processos da atividade fim da instituição) e os processos administrativos (processos necessários para a existência da instituição).

Todo evento de negócio ou evento administrativo deve gerar pelo menos um registro, que é um conjunto de informações.

Os registros podem assumir várias formas e estar contidos em vários tipos de mídias, como:

- Papel (Contratos, Relatórios);
- Arquivos Digitais;
- Mensagens Digitais;
- Bases de Dados;

- Códigos de Programas.
- Gravações de Áudio (como as pactuações dos Traders);
- Fotos;
- Vídeos (Imagem em Movimento) e outras...

Todos os processos de negócios são compostos de conjuntos de registros dos eventos relativos às entidades que compõem um processo de negócio, como:

- O Cliente;
- A **Parmetal DTVM** (O Cargo e a Pessoa que têm o poder de negociar e pactuar negócios com o Cliente);
- Produto ou Serviço (O objeto da negociação e pactuação entre o Cliente e a **Parmetal DTVM**);
- A Operação (A Pactuação formalizada);
- Direitos e Obrigações decorrentes das Pactuações (O Direito do Cliente é Obrigação da **Parmetal DTVM** e vice-versa).

Muitos destes conjuntos de registros, por requerimento legal ou infralegal, são “Dossiês” (Físicos ou Digitais), como:

- O Dossiê de Cadastro do Cliente;
- O Dossiê de Cadastro de Fornecedor;
- O Dossiê de Comunicação ao Coaf;
- O Dossiê da Operação; etc...

Os Dossiês e os Registros podem ser agrupados em arquivos (Físicos ou Digitais), obedecendo (ou NÃO) uma arquitetura de informações.

O objeto da **Segurança Cibernética** são os fluxos de informação realizados (no Ciberespaço ou NÃO) em determinada tarefa (tasks) de um determinado **sistema** para:

- Acessar;
- Criar;
- Alterar;
- Guardar;
- Recuperar;
- Proteger;
- Copiar;
- Transportar; e
- Destruir (Descarte).

Um determinado:

- Arquivo;
- Dossiê;
- Registro;
- Informação; ou
- Dado.

Que seja digital.

O Objeto da **Segurança da Informação** são as atividades realizadas em determinado **processo**, para:

- Acessar;
- Criar;
- Alterar;
- Guardar;
- Recuperar;

- Proteger;
- Copiar;
- Transportar; e
- Destruir (Descarte).

Um determinado:

- Arquivo;
- Dossiê;
- Registro;
- Informação; ou
- Dado.

Que existe fisicamente ou está guardado em alguma mídia física.

Lembrando que: **TODOS** os dados, de qualquer informação, estão armazenados em alguma mídia física em algum lugar.

Muitas vezes uma única atividade pode ser simultaneamente o objeto da Segurança Cibernética e da Segurança da Informação.

Isto ocorre quando o gerenciamento da mídia física que contém os dados for de responsabilidade da própria instituição; provocando tratamentos diferenciados de **Segurança de Tecnologia da Informação** para mídias físicas e para equipamentos que contenham embarcadas mídias físicas de responsabilidade da instituição.

Isto decididamente NÃO ocorre se:

- As atividades de processamento e armazenamento de dados e de computação em nuvem forem executadas por:
  - Prestadores de serviços à Terceiros;
  - Fornecedores, se somente a atividade tiver sido terceirizada;
- A responsabilidade dentro da instituição pelas atividades de:
  - Acessar;
  - Criar;
  - Alterar;
  - Guardar;
  - Recuperar;
  - Proteger;
  - Copiar;
  - Transportar; e
  - Destruir (Descarte);

  forem de áreas diferentes daquela que processa, armazena e realiza a computação em nuvem de dados (que podem se encontrar até em países diferentes).

Esta é a razão para Resolução 4.658 tratar simultaneamente:

- Segurança Cibernética, e a
- Contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

07. O Gerenciamento de Registros.

A unidade objeto da **Segurança da Informação** é o Registro de um determinado evento operacional ou administrativo da Instituição.

- Um **Arquivo** pode conter vários **Dossiês** e/ou vários **Registros**.
- Um **Dossiê** pode conter vários **Registros**;
- Um **Registro** pode conter várias **Informações**; e
- Uma **Informação** pode conter vários **Dados**.

Gerenciamento de Registros

É a habilidade sistemática e consistente e de custo eficiente de capturar/gerar/cadastrar, processar, qualificar, classificar, organizar, aceitar/homologar, alterar, guardar, proteger, transportar, controlar o acesso, recuperar e finalmente descartar/destruir, registros conforme os princípios e diretrizes desta Política e dos manuais relacionados, que são mandatórios se forem requerimentos de normativos legais e infralegais vigentes.

Qualificação de Registros.

Um único Dossiê ou Arquivo pode conter registros de qualificações diferentes.

A Qualificação de um Dossiê/Arquivo será aquela da mais alta qualificação de registro que contiver.

08. Classificação de Registros quanto à Confidencialidade.

Um único Dossiê ou Arquivo pode conter registros de diferentes classificações quanto a confidencialidade.

A Classificação quanto à confidencialidade de um Dossiê/Arquivo será aquela de mais alta classificação de registro que contiver.

Toda cópia de Registro tem a mesma classificação de confidencialidade do Registro original.

09. Classificação de Registros quanto ao Prazo de Guarda e Recuperação.

Um único Dossiê ou Arquivo pode conter registros de diferentes classificações quanto ao prazo de guarda e recuperação.

A Classificação quanto ao prazo de guarda e recuperação do Dossiê/Arquivo será aquela da mais alta classificação de registro que contiver.

Toda cópia de Registro tem a mesma classificação de guarda e recuperação do Registro original.

10. Descarte (Destruição) de Registros.

O descarte (destruição) de registros deve ser realizado por pessoas autorizadas (conforme o disposto nesta política) com a atenção necessária.

11. Materiais jogados no lixo e mídias com informações sensíveis descartadas.

Uma ação comum praticada por fraudadores é procurar no lixo e em mídias e equipamentos descartados materiais que contenham informações confidenciais, sensíveis ou que permitam ou auxiliem o acesso físico ou cibernético não autorizado.

A gravidade da situação é que no Brasil, esta prática **NÃO** constitui crime!

Todo material jogado no lixo ou descartado implica na abdicação dos direitos de propriedade e, desta forma, a **Parmetal DTVM**, **ANTES** de jogar no lixo ou descartar equipamentos e materiais sensíveis, deve garantir que todo dado, informação ou registros neles contidos, ou que alguma vez neles estiveram contidos, não sejam possíveis de ser recuperados (por mais avançada que seja a tecnologia empregada).

A única proteção da **Parmetal DTVM** é a garantia de destruição física de todos os registros, mídias e equipamentos no final da sua vida útil.

12. Procedimentos, Monitorações e Controles

A **Parmetal DTVM** possui procedimentos e mecanismos de monitoração e controle para:

- Segurança da Tecnologia da Informação;
- Segurança Cibernética; e
- Segurança da Informação.

13. Transparência

A **Parmetal DTVM** reafirma a sua disposição em participar de ações conjuntas para o compartilhamento de informações sobre incidentes relevantes, inclusive ataques cibernéticos ocorridos na própria **Parmetal DTVM** e nas empresas prestadoras de serviços a terceiros e fornecedores por ela contratados. (Inciso VII do Artigo terceiro da Resolução 4.658).

14. Prestação de Informações a Clientes.

A **Parmetal DTVM**:

- Não oferece a seus clientes nenhum serviço de autoatendimento ou que seja suportado por recursos mobile (móvel como celulares inteligentes), mesmo terceirizados;

- Não expõe seus clientes a qualquer risco cibernético na utilização do seu sítio na Internet (www.parmetal.com.br);

- Realiza todos os seus pagamentos e recebimentos financeiros, por:

  - Recursos tecnológicos dos bancos em que a **Parmetal DTVM** e as pessoas com que se relacionam possuem Contas de liquidação ou contas correntes; e
  - Espécie, presencialmente.

- Disponibiliza um Resumo desta Política de Segurança Cibernética em seu sítio na internet de forma pública.

15. Considerações Finais.

A **Parmetal DTVM** terá todo empenho em esclarecer qualquer dúvida a respeito desta sua **Política de Segurança Cibernética e Processamento e de Armazenamento de Dados**, a quem quer que seja.

Para isto, basta nos enviar uma mensagem pelo nosso sítio na internet (www.parmetal.com.br), e se identificar para que seja possível o encaminhamento da resposta.