VULTUS CYBERSECURITY ECOSYSTEM

CÓDIGO DE CONDUTA ÉTICA PROFISSIONAL

www.vultuscyber.com.br

PREZADOS COLABORADORES E PARTES INTERESSADAS

A elaboração do código de conduta ética profissional da Vultus Cybersecurity Ecosystem tem o objetivo de nortear os princípios éticos e as normas que devem conduzir a nossa atuação em relação a todos os diferentes públicos nos quais a nossa organização interage e que têm interesse no relacionamento e nos negócios.

Este é um instrumento que deve direcionar a nossa atuação no dia a dia, no relacionamento com fornecedores, funcionários, clientes, parceiros de negócios, investidores e poder público, dentre outros, levando-se em conta a importância em ressaltar que a concepção de um código de conduta ética profissional tem que partir necessariamente por conceitos, valores e hábitos presentes na cultura de nossa organização.

Com a aplicação deste código de conduta ética não temos a pretensão de discriminar todas as possibilidades de comportamentos dentro da atuação da organização, mas que sua aplicação seja um guia para a atuação de todos.

Sendo assim, esperamos que você o leia atentamente, compreenda e faça do código de conduta ética profissional o seu guia de atuação, e que seja um orientador nas suas relações íntegras e transparentes e de respeito em todos os seus relacionamentos, quer sejam agentes internos ou externos. Ao final deste documento apresentamos o Termo de Compromisso que deverá ser assinado atestando o seu compromisso.

Equipe Vultus Cybersecurity Ecosystem.

Sumário

1. ABRANGÊNCIA

Este é um documento de referência não só para os colaboradores, mas também para as sociedades controladas e os demais públicos com os quais a Vultus Cybersecurity Ecosystem se se relaciona. São esses diferentes públicos envolvidos no negócio que, ao fazerem suas escolhas cotidianas, reforçam a conduta ética na qual a Organização acredita.

O Código de Conduta Ética da Vultus Cybersecurity Ecosystem considera as relações com os seguintes públicos, embora não se limite a eles:

- Acionistas
- Investidores
- Clientes
- Colaboradores e demais públicos internos
- Comunidade e sociedade
- Concorrentes, Fornecedores e Parceiros Comerciais
- Governo e órgãos reguladores
- Imprensa

2. OBJETIVO

O Código de Conduta Ética Profissional da Vultus Cybersecurity Ecosystem. As páginas a seguir apresentam os elementos essenciais que devem ser considerados nas relações estabelecidas pela Vultus Cybersecurity Ecosystem com os seus mais diferentes públicos. Com este código, buscamos contribuir para a criação de parcerias de longo prazo que sejam compatíveis com os interesses e as aspirações mais legítimas da sociedade.

Este Código de Conduta Ética Profissional rege temas importantes que fazem parte da nossa forma de agir e de conduzir nossos negócios. O documento, no entanto, não apresenta de forma exaustiva todas as situações vivenciadas no dia a dia dos nossos Profissionais, mas é essencial para guiá-los, **por meio dos princípios contidos**, na realização de suas atividades diárias.

Contamos com a colaboração de todos para que este **Código de Conduta Ética Profissional** seja praticado durante as relações profissionais em nosso ambiente corporativo, já que um documento dessa natureza só ganha legitimidade com o tempo e com a prática constante.

"ÉTICA: A ética é uma disciplina composta de ações e regras destinadas a garantir que nos comportamos corretamente em determinado ambiente."

3. A CULTURA ORGANIZACIONAL

Os valores da nossa organização são uma expressão da personalidade e dos traços que originam a Vultus Cybersecurity Ecosystem.

MISSÃO

Construindo um mundo digital mais seguro.

Vivemos em um mundo hiper conectado. Dispositivos conectados à internet estão mudando a maneira como vivemos, convivemos, trabalhamos e nos expressamos. Na Vultus Cybersecurity Ecosystem, acreditamos que todos merecem uma experiência on-line segura. Com tecnologia, inteligência, experiência e mentes especialistas, estamos sempre um passo à frente dos ataques cibernéticos em constante evolução, rumo a uma sociedade digital mais resiliente e para tornar o nosso mundo digital mais seguro.

A Vultus Cybersecurity Ecosystem constrói fortes parcerias para criar e implementar esforços de conscientização de amplo alcance, capacitando usuários com as informações que precisam para manter a si mesmos, suas informações e sua organização como um todo protegidas, incentivando uma cultura de segurança.

OS VALORES VULTUS CYBERSECURITY ECOSYSTEM

Estar preparado para uma variedade de ameaças crescentes é parte fundamental de um modelo eficiente de gestão de riscos.

Colaboração

No ambiente colaborativo da Vultus Cybersecurity Ecosystem, não existem divisões. Contamos com o engajamento do time como um todo, o que permite que cada um tenha voz dentro da empresa para contribuir, podendo assim expor seu conhecimento, cultivando a aprendizagem constante e uma comunicação transparente.

Ética e Integridade

Agir com ética e integridade é um dos nossos valores fundamentais. Há uma confluência desses valores que permeiam o caráter dos funcionários de maneira pessoal, e resulta em um trabalho de excelência e compromisso para com cada cliente.

Respeito

Tratar alguém com respeito significa agir de uma maneira que demonstre que você entende seu valor, dignidade e singularidade. Aqui na Vultus é um elemento fundamental nas relações profissionais e na conduta ética.

Confiabilidade

Confiabilidade é construída com abertura, clareza e honestidade. Com o lado humano alinhado com as nossas soluções técnicas e inovadoras, queremos ajudar a criar uma sociedade mais segura. Trabalhamos com informações confidenciais, confiança e confiabilidade fazem parte da nossa essência.

Foco no Cliente

Trabalhamos para um bem maior: tornar o nosso mundo digital mais seguro. A paixão pelo que fazemos reflete o nosso propósito, o porquê que nos motiva. Nos colocamos na pele de nossos clientes, criamos uma parceria concreta, o que nos torna verdadeiros companheiros de jornada rumo a um mundo mais seguro.

4. AS ORIENTAÇÕES GERAIS DE CONDUTA

RESPEITO PELAS PESSOAS

A Organização segue os princípios da Declaração Universal dos Direitos Humanos e valoriza o direito à vida, à liberdade de expressão e à segurança. Esses princípios são a base para a justiça, a liberdade e a paz.

A Organização valoriza a diversidade e é **contra qualquer tipo de discriminação em razão de gênero, deficiência, origem, religião, cor da pele, orientação sexual, estado civil, idade** ou **condição social**. A Vultus Cybersecurity Ecosystem repudia qualquer forma de intimidação ou assédio sexual, moral, religioso, econômico, político ou organizacional. Não tolera agressões físicas e verbais, desrespeito, constrangimento e humilhações.

O colaborador que se considerar discriminado, humilhado ou alvo de preconceito, pressão, práticas abusivas ou em situação de desrespeito e que se sentir constrangido em tratar do assunto com seu superior hierárquico deve comunicar o fato ao Canal de Conduta Ética Profissional colocado à sua disposição, conforme item específico deste código de conduta.

A Vultus Cybersecurity Ecosystem quer construir um ambiente de trabalho que promova a realização pessoal e ofereça perspectivas de desenvolvimento profissional. É conduta esperada de todos ouvir e considerar novas ideias, opiniões distintas, questionamentos e argumentações que representam uma forma de aprendizado e melhoria dos processos.

A Vultus Cybersecurity Ecosystem valoriza a sinergia entre as células de negócio, a cooperação entre colaboradores e o compartilhamento de conhecimentos como forma de aprendizado e disseminação das melhores práticas, resguardados os critérios de confidencialidade.

IGUALDADE DE OPORTUNIDADES

A Vultus Cybersecurity Ecosystem valoriza a igualdade de oportunidades. A Organização acredita que todas as pessoas devem ter as mesmas chances de desenvolvimento profissional.

Esse direito deve ser assegurado por todos os profissionais envolvidos nos processos de contratação e de gestão de pessoas. A seleção dos candidatos elegíveis às posições é feita de forma objetiva, considerando o perfil para cada cargo, as características profissionais e os conhecimentos necessários para o desempenho

USO DE ÁLCOOL E DROGAS ILÍCITAS

Com o objetivo de manter um ambiente de trabalho saudável e respeitoso, algumas regras relativas ao consumo de álcool e drogas devem ser observadas.

Sempre que o consumo de álcool ocorrer dentro das nossas dependências ou em atividades externas relacionadas à Vultus Cybersecurity Ecosystem, ele deve ser realizado de forma moderada e apenas em momentos apropriados. Da mesma forma, não admitimos que um colaborador **desempenhe suas atividades** ou mesmo **permaneça dentro do nosso ambiente corporativo embriagado**.

Em relação à utilização de drogas ilícitas, é estritamente proibido que um colaborador da Vultus Cybersecurity Ecosystem **consuma ou esteja sob o efeito de drogas ilícitas enquanto desempenha suas atividades profissionais.**

CONFLITO DE INTERESSES

Há conflito de interesses quando os profissionais usam a **Organização**, a **função** ou a **influência interna** visando interesses pessoais ou para beneficiar terceiros. Interesse deve ser entendido não somente como a obtenção de qualquer vantagem para si, seja ela material ou não, mas também para familiares, amigos ou contrapartes com quem o profissional tenha relações políticas, pessoais ou comerciais.

Há conflito de interesses nos casos em que existe relacionamento pessoal ou societário em qualquer linha de subordinação ou na relação com clientes, fornecedores ou concorrentes que comprometa a imparcialidade nos negócios e que possa trazer benefícios aos envolvidos, prejuízos à Organização ou comprometer a isenção na avaliação de desempenho dos envolvidos. Eventuais situações deverão ser comunicadas e formalizadas pelo colaborador por meio do Canal de Conduta Ética.

"A Vultus Cybersecurity Ecosystem não compactua com relações conflituosas entre os negócios da Organização e seus públicos."

Algumas situações em que esses conflitos podem estar presentes são:

Atividades paralelas

As atividades extraprofissionais do interesse dos colaboradores e demais públicos internos, deverão ser realizadas de forma a não contrariar os interesses da Vultus Cybersecurity Ecosystem e devem ser realizadas fora do horário de trabalho contratado, bem como fora das dependências da Organização. Exercer voluntariado, ações corporativas e palestras com motivações empresariais é permitido, contanto que o conteúdo não exponha a estratégia ou a atuação da Organização.

Abertura de sociedade com outros profissionais

No caso de abertura de um negócio ou sociedade com outros profissionais da Vultus Cybersecurity Ecosystem ou de fora dela, a comunicação de tal fato deverá ser formalizada pelo colaborador.

Informações obtidas na Vultus Cybersecurity Ecosystem

É vedado o uso de informações obtidas na Vultus Cybersecurity Ecosystem para obter vantagens. Essas e outras situações que caracterizem potenciais desvios e conflitos de interesse deverão ser imediatamente reportadas ao gestor imediato e formalizadas por meio do Canal de Conduta Ética Profissional, que pode ser acessado através do link **materiais.vultuscyber.com.br/condutaetica**, para que sejam devidamente avaliadas pela Diretoria Interna, Head de Compliance, Head de Recursos Humanos. Até a conclusão da avaliação, as pessoas envolvidas no potencial conflito deverão, quando possível, ausentar-se da situação e aguardar orientações do gestor e das áreas competentes.

“Somos responsáveis pelas condutas pessoais que causam impactos na vida profissional. A ética não é temporária, é linear.” Douglas Fabiano de Melo

CONTRIBUIÇÕES E AFILIAÇÕES A PARTIDOS POLÍTICOS

A Vultus Cybersecurity Ecosystem respeita o direito individual do colaborador de se envolver em assuntos cívicos, realizar contribuições político partidárias e participar do processo político. Porém, tal participação deve ocorrer em seu tempo livre à sua própria custa. Nessa situação, o colaborador deve tornar claro que as manifestações são suas, e não da Organização, e não mencionar em qualquer situação o nome da Vultus Cybersecurity Ecosystem.

A Vultus Cyber não realiza contribuições a “candidatos, políticos e a partidos políticos”.

ANTICORRUPÇÃO

A Vultus Cybersecurity Ecosystem repudia todas as formas de condutas corruptas, tais como suborno, desvios e concessões de vantagens indevidas, assim como a ocultação ou dissimulação desses atos e o impedimento às atividades de investigação e fiscalização.

Não se pode oferecer ou entregar, direta ou indiretamente, qualquer vantagem indevida, pagamento, presente ou cortesia com a intenção de influenciar a imparcialidade de qualquer autoridade, servidores públicos, funcionários ou executivos, em qualquer ato ou decisão de forma a obter benefício impróprio para a Organização. Da mesma forma, os colaboradores, estagiários, aprendizes e administradores da Vultus Cybersecurity Ecosystem não devem aceitar vantagens indevidas.

PREVENÇÃO A FRAUDES

A Vultus Cybersecurity Ecosystem atua na prevenção a fraudes em todas as suas relações, alinhada à legislação vigente e aos valores da Organização.

Essa é a razão pela qual a Organização não tolera a prática de atos ilícitos no exercício de suas atividades ou em razão delas. Caso desvios desse tipo aconteçam, a Organização apurará os fatos e adotará as medidas necessárias para fazer valer seus direitos e valores, incluindo sanções administrativas e a propositura de ações judiciais visando à responsabilização civil ou criminal dos participantes.

PRÁTICAS CONCORRENCIAIS

A Vultus Cybersecurity Ecosystem está comprometida com a promoção da livre concorrência para a evolução do mercado e com o cumprimento da legislação concorrencial.

Nas interações com os concorrentes, os profissionais da Vultus Cybersecurity Ecosystem não devem compartilhar informações estratégicas, estabelecer acordos ou atuar de forma coordenada sobre preços, vendas, padronização de cláusulas contratuais, remuneração, divisão de mercado ou, ainda, sobre quaisquer estratégias comerciais de abordagem a clientes ou fornecedores.

PREVENÇÃO À LAVAGEM DE DINHEIRO

A Vultus Cybersecurity Ecosystem não compactua com práticas de lavagem de dinheiro e todos os colaboradores devem prestar especial atenção a situações suspeitas.

O crime de lavagem de dinheiro caracteriza-se pela realização de um conjunto de operações comerciais ou financeiras com o objetivo de ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedades de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal.

Geralmente, o processo de lavagem de dinheiro é composto por 3 (três) fases independentes que, com frequência, ocorrem de forma simultânea, quais sejam:

(a) Colocação: ingresso no sistema financeiro de recursos provenientes de atividade ilícitas, por meio de depósitos, compra de instrumentos financeiros ou compra de bens. Nesta fase, é comum a utilização de instituições financeiras para a introdução de recursos obtidos ilicitamente;

(b) Ocultação: execução de múltiplas operações financeiras com os recursos já ingressados no sistema financeiro, visando a ocultação dos recursos ilegais, por meio de transações complexas e em grande número para dificultar o rastreamento, monitoramento e identificação da fonte ilegal do dinheiro; e

(c) Integração: incorporação formal do dinheiro no sistema econômico, por meio de investimento no mercado de capitais, imobiliário, obras de arte, dentre outros.

Assim que identificados, os casos de suspeita de lavagem de dinheiro e corrupção deverão ser reportados ao Head de Compliance, que será responsável por respeitar e proporcionar a devida averiguação dos fatos.

PRESENTES, FAVORES E CORTESIAS

A Vultus Cybersecurity Ecosystem é contra a aceitação direta e indireta de presentes, favores, dinheiro ou cortesias que possam afetar decisões, facilitar negócios ou beneficiar terceiros.

O oferecimento de entretenimento e brindes institucionais a pessoas físicas ou jurídicas que trabalham com a Vultus Cybersecurity Ecosystem é permitido, desde que o entretenimento não seja oneroso em excesso e o brinde dado seja abaixo do valor de referência de US$ 100,00 (cem dólares). Nenhum deles deverá exceder os limites dos padrões comerciais normais no mercado local. Deve-se tomar cuidado para assegurar que o entretenimento ou o brinde não seja interpretado pela pessoa que o recebe como suborno ou indução inadequada.

Cortesias Institucionais:

Para o caso de aceitação de cortesias institucionais, vinculadas a ações de marketing e relacionamento com clientes, fornecedores e parceiros, os administradores e colaboradores devem obter a autorização prévia, por e-mail, dos níveis hierárquicos superiores, incluindo a autorização do reporte direto da Diretoria Interna, além de enviar um e-mail para a Célula de Compliance,

formalizando tal autorização (**compliance@vultuscyber.com.br**). Eventuais discordâncias por parte da área de Compliance em relação à autorização serão tratadas e podem ser submetidas aos membros do Fórum interno para deliberação.

Exemplos de cortesias institucionais:

Eventos para divulgação de marca, produtos, serviços (almoços, jantares, homenagens, entre outros);

Congressos ou **fóruns empresariais** para divulgação de tecnologia e técnicas, compartilhamento de conhecimentos, networking; Eventos esportivos, culturais ou artísticos patrocinados pela Organização que oferece os convites.

Exemplos de brindes:

Aparelhos eletrônicos (aparelhos celulares, notebooks, computadores, tablets, entre outros);

Utensílios domésticos (máquinas de café, entre outros).

As despesas que objetivem o fortalecimento do relacionamento com clientes, tais como refeições, desde que com objetivos de reunião de trabalho, são permitidas, contanto que contemplem valores razoáveis e não sejam proibidas por práticas comerciais conhecidas da organização de quem recebe.

Cortesias Não Institucionais:

No caso de cortesias desvinculadas de ações institucionais, os administradores e colaboradores da Vultus Cybersecurity Ecosystem não devem aceitar tais ofertas. Contudo, se as práticas de mercado contemplarem a troca de cortesias, a exemplo de presentes de Natal, as mesmas podem ser aceitas, porém, limitadas ao valor máximo de referência de US$ 100 (cem dólares).

Nesse caso, não é necessária a autorização, assim como para brindes de propaganda de pequeno valor, tais como **agendas, canetas, calendários, cadernos**, entre outros. Quando o valor for superior ao valor máximo de referência, o colaborador deverá recusar o presente. Caso a devolução não seja possível, o presente deve ser encaminhado à Célula de Compliance, que definirá sua destinação.

Além disso, é vedado aos colaboradores da Célula de Compras a aceitação de presentes, favores e cortesias desvinculados de ações institucionais, de qualquer tipo ou valor, com exceção para brindes de propaganda de pequeno valor. Também é vedado aos administradores e colaboradores da Vultus Cybersecurity Ecosystem a oferta ou aceitação de quaisquer presentes, favores ou cortesias para órgãos ou funcionários públicos, caso o valor for superior ao valor máximo de referência.

PRESERVAÇÃO E SEGURANÇA DA INFORMAÇÃO

A Vultus Cybersecurity Ecosystem preza pela segurança da informação.

Somente informações publicadas oficialmente pela Vultus Cybersecurity Ecosystem podem ser expostas ou discutidas com os públicos de interesses, como fornecedores, clientes, bancos, bandeiras, concorrentes, entre outros.

O uso do correio eletrônico não é permitido para assuntos pessoais. **São proibidos**: troca, resgate, armazenamento ou utilização de conteúdo obsceno, pornográfico, violento, discriminatório, racista ou difamatório, que desrespeite qualquer indivíduo ou entidade e/ou contrário às políticas e aos interesses da Vultus Cybersecurity Ecosystem.

Os colaboradores em geral não devem ter expectativa de privacidade na utilização desses sistemas e recursos. Por esse motivo, a Vultus Cybersecurity Ecosystem poderá, a seu critério, usar e monitorar qualquer informação transmitida ou residente nesses meios. Essa regra abrange a informação escrita ou armazenada em sistema eletrônico e qualquer outro meio associado. Inclui também as informações desenvolvidas tecnicamente, adquiridas por associações, aquisição, licença, compra ou confiadas à Organização.

Todos os arquivos e informações referentes à atividade profissional criados, recebidos ou armazenados nos sistemas eletrônicos são de propriedade da Vultus Cybersecurity Ecosystem e constituem bens comerciais e legais. Assim, em caso de mudança ou desligamento de um colaborador, essas informações mantidas por ele deverão ser encaminhadas à liderança imediata para guarda ou descarte.

A senha de acesso aos sistemas é de uso pessoal exclusivo, não sendo permitida sua concessão a terceiros, ainda que a um colega de trabalho.

Quaisquer tipos de software e programa não devem ser copiados ou instalados nos computadores da Organização sem a prévia autorização da Diretoria de Tecnologia de Informação.

Com exceção das informações classificadas como públicas, nenhuma informação da Vultus Cybersecurity Ecosystem e/ou de seus clientes pode ser divulgada ou publicada externamente, como por exemplo, em sites de relacionamentos e redes sociais.

Todos os públicos com os quais a Vultus Cybersecurity Ecosystem se relaciona são responsáveis por zelar pela segurança das informações, garantindo que sejam armazenadas, processadas e transmitidas somente em ambientes seguros. É vetado compartilhar ou enviar qualquer informação confidencial, estratégica e do negócio utilizando meios particulares como e-mail, pen-drive, armazenamento em nuvens, entre outros recursos. Esse cuidado também vale para o compartilhamento de

informações via redes sociais e, verbalmente, em locais públicos como ônibus, restaurantes, bares, aeroportos, aviões, estádios, táxis, entre outros.

Consideramos confidenciais dados pessoais e sensíveis de nossos colaboradores, fornecedores, clientes e parceiros e demais informações críticas e estratégicas da Vultus Cybersecurity Ecosystem. O acesso a essas informações é autorizado apenas para quem tem necessidade de conhecê-las em razão da atividade profissional exercida na Organização.

PROTEÇÃO DE DADOS PESSOAIS

A Vultus Cybersecurity Ecosystem protege seus dados pessoais e respeita a sua privacidade.

A Vultus Cybersecurity Ecosystem adota medidas técnicas e organizacionais visando proteger os dados pessoais de titulares contra a destruição, acidental ou ilícita, a perda, a alteração, a comunicação ou difusão ou o acesso não autorizado, além de garantir que o ambiente (seja ele físico ou lógico) utilizado pela Vultus Cybersecurity Ecosystem para o tratamento de dados pessoais seja estruturado de forma a atender os requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na **Lei Geral de Proteção de Dados Pessoais** (LGPD) – Lei 13.709/2018 e demais normas regulamentares aplicáveis.

Assim, caso participe de algum projeto ou atividade que realiza o tratamento de dados pessoais que estão sob nossa responsabilidade, seja na condição de colaborador, parceiro ou fornecedor, você possui um grande compromisso na aplicação e no monitoramento dos controles de segurança definidos.

Neste contexto, vale destacar alguns princípios que devem pautar as nossas atividades que envolvem dados pessoais:

- **Seja proativo** e não reativo; atue de modo preventivo, não corretivo;
- A privacidade do titular dos dados pessoais deve ser respeitada a todo o momento no exercício de suas atividades ou na criação de um novo produto ou serviço;
- Assegure que as partes envolvidas no tratamento de dados pessoais (outras células, parceiros, fornecedores etc.) realizem suas atividades de modo adequado, **observando as Políticas Internas da Vultus Cybersecurity Ecosystem** voltados à proteção de dados pessoais, e que entendam claramente quais são os objetivos do tratamento.

Com referidas medidas, a Vultus Cybersecurity Ecosystem reafirma seu compromisso de cumprimento da LGPD contribuindo para o fortalecimento da **proteção do direito à privacidade** do titular de dados pessoais; a liberdade de

expressão, de informação, de opinião e de comunicação; a inviolabilidade da intimidade, da honra e da imagem e o desenvolvimento seguro e tecnológico.

REDES SOCIAIS

A Vultus Cybersecurity Ecosystem tem seus canais oficiais nas redes sociais e somente eles representam a Organização.

Os colaboradores que optarem por cadastrar-se em redes sociais, deverão fazê-lo em nome próprio usando recursos particulares.
A publicação de opiniões deverá ser totalmente pessoal, evitando associação, direta ou indireta, à marca da Organização, bem como, é vetado divulgar boatos ou qualquer opinião que venha comprometer a imagem de administradores ou outros colaboradores da Organização.

Os perfis de redes sociais associados à marca da Vultus Cybersecurity Ecosystem, somente deverão ser cadastrados e utilizados pela Célula de Marketing, a qual é responsável por autorizar e publicar informações oficiais neste tipo de mídia.

RESPEITO AOS DIREITOS FUNDAMENTAIS DE CRIANÇAS E ADOLESCENTES

A Vultus Cybersecurity Ecosystem está comprometida com os direitos das crianças e dos adolescentes.

É contrária a qualquer forma de negligência, discriminação, crueldade, violência, exploração sexual de crianças e adolescentes e pornografia nas atividades da Organização, na utilização dos seus produtos e serviços e em sua cadeia de valor.

A Organização repudia o trabalho infantil e não compactua com quaisquer situações que potencialmente envolvam o trabalho irregular de adolescentes menores de 16 anos (exceto quando na condição de aprendizes, a partir dos 14 anos).

TRABALHO ESCRAVO

A Vultus Cybersecurity Ecosystem é contra o trabalho escravo e a situações que potencialmente envolvam coerção, castigos a qualquer pretexto, medidas disciplinares degradantes ou punição, bem como a violação às normas do salário mínimo e jornada de trabalho, pelo exercício de qualquer direito fundamental.

A Organização não compactua com tais práticas na utilização de seus produtos e serviços e em sua cadeia de valor e nem aceita que seus fornecedores, parceiros ou terceiros compactuem ou utilizem dessa prática.

SAÚDE E SEGURANÇA NO TRABALHO

A Vultus Cybersecurity Ecosystem zela pela Saúde e Segurança do Trabalho em suas atividades e nas relações de trabalho.

A Organização garante um ambiente seguro e condições previdenciárias e assistenciais que propiciem melhoria da qualidade de vida e facilitem o bom desempenho profissional.

MEIO AMBIENTE

A Vultus Cybersecurity Ecosystem está comprometida com o desenvolvimento sustentável e boas práticas para preservação do meio ambiente.

Ao realizar suas atividades, a Vultus Cybersecurity Ecosystem pretende assegurar o sucesso do negócio no longo prazo, contribuindo para a construção de uma sociedade mais segura digitalmente e justa, para o desenvolvimento econômico e a preservação ambiental.

Os aspectos ambientais são respeitados durante o ciclo de desenvolvimento de atividades, produtos e serviços, considerando o uso de energia renovável; a gestão e redução das emissões de Gases de Efeito Estufa;

o uso racional dos recursos naturais; o uso de materiais de origem certificada; a gestão e o descarte adequado de resíduos; a reciclagem de materiais, entre outros.

USO DE RECURSOS, ATIVOS E PROPRIEDADES DA ORGANIZAÇÃO

Os colaboradores devem zelar pelas instalações, recursos, equipamentos, máquinas, móveis e veículos, entre outros materiais de trabalho.

Os ativos e recursos da organização não devem ser utilizados para a obtenção de vantagens ilícitas ou indevidas, pessoais ou para terceiros, **direta** ou **indiretamente**.

A Organização tem por direito, acesso aos registros de uso de internet, e-mail e informações armazenadas nos computadores, telefonia móvel e fixa da Organização.

ACIONISTAS E INVESTIDORES

Os acionistas e investidores têm um papel fundamental para o sucesso do negócio. A Vultus Cybersecurity Ecosystem tem uma equipe engajada a conquistar

resultados que garantam os melhores índices de rentabilidade, sempre prezando pela transparência e equidade.

Clientes

A Vultus Cybersecurity Ecosystem entende que o caminho mais curto para tornar realidade sua missão é **contribuir de maneira efetiva para o sucesso dos clientes**. A organização preza pela transparência e confidencialidade das informações, preservando a relação de confiança e a sintonia com os nossos clientes, cumprindo o que foi contratado e buscando, constantemente, a excelência na prestação dos serviços.

As informações sobre nossos produtos e serviços devem ser sempre claras e verdadeiras. Dados técnicos, em especial requisitos de segurança, saúde e meio ambiente, **serão obrigatoriamente informados aos clientes**.

É proibido fazer pagamentos impróprios a qualquer pessoa com o intuito de facilitar a venda de nossos produtos ou serviços, mesmo ao custo de perdermos oportunidades de negócio.

É de nossa responsabilidade a confidencialidade das informações sigilosas a nós repassadas por nossos clientes e parceiros.

Colaboradores

A paixão é uma característica marcante dos colaboradores da Vultus Cybersecurity Ecosystem e é essencial para o sucesso do negócio. O respeito às diferenças está no DNA da Organização, e isso se reflete nas **atitudes** e **posicionamentos**. A relação da Vultus Cybersecurity Ecosystem com seus colaboradores se baseia nos **valores**, **princípios éticos** e na **legislação trabalhista**.

A Vultus Cybersecurity Ecosystem preza pela meritocracia, a transparência, o diálogo aberto e o reconhecimento das melhores práticas, com colaboradores inspirados e que fazem a diferença, expondo ideias e percepções alinhadas ao planejamento do negócio, de maneira que contribuam com os resultados.

A organização investe constantemente em um ambiente de realização pessoal e profissional que seja saudável e que ajude a promover o **bem-estar físico e emocional dos profissionais.**

É responsabilidade de cada colaborador zelar pelo patrimônio da Vultus Cybersecurity Ecosystem e cuidar da imagem da Organização. As atitudes de todos os administradores e colaboradores devem refletir o comprometimento com os seus valores e a perenidade da Organização.

COMUNIDADE E SOCIEDADE

“Sustentabilidade e Responsabilidade Corporativa” é um dos valores da Vultus Cybersecurity Ecosystem. Reforça o compromisso em contribuir com o desenvolvimento seguro e sustentável da sociedade.

É dever da organização identificar oportunidades de melhoria em processos, produtos e serviços, na tentativa de minimizar os impactos socioambientais causados pelo negócio.

A Vultus Cybersecurity Ecosystem visa contribuir com políticas públicas inerentes a segurança digital definidas por todas as instâncias de governo, de modo a cooperar com o avanço da sociedade brasileira.

CONCORRENTES

Vultus Cybersecurity Ecosystem respeita os concorrentes e acredita que a concorrência leal contribui para o **aperfeiçoamento do mercado de Cybersecurity**. Assuntos estratégicos do negócio não deverão ser discutidos ou repassados, a qualquer pretexto, aos concorrentes sem a devida autorização.

É vedado ao colaborador adotar qualquer atitude que denigra a imagem de concorrentes ou parceiros comerciais da Vultus Cybersecurity Ecosystem.

FORNECEDORES

A relação com os fornecedores deve ser caracterizada pela observância dos preceitos do Código de Conduta Ética Profissional. A Vultus Cybersecurity Ecosystem pratica a **livre concorrência**, a **transparência** e a **imparcialidade** no processo de contratação de fornecedores, bem como o rigoroso cumprimento dos contratos. O incentivo às boas práticas, valorizando as questões de sustentabilidade, deve ser buscado constantemente.

Serão especialmente observadas as práticas do fornecedor referentes a assuntos como meio ambiente, consumo consciente, trabalho infantil e escravo, exploração sexual de crianças e adolescentes, inclusão social, cumprimento da legislação, dentre elas, regulamentações relativas a prevenção e combate à corrupção.

A Vultus Cybersecurity Ecosystem poderá encerrar uma relação de negócio com um fornecedor sempre que houver prejuízo de seus interesses ou desconsideração de questões legais, tributárias, de meio ambiente e de saúde e segurança no trabalho.

É de responsabilidade da Vultus Cybersecurity Ecosystem a confidencialidade das informações sigilosas a nós repassadas por nossos fornecedores.

GOVERNO E ÓRGÃOS REGULADORES

A Vultus Cybersecurity Ecosystem cumpre a legislação vigente, atua de forma transparente e tem interesse em contribuir com o desenvolvimento social e econômico do país, assumindo um papel importante no sistema de segurança cibernética brasileiro, como, por exemplo, no auxílio ao **combate do terrorismo digital e vazamento de dados** (LGPD).

O fornecimento de informações a todas as esferas de governo, incluindo órgãos públicos municipais, estaduais e federais, deve ser efetuado sempre por escrito, mediante protocolo e com a devida orientação da Célula Jurídica ou de Compliance, a depender do assunto envolvido.

A Vultus Cybersecurity Ecosystem proíbe veementemente a **realização de pagamentos**, a título de gratificação, ou o **oferecimento de qualquer vantagem** a empregados públicos.

IMPRENSA

A Vultus Cybersecurity Ecosystem preza pela confiabilidade das informações transmitidas aos veículos de comunicação e garante que todos os comentários, declarações ou pronunciamentos em nome da Organização sejam feitos somente por pessoas expressamente autorizadas.

O colaborador não deve promover a **divulgação de informações sigilosas** ou **inverídicas** na imprensa.

O contato com profissionais da imprensa não deve ser tratado, em hipótese alguma, como um relacionamento comercial. Dessa forma, não envolve favores ou pagamento de nenhuma espécie.

A construção e o fortalecimento da imagem e da reputação da Vultus Cybersecurity Ecosystem também se dão por meio de nosso diálogo e comportamento para com os públicos com os quais nos relacionamos. Para tanto, nosso agir, dentro e fora da Organização, deve estar sempre em consonância com os princípios e os valores da Vultus Cybersecurity Ecosystem.

5. DESCUMPRIMENTO DO CÓDIGO DE CONDUTA ÉTICA PROFISSIONAL

FÓRUM DE ÉTICA VULTUS CYBERSECURITY ECOSYSTEM

O Fórum Vultus Ética, formado pela Diretoria em exercício (Diretoria de Estratégia e Diretoria Técnica Operacional), com o apoio da Célula de Compliance e secretariado pela Célula de Pessoas RH, é a última instância de gestão do Código de Conduta Ética Vultus Cybersecurity Ecosystem. Seus objetivos são:

- Zelar pelo **aperfeiçoamento constante** do teor do Código de Conduta Ética Profissional da Vultus Cybersecurity Ecosystem;
- Garantir que os preceitos do Código sejam a referência do processo de gestão da Vultus Cybersecurity Ecosystem e que **sejam respeitados no dia a dia de trabalho**;
- Deliberar, como órgão de última instância, sobre as situações que forem identificadas como desvios aos princípios contidos neste Código.

DESVIOS AOS PRECEITOS DO CÓDIGO

Os colaboradores, estagiários e administradores da Vultus Cybersecurity Ecosystem são responsáveis pela aplicação das orientações do código em todas as suas relações profissionais e devem atuar como guardiões, reportando toda e qualquer situação que possa indicar o **não cumprimento das orientações/diretrizes**, sob condição de punição legal por parte da Organização. Todos os profissionais deverão assinar a adesão formal ao código e renová-la quando houver uma nova edição do documento.

Caso ocorra alguma dúvida se determinada situação é um desvio aos preceitos estabelecidos neste Código, os profissionais deverão, antes de formalizar o potencial desvio, buscar orientação junto ao seu gestor imediato ou mediato, a Célula de Recursos Humanos e Jurídico e aos representantes da Célula de Compliance.

Caso uma situação de conflito com o Código de Conduta Ética seja presenciada, mesmo que o colaborador não esteja envolvido, também poderá formalizar o desvio por meio do Canal de Conduta Ética.

CANAL DE CONDUTA ÉTICA

materiais.vultuscyber.com.br/condutaetica

O objetivo deste canal é zelar pela manutenção e cumprimento do Código de Conduta Ética Profissional da Vultus Cybersecurity Ecosystem.

A identidade será mantida sob sigilo se esse for o desejo do relator. O canal preza pela confidencialidade da informação e autoria das denúncias e garante absoluto sigilo.

GESTÃO DOS RELATOS

As informações registradas pelo Canal de Conduta Ética são utilizadas por grupos especialmente designados para a **apuração dos fatos**. Esses grupos serão formados de acordo com a natureza e a origem do potencial desvio de conduta ética. O Fórum de Ética Vultus Cybersecurity Ecosystem, em última instância, delibera sobre as violações e sanções disciplinares.

A gestão dos relatos é realizada conforme as seguintes premissas:

- O sigilo da apuração será rigorosamente mantido;
- O anonimato será assegurado a quem assim o desejar;
- A apuração será conduzida com imparcialidade e independência;
- Denúncias ou acusações sem fundamentação consistente serão desconsideradas;
- Denúncias ou acusações de má-fé, visando prejudicar alguém, estarão sujeitas às sanções disciplinares;
- Sanções disciplinares estão previstas contra qualquer tentativa de retaliação.

Ao agir com base nas diretrizes de conduta da Vultus Cybersecurity Ecosystem, o colaborador reforçará os princípios éticos da organização e contribuindo para manter esse Código sempre vivo e atual.

SOBRE A VULTUS CYBERSECURITY ECOSYSTEM

A Vultus Cybersecurity Ecosystem é fruto da combinação da vasta experiência técnica da GC Security, adquirida desde 2008 no mercado de cibersegurança, enquanto a Trust Cybersecurity Ecosystem vem somando com uma sólida expertise em gestão empresarial no seguimento de segurança da informação desenvolvida pela Falconi, reconhecida como uma das maiores consultorias globais.

Ampliamos a visibilidade sobre vulnerabilidades e falhas de segurança para proteger ativos, dados, aplicações, usuários e sistemas.

Criamos um framework exclusivo que inclui práticas dos mais avançados padrões de segurança do mercado como NIST, PCI-DSS, ISO 27.001 e 27.005 e guiamos nossos clientes através da prevenção de riscos digitais, proteção e continuidade de negócios.

Pessoas

Nossa equipe é formada por mais de 50 profissionais especializados em segurança cibernética, com formação multidisciplinar, certificações técnicas e grande capacidade de pesquisa e desenvolvimento de proteções contra ameaças digitais.

A expertise em cyber Security, gestão de vulnerabilidades, compliance, gestão de risco digital e ethical hacking permite que a Vultus crie soluções eficientes, sempre um passo à frente das táticas de ataque usadas por cibercriminosos.

+55 (11) 2972-8999

contato@vultuscyber.com.br

São Paulo - SP

Rua Jaceru, 384, conjunto 1909
Vila Gertrudes • 04705-000

www.vultuscyber.com.br