Política de segurança da informação

03 DE AGOSTO DE 2023

Responsável pela Política: HR4 CONSULTORIA EM RECURSOS HUMANOS LTDA
CNPJ: 11.749.530/0001-53
Versão: 2.0

OBJETIVO

A presente política de uso de segurança da informação visa proteger e garantir os princípios da segurança da informação: confidencialidade, integridade e disponibilidade da informação, autenticidade, controle de Acesso, irretratabilidade e conformidade.

Além disso, é projetada para assegurar a aplicação dos princípios e diretrizes de proteção da propriedade intelectual e das informações da HR4, dos usuários e do público em geral, observando as regulamentações aplicáveis e melhores práticas de mercado, conforme exigido pela ABNT NBR ISO 27001 e 27002.

Introdução

1. A informação é um dos principais bens de qualquer organização.
   Para a devida proteção desse bem, a HR4 Consultoria em Recursos Humanos Ltda, estabelece a presente Política de Segurança da Informação, a fim de garantir a aplicação dos princípios e diretrizes de proteção da propriedade intelectual e das informações da organização, dos clientes e do público em geral.
2. Nossa estratégia de Segurança da Informação foi desenvolvida para evitar violações da segurança dos dados, minimizar os riscos de indisponibilidade dos nossos serviços, proteger a integridade e evitar qualquer vazamento de informação.
3. Para alcançarmos esse objetivo nossa estratégia está baseada na proteção de perímetro expandido, apoiado em processos de controle para detecção, prevenção, monitoramento e resposta a incidentes garantindo a gestão do risco de segurança cibernética e a construção de um alicerce robusto para o futuro cada vez mais digital da empresa.
4. O conceito de perímetro expandido considera que a informação deve ser protegida independentemente de onde ela esteja, seja em um prestador de serviço ou em uma unidade internacional, em todo o seu ciclo de vida, desde o momento que ela é coletada, passando pelo processamento, transmissão, armazenamento, análise e seu descarte.

Público-alvo

Colaboradores da HR4 CONSULTORIA EM RECURSOS HUMANOS LTDA e prestadores de serviços, entre eles: funcionários, estagiários, menor aprendiz, terceirizados ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, infraestrutura ou informações desta empresa.

Regras

1. Todas as políticas de segurança da informação precisam estar disponíveis em local acessível aos colaboradores e devem ser protegidas contra alterações.
2. As políticas de segurança da informação são revisadas anualmente pela HR4.
3. A adesão a essa Política e eventuais desvios são reportados periodicamente pelo Data Protection Officer – DPO ou Encarregado.

Princípios de Segurança da Informação

Nosso compromisso com o tratamento adequado das informações da HR4, clientes e público em geral está fundamentado nos seguintes princípios:

- **Confidencialidade:** garantimos que o acesso à informação seja obtido somente por pessoas autorizadas e quando ele for de fato necessário;
- **Disponibilidade:** garantimos que as pessoas autorizadas tenham acesso à informação sempre que necessário;
- **Integridade:** garantimos a exatidão e a completude da informação e dos métodos de seu processamento, bem como da transparência no trato com os públicos envolvidos.
- **Disponibilidade:** garantimos que a informação estará disponível sempre que for preciso.
- **Autenticidade:** garantimos a veracidade da autoria da informação e o não repúdio, porém, não garante a veracidade do conteúdo da informação
- **Controle de Acesso:** garantimos o controle de acesso dos usuários.
- **Irretratabilidade (não-repúdio):** A Autenticidade garante também um subproduto, que é o Não Repúdio. O Não Repúdio está contido na autenticidade e significa que o autor da informação não tem como recusar que ele é o verdadeiro autor. Ou seja, o Não Repúdio é a incapacidade da negação da autoria da informação
- **Conformidade:** garantimos que a informação sempre estará em conformidade com as normas e legislações vigentes.

Diretrizes de Segurança da Informação

1. A HR4 estabelece que as informações internas, dos clientes e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida.
2. A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada, em conformidade com as outras Políticas divulgadas.
3. Todo processo, durante seu ciclo de vida, deve garantir a segregação de funções, por meio da participação de mais de um colaborador ou equipe de colaboradores, para que a atividade não seja executada e controlada pelo mesmo colaborador ou equipe.

4. O acesso às informações e recursos só deve ser feito se devidamente autorizado.
5. A identificação de qualquer colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.
6. A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades.
7. Todo colaborador deve reportar os riscos às informações ao DPO.
8. O DPO deve divulgar amplamente as responsabilidades sobre Segurança da Informação aos colaboradores, que devem entender e assegurar estas diretrizes.

Processo de Segurança da Informação

Para assegurar que as informações tratadas estejam adequadamente protegidas, a HR4 adota os seguintes processos:

Tipo	Descrição
Gestão de Ativos da Informação	Entende-se por Ativos da Informação tudo o que pode criar, processar, armazenar, transmitir e até excluir a informação. Podem ser tecnológicos ("software" e "hardware") e não tecnológicos (pessoas, processos e dependências físicas). Os ativos da informação, de acordo com sua criticidade, devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos, fisicamente (salas com acesso controlado) e logicamente (configurações de blindagem ou "hardening", patch management, autenticação e autorização) e ter documentação e planos de manutenção atualizados anualmente.
Classificação da Informação	As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis: • Restrita • Confidencial • Interna e • Pública. Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.
Gestão de Acessos	As concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos da HR4.

	Os acessos devem ser rastreáveis, a fim de garantir que todas as ações passíveis de auditoria possam identificar individualmente o colaborador, prestador de serviço, para que seja responsabilizado por suas ações.
Gestão de Riscos	Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação da HR4, para que sejam recomendadas as proteções adequadas. Os cenários de riscos de segurança da informação são escalonados nos fóruns apropriados, para decisão.

Gestão de Riscos em Prestadores de Serviços

Para avaliação de risco, é utilizado um Baseline de Fornecedores, que consiste em um documento com diversos controles de segurança baseado em padrões internacionais e melhores práticas do segmento.

Existe um canal de comunicação para que os prestadores de serviços, que prestam serviços a HR4, informem as ocorrências de incidentes relevantes relacionados as informações da HR4 armazenadas ou processadas na empresa contratada, em cumprimento às determinações legais e regulamentares.

Tipo	Descrição
Tratamento de Incidentes de Segurança da Informação e Cyber Security	A área de Cyber Security realiza a monitoração de segurança do ambiente tecnológico da HR4, analisando os eventos e alertas com o objetivo de identificar possíveis incidentes. Os incidentes que são identificados pelos alertas são classificados com relação ao impacto de acordo com os critérios adotados pela HR4. Todos os incidentes passam por um processo de tratamento e comunicação, onde são registradas todas as informações pertinentes aos incidentes como causa, impacto, classificação etc., de acordo com o procedimento operacional. Visando aprimorar a capacidade da HR4 na resposta a incidentes cibernéticos, alguns cenários que possam afetar a continuidade de negócios são considerados nos testes. Os incidentes de Segurança da Informação e cibernéticos da HR4 devem ser reportados ao DPO.

	O DPO elaborará um Relatório Anual contendo os incidentes relevantes ocorridos no período, ações realizadas de prevenção e respostas aos incidentes e resultados dos testes de continuidade.
Conscientização em Segurança da Informação e Cyber Security	A HR4 promove a disseminação dos princípios e diretrizes de Segurança da Informação por meio de programas de conscientização e capacitação, com o objetivo de fortalecer a cultura de Segurança da Informação. Periodicamente, são disponibilizadas campanhas de conscientização ou treinamentos que podem ser presenciais ou on-line, relacionados a confidencialidade, integridade e disponibilidade da informação. Estas campanhas são veiculadas através de e-mails, portal corporativo, e-learning, mídia indoor, redes sociais aos colaboradores e clientes.
Governança com as Áreas de Negócio e Tecnologia	As iniciativas e projetos das áreas de negócio e tecnologia devem estar alinhadas com as diretrizes e arquiteturas de segurança da informação, garantindo a confidencialidade, integridade e disponibilidade das informações.

Segurança Física do Ambiente

O processo de Segurança Física visa estabelecer controles relacionados à concessão de acesso físico ao ambiente somente a pessoas autorizadas, de acordo com a criticidade das informações previamente mapeadas e declaradas à Administração Predial.

Segurança no Desenvolvimento de Sistemas de Aplicação

O processo de desenvolvimento de sistemas de aplicação deve garantir a aderência às políticas de segurança da HR4 e às boas práticas de segurança.

Gravação de LOG's

É obrigatória a gravação de logs ou trilhas de auditoria do ambiente computacional de forma a permitir identificar: quem fez o acesso; quando o acesso foi feito; o que foi acessado e como foi acessado.

As informações dos registros (logs) ou trilhas de auditoria devem ser protegidas contra modificações e acessos não autorizados.

Programa de Cyber Security

O Programa de Cyber Security da HR4 é norteado pelos seguintes fatores:

- Regulamentações vigentes;
- Melhores práticas;
- Cenário mundiais.

Conforme sua criticidade, o programa divide-se em:

- **Ações críticas** - Consiste em correções emergenciais e imediatas para mitigar riscos iminentes;
- **Ações de Sustentação** - Iniciativas de curto / médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro, respeitando o apetite de risco da Organização e permitindo que ações de longo prazo/estruturantes possam ser realizadas;
- **Ações Estruturantes** - Iniciativas de médio / longo prazo que tratam a causa raiz dos riscos.

Proteção de perímetro

Para proteção da infraestrutura da HR4 contra um ataque externo, utilizamos ferramentas e controles contra:

- Ataques que afetem a disponibilidade (DDoS),
- Spam,
- Phishing,
- Ataques avançados persistentes (APT),
- Malware,
- Invasão de dispositivos de rede e servidores,
- Ataques de aplicação e
- Scan externos.

São instaladas ferramentas preventivas contra vazamento de informação, instaladas em estações de trabalho, no serviço de correio eletrônico, no serviço de navegação da WEB, no serviço de impressão, além de criptografia de disco em notebooks e solução de proteção de dispositivos móveis.

Avaliação Independente da Auditoria

A efetividade das políticas de Segurança da Informação poderá ser verificada por meio de avaliações periódicas de Auditoria Interna.

Propriedade Intelectual

A propriedade intelectual é composta por bens imateriais, tais como: marcas, sinais distintivos, slogans publicitários, nomes de domínio, nomes empresariais, indicações geográficas, desenhos industriais, patentes de invenção e de modelo de utilidade, obras intelectuais (tais como obras literárias, artísticas e científicas, base de dados, fotografias, desenhos, ilustrações, projetos de arquitetura, obras musicais, obras audiovisuais, textos e etc.), programas de computador e segredos empresariais (inclusive segredos de indústria e comércio).

Quaisquer informações e propriedade intelectual que pertençam a HR4, ou por ele disponibilizadas, não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas, inferidas ou desenvolvidas pelo próprio colaborador em seu ambiente de trabalho

Declaração de Responsabilidade

Periodicamente os Colaboradores e Prestadores de Serviços diretamente contratados pela HR4 devem aderir formalmente a um termo, comprometendo-se a agir de acordo com as políticas de Segurança da Informação e Privacidade.

Os contratos firmados com a HR4 devem possuir cláusula que assegure a confidencialidade das informações.

Medidas Disciplinares

As violações a esta política estão sujeitas às sanções disciplinares previstas nas normas internas das empresas da HR4, e na legislação vigente no Brasil e nos países onde as empresas estiverem localizadas.

Condições preliminares

Ao acessar e/ou utilizar o site da HR4, o usuário declara ter, no mínimo 18 (dezoito) anos, e capacidade plena e expressa para a aceitação dos termos e das condições estabelecidos e predispostos a todos.

Caso o usuário tenha entre 16 e 18 anos, deve seguir o artigo 14, da Lei nº 13.709/2018, onde o tratamento de dados pessoais deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Caso o usuário não se enquadre na descrição acima e/ou não concorde, ainda que em parte, com os termos e as condições contidos nesta Política de Privacidade, não deverá acessar e/ou utilizar os serviços oferecidos, bem como os sites e serviços operados pela HR4.

Definições desta Política

- **Sites:** qualquer página da web sob o domínio da HR4;
- **Cookies:** arquivos enviados pelo servidor do site para o computador do usuário, com a finalidade de identificar o computador e obter dados de acesso, como páginas navegadas ou links clicados, permitindo, desta forma, personalizar a utilização do site, de acordo com o seu perfil;
- **IP:** abreviatura de Internet Protocol. É um conjunto de números que identifica o computador do usuário na Internet;
- **Logs:** registros de atividades do usuário efetuadas no site;
- **Session ID:** identificação da sessão do usuário no processo de inscrição ou quando utilizado de alguma forma o site;
- **Usuário:** todo aquele que passar a usar o site;
- **Sistemas:** sites e/ou programas de computador que a HR4 utiliza para realizar os seus processos seletivos, matrículas, aulas e demais atividades acadêmicas.
- **Biometria Facial:** tecnologia de reconhecimento do rosto a partir da análise de foto capaz de identificar uma pessoa.
- **Consentimento:** manifestação livre, informada e inequívoca de uma pessoa (titular) com o tratamento dos seus dados pessoais para as finalidades apresentadas neste documento, ou seja, sua autorização.
- **Dados Anônimos:** dado relativo a uma pessoa que não pode ser identificada, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.
- **Dados Pessoais:** quaisquer dados que possam identificar uma pessoa.
- **Dados Pessoais Cadastrais:** dados pessoais de interesse público que identificam e qualificam a pessoa e que não são sigilosos, como por exemplo, nome, RG, CPF, endereço, estado civil, profissão, data de nascimento, nome da mãe etc.
- **Dispositivos:** são computadores, notebooks, tablets, smartphones e quaisquer outros aparelhos utilizados por você para acessar a internet.

O acesso, a navegação e utilização da Web para acessar o site institucional e as redes sociais da HR4 implicam na aceitação expressa e sem reservas de todos os itens contidos na presente "Política", que está refletida no "Termo de Consentimento" disponibilizado aos usuários, cuja validade e eficácia são equivalentes à de qualquer contrato celebrado por escrito e assinado.

Sua observância e conformidade serão aplicáveis com relação a qualquer pessoa que acesse, navegue ou use a Web para acesso ao site ou às redes sociais da HR4.

Portanto, se você não concordar com estas Condições de Uso ou por qualquer motivo não as cumprir, deve interromper, imediatamente, a navegação e abster-se de usar a Web para acessar os sítios eletrônicos relacionados com a HR4.