HSBC

**CÓDIGO DE CONDUCTA**

# Contenido

## 1. INTRODUCCIÓN

El objetivo del presente Código de Conducta es asegurar que todos los empleados de HSBC Bank (Uruguay) S.A. tengan conocimiento de los principios de integridad personal que se les exige ejercer en la conducción de los negocios del Banco y de sus asuntos privados y financieros.

En el capítulo 3 del presente código, se exponen los estándares mínimos de actuación, aplicables a todos los empleados del Banco, mientras que en el capítulo 6 se detallan las responsabilidades específicas de los niveles gerenciales para garantizar que el personal a su cargo cumpla con los estándares mencionados.

## 2. DEFINICIÓN Y ÁMBITO DE APLICACIÓN

Se entiende por Código de Conducta al conjunto de reglas, principios y normas de aplicación obligatoria por parte de los empleados de HSBC Bank (Uruguay) S.A., en el desarrollo de sus actividades dentro del Banco, así como los estándares de comportamiento ético que se espera de todos los integrantes de la Organización. El presente Código constituye, en consecuencia, un modelo de conducta que incluye una serie de recomendaciones para actuar correctamente y para orientar las relaciones entre los miembros de la Organización y con otras personas.

Ámbito de Aplicación

El Código de Conducta se aplica, con carácter obligatorio, a todos los empleados de HSBC Bank (Uruguay) S.A., incluso a aquellos contratados a término o que se encuentren prestando funciones en el período de prueba, así como a los miembros del Directorio y el Personal Superior del Banco. El Código no modifica la relación laboral existente entre la Banco y sus empleados, ni crea derechos, ni vínculos contractuales.

El alcance se hace extensivo, asimismo, a los asesores externos y a cualquier tercero que, en virtud de la naturaleza de su vinculación con el Banco, pueda afectar de alguna manera la reputación de HSBC Bank (Uruguay) S.A.

Es obligación de los empleados de HSBC Bank (Uruguay) S.A. la lectura, conocimiento y cumplimiento de lo establecido en el presente Código. Cualquier duda o controversia sobre sus contenidos o sobre comportamientos éticos en el desempeño de las tareas deberán ser formuladas por escrito a Recursos Humanos con copia al Gerente de la línea.

## 3. ESTANDARES ÉTICOS Y VALORES CLAVE EN LA CONDUCCION DE NEGOCIOS DEL BANCO

El Grupo HSBC tiene un fuerte compromiso por el cumplimiento de la normativa local y del Grupo.

La reputación del Grupo y el valor de la marca constituyen el activo más preciado que debe ser protegido siguiendo los parámetros éticos de la buena conducta y de las sanas prácticas del mercado.

En todos los casos, se debe evitar que el Banco sea utilizado como medio para el lavado de activos provenientes de actividades ilícitas y para el financiamiento del terrorismo. Si un empleado advierte que las operaciones de un cliente resultan sospechosas o inusuales, en los términos de la legislación nacional y restricciones definidas por HSBC, debe reportar el hecho, en forma inmediata, a la gerencia de línea y a Recursos Humanos. Debe tenerse presente que la complicidad implícita o explícita constituye una falta grave y por ende, causa directa de finalización de la relación laboral. Sin perjuicio de las sanciones legales y regulatorias.

Cuando un empleado tome conocimiento, a través del ejercicio de las funciones inherentes a su cargo, de la existencia de infracciones a las regulaciones dictadas por el Banco Central del Uruguay, debe informar al Oficial de Cumplimiento sin perjuicio de lo establecido por la regulación Titulo II Conductas de mercado Capítulo 1 Código de Ética.

### *3.1. Estándares éticos*

Todos los empleados de HSBC Bank (Uruguay) S.A., deben poseer y mantener los mayores estándares éticos y profesionales.

Ellos son:

*Integridad:* Hacer lo que se dice y no prometer lo que no se puede cumplir, manteniendo la rectitud en todos los casos.

*Honestidad:* Decir la verdad, requiere por lo tanto un acercamiento a la verdad no mediatizado por los propios deseos.

*Justicia:* Darle a cada uno lo que le corresponde; en todos los ámbitos.

*Responsabilidad:* Consiste en el cumplimiento de las obligaciones y en la respuesta por los propios actos.

*Excelencia*: Búsqueda de la superación constante con el objetivo de obtener una mayor calidad.

*Independencia:* Realización de las actividades y las decisiones desde una perspectiva objetiva.

*Compromiso:* Visualizado no como el simple deber de hacer o cumplir sino como el deber ser del empleado con el Banco, los Clientes y los compañeros de labores directos e indirectos.

Se espera que los empleados compartan los estándares éticos establecidos en el presente Código, así como las normas de comportamiento establecidas por los usos y costumbres y los parámetros sociales admitidos.

### *3.2. Valores del Grupo*

**Nuestro Propósito**

Abriendo un mundo de oportunidades

Estamos aquí para usar nuestra experiencia, capacidades, alcance y perspectivas únicas para abrir nuevas oportunidades en provecho de nuestros clientes. Conjuntamos personas, ideas y capital para fomentar el progreso y el crecimiento, lo que ayuda a crear un mundo mejor para nuestros clientes, nuestros colegas, nuestros inversionistas, nuestras comunidades y el planeta que compartimos.

**Nuestros valores**

En HSBC, nuestros valores nos guían en todas nuestras acciones, desde la toma de decisiones estratégicas hasta las interacciones cotidianas con los clientes y entre nosotros. Se basan en la historia, el legado y el carácter de HSBC y nos ayudan a cumplir con nuestro propósito.

Estos son:

Valoramos la diferencia
- Buscamos nuevas perspectivas

Avanzamos juntos
- Colaboramos de manera global

Asumimos la responsabilidad
- Nos responsabilizamos de nuestras acciones con una visión de largo plazo

Hacemos que las cosas sucedan
- Nos movemos a un ritmo constante y conseguimos resultados

**Nuestra estrategia**

Nuestra estrategia respalda nuestra ambición de ser el socio financiero internacional preferido de nuestros clientes. Esta tiene cuatro pilares fundamentales:

1. Enfocarnos en nuestras fortalezas: enfocamos nuestra energía e inversiones hacia donde podemos marcar la mayor diferencia para nuestros clientes.
2. Digitalizar a escala: ponemos todo el poder de nuestro banco en el bolsillo de cada cliente, con una banca digital más fácil y segura.
3. Energizar para crecer: motivamos una cultura dinámica e inclusiva y fortalecemos a nuestros empleados ayudándolos a desarrollar habilidades para el futuro.
4. Apoyar la transición a cero emisiones netas: lideramos la transición a una economía de cero emisiones netas transformándonos nosotros mismos, además de apoyar y financiar a nuestros clientes para que realicen sus propias transiciones.

**Principios empresariales**

Nuestros principios de negocio dirigen cómo se ejecuta nuestra estrategia comercial. Establecen un estándar sobre cómo tomamos decisiones comerciales:

- Solidez financiera: mantener la fortaleza del capital y la liquidez
- Gestión de riesgos: ser emprendedor y comercial, comprender y ser responsable del impacto de nuestras acciones, tomar decisiones prudentes.
- Velocidad: ser rápidos y receptivos, tomar decisiones basadas en nuestros principios.
- Enfoque de rendimiento: liderar niveles competitivos de rendimiento, actuar con urgencia e intensidad, priorizar y simplificar.
- Eficiencia: enfocarnos en la disciplina de costos y la eficiencia del proceso.
- Calidad: buscar la excelencia.
- Enfoque al cliente: brindar una experiencia excepcional al cliente.
- Sustentabilidad – teniendo una perspectiva a largo plazo, entendiendo el impacto de nuestras acciones en nuestros grupos de interés, marca y reputación.

**Esto significa que:**

No debes participar en actividades comerciales o negocios que pudieran de algún modo estar relacionados o ser considerados como apoyo de actividades ilegales/ delictivas o contrarias al interés nacional del país en el cual el Grupo opera.

No debes participar en actividades comerciales o negocios con los cuales el Grupo no desea relacionarse, incluso cuando el negocio sea legal en el país en el cual se realizará o se ajuste a las prácticas y costumbres locales. Deberás ser cuidadoso en evitar comportamientos ilegales, fraudulentos, deshonestos o no éticos en todas sus relaciones ya sea comerciales como personales.

Debes informar a el área de cumplimiento que corresponda sobre cualquier conducta o comportamiento que pudiera ser contrario a la ley, los requisitos normativos / valores y principios o políticas comerciales del Grupo.

### *3.3. Valores clave en la conducción de los negocios*

Los valores clave para la conducción de los negocios del Banco incluyen la adopción de un fuerte compromiso de todo el personal de:

- Obtener los más altos principios personales de integridad en todos los niveles;
- Aplicar la verdad y equidad a las operaciones;
- Incluir calidad y competencia en todos los servicios brindados;
- Poner los intereses del Grupo HSBC por sobre los del empleado en particular;
- Cumplir con el espíritu y la letra de todas las leyes y regulaciones, dondequiera que se lleven a cabo los negocios.

La reputación del Grupo HSBC constituye su bien más preciado y se funda en el acatamiento de los valores arriba mencionados. Todos los empleados del Banco deberán acatar estos valores en la conducción de sus asuntos. Debe recordarse que toma años construir la reputación de una institución financiera y la misma puede perderse de la noche a la mañana por conductas irresponsables o deshonestas de sus integrantes.

Los niveles gerenciales y de supervisión del Banco deberán realizar el máximo esfuerzo posible para asegurar que las operaciones diarias se realicen de acuerdo con los Valores de Negocios Clave del Grupo. En particular, los Gerentes deberán corroborar que existan disposiciones de Cumplimiento adecuadas en toda su área de responsabilidad. Asimismo, deberán dar el ejemplo estableciendo altos estándares de honestidad y negocios equitativos y el cumplimiento, tanto con el espíritu como con la letra, de los requisitos legales y reglamentarios vigentes.

Los Gerentes y Supervisores deberán asesorarse con el Oficial de Cumplimiento sobre la mejor manera de cumplir con estas responsabilidades. El asesoramiento deberá incluir orientación sobre:

- ✓ La identificación de todas las leyes, regulaciones y códigos de práctica correspondientes
- ✓ El establecimiento de sistemas, procedimientos y manuales adecuados
- ✓ La instrumentación de capacitación en temas relacionados con Cumplimiento
- ✓ La instrumentación de disposiciones adecuadas de control y supervisión
- ✓ La revisión de nuevos productos u otros desarrollos que impliquen regulaciones que requieran cambios en los sistemas, procedimientos o capacitación del personal.

### *3.4. Trato con la prensa*

Ningún empleado de HSBC Bank Uruguay S. A. debe realizar ningún comentario a los medios de comunicación acerca de los asuntos internos del Grupo sin la previa del Responsable de Comunicaciones Externas.

### *3.5. Compromisos Externos*

Los negocios externos a la compañía o intereses profesionales deben ser transparentes y no deben constituir ningún potencial conflicto de interés.

**Cargos de dirección**

Ningún empleado de HSBC podrá asumir cargos de dirección, empleo u obligaciones comerciales de dedicación parcial fuera del Grupo, ya sean a título gratuito u oneroso, sin autorización escrita por el área de Recursos Humanos y Cumplimiento Regulatorio
En términos generales, se otorgará aprobación para asumir un cargo de dirección únicamente cuando esto no genere conflictos de interés con el Grupo. Ponga especial cuidado en asegurar que el nombre del Grupo solo se asocie a personas o compañías de la más alta integridad.

En los casos en que se autoricen dichos cargos, deberá asegurar que se encuentra familiarizado con las responsabilidades legales del cargo y tiene pleno conocimiento de las actividades y operaciones de la entidad en cuestión. Busque asesoramiento legal en especial en aquellos casos donde se realicen modificaciones legales a dichas responsabilidades.
Consultar la Sección 6 del Manual de normas de Grupo (GSM) para los casos donde el cargo de dirección forma parte de los servicios de administración de la compañía por medio de la cual el director brinda sus servicios según lo establecido en un contrato o acuerdo con el cliente.

**Cargos no laborales**
Las reglas descritas anteriormente no son de aplicación a cargos que no tengan ninguna relación con lo laboral, como por ejemplo asociaciones de residentes, clubes deportivos u organizaciones benéficas, así como tampoco a compañías de inversión privada donde se le puede solicitar que asuma un cargo de dirección de acuerdo con las necesidades de ese negocio específico.

## 4. DIVERSIDAD E INCLUSIÓN

La construcción de una cultura diversa e inclusiva es de vital importancia para nuestra marca y valores. Una cultura inclusiva nos ayuda a dar respuesta a nuestra base global de clientes cada vez más diversa que a la vez permite crear y mantener una fuente segura de colaboradores capacitados y comprometidos.

Nuestro ambiente laboral está definido por un Trato Justo en todos los niveles de la organización; este comportamiento aplica en cualquier momento y espacio durante la jornada laboral, en las sesiones de retroalimentación de desempeño y en cada foro de expresión de ideas y opiniones. Cualquier acción, situación o insinuación de acoso, hostigamiento o violencia física o verbal queda prohibida.

Hay cero tolerancia a cualquier práctica o insinuación de acoso sexual, hostigamiento físico y/o verbal, intimidación, o discriminación; tampoco es tolerado el acoso laboral (mobbing o bullying), parcialidad, prejuicio, discriminación o burla en ninguna de sus formas y bajo ninguna circunstancia.

Todos en HSBC somos responsables de tratar a nuestros colegas y clientes con dignidad y respeto, así como generar un ambiente de trabajo en el cual no haya ningún tipo de discriminación indebida, acoso sexual u hostigamiento, sin importar el sexo, identidad de género, embarazo, período de lactancia, edad, estado civil, discapacidad, sexualidad, raza, color de piel, creencia religiosa o nacionalidad, doctrina política o condición social.

No se aceptará ningún tipo de parcialidad, prejuicio, discriminación, acoso, hostigamiento o burla en ninguna forma y bajo ninguna circunstancia. Para mayor información, puedes consultar el Código Global de HSBC contra el Bullying, el Acoso u Hostigamiento en HRDirect. Asimismo puedes denunciar cualquier comportamiento que sea contrario a lo mencionado anteriormente a:

HSBC Confidential

http://home.global.hsbc/gc/home.nsf/gcms?open&ref=UKCM9Y7ENY114754AM07072015&language=es

## 5. COMPROMISOS Y PAUTAS DE ACTUACIÓN

Los empleados de HSBC Bank (Uruguay) S.A. deben actuar de manera de garantizar que los negocios y actividades del Banco se ajusten a las normas contenidas en el presente Código. En tal sentido, se exponen en este capítulo los compromisos y pautas de actuación de los empleados -incluyendo Gerentes, miembros del Directorio y Personal Superior- respecto del Banco y en sus relaciones con terceros.

### *5.1. Aspectos Generales*

*Acuse de recibo*: Se entregará una copia del presente Código a todos los empleados. Los empleados deberán leer cuidadosamente el texto y en caso de existir puntos que no entiendan, deberán consultar a su gerente o a Recursos Humanos. Luego deberán firmar el compromiso que se expone como ANEXO 1 y entregarlo al Departamento de Recursos Humanos a fin de acusar recibo de que han leído y comprendido sus responsabilidades según el Código. La entrega del acuse de recibo, se podrá realizar por medios electrónicos.

*Capacitación inicial:* Todos los empleados nuevos deberán recibir el Código y en caso de dudas deberán solicitar asesoramiento a Recursos Humanos.

*Asesoramiento de Cumplimiento:* Cualquier empleado que necesite asesoramiento u orientación sobre algún aspecto de este Código, deberá consultar a su Gerente o a Recursos Humanos. Las consultas deberán ser respondidas en menos de una semana desde la realización del planteamiento.

### *5.2. Cumplimiento de leyes y decretos*

Los procedimientos internos establecidos por HSBC Bank (Uruguay) S.A. cumplen estrictamente con las leyes y regulaciones vigentes en nuestro país. En tal sentido, el personal deberá asumir, sin excepción alguna, la obligación de cumplir estrictamente con las leyes y regulaciones que rigen las operaciones desarrolladas por el Banco.

Los empleados deberán, en la realización de las operaciones del Banco, privilegiar la legalidad y la observancia de los principios éticos sobre el logro de las metas comerciales. En efecto, los objetivos comerciales sólo podrán ser alcanzados con operaciones que cumplan cabalmente con las normas legales y reglamentarias vigentes, en particular aquellas emitidas por el Banco Central del Uruguay, y con las políticas y procedimientos internos, tanto aquellos adoptados a nivel local como los establecidos por el Grupo HSBC.

Los empleados de HSBC Bank (Uruguay) S.A. no podrán efectuar cualquier operación que suponga un incumplimiento al marco jurídico de la República Oriental del Uruguay, a las normas generales e instrucciones particulares establecidas por el Banco Central del Uruguay y/o a las políticas y procedimientos internos del Banco.

### *5.3. Lavado de Activos*

El lavado de activos es la actividad realizada por personas físicas o jurídicas tendiente a convertir fondos o recursos provenientes de actividades ilícitas, ocultando o disimulando su procedencia.

Los bancos y otras instituciones financieras pueden, sin advertirlo, ser utilizados como intermediarios para el depósito o transferencia de fondos derivados de actividades delictivas y por lo tanto, verse involucrados en el proceso de lavado de dinero.

Muchos países del mundo al igual que Uruguay, cuentan con leyes contra el lavado de dinero que establecen que se incurre en delito toda vez que una persona:

- A sabiendas colabore con un lavador de dinero sin informar sus sospechas a la autoridad correspondiente;
- No informe una sospecha razonable sobre la existencia de lavado de dinero a la autoridad correspondiente;
- Revele a una persona que ésta es objeto de un informe sobre sospecha o de una investigación penal.

El Grupo HSBC cuenta con procedimientos contra el lavado de dinero -Programa de Prevención de Lavado de Dinero - Procedimientos y Políticas Globales (GPP) -los cuales se aplican a todas las compañías del Grupo.

Los puntos principales de los GPP son:

- Se deberá verificar cuidadosamente la identidad de todos los clientes nuevos y deberá identificarse adecuadamente a los titulares de todas las cuentas;
- Los clientes nuevos que no puedan probar su identidad no deberán participar en transacciones;
- Los movimientos de cuenta que se caractericen por ser inusualmente importantes o extraños en la operatoria normal de la cuenta, o de acuerdo con la actividad conocida del cliente, así como los planteos inusuales deberán informarse inmediatamente al Oficial de Cumplimiento y al Gerente del Departamento.

Sin perjuicio de las políticas y procedimientos del Grupo, el Banco ha adoptado a nivel local un conjunto de políticas, procedimientos, sistemas y controles internos para la adecuada gestión de los riesgos de Lavado de Activos que son de cumplimiento obligatorio, los cuales se encuentran comprendidos en el Manual de Prevención del Lavado de Activos disponible en la intranet local.

Todos los empleados deberán capacitarse adecuadamente en la materia, de modo de conocer y aplicar los principios establecidos en Estándares Globales del Grupo, en las normas legales y reglamentarias nacionales y en las normas internas adoptadas a nivel local por el Banco.

En particular, los empleados que identifiquen la existencia de una operación o planteo inusual o sospechoso, en los términos de la legislación nacional o en la guía de operaciones inusuales (política AML disponible en Intranet local), deberán reportarla al Oficial de Cumplimiento en forma inmediata, siguiendo el procedimiento de reporte interno previsto en el Manual de Procedimientos. Asimismo, deberán mantener absoluta

reserva respecto de las transacciones que están siendo analizadas, debiendo abstenerse de informar al cliente.

Los empleados deben recordar:

- Que no es necesario estar seguros de que una transacción implique dinero ilícito para elaborar un reporte interno, la sospecha razonable es suficiente.
- Que deberán estar alertas y prestar atención a las transacciones inusuales y/o que puedan dar lugar a sospechas.
- Que deberán informar toda transacción sospechosa que observen.
- Que si una transacción parece demasiado beneficiosa para ser verdadera, probablemente sea sospechosa.

Los empleados que necesiten mayor asesoramiento sobre este importante tema deberán consultar a Recursos Humanos.

### *5.4. Financiamiento del terrorismo*

De acuerdo a la O.N.U., se define como acto terrorista a cualquier acto destinado a causar la muerte o lesiones corporales graves a un civil o a cualquier otra persona, que no participe directamente en las hostilidades en una situación de conflicto armado, cuando el propósito de dicho acto, puesto de manifiesto por su naturaleza o su contexto, sea intimidar a una población u obligar a un gobierno o a una organización internacional a realizar un acto o a abstenerse de hacerlo.

Por su parte, el financiamiento del terrorismo consiste en que alguien por el medio que fuere, directa o indirectamente, provea o recolecte fondos con la intención de que se utilicen, o a sabiendas de que serán utilizados, en todo o en parte para financiar las actividades delictivas descritas en el párrafo anterior, aun cuando ellas no se desplegaren en el territorio nacional.

### *5.5. Conflictos de interés*

Conflicto de interés significa tener la potencialidad y el riesgo de no actuar de forma objetiva, justa, responsable, diligente con el Banco a causa de haber asumido responsabilidades externas.

El personal actuará siempre en defensa de los intereses del Banco. En tal sentido, los empleados evitarán colocarse en situaciones que puedan afectar su objetividad profesional o significar un conflicto entre sus intereses personales o los de personas o entidades estrechamente vinculadas a ellos (miembros de su familia, personas o empresas con quien comparten un interés económico) y los del Banco.

Anualmente, desde Comunicación Interna se les recordará a todos los empleados del Banco que declaren acerca de sus conflictos de interés dentro de la plataforma de Conducta del Grupo HSBC, con el fin de identificar la existencia de tales conflictos. En caso que el Comité de Gerencia considere que implica un riesgo muy elevado se le solicitará al empleado que elija la opción que más le convenga.

Deberán adoptarse todas las medidas tendientes a evitar o a solucionar conflictos de interés. Los empleados que tengan alguna duda acerca de la corrección de una acción o que consideren que sus propios intereses estén o puedan entrar en conflicto con los del Banco o el Grupo HSBC, deberán procurar el asesoramiento de Recursos Humanos/Cumplimiento Regulatorio.

Los empleados deberán obrar con cuidado para cerciorarse de no brindar un asesoramiento viciado por conflictos de interés, en situaciones tales como:

- Cuando una empresa del Grupo haya convenido brindar asesoramiento a un cliente (por ejemplo, en una oferta pública para la adquisición de acciones de control) y asesora a otra persona participante de la oferta;

- Cuando se recomiende la compra de contratos de derivados que ofrezcan ganancias al Banco pero en los que el cliente no pueda comprender de manera cabal los riesgos y no pueda afrontar la pérdida de su capital;

- Cuando se recomiende la liquidación de inversiones para reinvertir, cuando no exista una ventaja evidente para el cliente pero se generen comisiones para el Banco;

- Cuando se asesore en la compra de un producto específico y el empleado tenga objetivos de venta para tal producto, que no se ajusta a las necesidades y objetivos del cliente;

- Cuando se asesore la compra o venta de títulos con el fin de respaldar una oferta pública para la adquisición de acciones de control (o para evitar ese tipo de adquisiciones) cuando una empresa del Grupo se encuentre operando como asesora;

- Cuando se asesore la compra de títulos solamente para permitirle a otro cliente vender (por ejemplo, en un mercado con pocas transacciones) y así generar una comisión. También en el caso contrario cuando otro cliente quiera comprar acciones y el mercado es poco profundo;

- Cuando se recomiende la aceptación de la colocación de una emisión nueva para permitir que el Banco cumpla compromisos asumidos con el emisor (o suscriptor), cuando la inversión pueda ser inconveniente para el cliente.

Los empleados pueden realizar tareas externas al Banco siempre y cuando no impliquen un conflicto de interés y que la realización de esa tarea no influya negativamente sobre la actividad de HSBC Bank (Uruguay) S.A. En todos los casos, se deberá comunicar la situación a Recursos Humanos y Cumplimiento Regulatorio.

**Declaración de Relaciones Personales en el trabajo**

HSBC espera que nuestra gente se comporte profesionalmente en el trabajo. Establecemos estándares claros para nuestra gente por lo que pedimos que actúen con la mayor integridad y honestidad en todos sus tratos personales y comerciales.

Entendemos que las relaciones personales de naturaleza romántica o sexual pueden desarrollarse en el lugar de trabajo y también sabemos que nuestra gente a veces trabaja junto a familiares o amigos cercanos. No buscamos intervenir en las relaciones personales, pero es importante que nos aseguremos de que estas relaciones no afecten negativamente a nuestros clientes, otros colegas o nuestro negocio y/o creen un conflicto real o percibido en las acciones que toma nuestra gente.

Por esta razón, requerimos lo siguiente:

1.- No permitimos que los miembros de la familia o aquellos en relaciones románticas o sexuales tengan responsabilidades administrativas o de supervisión el uno con el otro. Es posible que le solicitemos a uno o a ambos que cambien roles o realicen ajustes de trabajo.

2.- Si estás en una relación romántica o sexual con alguien que trabaja para HSBC o tienes un familiar cercano que trabaja en HSBC o si trabajas en el mismo negocio o función que tu familiar, debes declarar esta relación por escrito (mediante el envío de un correo electrónico o un caso de HRDirect) a Recursos Humanos y tu gerente de línea. Si no estás seguro de si estás obligado de declarar, debes errar de precavido y declarar la relación.

3.- Reconocemos que muchas relaciones románticas o sexuales comienzan en el trabajo y HSBC no prohíbe las relaciones consensuadas entre colegas. Si deseas pedir una cita a un colega, debes tener cuidado: considera si alguna diferencia en la antigüedad o el poder podría hacer que la otra persona se sienta presionada o influir en su respuesta. Si no puedes estar seguro de que no serán influenciados como resultado de su puesto en el trabajo, no debes preguntarle. Si preguntas y la otra persona no dice "sí", no debe persistir. Perseguir o insistir el comenzar una relación con alguien que no quiere puede ser acoso.

4.- Se espera que te comportes de manera adecuada y profesional en todo momento durante cualquier relación romántica o sexual con un colega. Si una relación llega a su fin, se espera que manejes la situación de forma privada fuera del lugar de trabajo. No debes permitir que una relación romántica o sexual con un colega afecte su entorno laboral, sus relaciones laborales o el desempeño de sus funciones.

5.-Debes cumplir con la política de conflictos de intereses pertinente en relación con cualquier relación con clientes, colegas u otras partes interesadas. Esta política de relaciones personales no reemplaza ni sustituye ninguna obligación contenida en la Política de conflictos de intereses y si no está seguro de que política aplica, debes buscar orientación de tu gerente de línea.

### *5.6. Relacionamiento con los clientes*

Los servicios básicos que se brindarán al cliente deberán confirmarse por escrito, por ejemplo, en un acuerdo con el cliente. En todos los casos en que se brinde asesoramiento a un cliente:

- Es esencial instrumentar un acuerdo adecuado con el cliente;
- No deberá brindarse asesoramiento específico a menos que el empleado tenga suficiente información acerca del cliente (por ejemplo, las inversiones realizadas

hasta el momento, su situación financiera general, los objetivos de sus inversiones y su actitud con respecto al riesgo) a fin de garantizar que el producto recomendado es el adecuado. La información recibida del cliente y el asesoramiento brindado deberán registrarse por escrito;

- El asesoramiento tendrá que ser adecuado para el cliente de acuerdo con las circunstancias. Aunque el asesoramiento no se brinde, es importante asegurarse que los clientes no sean mal asesorados y que no se los aliente a asumir riesgos que no puedan afrontar.

### *5.7. Confidencialidad de la información*

La información relacionada con los negocios y los sistemas del Banco o sobre cualquier otro miembro del Grupo HSBC es confidencial y debe ser tratada en consecuencia.

Los negocios y asuntos privados de los clientes deben ser tratados con estricta confidencialidad. No deben ser revelados a ningún cliente, ni a terceros, ni siquiera a ningún miembro del Grupo o compañía asociada, sin el consentimiento del cliente.

En algunos casos, debido a conflictos de interés, la información conocida por un miembro del Banco no debe darse a conocer a otra parte del Grupo, por ejemplo:

- No se debe dar a los vendedores de títulos información confidencial con respecto a clientes corporativos ya que esto podría resultar en el uso abusivo de dicha información.

En dichos casos, se cuenta con Murallas Chinas para evitar la transmisión de información confidencial. Estos procedimientos deben acatarse rigurosamente ya que su inobservancia podría dar lugar a acciones penales en virtud de la ley contra las operaciones que se basan en el abuso de información confidencial.

Como condición de su empleo, se exige que todos los empleados firmen y devuelvan el Convenio de Declaración de Confidencialidad del Banco que garantiza la misma en todas las cuestiones comerciales relacionadas con el Banco y con sus clientes.

### *5.8. Protección de datos*

Todos los empleados tienen la responsabilidad de garantizar que los datos computarizados sean precisos, actualizados y que permanezcan seguros. La información almacenada en las computadoras deberá utilizarse solamente para los fines con que fue obtenida. Su revelación no autorizada está prohibida.

Los mismos principios deberán aplicarse a toda información obtenida de los clientes.

### *5.9. Secreto Profesional*

El revelar información sobre un cliente a personas no autorizadas constituye una infracción a la ley. Se podrá dar información sobre un cliente, un accionista de HSBC Bank (URUGUAY) S.A. o una transacción comercial específica a particulares, organizaciones u organismos gubernamentales que lo requieran, únicamente con el consentimiento de la persona u Organización involucrada si se ha recibido un oficio judicial, dentro de los casos permitidos por el art. 25 del Decreto-Ley 15.322 (Secreto

Profesional y Secreto Bancario). Dichos oficios deberán remitirse de inmediato a la Gerencia local, antes de divulgar dato alguno.

Los empleados del Banco, de acuerdo al Decreto-Ley 15.322, no podrán facilitar información alguna sobre los fondos o valores que tengan en cuenta corriente, depósito o cualquier otro concepto, pertenecientes a persona física o jurídica determinada. Tampoco podrán dar a conocer información confidencial que reciban de sus clientes o sobre sus clientes. Las operaciones e información referidas se encuentran amparadas por el Secreto Profesional, y solo pueden ser reveladas con autorización expresa y por escrito del interesado o por resolución fundada de la Justicia Penal o de la Justicia competente si estuviera en juego una obligación alimentaria y en todos los casos, sujeto a las responsabilidades más estrictas por los perjuicios emergentes de la falta de fundamento de la solicitud.

No se admitirá otra excepción que las establecidas en esta ley.

La ley prevé que quienes incumplieran el deber establecido el artículo referido, serán sancionados con tres meses de prisión a tres años de penitenciaría.

### *5.10. Inversiones personales, créditos y depósitos en el Banco*

Operaciones en valores

Los empleados pueden realizar las operaciones de inversión en valores que consideren conveniente siempre y cuando esté alineada a las política de negociación del personal PAD - Staff Dealing Rules.

El Banco permite a sus empleados realizar transacciones por propia cuenta y que no opere en perjuicio de ningún cliente o empresa del Grupo. Los empleados deberán comprender que su responsabilidad primordial es atender los negocios del Banco y que sus negocios personales se encuentran subordinados a los intereses de los clientes y del Banco. Los empleados deben entender que frecuentemente es necesario restringir las operaciones de determinadas acciones, en ciertas ocasiones, sin explicación a efectos de evitar conflictos de intereses con tareas desarrolladas por otras compañías del Grupo (como por ejemplo adquisiciones y fusiones).

Los principios de operaciones del Banco para los empleados son los siguientes:

- Ningún empleado debe operar, ni promover, recomendar o causar que otra persona realice inversiones, en relación con las cuáles haya adquirido información crítica confidencial que pudiera influir sobre los precios, ni en ninguna inversión relacionada;

- Ningún empleado debe operar, ni promover, recomendar o causar que ninguna otra persona negocie, sobre la base de información confidencial que se encuentre en su poder como resultado de su condición de empleado del Banco;

- Ningún empleado debe operar en circunstancias que impliquen conflictos de interés con los clientes del Banco;

- Ningún empleado debe operar cuando tal operación pueda potencialmente incurrir en obligaciones financieras que no pueda cumplir fácilmente sobre la base de los

fondos disponibles o que complique la situación de los recursos financieros del empleado;

- Ningún empleado debe operar cuando tal operación pueda afectar la buena posición o reputación del empleado, o la buena posición, reputación o mejores intereses del Banco;

- Ningún empleado debe operar en circunstancias que afecten sus obligaciones para con el Banco;

- Ningún empleado debe operar ni promover, recomendar o causar que ninguna otra persona realice alguna inversión (o inversión relacionada) sobre la cual tenga conocimiento de que se encuentra sometida a alguna investigación, recomendación o análisis a ser publicados por una Empresa del Grupo dentro de un plazo de 5 días hábiles y que pudiera dar lugar a inferir que el precio de la inversión o cualquier inversión relacionada podría verse afectado:

- Todo empleado debe respetar el espíritu de estos principios y el de todo requisito o legislación reglamentaria vigente.

El Banco ha emitido para todos sus empleados un conjunto de normas aplicables a las operaciones del personal (http://intra.uy.hsbc/areas/compliance/area_compliance.asp Staff Dealing Rules 1.5) las cuales contienen los principios mencionados más arriba y las siguientes normas:

- Los empleados deben respetar la política del Grupo HSBC sobre operaciones de Títulos del grupo HSBC, la cual se establece periódicamente;

- Los empleados que de acuerdo a la política PAD sean considerados “cubiertos”, en el ejercicio normal de sus tareas, ejecuten u operen títulos u otras inversiones (tales como cambio de divisas, operaciones en metales preciosos y commodities) para los clientes o para el Banco deben contar con la aprobación previa de sus superiores antes de realizar transacciones en tales títulos o inversiones por su propia cuenta.

Es deseable que los funcionarios negocien exclusivamente por intermedio del Banco.

Estas normas se encuentran contempladas en el manual de normas para operaciones de empleados del Grupo, disponible en la intranet http://fim.ghq.hsbc/FIM/home.nsf/ByRef/UKWEBMMJKX14075112032020?Open&language=EN

Si un miembro del personal tiene dudas con respecto a las Normas de Negocios para el Personal puede contactar a su Gerente o a Recursos Humanos.

Operaciones en cuentas de los empleados

Los empleados no deben tomar prestado dinero de los clientes u otros empleados, ni prestarles, excepto durante el transcurso de negocios autorizados.

Los empleados deben administrar sus asuntos financieros personales de una manera prudente y no deben involucrarse en compromisos financieros que no puedan razonablemente cumplir.

El Grupo HSBC estimula y busca que los empleados realicen sus operaciones bancarias en el propio Banco.

Los empleados se rigen por el reglamento vigente de préstamos a funcionarios, que se encuentra en la intranet de Recursos Humanos.

Las cuentas personales de los empleados, deben utilizarse expresamente para fines personales, no pudiendo en ningún caso realizar transacciones para terceros no integrantes de la cuenta.

Cuando un empleado realice una operación fuera de lo habitual, deberá comunicarlo a Uruguay FCC Operaciones Entre otras, se entiende como operaciones fuera de lo habitual, la venta de un inmueble o la venta de un vehículo.

### *5.11. Malas prácticas de operaciones*

Todos los casos de malas prácticas de operaciones, como los enumerados a continuación, que intenten favorecer injustamente al empleado a expensas del Banco, de sus clientes o del mercado, serán considerados muy graves:

- Las demoras en el registro de las transacciones en beneficio de la cuenta personal del empleado o de la cuenta de clientes favorecidos;
- El uso de información confidencial o difusión de información confidencial a terceros que les permita negociar como especuladores. Incluye los negocios en nombre del Banco o cualquier otra compañía del Grupo, las operaciones personales de los empleados y las operaciones, de o en representación de, clientes u otros terceros;
- Las operaciones que se anticipan a la publicación del material de investigación;
- Las operaciones a costa de las órdenes de clientes a fin de obtener un mejor precio que el cliente;
- Las operaciones en carácter de mandatario en perjuicio del Banco;
- Las cancelaciones de contratos y registro de operaciones en otras cuentas de manera de perjudicar al Banco o a sus clientes.

### *5.12. Pautas de comportamiento interno*

Relaciones con los demás

Usted deberá tratar a sus colegas, clientes y otras personas con amabilidad, imparcialidad, cortesía y respeto.

HSBC Bank (Uruguay) S.A. no tolerará ningún tipo de discriminación, ni ninguna conducta deshonesta, falta de ética o inapropiada. Es parte de la política de HSBC Bank (Uruguay) S.A. asegurar la existencia de un ambiente emocionalmente cómodo y armonioso, con igualdad de oportunidades laborales para todos, sin discriminación de edad, sexo, raza, religión, color, nacionalidad de origen, estado civil, preferencia sexual, incapacidad o condición de incapacitado, así como tratar a todos los clientes y posibles clientes sin ningún tipo de distinción. Si usted cree ser víctima de alguna forma de hostigamiento o discriminación, comuníquelo inmediatamente a la Gerencia Local y/o Recursos Humanos.

Si usted supervisa a otras personas, es responsable directamente de implementar y practicar esa política. Además se espera que usted mantenga un ambiente de trabajo libre de todo tipo de hostigamiento, intimidación y ofensa.

Acoso

HSBC tiene un compromiso con las Políticas anti acoso en el ámbito de trabajo así como contra toda conducta de discriminación por razón de género y orientación sexual.

Se considerará falta grave aquellas conductas que puedan configurar situaciones de acoso de cualquier naturaleza. De configurarse tales supuestos, y luego de investigar y analizar las circunstancias, garantizando los derechos de todas las partes involucradas, se tomarán las medidas disciplinarias pertinentes.

Políticas sobre el uso de Internet y el correo electrónico

El uso del correo electrónico y el acceso al sistema de computadoras externo por Internet, se suministrarán para asuntos comerciales solamente y están sujetos a la política de Internet vigente. El uso inadecuado de los mismos, provocará la aplicación de procedimientos disciplinarios, incluyendo la revocación de los privilegios de acceso y de la relación de empleo.

El acceso a Internet y al correo electrónico no debe ser utilizado para los siguientes propósitos expresamente prohibidos: solicitud de correspondencia no relacionada con actividades de negocios, mensajes ilegales, difamatorios u ofensivos, perjuicios u hostigamiento ya sean raciales, sexuales o de cualquier tipo, acciones perjudiciales al negocio de otros, su reputación o su acceso a Internet (insulto, difusión abusiva, etc.) para la baja de pornografía, juegos de software u otro material lascivo o frívolo, para obtener o comprar software (.exe) sin la aprobación previa específica o material de video, audio, musical, tampoco para la participación en foros de discusión, grupos de usuarios o salas de charlas, tampoco para la emisión de cualquier aviso comercial no autorizado formalmente, compromiso legal asumido por correo electrónico a favor de cualquier miembro del Grupo HSBC, ni para la comunicación de cualquier forma de acuerdo contractual comercial; ni para la comunicación de cualquier material de publicidad/marketing sin la aprobación de la Oficina de Cumplimiento. Por dudas sobre la aplicación consultar a las condiciones de uso de Internet y correo electrónico.

Asimismo, el Banco podrá acceder en cualquier momento a controlar el correo electrónico y el uso de internet sin aviso y sin necesidad de recoger el consentimiento del empleado.

### *5.13. Soborno y corrupción*

La Política y principios de negocio del Grupo para combatir el soborno (BPP) se aplican tanto al soborno de funcionarios públicos como a transacciones y relaciones comerciales. Los BPP brindan una norma mínima para todo el Grupo, conforme a los principios de negocio y valores del Grupo.

Ningún miembro o empleado del Grupo deberá involucrarse de ninguna forma en un soborno, ya sea directa o indirectamente. Como "soborno" se entiende "todo ofrecimiento o recepción de regalos, préstamos, comisiones, recompensas u otras ventajas a cualquier persona o de cualquier persona, incluso un empleado, como incentivo en la conducción de negocios por parte del miembro del Grupo, en particular cuando esa oferta o recepción de soborno sea deshonesta, ilegal o represente un abuso de confianza'. Podría considerarse un delito penal cuando no exista la intención de evitar un soborno.

La política existente del Grupo permite una serie de excepciones específicas limitadas, que no se consideran dentro de la definición de soborno.

Los empleados no deberán solicitar ni aceptar ningún regalo ni incentivo, al margen de obsequios tales como agendas y almanaques. La aceptación de regalos o incentivos demasiado generosos podría dar lugar a un conflicto de intereses y dañar la reputación del Banco.

En el mismo sentido, los empleados no deberán ofrecer ni dar regalos o incentivos que puedan interpretarse como sobornos o que puedan de alguna manera dañar la reputación del Banco.

Se hará una excepción específica a ésta prohibición si no hay o no parece haber una posibilidad razonable de influencia indebida en el cumplimiento de las obligaciones en nombre de HSBC Bank (Uruguay) S.A. y si el beneficio personal cae dentro de una de las categorías siguientes:

- Cortesías comerciales normales, tales como comida o partidas de golf, en que sólo se incluyan servicios o amabilidades usuales;
- Viajes pagados o servicios de hospedaje en los casos en que se represente formalmente a una unidad del Grupo HSBC o que puedan ser o sean correspondidos en forma personal;
- Regalos (que no fuesen dinero) que no sean de gran valor, tales como obsequios durante las fiestas, excepto si son de proveedores de la corporación;
- Regalos recibidos por parentesco, matrimonio o relaciones sociales enteramente independientes de todo tipo de relación comercial;
- Honorarios u otros tipos de compensación recibidos de parte de una Organización de la que se es miembro o en la que se ocupe un cargo oficial, después de haber recibido por escrito la aprobación de HSBC Bank (Uruguay) S.A.

Salvo las excepciones mencionadas anteriormente, todo beneficio personal recibido deberá ser comunicado a la Gerencia local y el beneficio en cuestión deberá ser devuelto

inmediatamente al otorgante. Se deberá consultar al Departamento de Cumplimiento en los casos que los regalos antes mencionados excedan los USD 100.

Todo incumplimiento de la Política y principios de negocio debe notificarse de inmediato al Funcionario Local de Compliance (FCC Sanctions), quien presentará el informe a la estructura de Compliance que corresponda.

Contribuciones voluntarias

Quizás desees, o recibas un pedido de colaborar en la compra o comprar algo para una persona o compañía. Por lo general, este tipo de situaciones se da para una boda, la cena anual, eventos de caridad u otras celebraciones. Asegúrate que las contribuciones voluntarias que realices no están siendo utilizadas para esconder un acto de soborno.

Todos los temas de campañas de voluntariado entre empleados para apoyar alguna causa particular, están fuera del alcance de esta política. Sugerimos esos temas verlos de forma interna con Sustentabilidad Corporativa y Recursos Humanos.

Consulta el punto C.1.1 Global Anti Bribery and Corruption Policy - Guidance 1- Employee Risk C.1 Global Anti Bribery and Corruption Policy Guidance (uk.hsbc)

Deberás informar cualquier incidente conocido o presunto de soborno y cualquier incumplimiento de este Código a tu line manager, Oficial de Cumplimiento, Oficial Anticorrupción o a través del portal confidencial de HSBC (a través de HR Direct). Antes de usar HSBC Confidential, por favor consulta la guía sobre cómo funciona.

### *5.14. Denuncia de actividades ilegales*

El Grupo HSBC ha creado una Línea de Denuncia Telefónica de Compliance (HSBC Confidential - The Compliance Disclosure Line - Intranet) la cual está diseñada para permitirles a todos los empleados presentar denuncias sobre los asuntos que se enlistan a continuación, cuando los canales normales para aclarar agravios o inquietudes no están disponibles o resultan inapropiados. Los empleados que utilicen la Línea de Denuncia Telefónica de Compliance deben tener razones para creer que el asunto que están informando es cierto. Todas las llamadas comprendidas dentro de la injerencia de la Línea de Denuncia Telefónica de Compliance se manejarán de una manera que garantice que la persona que haga la llamada no sufra ninguna represalia o consecuencia negativa dentro de la organización. A los empleados cuyas llamadas estén fuera de la injerencia de esta Línea Telefónica, el departamento de Group Compliance (GMO CMP) les notificará este hecho y las razones del mismo.

Todas las oficinas del Grupo pueden utilizar la Línea de Denuncia Telefónica de Compliance.

Cualquier empleado del Grupo que se entere de cualquiera de las situaciones listadas a continuación, o que sepa de cualquier intento deliberado de ocultar dichos situaciones, puede hacer su denuncia de forma confidencial a través de la Línea de Denuncia Telefónica de Compliance sin temor a represalias de cualquier tipo:

a. Acusaciones de soborno o de la corrupción, incluyendo cualquier incentivo tentada o efectivamente recibida por HSBC o cualquiera de sus directores, oficiales o empleados; sus afiliados o representantes.

b. Infracción de requisitos legales y regulatorios por parte de cualquier compañía del Grupo, incluyendo la comisión de un acto criminal, una injusticia o el incumplimiento de una obligación legal.

c. Incumplimiento de adoptar políticas consistentes con el Manual de Normas del Grupo.

d. Fraude o error deliberado en la preparación, evaluación, revisión o auditoría de estados financieros de cualquier compañía del Grupo.

e. Fraude o error deliberado en el registro y mantenimiento de los registros financieros de cualquier compañía del Grupo.

f. Deficiencias o incumplimiento de los controles contables internos de cualquier compañía del Grupo.

g. Cuando la condición financiera de cualquier compañía del Grupo no sea informada de forma veraz y completa.

h. Maniobra fraudulenta o declaración falsa hecha ante o por un Group Executive Officer o Accountant en relación con asuntos contenidos en los registros financieros, informes financieros o auditorías de cualquier compañía del Grupo.

i. Cuando la salud y seguridad de un individuo estén en peligro o cuando se esté dañando el ambiente.

Si la denuncia hecha por un empleado a través de la Línea de Denuncia Telefónica de Compliance está dentro de la injerencia de los puntos (a) al (h) listados anteriormente y el empleado desea permanecer anónimo, GMO CMP se apegará a la solicitud de anonimato. En todos los demás casos, se hará todo lo posible para garantizar que la identidad del denunciante se mantenga estrictamente confidencial. Sin embargo, puede haber situaciones en las que estemos obligados por ley a revelar la identidad del denunciante (excepto cuando la denuncia se haya hecho de forma anónima), por ejemplo, cuando la investigación dé como resultado que se inicie un proceso legal. En caso que se tenga que revelar la identidad del denunciante, GMO CMP le hará saber este hecho al denunciante antes de hacer revelación alguna.

**Cuando utilizar la Línea de Denuncia Telefónica de HSBC Confidential**

Los empleados deberán normalmente informar cualquiera de las situaciones arriba listadas en primera instancia a sus jefes inmediatos o a Recursos Humanos, quienes cuentan con políticas para lidiar con una amplia gama de agravios. La Línea de Denuncia Telefónica de Compliance deberá utilizarse en las siguientes circunstancias, cuando un empleado crea que:

No es posible utilizar los canales normales de información;

No se cuenta con otros medios a nivel organización para expresar sus inquietudes;

Será objeto de intimidación o represalias.

Si la inquietud se relaciona con cualquiera de las situaciones listadas en los puntos (c) al (g), la haremos del conocimiento del Group Audit Committee, cuando corresponda, como parte de nuestros requisitos legales y regulatorios.

**Cómo levantar una denuncia en la Línea de Denuncia Telefónica de Compliance**

Los empleados deberán llamar al International Internal HSBC Tie Line: 71 44 7991 1110 quienes serán tratados con estricta confidencialidad.

Los empleados también pueden presentar sus denuncias mediante un correo electrónico a hsbc.confidential@hsbc.com

Por más información:

http://home.global.hsbc/gc/home.nsf/gcms?open&ref=UKCM9Y7ENY114754AM0707 2015

**Denuncias por Escrito**

• Las denuncias por escrito (excepto correos electrónicos) deberán dirigirse a: Head of Group Compliance, Level 41, 8 Canada Square, London E14 5HQ.

**Cómo se manejan las denuncias**

• Group Compliance es responsable por la operación de la Línea de Denuncia Telefónica de Compliance y el manejo de las denuncias. Se revisarán todas las denuncias y se les remitirá para investigación cuando corresponda. Se le dará aviso de recepción de su denuncia y se le notificará las acciones iniciales que se están tomando en relación con la misma. También se le notificará el resultado de su denuncia una vez que se haya resuelto.

Denuncias dentro del alcance de estos procedimientos

- GMO CMP remitirá las denuncias que caigan dentro del alcance de estos procedimientos para investigación, lo cual puede requerir que se les remita a otro departamento. GMO CMP le notificará al denunciante sobre la acción realizada.
- La duración de la investigación varía dependiendo de las circunstancias particulares de cada denuncia. Los denunciantes pueden ponerse en contacto con GMO CMP para saber el estatus actual de su informe.

GMO CMP les notificará a todos los denunciantes sobre los resultados de la investigación hecha como resultado de su informe. Toda pregunta respecto al alcance u operación de la Línea de Denuncia Telefónica de Compliance deberá remitírsele al Senior Manager, GMO CMP.

Para mayor información dirígete a la siguiente liga:

http://home.global.hsbc/gc/home.nsf/gcms?open&ref=UKCM9Y7ENY114754AM07072015&language=es

Los empleados deberán estar alertas ante las posibilidades de estafa, robo y otras actividades ilegales que puedan dañar al Banco o a nuestros clientes. En el mismo sentido, los empleados deberán reconocer el daño potencial para la reputación del Banco que pudiera resultar del incumplimiento de los requisitos reglamentarios. Si un empleado advierte alguna de tales actividades e incumplimientos deberá informarlos inmediatamente a su Gerente de línea o a Recursos Humanos. No informar tales cuestiones se considerará una falta disciplinaria grave.

La Ley sobre Divulgación de Interés Público (Public Interest Disclosure Act) entró en vigencia en julio de 1999 y prohíbe victimar a los empleados (que incluye a consultores, subcontratistas y trabajadores de agencia) cuando existe una preocupación genuina sobre malas prácticas (incluye delitos penales, seguridad e higiene, error judicial y riesgo ambiental). Cuando los empleados tengan un problema genuino deberían, a menos que consideren que existe una razón para no hacerlo (por ejemplo, exposición a ser victimados), dirigirse a la Gerencia de línea. Si los empleados consideran que dichos procedimientos no son adecuados, en ese caso se deben contactar a la Compliance Disclosure Line.

-Los empleados deben llamar al Phone: (+44) 20 7991 1110

International Internal HSBC Tie Line: 71 44 7991 1110.

Los empleados que llaman a HSBC Confidencial fuera de las horas de oficina en el Reino Unido pueden dejar su nombre, número telefónico y/o dirección de correo electrónico. Todas las llamadas o mensajes que se dejen en Compliance Disclosure Line serán respondidos por GMO CMP y serán tratados con estricta confidencialidad.

-Por correo electrónico a: hsbc.confidential@hsbc.com

### *5.15. Prevención de Fraudes*

La condición fundamental para la prevención de un fraude o una actividad delictiva radica en la integridad de las personas en el sentido ético y técnico-profesional. Es obligación de todos los empleados cumplir con dicho requisito, desarrollando sus actividades en forma óptima y diligente, evitando incurrir en pérdidas derivadas de los incumplimientos.

Cada funcionario de las diferentes unidades de negocios y operativas debe asegurar el cumplimiento, o en su defecto denunciar, en caso que no ocurra, los requerimientos que se mencionan a continuación:

- Existen Lineamientos sobre la Protección de Personas, Activos e Información que abarque el área.

- Se proporciona un entorno de trabajo seguro al personal.

- Se trabaja en instalaciones y sistemas del Grupo a fin de minimizar los riesgos y garantizar la seguridad personal, de los clientes y del público.

- Se investigan todos los casos de sospecha de delitos, ya sea internos o externos, en forma decidida y cuidadosa.

- Se coopera en su totalidad con las autoridades de seguridad en la medida permitida según las leyes o reglamentaciones relevantes.

- Las Oficinas del Grupo evalúan los riesgos de delitos y fraudes internos y externos y verificar que los controles relacionados con fraudes se encuentren funcionando de manera efectiva para mitigar dichos riesgos en un nivel aceptable. Entre los controles relacionados con fraudes se aplican los siguientes:

  - Políticas y procedimientos para la protección de información confidencial.

  - Verificación e identificación exhaustiva de los clientes.

  - Sistemas de detección y control automatizados que incluyan transacciones de alto riesgo, cambios en los registros de los clientes y actividad relacionada con el personal.

  - Investigación de la solicitud del cliente.

  - Procedimientos de adquisiciones.

  - Segregación de funciones.

Existe un manual llamado “Prevención y acción en caso de fraude”, con acceso a todo el personal. El mismo debe ser consultado ante dudas respecto de situaciones comprendidas dentro del concepto de fraude.

### *5.16 Obligación de información al Banco Central del Uruguay*

Los empleados de las empresas controladas por el Banco Central del Uruguay, tienen la obligación de informar al Banco Central acerca de las infracciones a las leyes y los decretos que rigen la actividad de intermediación financiera o a las normas generales e instrucciones particulares dictadas por el Banco Central, de las tengan conocimiento en el ejercicio de sus funciones. (Art. 3 Ley 17613 – art 20 Decreto Ley 15322 – art 2 Ley 16327).

La existencia de la denuncia y la identidad del denunciante están comprendidas en el deber de secreto (art 22 y 23 de la Ley 16696)

### *5.17 Consumo de alcohol o drogas*

Se acuerda el uso del protocolo establecido a estos efectos – “Protocolo de actuación ante situaciones de alcohol y/o drogas en el trabajo”. La aplicación del mismo se realizará de acuerdo al Convenio Colectivo vigente y deberá contactarse a la Comisión de Salud o a Recursos Humanos a estos efectos de forma de hacer seguimiento de los casos.

## 6. COMPROMISOS Y PAUTAS DE ACTUACIÓN ESPECÍFICOS PARA GERENTES

Sin perjuicio de las pautas de actuación establecidas con carácter general para todo el personal del Banco –establecidas en el capítulo 4-, los empleados que ocupen niveles gerenciales dentro de la estructura de la Organización deberán adoptar los compromisos y pautas de actuación que se detallan seguidamente.

### *6.1 Obligaciones con respecto al personal*

Contratación de personal

Los Gerentes deberán trabajar con el Departamento de Recursos Humanos para asegurar que únicamente se contraten personas adecuadas. Los procedimientos de contratación normales deberán asegurar, entre otras cosas, que:

- Se obtenga un Currículum Vitae completo y que se revise con detenimiento
- Se verifique la identidad del postulante
- Cuando sea posible, se obtengan referencias
- Se explique claramente la falta de antecedentes de empleo
- Los postulantes cuenten con la experiencia, capacitación e idoneidad necesaria para el cargo
- Se posea evidencias de las aptitudes
- Si es necesario que se registren con algún organismo regulador, que no exista razón por la cual su registro pueda no ser aceptado.

Difusión del Código

Los Gerentes deberán asegurarse de que todos los empleados reciban una copia de este Código y acusen recibo de haberlo leído y comprendido.

Capacitación

Todos los empleados y funcionarios deben completar en tiempo los cursos de capacitación obligatorios asignados por la institución, ya sea como una iniciativa única para cumplir un requisito especifico o anualmente para garantizar que los empleados estén informados sobre ciertos temas y asuntos. Además, es posible que se te solicite mantener y/u obtener ciertas acreditaciones según corresponda a tu función.

Completar los cursos de capacitación en tiempo y obtener y/o mantener las acreditaciones relevantes son una condición para tu empleo continuo. Si no lo haces, puedes ser removido de tu puesto (temporal o permanentemente) asi como ser sujeto a otras acciones disciplinarias, incluida la terminación del empleo.

Para más información, consulta el FIM de RH:

http://fim.ghq.hsbc/FIM/home.nsf/ByRef/UKWE9LEKDA15482325062014?Open&language=EN

Confidencialidad

Los Gerentes deberán garantizar que todos los empleados hayan firmado el Acuerdo de Declaración de Confidencialidad del Banco.

### *6.2 Lavado de dinero*

Los Gerentes serán responsables de asegurar que su personal esté debidamente entrenado en la materia. Asimismo, deberán adoptar los recaudos necesarios para que en sus áreas de negocio se cumpla con el Programa de Prevención adoptado por el Banco, tanto en aplicación a las políticas y normas internas como en función de los Procedimientos y Políticas Globales (GPP), consultando al Oficial de Cumplimiento, cuando lo entiendan necesario.

### *6.3 Financiamiento del terrorismo*

De acuerdo a la O.N.U., se define como acto terrorista a cualquier acto destinado a causar la muerte o lesiones corporales graves a un civil o a cualquier otra persona, que no participe directamente en las hostilidades en una situación de conflicto armado, cuando el propósito de dicho acto, puesto de manifiesto por su naturaleza o su contexto, sea intimidar a una población u obligar a un gobierno o a una organización internacional a realizar un acto o a abstenerse de hacerlo.

Por su parte, el financiamiento del terrorismo consiste en que alguien por el medio que fuere, directa o indirectamente, provea o recolecte fondos con la intención de que se utilicen, o a sabiendas de que serán utilizados, en todo o en parte para financiar las actividades delictivas descritas en el párrafo anterior, aun cuando ellas no se desplegaren en el territorio nacional.

### *6.4 Compatibilidad con actividades externas*

Se espera que todos los empleados del Banco dediquen todos sus esfuerzos en el interés del Banco. Las excepciones pueden incluir la participación en tareas de organizaciones de beneficencia, cívicas, religiosas o políticas, cuando no interfieran en la capacidad del empleado para realizar su trabajo. En general, ningún trabajo externo podrá interferir con el trabajo del empleado en el banco**.** (Importante referirse al capítulo 6.5 del GSM como referencia).

Se considera una actividad externa (outside activity) a aquellos roles que empleados de HSBC llevan a cabo en adición a su rol dentro de la organización. El propósito de éste procedimiento es servir de soporte a la politica de Conflictos de Interés (FIM de RC B.4) así como de proteger la reputación, la imagen y los intereses del Grupo y mitigar los riesgos asociados a conflictos de interés, sustentabilidad y soborno y anticorrupción.

No deberás asumir ninguna actividad externa en alcance de este procedimiento, sin contar con la aprobación previa de tu line manager. Las actividades externas en alcance pueden incluir aceptar un puesto de dirección en otra organización, tener un empleo adicional (tiempo completo o tiempo parcial), tener un negocio personal o familiar, entre otros. Los

roles de naturaleza politica, como candidato de un partido politico local, también estará sujeto a las aprobaciones necesarias.

Para mayor información sobre las actividades en alcance y/o sobre las actividades prohibidas, o si tienes alguna duda acerca del proceso puedes consultar el FIM de HR, consultar el material de apoyo en HRDirect o bien; crear un caso en HRDirect para solicitar apoyo.

http://fim.ghq.hsbc/FIM/home.nsf/ByRef/EMEA75NNGW18275001082007?open&language=en

El personal superior es contratado en exclusividad y no está excluido del derecho de limitación de jornada, por tanto no puede desarrollar tareas externas remuneradas.

### *6.5 Conflictos de interés*

En la prevención y detección de eventuales conflictos de interés, los niveles gerenciales cumplen un rol activo. En efecto, los Gerentes deberán identificar todos los potenciales conflictos de interés. Si los mismos no pueden ser evitados, el Gerente deberá implementar procedimientos adecuados para resolver estos conflictos. Dichos procedimientos deberán asegurar que los intereses legítimos de los clientes estén protegidos y que no se encuentren en situaciones desventajosas injustamente.

En especial, los Gerentes deberán evitar la creación de conflictos de interés al estructurar paquetes de remuneraciones o al establecer objetivos de venta que alienten la compraventa repetida de valores para generar comisiones adicionales o la venta de productos inadecuados. Se deberán revisar los patrones de venta para controlar si existen evidencias de que se han ejercido presiones indebidas sobre el personal de ventas.

Cuando se implementan procedimientos administrativos para manejar conflictos de interés, por ejemplo, Murallas Chinas, éstos se deberán revisar periódicamente para asegurar que son adecuados para su propósito y que son comprendidos por aquéllos que deben cumplirlos.

### *6.6 Relacionamiento con Clientes*

Los Gerentes deberán implementar procedimientos para asegurar que el asesoramiento específico que se brinda a los clientes sea adecuado de acuerdo con las circunstancias personales. Se deberán mantener registros para poder demostrarlo después de los hechos.

Es importante que las responsabilidades fiduciarias del Banco se cumplan por medio de honorarios y comisiones debidamente divulgados para la administración discrecional y para las operaciones de corretaje para clientes privados que realice el Banco. Deben instrumentarse sistemas para asegurar que las instrucciones de los clientes sean respetadas, las transacciones estén debidamente asignadas y que se pongan, en primer lugar, los intereses de los clientes.

Cuando el Banco actúe como mandatario o corredor, deberá desempeñar sus responsabilidades fiduciarias hacia sus clientes. En especial, no se deberán obtener ganancias secretas, por ejemplo, a través de movimientos secretos.

El material publicitario deberá ser claro y no engañoso cuando se vendan productos y servicios, como títulos (incluye la administración discrecional), fideicomisos, fondos comunes de inversión, productos con depósitos en moneda extranjera, pólizas de seguros y otros paquetes de productos de inversión. Se deberá revisar que su divulgación sea correcta, en especial con respecto a los riesgos involucrados y para asegurar que la declinación de responsabilidad se establezca en forma clara, equitativa y razonable.

Como regla general, los productos derivados implican riesgos que no son adecuados para los clientes minoristas, y por lo tanto, se deberá desalentar su uso. Cuando se realicen estas ventas, las mismas deberán ser controladas en forma estricta.

Se deberá prestar especial atención a los reclamos de los clientes y se deberá cumplir con el Procedimiento de Reclamos para asegurar que sean manejados de manera justa, objetiva y diligente.

En base a lo expresado anteriormente, la Gerencia deberá velar por el cumplimiento del Manual de Buenas Prácticas Bancarias.

### *6.7 Confidencialidad de la información*

*Información sobre los clientes*: los Gerentes serán los responsables de instrumentar y garantizar el cumplimiento de la normativa, manteniendo debidamente informado al Oficial de Cumplimiento.

*Protección de datos:* los Gerentes deberán instrumentar procedimientos para asegurar que se cumplan todos los requisitos sobre protección de datos.

*Principio de necesidad de conocer la información:* la responsabilidad de los Gerentes es que los empleados tengan accesos a la información necesaria para desempeñar las actividades laborales asignadas (Need to knowbasis).

### *6.8 Inversiones personales, créditos y depósitos en el Banco*

*Operaciones en valores del personal*: los Gerentes deberán asegurarse que:

- Las normas de operaciones del personal se emitan para todos los empleados;
- Existan procedimientos para la autorización previa de operaciones personales cuando sea necesario;
- Se implementen procedimientos adecuados para controlar las operaciones personales de los empleados.

Se debe prestar especial atención ante la posibilidad de malas prácticas en las operaciones.

### *6.9 Pautas de comportamiento interno*

*Relaciones con los demás*: los Gerentes deberán mantener un adecuado ambiente de trabajo de forma que no existan tensiones derivadas del mismo como consecuencia del incumplimiento de este punto. Asimismo debe reportarse al funcionario de Cumplimiento en caso de verificarse estas situaciones.

*Acoso:* los Gerentes deberán denunciar en caso que en sus áreas verifiquen una situación de acoso ya sea: personal, laboral, político, religioso, raza, sexo. Al área de Recursos Humanos o a HSBC Confidential

### *6.10 Regalos e incentivos*

Los Gerentes deberán implementar la política del Banco sobre regalos e incentivos.

### *6.11 Denuncia de actividades ilegales y violaciones a las normas*

Las actividades ilegales o violaciones a las normas sobre las cuales la gerencia toma conocimiento deberán ser informadas inmediatamente a Auditoría y Cumplimiento. Los Gerentes sabrán que los funcionarios de Cumplimiento tienen el deber de informar sobre violaciones de las normas a la línea jerárquica funcional del Grupo. También se les recuerda a los Gerentes que la política del Banco es informar todos los casos de conductas delictivas a la policía.

### *6.12 Asesoramiento de Cumplimiento*

Los Gerentes deberán trabajar en forma conjunta con el Oficial de Cumplimiento para asegurar que existan procedimientos de Cumplimiento adecuados y que se respeten debidamente.

Los funcionarios del Departamento de Cumplimiento deberán ser consultados oportunamente cuando se consideren nuevos productos o servicios, cuando se contemple un nuevo negocio o una reestructuración o cuando se pongan en vigencia nuevas leyes o regulaciones. También deberán ser consultados cuando se detecte la ocurrencia de incumplimientos o cuando los reclamos de los clientes indiquen un incumplimiento de las normas vigentes.

El Departamento de Cumplimiento deberá asesorar sobre la acción correctiva a tomar, respondiendo en un plazo menor a una semana contando a partir de la fecha de realización del planteo por parte de las áreas comerciales.

### *6.13 Fraude*

Los Gerentes deberán acatar y en su caso, ser medio de rápida acción para la respuesta, disminuyendo la probabilidad de incrementar la pérdidas.

## 7. RIESGO DE LA SEGURIDAD DE LA INFORMACION

Durante su relación laboral, excepto en el debido ejercicio de sus funciones y cumplimentando las políticas vigentes de seguridad de la información, o una vez terminada la misma con previa aprobación por escrito del Head del área de negocio y del Head de ISR (Riesgo de Seguridad de la Información), no debe difundir o hacer uso de información ni de correspondencia, cuentas, vinculaciones u operaciones del Grupo HSBC o sus clientes, o de información obtenida en relación con el ejercicio de sus funciones.

De ningún modo, debe utilizar información adquirida durante su relación laboral con el fin de obtener un beneficio económico. Asegúrese de cumplir con los siguientes requisitos de modo tal que se mantenga la confidencialidad y seguridad de la información:

- Trate los asuntos relacionados con clientes como confidenciales y solo revele información confidencial a aquellas personas dentro del Grupo que por su función así lo requieran.

- Evite tratar con colegas asuntos relacionados con clientes, proveedores, socios y el Grupo en lugares públicos o, si fuera necesario, asegúrese de que nadie escuche su conversación.

Toda la información se clasifica con base al riesgo potencial para HSBC y las partes relacionadas (incluyendo, sin limitarse a ello, los clientes, accionistas, empleados y/o terceros/proveedores). Esta clasificación se utiliza para crear políticas y procedimientos que protejan la confidencialidad e integridad de la información de HSBC.

Todos somos responsables del acceso seguro, generación, almacenamiento, consulta, modificación, transferencia y destrucción de la información de HSBC, ya sea en forma física o electrónica. Dicha responsabilidad rige para toda la información en cualquier medio.

Cualquier violación o sospecha de incumplimiento del deber de tratamiento seguro de la información deberá ser informado de manera inmediata a su líder de equipo y al Equipo de Gestión de Incidentes de Seguridad (REACT Uruguay/HBUY/HSBC).

La identificación de usuarios y contraseñas es única, todos los empleados son responsables de proteger y mantener la confidencialidad de las contraseñas y evitar que otras personas utilicen los derechos de acceso de las mismas. Cada individuo es responsable por sus propias contraseñas y por todo lo que con ella se haga o ejecute. No divulgues tus contraseñas o aquellas que te fueron proporcionadas para cumplir con tu tarea. Se recomienda elegir contraseñas fáciles de recordar pero difíciles de adivinar.

Todos los empleados deben cumplir con todos los requerimientos relacionados con Seguridad de la información, que están publicados en la sección B.10 Global Risk FIM.

### *7.1 Sistemas de comunicación electrónica: Uso del correo electrónico, Internet, etc.*

El uso de los sistemas de comunicación electrónica del Grupo, que incluyen Internet, Intranet, correo electrónico y mensajería instantánea, debe cumplir con las siguientes directivas que se aplican de igual manera a los textos y a cualquier documento adjunto.

- La información enviada a través de los sistemas de comunicación electrónica, como Internet, Intranet, correo electrónico y mensajería instantánea, debe estar relacionada con la naturaleza del negocio, de acuerdo con las responsabilidades y el nivel aprobado de autoridad del empleado. Cuando el correo electrónico se utilice para una comunicación de negocios, éste debe tratarse con la formalidad de una carta firmada en papel membretado de HSBC. La confirmación automatizada de recepción del correo debe utilizarse para los correos electrónicos importantes, siempre que se cuente con esta herramienta.

- Deberá tenerse cuidado al redactar y enviar mensajes, ya sea interna o externamente. Toda la correspondencia, tanto electrónica como en papel, es potencialmente susceptible de generar un litigio o en incumplimiento de procedimientos reglamentarios que afecten al Grupo; por tanto, es fundamental que los empleados tengan conocimiento de esto y eviten utilizar cualquier tipo de comentario o declaración que pudiera ocasionar un perjuicio a la posición jurídica de HSBC o por el que HSBC pudiera sufrir alguna situación vergonzosa o en la que su reputación se viera afectada.
- Los empleados no deben crear, ver, descargar, modificar, enviar ni reenviar, de ninguna forma y por ningún medio de comunicación, cualquier material inadecuado, incluyendo:
- Imágenes de pornografía, sexo explícito u obscenas, imágenes o mensajes racistas u otro material obsceno o frívolo
- La producción y el envío de mensajes ilegales, difamatorios u ofensivos, incluyendo información que sirva para difamar, avergonzar, amenazar, acosar, ofender o lastimar a los empleados, proveedores de servicios, clientes o a cualquier otra persona
- Todo tipo de material que carezca de ética o sea malicioso o que pueda incumplir algún contrato o ley aplicable, como la de protección de información, de derechos de autor o de derechos de propiedad intelectual, ya sea en el país de origen o en el de destino
- Cualquier tipo de información privilegiada que pueda generar un daño en la reputación del Grupo o pueda ponerlo en desventaja comercial
- Acciones que perjudiquen los negocios de otros, su reputación o su acceso a Internet
- Mensajes que inicien o continúen correspondencia del tipo de “cadenas” o “pirámides”
- Uso de software no autorizado

**Redes Sociales**

Los medios sociales se definen como cualquier herramienta o servicio basado en la web o móvil que facilita la comunicación a través de Internet entre organizaciones, comunidades y personas.

Aunque se pueden derivar beneficios potenciales del uso de las redes sociales, el uso indebido de estas puede poner en riesgo la marca y la reputación del Grupo HSBC, así como también puede poner en peligro nuestro cumplimiento de las leyes y normativas pertinentes, especialmente cuando se trata de información confidencial o sensible y la información interna ingresa al dominio público.

Es importante que, como empleado de la institución; tengas plena conciencia de las implicaciones del uso de las redes sociales a título personal y de corresponder; de forma profesional. Ten presente que no debes cometer ningún error o acción que pueda desacreditar a la institución. En particular, no debes actuar como representante o portavoz de HSBC (a menos que esté debidamente autorizado para hacerlo). Debes consultar los

“Principios para uso de medios y redes sociales para empleados de HSBC” para obtener orientación y conocimiento de las expectativas de la institución para los empleados sobre el uso seguro y apropiado de las redes sociales. Esta política se aplica a todos los empleados y funcionarios de la institución, así como a los contratistas, trabajadores eventuales y terceros que tienen acceso a los sistemas y equipos de la institución, y / o tienen autorización para usar las redes sociales en nombre de la misma.

El uso de las redes sociales aplica tanto para fines comerciales como personales. Además, se aplica independientemente de si se accede a las redes sociales utilizando las instalaciones y equipos de IT de la institución o de otro modo. La política de la institución con respecto a la seguridad de la información se aplica igualmente a las redes sociales. Sin perjuicio del contenido de las políticas de seguridad de la información, HSBC se reserva el derecho de supervisar, interceptar y revisar cualquier actividad en las redes sociales publicadas utilizando los sistemas o equipos de la institución.

Se hace de tu conocimiento que cualquier mensaje, publicación en las redes sociales, conversación o cualquier otro tipo de información o comunicación enviada o recibida utilizando los sistemas del Grupo será monitoreada y no permanecerá privada.

Además de lo anterior, también podemos revisar cualquier actividad en las redes sociales publicadas utilizando equipos externos, si el contenido hace referencia (explícita o implícita), refleja o podría verse reflejado en la institución de cualquier manera. El incumplimiento de cualquier parte de esta política puede dar lugar a una acción disciplinaria, independientemente de si la violación se comete durante o fuera del horario de trabajo, e independientemente de si se utiliza el equipo de trabajo o personal.

Es posible que se te pida que elimines las publicaciones o las comunicaciones en Internet, desactives el acceso a las cuentas, proporcione las contraseñas / detalles de inicio de sesión pertinentes o colabore de algún otro modo con cualquier investigación sobre posibles incumplimientos.

Para obtener más información consulta:

https://university.global.hsbc/sites/HSBCUni/en-gb/strategy-and-performance/digital-curriculum/social-media-principles

Los empleados no deberán representar a HSBC ni compartir ningún tipo de información del Grupo HSBC en foros de discusión por Internet, redes sociales o laborales, grupos de noticias o salas de chat (chat rooms), a menos de que el Head del área de negocios correspondiente y el Head de ISR (Riesgo de Seguridad de la Información), lo justifique y autorice de forma expresa.

Queda prohibido el uso de correo electrónico no autorizado (por ejemplo, AOL, Hotmail, Yahoo, etc.) o sistemas no autorizados de mensajería instantánea (por ejemplo, AOL, Microsoft Messenger, NetMeeting, etc.), a menos que esté expresamente justificado en razón del ejercicio de sus funciones y autorizado por el Head del área de negocio y del Head de ISR (Riesgo de Seguridad de la Información).

Los correos electrónicos relacionados con el negocio únicamente deberán enviarse a través de los sistemas de correo electrónico del Grupo; no deberán usarse los sistemas de correo electrónico privado para los fines del Grupo.

**Uso del correo electrónico y de Internet con fines personales**

Las herramientas de Internet, Intranet, correo electrónico y mensajería instantánea se suministran fundamentalmente con fines de negocios; sin embargo, los empleados de vez en cuando pueden requerir enviar mensajes de índole personal a través de los sistemas de comunicación electrónica del Grupo.

Está permitido el uso personal limitado, siempre que dicho uso no infrinja los términos y condiciones de la política del Grupo ni interfiera con el trabajo del empleado, y debe mantenerse al mínimo absoluto.

La información Interna, Restringida y Altamente Restringida únicamente deberá enviarse de manera externa con fines comerciales autorizados. Los empleados no deberán enviar información Interna, Restringida y Altamente Restringida a su cuenta de correo electrónico personal (aquélla que no es cuenta de HSBC), salvo que sean los únicos titulares de dicha información (información personal). Las siguientes soluciones para el envío de información al exterior en un formato electrónico se listan en orden de preferencia desde una perspectiva de seguridad e incluyen el nivel requerido de controles de acuerdo con la clasificación de la información:

- Correo electrónico – Deben cifrarse todos los correos electrónicos que contengan información Restringida o Altamente Restringida. En caso de que no sea práctico cifrar el correo electrónico, la información debe colocarse en un archivo adjunto cifrado.
- Facsímile (fax) – No se recomienda el uso de fax para enviar información Restringida, por lo que debe considerarse el uso de métodos alternativos. Asimismo, el uso de fax está prohibido para el envío de información Altamente Restringida.
- Mensajes instantáneos – Está prohibido enviar información Restringida y Altamente Restringida a través de mensajes instantáneos.
- SMS (mensajes de texto) – Está prohibido el uso de mensajes SMS para el envío de información Restringida y Altamente Restringida, excepto en el caso de las comunicaciones “fuera de banda” (a través de un método de comunicación para enviar licencias que protejan la comunicación por un método diferente) o SMS generados por el sistema y que hayan sido aprobados por ISR. Antes de solicitar la aprobación de ISR, deberá considerarse retirar los detalles innecesarios de manera que el contenido del SMS se clasifique como “información interna”.

**Monitoreo del uso de comunicaciones electrónicas**

El uso de Internet, Intranet, correo electrónico y mensajería instantánea (ya sea con fines personales o comerciales) está sujeto a un monitoreo y por tanto, el uso que hagan de los sistemas del Grupo HSBC o de Internet desde las oficinas del Grupo no será privado.

HSBC lleva a cabo controles del correo electrónico que se envía a destinatarios externos. El uso inapropiado de las herramientas de comunicación y el incumplimiento de la política destinada a asegurar la información que se envía hacia el exterior puede llevar a una sanción disciplinaria.

Los correos electrónicos y los mensajes instantáneos, así como los archivos adjuntos, pueden recuperarse y emplearse como evidencia en procesos legales.

### *7.2 Otros aspectos de importancia para los líderes de equipo.*

Debe identificar y tener un manejo adecuado de la Computación de Usuario Final (EUC) de modo tal de asegurar la integridad, disponibilidad y confidencialidad de la información contenida o procesada dentro de cada EUC.

Autorice el trabajo remoto sólo si existen suficientes controles para manejar cualquier riesgo que se pudiera identificar.

El acceso de terceros a información Restringida e información Altamente Restringida debe autorizarse sólo si existen controles adecuados y arreglos contractuales de confidencialidad.

Informe a Recursos Humanos, Riesgo de Seguridad de la Información y Seguridad Física de la transferencia de empleados con el fin de asegurar un acceso adecuado a la información, sistemas e instalaciones de HSBC

## 8. INFORMACIÓN PRIVILEGIADA

La información privilegiada es aquella que contiene datos específicos que están relacionados con mercados de valores y que algunos colaboradores o personas tienen acceso a estos datos relevantes, así también pudiera influir en términos de precios o aquella información no pública que pueda obtener durante su empleo o vinculación con el Grupo. Si se utiliza esta información para beneficio propio o de otros se comete delito grave.

En ningún momento podrás comerciar de manera directa o indirecta con acciones u otros valores de una compañía que cotice o no en bolsa cuando posea información privilegiada. Se trata de información que no suele estar disponible para los accionistas de una compañía o el público y que, de estarlo, podría afectar el precio de mercado de las acciones u otros valores de la compañía. No deberá divulgar dicha información a terceros.

Existen procedimientos destinados a controlar el manejo y uso de la información sensible en relación a precios, relevancia y/o confidencialidad que pueda obtener durante el curso de sus funciones.

– Consulte la sección B2.5 del FIM de Legal & Compliance

***Evento Relevante***

La Ley del Mercado de Valores describe el concepto de evento relevante en los artículos 362 y 105 que se describen detalladamente en el Anexo 1A (Normatividad Aplicable).

***Normas de actuación en supuestos de Información Privilegiada (Evento Relevante)***

- Los colaboradores que se ubiquen en los supuestos de Evento Relevante deberán controlar el acceso, disponibilidad y uso de la misma en los términos previstos en este Código de Conducta.
- Cuando un colaborador disponga de Información Privilegiada considerada Evento Relevante deberá comunicar al director responsable de su área los valores respecto de los que disponga de aquella información, comunicándolo aquél, a su vez, al área de Cumplimiento.

- Los colaboradores que dispongan de Información Privilegiada deberán abstenerse de utilizarla de forma abusiva o desleal, previniendo y evitando en lo posible esta forma de utilización y adoptando además, las medidas necesarias para corregir las consecuencias que de ello pudieran derivarse, atendiendo también a lo dispuesto por el artículo 7° del Código de Ética Profesional de la Comunidad Bursátil Mexicana. La Información Privilegiada de que se disponga en cualquier área del Grupo podrá trasladarse a cualquier otra área, con la autorización previa del área de Cumplimiento.
- Los colaboradores que se ubiquen en un supuesto de Evento Relevante deberán abstenerse de ejecutar por cuenta propia o ajena, directa o indirectamente, las siguientes conductas:

– Preparar o realizar, por cuenta propia o ajena, especialmente por cuenta de Grupo Financiero HSBC o sociedades integrantes del Grupo, cualquier tipo de operación en el mercado sobre los valores a que la información se refiera.
– Comunicar dicha información a terceros, salvo en el ejercicio normal de su trabajo, profesión o cargo, de conformidad con lo previsto en este Código de Conducta.
– Recomendar a un tercero que adquiera o transmita valores o que haga que otro los adquiera o transmita basándose en dicha información.

El área de Cumplimiento mantendrá actualizada una relación de “Valores Restringidos” (valores respecto de los que se le haya comunicado la existencia de Información Privilegiada) y una lista que contendrá los nombres de las personas que se ubican en el supuesto de Evento Relevante, en caso de existir alguna duda sobre este particular, será necesario consultarlo con el área de Cumplimiento.

***Control sobre el uso de Información Privilegiada considerada Evento Relevante***

Se considerará que todos los colaboradores y directivos que prestan sus servicios en las áreas que se mencionan a continuación tienen acceso a Información Privilegiada y/o podrían llegar a tener contacto con la misma:

1.- EXCO

2.- Direcciones Generales de las Subsidiarias del Grupo

3.- Custodia

4.- Finanzas

5.- Análisis

6.- Sociedades de Inversión

7.- Global Banking & Markets

8.- CMB

9.- Área de Riesgos

10.- Banca Privada

11.- Legal

12.- FCC y Regulatory Compliance

13.- Seguridad y Fraudes

Los Colaboradores que formen parte de las áreas antes señaladas deberán observar en todo momento los principios que se mencionan a continuación:

- Transparencia en la celebración de las operaciones.
- Igualdad de oportunidades frente a los demás participantes del mercado en la celebración de operaciones con valores.
- Protección de la confianza en el mercado de valores.
- Observancia de los usos y sanas prácticas bursátiles.
- Ausencia de conflictos de interés.
- Prevención de conductas indebidas que puedan tener como origen el uso de Información Privilegiada o Confidencial relativa a valores o inversiones.

Los colaboradores que presten sus servicios en las áreas de referencia, así como las Sociedades o personas que pretendan realizar una oferta pública y a las cuales Grupo Financiero HSBC o cualquiera de sus filiales preste o les haya proporcionado sus servicios, clientes que reciban asesoría de inversión, Emisoras, en relación con los Contratos de intermediación bursátil que celebren, para realizar operaciones de adquisición o enajenación de acciones propias son susceptibles de tener contacto con Información Privilegiada, por lo cual las inversiones que realicen por cuenta propia estarán sujetos a la elaboración y envío de una declaración periódica (trimestral), la cual contendrá los datos generales del directivo o colaborador que realice la operación, el precio de la operación, emisora, volumen, tipo, serie o clase de valores objeto de la operación y la fecha de su celebración, esta declaración deberá ser dirigida al Área de Cumplimiento, en el formato que se anexa al presente como Anexo 2.

Los colaboradores y directivos de las áreas antes señaladas deberán abstenerse de realizar operaciones por cuenta propia o a través de interpósita persona, sobre valores de las emisoras con las que se encuentren trabajando, durante todo el tiempo que dure el proyecto y 30 días naturales después de concluido este.

***Barreras de Información***

Son barreras de información las medidas, normas de actuación y procedimientos organizativos que se adoptan con el fin de garantizar la confidencialidad de la información y de controlar el flujo de Información Privilegiada entre cada una de las áreas del Grupo, evitando su transmisión sin control. Para ello, se procederá conforme a lo siguiente:

- En cada área del Grupo existirá un Responsable Local de Cumplimiento nombrado por la Dirección Ejecutiva de Cumplimiento, quien será la persona encargada de relacionarse con alguno de los Directores del área de Cumplimiento (dependiendo del área de que se trate), de observar sus instrucciones así como de vigilar la aplicación del Código de Conducta. Debe conocer los valores respecto de los que se disponga de Información Privilegiada, comunicarlo al área de Cumplimiento y comunicarle de manera precisa los datos de las personas que disponen de dicha información.

- De conformidad con las instrucciones que reciba del área de Cumplimiento, el Director Responsable adoptará los procedimientos administrativos precisos para garantizar la confidencialidad en la actuación de su área y, especialmente, con el fin de evitar que la Información Privilegiada pueda fluir sin control a otra área. Con el fin de hacer efectivas las Barreras de Información, se deberán establecer las siguientes medidas:
- Mantener una adecuada separación física entre las áreas que manejen información privilegiada.
- Establecer mecanismos que restrinjan el acceso a oficinas o despachos de las personas no incluidas dentro del área en cuestión.
- Procurar la protección de documentos, estudios, informes y archivos. Todos los documentos y archivos confidenciales deben salvaguardarse con un adecuado sistema de seguridad. Los documentos y borradores confidenciales que dejen de ser necesarios deben ser destruidos. Es importante mencionar que se deberá cumplir con la Clasificación de Información de acuerdo a la política de Seguridad de la Información.
- No suministrar a terceros, sin autorización del área de Cumplimiento, los documentos relacionados con las distintas áreas o sus clientes.
- No mencionar ni comentar con terceros los nombres de los clientes, los nombres de las personas con las que se mantiene contacto, ni cualquier otra información que sea o pueda ser confidencial, a no ser que sea necesario o recomendable para la correcta ejecución del trabajo de la persona que reciba o da la información.
- No comentar los asuntos de un cliente que implique Información Privilegiada de un área con personas de otra área, salvo que se esté expresamente autorizado para ello.
- Procurar la protección, mediante nombres en clave (passwords), de ficheros y bases de datos, programas informáticos y computadoras que contengan Información Privilegiada referidos a la actividad de su área.
- Utilizar códigos de trabajo o nombres en clave para la designación de proyectos sensibles dentro de su área, con el fin de proteger los intereses de los clientes y las operaciones que se pudieran estar analizando o ejecutando. Una vez decidida la utilización de un nombre en clave, se deberá comunicar al área de Cumplimiento.
- Procurar que en las comunicaciones a través del correo electrónico (mail) se respete la división de las áreas involucradas, con el fin de excluir a personas que no deban tener acceso a la información.
- Prestar especial atención a las comunicaciones telefónicas y mediante fax. Las comunicaciones o documentación a remitir se deberán realizar a través de los números que sean proporcionados por y para cada una de las áreas.
- No utilizar teléfonos móviles (teléfonos celulares, radiocomunicadores, o cualquier otro medio de comunicación inalámbrica) en las salas de contratación y en el centro habitual de trabajo de los colaboradores, para operar, para recibir instrucciones de clientes o incluso para emitir cualquier tipo de opinión, recomendación o asesoramiento. Queda igualmente prohibido que los colaboradores que trabajen en puestos grabados utilicen sus teléfonos móviles (teléfonos celulares, radiocomunicadores, o cualquier otro medio de comunicación inalámbrica) para dar instrucciones u órdenes de ejecución de operaciones por cuenta propia.
- Suscribir un documento, de acuerdo con el modelo que se suministre, por cada uno de los colaboradores que trabajen en áreas con Barreras de Información

"Murallas Chinas" ("Chinese Walls") establecidas, asumiendo el compromiso expreso de no transmitir a cualquier persona ajena a la propia área en cuestión información privilegiada, sin autorización previa del área de Cumplimiento.

***Control del traspaso de Información Privilegiada entre las distintas áreas del Grupo***

Cuando por razones profesionales y para el adecuado desarrollo de una operación, sea preciso por alguna de las áreas involucradas en un proyecto disponer de información perteneciente a otra área del Grupo Financiero HSBC, o donde se vea implicada la Actividad de Análisis, siempre que en estos casos pueda verse afectada, directa o indirectamente, la revelación de Información Privilegiada, o pudiera crearse un conflicto de intereses, se procederá cumpliendo las siguientes normas de actuación:

- Los supuestos de rupturas de las Barreras de Información deben limitarse a los casos en los que realmente exista necesidad de recibir colaboración de otras áreas y la información que se solicite y la que se suministre ha de ser sólo la necesaria.
- La petición será realizada por el Director Responsable del área que la solicite. La concesión de la autorización, en su caso, corresponde al área de Cumplimiento, área que tendrá en cuenta una lista de Valores Restringidos y una lista en relación a las personas que disponen de Información Privilegiada (Evento Relevante), y previa conformidad con el Director Responsable del Área que suministra la información, asistencia o colaboración.
- Se debe considerar el momento oportuno para traspasar la información. Es recomendable que el período de tiempo entre el traspaso de información y el cierre de la operación, o su anuncio, sea el menor posible, con el fin de que la persona receptora de la Información Privilegiada (Evento Relevante) que, como consecuencia de ello habrá sido incluida en la lista de referencia a las personas que se ubiquen en el supuesto de un Evento Relevante, no se encuentre inhabilitada por un largo período de tiempo.
- El área de Cumplimiento tendrá en cuenta los riesgos de conflictos de intereses y la existencia, si se plantea un conflicto, de un margen de seguridad de que se resolverá de modo no perjudicial para el cliente o, de estar implicados dos clientes, de modo no perjudicial para el cliente relacionado con el área de donde proceda la información. En ningún caso podrá autorizarse la transmisión de información en contravención de los acuerdos de confidencialidad suscritos por las áreas del Grupo.
- La persona que reciba la Información Privilegiada (Evento Relevante), será incluida por el área de Cumplimiento en la lista referida a las personas que disponen de la misma, con indicación de la fecha y hora en que se le suministró, y tendrá la obligación de guardar secreto sobre la información transmitida y evitar realizar cualquier operación afectada por aquélla.
- Cuando la Dirección de Finanzas Corporativas actúe como líder colocador o rector en la colocación de valores procedentes de emisiones u ofertas públicas de venta, deberá comunicar las informaciones y manifestaciones del folleto informativo o prospecto al área de Cumplimiento, con el fin de que contraste la existencia de Información Privilegiada referido a dichos valores y pueda comprobar la exactitud y veracidad del prospecto informativo al respecto.

- Relación entre las Áreas que tienen acceso a información privilegiada y los Colaboradores que por su labor se encuentren situados por encima de las Barreras de Información.
- El área de Cumplimiento especificará las personas que, encontrándose por encima de las Barreras de Información y, por tanto, no sometidas a las limitaciones ni procedimientos que son de aplicación al personal de las áreas involucradas en algún proyecto, puedan acceder en el ejercicio de sus cargos o funciones a la información de todo tipo de que disponga el resto de la organización y, en concreto, las áreas antes mencionadas.
- Sin perjuicio de lo anterior, los Responsables Locales de Cumplimiento responsables de las áreas involucradas y de la Actividad de Análisis comunicarán al área de Cumplimiento, en la forma y términos que se establezcan, las personas situadas por encima de las Barreras a las que se les haya suministrado Información Privilegiada.
- Las personas que hubieran tenido acceso a Información Privilegiada (Evento Relevante) tendrán obligación de guardar secreto sobre la información y evitar realizar cualquier operación afectada por ésta.
- Cuando corresponda al Consejo de Administración de Grupo Financiero HSBC o a cualquier otro órgano colegiado de las áreas del Grupo una decisión y/o recomendación concreta sobre determinados valores, deberán abstenerse de intervenir aquellas personas que hayan tenido acceso a la información privilegiada con respecto a los valores de que se trate, comunicándolo al área de Cumplimiento.

***Grabaciones***

Las entidades de Grupo Financiero HSBC relacionadas con los mercados de valores cuentan con sistemas de grabación a fin de registrar las operaciones de mercado que se realicen y resolver las controversias que puedan plantearse.

**La Dirección de cada entidad pondrá en conocimiento de todos y cada una de los colaboradores cuyas conversaciones telefónicas vayan a ser objeto de grabación esta circunstancia.**

Las grabaciones se conservarán durante los plazos marcados por la regulación y/o políticas internas. En el caso de que haya alguna incidencia en relación con una transacción, se conservará hasta que dicha incidencia se haya resuelto.

La Dirección de cada entidad asegurará que el acceso a los sistemas de grabación y a las cintas esté estrictamente controlado. Las grabaciones podrán ser utilizadas por el Área de Auditoría Interna, Prevención e Investigación de Fraudes, Contraloría Normativa, Dirección de Recursos Humanos o cualquier otro departamento para el que resulte imprescindible dicha utilización como instrumento de control del cumplimiento de este Código de Conducta. También pueden utilizarse como medio de prueba de cualquier infracción de las normas contenidas en este Código de Conducta, siempre que el área de Cumplimiento lo precise.

**Registro sobre Acceso a Información Privilegiada o Altamente Restringida.**

El área de Cumplimiento con apoyo de los Responsables Locales de Cumplimiento de cada una de las áreas que tuviesen o pudieran llegar a tener acceso a Información

Privilegiada o Altamente Restringida, establecerán un registro que controlará las fechas, horas y nombres de las personas que hayan tenido acceso a Información Privilegiada o Altamente Restringida sobre valores o inversiones. Los Responsables Locales de Cumplimiento quedan designados como responsables del manejo de la información que se genere en cada una de sus áreas, debiendo verificar que la información solo sea del conocimiento de las personas que debido a su función deban tener acceso a la misma, de igual forma deberán verificar que todos los responsables de su área hayan suscrito el convenio de confidencialidad respectivo. Se generará una lista con los nombres de todas las personas que hayan tenido contacto con Información Privilegiada o Altamente Restringida, el Responsable Local de Cumplimiento será responsable de que dicho documento sea enviado al área de Cumplimiento del Grupo.

El Grupo Financiero HSBC se reserva el derecho a SUSPENDER o cancelar las facultades de acceso a cualquier persona que represente un RIESGO para la confidencialidad, integridad o disponibilidad de la información

**Confidencialidad de la Información (*Insiderlist*)**

Con base al Código del Grupo para operar con valores del mismo grupo *"Code for Dealing in HSBC Group Securities"*, se deberá considerar la elaboración de una lista del personal denominada *"Insiderlist"*. Esta lista contendrá el nombre de los funcionarios que por su nivel jerárquico y/o funciones desempeñadas, tienen acceso a información confidencial del Grupo.

La *"Insiderlist"* será actualizada en forma periódica, para tal efecto el área de Recursos Humanos notificará al área de Cumplimiento acerca de las altas, bajas o cambios del personal, a su vez dicha área notificará al área de Cumplimiento del Grupo.

## 9. RÉGIMEN SANCIONATORIO

HSBC Bank (Uruguay) S.A. requiere un alto estándar de conducta de parte de todos sus empleados.

El incumplimiento de las disposiciones establecidas en el presente Código será pasible de sanciones previstas en el presente capítulo, sin perjuicio de aquellas de carácter civil o penal que puedan corresponder de conformidad con las leyes de la República y/u otras regulaciones aplicables.

Se considera falta, la violación de cualquiera de las normas contenidas en el presente Código, ya sea a título culposo o doloso.

Se entiende que existe actuación culposa cuando, por impericia, negligencia o desatención, se viola cualquiera de las previsiones del presente Código, sin que exista voluntad de violarlo.

Se entiende que existe dolo cuando:

- Existe voluntad cierta y directa de realizar una operación con conciencia de que la misma infringe o viola alguna de las disposiciones del Código de Conducta, o

- Existe voluntad cierta y directa de realizar una operación sin intención de generar una violación de las reglas del Código de Conducta, pero con conciencia de que puede generarse un resultado que violente las reglas o principios consagrados en el mismo.

Toda falta, culpable o dolosa, determinará la aplicación de una sanción. La misma se graduará atendiendo a la gravedad de la infracción y a la voluntad de quien la infringió, siguiendo los criterios que se establecen a continuación y el procedimiento previsto en el convenio colectivo:

- Las faltas cometidas con dolo serán consideradas en todos los casos faltas graves, y serán sancionadas como mínimo con la suspensión del empleado, pudiendo llegar, en caso de ser consideradas muy graves, al despido por notoria mala conducta;

- En todos los casos de faltas cometidas a título doloso, se cursará comunicación al Banco Central del Uruguay, a los efectos que pudieren corresponder. Cuando exista la presunción de la comisión de un delito, en particular, lavado de dinero, se cursará además inmediata notificación a las autoridades policiales y a los jueces penales competentes.

Las faltas cometidas a título culposo, podrán ser sancionadas con las siguientes penas:

- Observación con apercibimiento de la aplicación de sanciones más graves en caso de reiteración. Esta sanción corresponderá en el caso de violaciones leves e incluso muy leves.

- Suspensión sin goce de remuneración, en caso de faltas intermedias y graves.

- Despido sin derecho a indemnización en caso de faltas muy graves o reiteración de faltas graves.

Las sanciones aplicables a los empleados de los Bancos son las siguientes:

a) Observación;
b) Apercibimiento;
c) Suspensión;
d) Traslado;
e) Cese.

Las sanciones disciplinarias se dividen en bajas, medias y altas. Se consideran bajas, la observación, el apercibimiento y la suspensión de hasta seis días inclusive.

Se consideran medias, las suspensiones entre siete y quince días inclusive. Se consideran altas la suspensión por más de dieciséis, el traslado de dependencia y el cese.

En los casos en que un Banco disponga la aplicación de una sanción baja, deberá notificar al empleado, que podrá efectuar sus descargos dentro de las cuarenta y ocho horas hábiles bancarias siguientes a la notificación de la misma.

En los casos que el empleado sea suspendido, no tendrá derecho al cobro de salario ni ningún beneficio generado por la relación laboral.

Las sanciones medias y altas serán aplicadas previa la instrucción de sumario administrativo.
En caso de advertir una irregularidad el Banco instruirá el sumario correspondiente; luego de completada la instrucción respectiva el empleado podrá ser asistido por su abogado el que podrá solicitar ampliación del mismo para agregar nuevas pruebas para lo que dispondrá de cinco días hábiles.

El proyecto de resolución deberá ser notificado al interesado el que dispondrá de un plazo de diez días hábiles, prorrogables por dos días hábiles para presentar descargos. De no presentarse escrito durante el plazo o su prórroga la resolución quedará firme.

**Manejo de las Consecuencias por Conductas Inapropiadas**

Conductas inapropiadas (PCC – Personal Conduct Cases por sus siglas en inglés) se define como "con conocimiento de causa, imprudentemente, o por negligencia se violan procedimientos, normas o valores, perjudicando la Reputación de HSBC".

El Departamento de Recursos Humanos local debe ser consciente de todos los PCC que existan así como las razones de las mismas, así como elevar los mismos al Comité de Valores y Conducta para tomar las acciones correspondientes.

De esta forma se garantiza la coherencia y un adecuado nivel de severidad ante la mala conducta.

Serán considerados como conductas inapropiadas:

- Incumplimiento de la legislación laboral, requerimientos regulatorios o al Código de Conducta: Abusos verbales o no verbales, humillaciones, amenazas, conductas negativas y pérdida de confianza. Así mismo, tratos desfavorables hacia un empleado en comparación con otros (por ejemplo: raza, género, religión, discapacidad, edad, orientación sexual).
- Fraude tanto en contra de clientes como en contra del Banco.
- Manejo inadecuado e intencional de la información y de los procesos
- Incumplimiento de los deberes regulatorios para los clientes y otras contrapartes
- Fallas intencionales en contabilidad.
- Errores operativos intencionales.
- Robo o facilitar el mismo.

Se encuentran sujeto a Manejo de Consecuencias (o Consequence Management por sus siglas en inglés) los siguientes hechos: (ver más detalles en FIM HR HSBC- intranet)

- Fraude
- Discriminación
- Acoso
- Incumplimiento de cursos mandatorios
- Incumplimiento de core leave
- Incumplimiento relacionado con la seguridad de la información

- Incumplimiento del código de conducta
- Incumplimiento del Manual de Lavado de Dinero
- Comportamientos no éticos.

Ante cualquier acto de Fraude o sospecha de Fraude, los Departamentos de Riesgos, Cumplimiento y Prevención de Lavado de Dinero y Recursos Humanos realizarán la investigación y análisis que fuera necesario para recabar información de la situación y personas involucradas. En forma conjunta realizarán un informe que será presentado al Comité de Valores y Conducta con el plan de acción sugerido.

El Comité de Valores y Conducta analizará el informe presentado y determinará las sanciones que correspondan y las acciones a tomar.

**ANEXO 1**

Gerente de Recursos Humanos
PRESENTE.

De mi mayor consideración:

Por la presente me dirijo a usted para asegurar que he leído completamente el Código de Conducta en su edición más reciente, lo he entendido en todos sus parámetros y me adhiero firmemente a todos los puntos y valores en su forma y espíritu; comprometiéndome por tanto a su aplicación.

Conozco las sanciones a las que soy pasible en caso de incumplimiento y los medios de asesoramiento por parte de la Oficina de Cumplimiento.

Sin otro particular, saluda atentamente.

Firma:

Aclaración: _____

Cédula: _____