COMUNICADO

Visando dar continuidade a implantação da Política de Segurança da Informação na CH MASTER DATA | ASTREIN, nomeamos abaixo o Encarregado de Dados e detalhamos abaixo os mecanismos de formação do Comitê de Segurança da Informação.

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas da CH MASTER DATA | ASTREIN, para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

A PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

Com a intenção de aumentar a segurança da infraestrutura tecnológica, a PSI foi desenvolvida para garantir a Norma de Segurança da Informação e exigências da LGPD (Lei Geral de Proteção de Dados), visando a orientação de nossos clientes, fornecedores e colaboradores para a utilização dos ativos de tecnologia da informação disponibilizados.

As diretrizes ali estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte durante a realização de projetos.

É também obrigação de cada colaborador se manter atualizado em relação a PSI e aos procedimentos e normas relacionadas, buscando orientação do seu Gestor sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela CH MASTER DATA | ASTREIN pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais.

A CH MASTER DATA | ASTREIN por meio da equipe de Infraestrutura e Segurança da Informação, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

Caberá a essa área analisar criticamente incidentes em conjunto com o Comitê de Segurança da Informação, apresentar as atas e os resumos das reuniões do Comitê de Segurança da Informação, destacando os assuntos que exijam intervenção do próprio comitê ou de outros membros da diretoria.

Manter comunicação efetiva com o Comitê de Segurança da Informação sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar a CH MASTER DATA | ASTREIN.

Buscar alinhamento com as diretrizes corporativas da instituição.

Do Comitê de Segurança da Informação

O Comitê de Segurança da Informação será coordenado pelo Encarregado de Dados que atuará como canal de comunicação entre a CH MASTER DATA | ASTREIN, os titulares dos dados e a ANPD – Autoridade Nacional de Proteção de Dados.

Encarregado de Dados / Coordenador do Comitê de Segurança da Informação
MARCELLO ARAUJO MARTINS – marcello@chmasterdata.com – (21) 2421-8105

As atividades do Encarregado de Dados consistem em:

- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- Receber comunicações da autoridade nacional e adotar providências;
- Orientar os funcionários e os contratados da CH MASTER DATA | ASTREIN a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
- Nomear os membros do Comitê de Segurança da Informação.

O Comitê de Segurança da Informação deve ser formalmente constituído por colaboradores com nível hierárquico mínimo gerencial, nomeados para participar do grupo pelo período de um ano.

O Coordenador do Comitê de Segurança da Informação nomeará os colaboradores, sendo que a composição mínima deve incluir um colaborador de cada uma das áreas: PMO – Escritório de Projetos, INFRA – Infraestrutura de Tecnologia, SUP – Suporte Técnico, P&D – Pesquisa e Desenvolvimento, IMPL – Implantação de sistemas, SAN – Saneamento de cadastros, GOV – Governança de cadastros, COM – Comercial e MKT - Marketing.

Deverá o CSI reunir-se formalmente pelo menos uma vez a cada seis meses. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para a CH MASTER DATA | ASTREIN.

O CSI poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.

Cabe ao CSI:

- Propor investimentos relacionados à segurança da informação com o objetivo de reduzir riscos;
- Propor alterações da PSI, inclusão, eliminação ou mudança de normas complementares;
- Avaliar os incidentes de segurança e propor ações corretivas;
- Definir as medidas cabíveis nos casos de descumprimento da PSI e/ou das Normas de Segurança da Informação complementares.

Da Área de Infraestrutura e Segurança da Informação

Caberá a área de Infraestrutura e Segurança da Informação testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais e acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI, e em sua versão educacional, pelas Normas de Segurança da Informação complementares.

Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

Segregar as funções administrativas, operacionais e educacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a CH MASTER DATA | ASTREIN.

Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

- Os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.
- Os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro da empresa.

Realizar auditorias periódicas de configurações técnicas e análise de riscos.

Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.

Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.

Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

Monitorar o ambiente de TI, gerando indicadores e históricos de:

- Uso da capacidade instalada da rede e dos equipamentos;
- Tempo de resposta no acesso à internet e aos sistemas críticos da CH MASTER DATA | ASTREIN;
- Períodos de indisponibilidade no acesso à internet e aos sistemas críticos da CH MASTER DATA | ASTREIN;
- Incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
- Atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);

São Paulo, 20 de setembro de 2024.

MARCELO AVILA FERNANDES:68721862753

Assinado de forma digital por MARCELO AVILA FERNANDES:68721862753
Dados: 2024.09.20 10:40:47 -03'00'

CATALOG HUB MASTER DATA SISTEMAS E CONSULTORIA S/A

CNPJ 01.195.269/0001-33

Marcelo Ávila Fernandes

Vice-presidente