BANCO SAENZ

CÓDIGO DE ÉTICA Y CONDUCTA

Versión 3.2

Fecha de Vigencia 29/05/2020

INTRODUCCIÓN

El presente Código se establece con el objeto de facilitar el conocimiento y comprensión de los principios éticos y de conducta que cada uno de los integrantes de Banco Saenz deberá cumplir en su desempeño con eficiencia, calidad y transparencia, respetando la ley y las más altas normas de conducta, tanto en el negocio como en nuestros asuntos personales y financieros.

Nuestros valores y principios proporcionan un marco para ayudarnos a tomar las decisiones comerciales correctas y mitigar el riesgo de impedir incorreciones, que permitan generar ganancias sostenibles a largo plazo para nuestra organización.

En todo lo que cada uno de nosotros hacemos se debe actuar con integridad manteniéndonos firme en lo que implica integralidad y corrección que permitan:

- ✓ Ser confiables
- ✓ Estar abiertos a diferentes ideas y culturas.
- ✓ Estar conectados con nuestros clientes, comunidades, reguladores y entre nosotros mismos.

En ningún caso ningún empleado del banco debe participar en actividades comerciales o negocios que pudieran de algún modo estar relacionados o ser considerados como apoyo de actividades ilegales/delictivas fraudulentas, deshonestas o no éticas contrarias en particular al interés del Banco y/o en lo general al país. Aplica en todas sus relaciones ya sea comerciales como personales.

El cumplimiento del código de conducta asegura que se mantenga nuestro compromiso con:

Clientes: brindándoles un trato justo, respondiendo a sus necesidades, construyendo una buena relación y actuando con transparencia**.**
Colaboradores: brindándoles un trato justo, demostrándoles que nos importan ofreciendo crecimiento y desarrollo y creando un clima de compañerismo que permita un ambiente cordial de trabajo.
Accionistas: Garantizando el retorno sobre capital y dividendos sostenibles, cumpliendo las leyes y reglamentos, actuando con prudencia y responsabilidad.
Proveedores: brindándoles un trato justo y cumpliendo con nuestros compromisos.
Comunidad y sociedad: actuando de manera responsable y como apoyo a la sociedad.

Los empleados:

- Deben consultar y cumplir las políticas y las normas establecidas.
- No deben hacer nada que pueda afectar la confianza que Banco Saenz ha depositado en ellos
- Tratar a todos los integrantes del Banco con respeto, absteniéndose de cualquier agravio, violencia y de todo tipo de discriminación. -
- Comportarse, dentro y fuera del Banco, con honestidad, equidad, prudencia y apego a la ley.
- Está prohibido trabajar bajo los efectos del alcohol y otras drogas. Se prohíbe estrictamente el consumo, posesión, intento de venta y/o venta, distribución de drogas o de cualquier otra substancia controlada, sin importar la cantidad o la forma en que sea, mientras desarrollen actividades en horarios de trabajo, y se encuentren dentro de las instalaciones del Banco y/o a empleados del Banco en adyacencias del Banco. Los empleados deben consultar al médico en el caso de medicamentos que puedan implicar riesgos a la seguridad propia o ajena.
- El Banco prohíbe la posesión de cualquier tipo de arma en el lugar de trabajo.
- Todas las dependencias de banco Saenz son libres de humo.

Deben informar cualquier incumplimiento a las normas o reglamentos a su gerente o al gerente apropiado tan pronto como tenga conocimiento de ello.
Cualquier incumplimiento dará lugar a una acción disciplinaria y puede en su caso dar lugar a un proceso penal.

I – CONFLICTO DE INTERESES

Se entiende por conflicto de intereses aquellas situaciones en donde existan intereses contrapuestos entre los intereses personales confrontados con los intereses de la empresa y en definitiva se considere comprometidos a los mismos y/o a su imagen en forma pública o privada.

Todos los empleados se apartarán de situaciones que puedan parecer o significar un conflicto de intereses. Los temas que merecen principal atención son:

1- Participación en actividades que compitan con los intereses del Banco.
2- Avales/ Préstamos/ Depósitos/ Inversiones en títulos públicos y/o privados.
3- Actividades Fiduciarias.
4- Poderes o Representaciones.
5- Uso de cuentas y operaciones de empleados del Banco.
6- Relaciones de Negocios.
7- Aceptación de regalos y/o gratificaciones.
8- Contribuciones políticas.

- 1-Participación en actividades que compitan con los intereses del Banco

• Ningún empleado del Banco puede participar en forma directa o indirecta en relaciones jurídicas, comerciales y en actividades en general que impliquen intereses contrapuestos o conflictivos con los del Banco.

• Se deberá comunicar, inmediatamente de conocido, todo interés directo o indirecto que tuviera el empleado o sus familiares directos (padres, hermanos, esposo/a, hijos), en actividades potencialmente competitivas o que impliquen relaciones de negocios con el Banco (Ejemplos: contratos de suministros, compras, servicios, etc.). En estos casos, la comunicación deberá ser dirigida a Recursos Humanos realizándolo por escrito.

•En ningún caso los empleados podrán autorizar o conceder operaciones de riesgo para el Banco, en favor propio, de un familiar o de un tercero relacionado.

• En las relaciones comerciales con clientes y proveedores, los empleados solamente pueden ofrecer los servicios que el Banco brinda. No deben representar otros servicios o producto alguno. Esta prohibición es aplicable tanto a conflicto de intereses actual, debiendo prever circunstancias que puedan determinar la aparición de futuros conflictos.

➢ 2. Avales/ Préstamos/ Depósitos/ Inversiones en títulos públicos y/o privados

• Los empleados no deben otorgar avales ni préstamos con recursos propios a ningún cliente o proveedor con excepción de:

- Miembros de su familia inmediata.
- Compra de deuda en instrumentos financieros negociada públicamente y permitida.
- Mantener una cuenta de depósito en otra institución financiera, en iguales términos que los normalmente disponibles por esa entidad, para el público en general.

• Tampoco debe un empleado recibir préstamos de clientes o proveedores, con excepción de un miembro de su familia inmediata u otra institución financiera en iguales términos que los disponibles por esa entidad, para el público en general.

• No está permitido entre los empleados del Banco otorgar o recibir dinero en préstamo.

➢ 3. Inversiones

• Los empleados no deben invertir en acciones, bonos u otro tipo de instrumentos financieros de un cliente o proveedor que no sean los negociados públicamente en Mercado de Valores regulados y bajo las siguientes condiciones:

- ❖ La inversión debe responder a valor de mercado
- ❖ La inversión debe estar a disposición del público en general y no estar basada en información confidencial.
- ❖ La inversión no debe exceder el 5% del total de las acciones en circulación.

➢ 4. Poderes o Representaciones

• Los empleados no deben aceptar posiciones de representación excepto a nombre de miembros de su familia o aquellas representaciones asignadas por el Banco en cumplimiento de las responsabilidades inherentes a la función asignada.

➢ 5. Uso de cuentas y operaciones de empleados del Banco

- Los beneficios asociados a los productos bancarios que el Banco otorga a sus empleados en su carácter de tales están dirigidos exclusivamente a los empleados, es decir, no podrán ser

contratados para beneficio de terceros, familiares, o con fines comerciales, o en relación con operaciones o actividades que generen un conflicto de interés con la posición del empleado dentro de la organización.

- Del mismo modo, las relaciones comerciales entre los empleados del Banco y su cartera de clientes deberán mantenerse dentro del marco corporativo. Bajo ningún concepto los empleados podrán:
    - ❖ Canalizar operaciones de clientes a través de sus cuentas personales.
    - ❖ Invertir en Plazos Fijos de clientes, con excepción de los casos en que los titulares tengan una relación de parentesco demostrable con el empleado.
    - ❖ La condición de empleado del Banco no exime del cumplimiento de las políticas, normas y controles vigentes, aplicables a la cartera de clientes en general y a la prevención de lavado de activos y de financiamiento al terrorismo en particular.

➢ 6. Relaciones de Negocios

• Los empleados no deben establecer relación de negocios (sociedades, compañías de capital de riesgo, etc.) en forma personal o en representación, de clientes o prestadores de servicios vinculados con el Banco que no sean miembros de su familia inmediata o amigos personales y que las circunstancias dejen claro que el factor motivante es la relación personal y no la relación Banco-cliente.

• Los empleados deberán evitar toda situación - como la aceptación de un descuento por una compra personal -, que suponga el aprovechamiento personal de un beneficio obtenido mediante el Banco.

• La compra de todo equipo, suministro y servicios necesarios se hará sobre las bases de calidad, utilidad y precio ofrecido por el proveedor. En ninguna circunstancia se dará un trato preferencial a clientes del Banco en negociaciones con proveedores o transacciones que abarquen compras del Banco.

• En la relación con los clientes y proveedores los empleados deben guiarse de manera responsable, a fin de conservar la armonía y mantener un equilibrio satisfactorio al tomar decisiones de negocio.

➢ 7. Aceptación de regalos y/o gratificaciones

• No está permitido al personal del Banco, ya sea en forma grupal o personal, aceptar directa o indirectamente nada de valor cuyo recibido pudiera influenciar su decisión con respecto a la forma de hacer negocios practicada por el Banco con cualquier persona o entidad.

• Los empleados podrán aceptar únicamente comidas, bebidas o agasajos que sean razonables en su cantidad, y regalos o artículos promocionales cuyo valor no supere los $ 10.000.- Tales cortesías comerciales o regalos no deben haber sido solicitados, y deben haber sido otorgados de acuerdo con las prácticas habituales y aceptables del negocio.

• No se deben aceptar reembolsos por gastos de alojamiento o viajes, o alojamiento y viajes gratis sin la aprobación expresa del supervisor/ gerente responsable.

• El dinero en efectivo en cualquier forma, denominación o cantidad no es considerado como un regalo aceptable y por lo tanto está terminantemente prohibido recibirlo.

- 8. Contribuciones políticas

• No está permitido al personal contribuir con fondos, productos, servicios u otros recursos del Banco para ninguna causa, partido o candidato político en nombre del Banco.

• Los empleados podrán hacer contribuciones voluntarias a cualquier causa política legal, partidos o candidatos políticos siempre y cuando no se dé a entender que dichas contribuciones provienen del Banco.

¿Qué hacer Si surge un conflicto de Interés?

Si tiene alguna duda acerca de algún curso de acción o crees que tus intereses entran o pueden entrar en conflicto con los intereses de la institución o de tus clientes, consulta inmediatamente con tu responsable, describe los hechos que dieron lugar al conflicto y evita participar en la toma de decisiones de la transacción en cuestión

II – REGISTROS BANCARIOS Y ASIENTOS CONTABLES

Toda información registrada debe reflejar en forma fidedigna las transacciones celebradas. La omisión o registro incompleto o erróneo de operaciones y/o datos, es considerada una falta grave y por ello un acto muy comprometido.
Toda modificación a estas políticas, normas y procedimientos, previa aplicación, debe ser aprobada por las instancias que correspondan.
Debe recordarse que la función de control se ejercerá uniendo el cumplimiento de las normas con la responsabilidad de los individuos.

III CAPACITACION

Todos los empleados y funcionarios deben completar los cursos de capacitación obligatorios asignados por la institución, ya sea como iniciativa para cumplir un requisito especifico o anualmente para garantizar que los empleados estén informados sobre ciertos temas. El no cumplimiento puede ser causal de despido.

IV LAVADO DE DINERO

El Banco está profesionalmente comprometido en combatir activamente la realización de operaciones financieras con recursos de procedencia ilícita.
En este contexto, el Banco tiene como política institucional permanente el mantener cerradas sus puertas y la de todas sus vinculadas, a aquellas operaciones con recursos que puedan proceder de ilícitos.
Es política del Banco mantener con sus clientes una relación estrecha que permita proporcionarles un servicio de excelente calidad y conocer sus actividades, a efectos de garantizar prácticas bancarias sanas y el cumplimiento del marco jurídico en vigor.
El personal de la Institución debe apegarse estrictamente a la normativa interna, basada en la legislación vigente, respecto del registro de operaciones, identificación y "Conocimiento del Cliente", y de las acciones a tomar frente a Operaciones Inusuales / Sospechosas.
Los empleados están obligados a informar sobre cualquier hecho o sospecha razonable que implique una infracción al presente código, a través de la Gerencia de RRHH. Si decidiera realizarla de manera confidencial o anónima, el Banco asegura mantener la identidad del denunciante en total anonimato.

V SOBORNO Y CORRUPCIÓN

El sistema Bancario se basa en la integridad y confianza mutua, debemos asegurar que BANCO SAENZ no se encuentra involucrado en malas prácticas o todo aquello que pueda interpretarse como mala practica
No participes de ninguna forma de soborno, ya sea de manera directa o indirecta

¿Qué es soborno?

Un soborno es cualquier ofrecimiento o aceptación de regalo, préstamo, honorario o recompensa o cualquier otra ventaja monetaria o no monetaria aceptada u otorgada a una persona (incluyendo a un colaborador) como incentivo para llevar a cabo un negocio, en particular en aquellos casos donde el ofrecimiento o aceptación de algún tipo de soborno sea deshonesto, ilegal y de abuso de confianza.

No evitar un soborno puede ser considerado delito.

De manera activa, pero con tacto, deberás desalentar a clientes, proveedores y otras personas de ofrecer regalos, gestos de hospitalidad, otros beneficios personales de cualquier tipo ya sea para ti o a otras personas del banco.
Quedan expresamente prohibidos los certificados o cheques de regalos, dinero en efectivo o cualquier otro equivalente de efectivo
No debes aceptar ni ofrecer regalos, u otro beneficio personal de terceros o a terceros que pudiesen ejercer influencia o que se pudiese creer que ejercen influencia en sus decisiones o entren en conflicto con sus obligaciones.
No debes ofrecer soborno ni ningún otro incentivo cualquiera sea su forma, incluyendo comisiones, en ninguna instancia de un pago contractual
No debes utilizar otras vías o canales para proporcionar beneficios inapropiados a clientes, agentes, contratistas proveedores o sus colaboradores, o a funcionarios de gobierno a favor de un negocio del banco

Pago de Facilitación

Son pequeñas cantidades de dinero que se entrega a cambio de asegurar o agilizar el curso de un trámite o acción necesaria sobre la cual el responsable del pago de facilitación tiene un derecho conferido por ley o de otro tipo. Los pagos de facilitación constituyen una forma de soborno, por ello están prohibidos.

Existen algunas excepciones a la prohibición general de solicitar o aceptar algo de valor, como:

Comidas, cenas y otras formas de entretenimiento ofrecidos en el curso ordinario de los negocios de proveedores o clientes y en las situaciones en las que normalmente reembolsaríamos el costo como gastos comerciales.
Regalos promocionales como lápices, encendedores, etc. u obsequios relacionados con eventos tradicionales como navidad, promociones, etc.
No podrás aceptar regalos en efectivo, cheques o certificados de regalo convertibles en efectivo.

VI SEGURIDAD DE LA INFORMACION Y FISICA

La información de la institución es un activo privado al que tendrás acceso en carácter de colaborador o funcionario y al que te obligas a proteger de cualquier acto que pudiera atentar contra su confidencialidad, integridad y disponibilidad, aun después de terminar tu relación de trabajo.
Durante tu relación laboral o una vez terminada la misma, excepto en el debido ejercicio de tus funciones o con previa aprobación por escrito de RRHH no debes revelar o hacer uso de información ni de correspondencia, cuentas, vinculaciones u operaciones de Banco Saenz o tus clientes, o los accionistas o directivos y/o sus allegados y/o los empleados del Banco de información obtenida en relación con el ejercicio de tus funciones.

Si un colaborador viola las disposiciones de estas políticas, por negligencia o intencionalmente Banco Saenz se reserva el derecho de tomar las medidas correspondientes, tales como acciones disciplinarias internas, acciones legales u otras que tuvieran lugar.
Todos somos responsables del cuidado de la información, del acceso seguro, almacenamiento, transferencia y destrucción de la misma, ya sea en forma física o electrónica.

Todos los colaboradores, funcionarios o tercero que presten algún servicio dentro de Banco Saenz estamos obligados a reportar las deficiencias, vulnerabilidades, fallas o violaciones de seguridad que identifiquemos durante el procesamiento, almacenamiento, intercambio o disposición de los activos de información, aun y cuando se trate de una simple sospecha

VII – TECNOLOGIA INFORMATICA

Uso de recursos informáticos

- Todas las personas que trabajen para Banco Sáenz, incluyendo consultores y contratistas, está totalmente prohibido el uso de cualquier tipo de herramienta (software o hardware) que vaya en contra de la Política de Protección de Activos de Información de la Entidad, a menos que esté expresamente aprobado con el Comité de Tecnología para el desarrollo de algún trabajo, monitoreo o pruebas.
- Protección de Activos de Información se encargará de definir el estándar de uso de herramientas a ser cumplido por los terceros durante el tiempo de permanencia en la Entidad.
- Las computadoras (PC's y notebooks) del Banco deben estar conectadas a la red interna y protegidas mediante contraseña de arranque y con controles de bloqueo por inactividad.
- Los archivos que deban ser transportados en algún medio de almacenamiento, deben guardarse en un lugar distinto a la computadora. No deben utilizarse nombres de compañías y de ser posible, si la aplicación de uso lo permite, los archivos "portables" deben protegerse con contraseñas de apertura. A partir del momento de aprobación de la presente política todo nuevo dispositivo de almacenamiento adquirido por el Banco deberá permitir la protección con contraseñas.

Identificación y autenticación de usuarios:

- Los identificadores y autenticadores de usuarios definidos para el uso de los sistemas del Banco y que son poseídos por el personal que trabaja en la Entidad, son de exclusiva responsabilidad de estos, por lo que deben ser de carácter personal e intransferible. Los mismos deben ser utilizados por los empleados para ingresar a los sistemas. Los usuarios deben descontarse de la red informática, bloqueando su estación de trabajo o cerrando la sesión, cuando se retire al final del día o cuando se ausente de su puesto de trabajo durante un tiempo prolongado.

- El ingreso a los sistemas debe realizarse utilizando el usuario y clave (contraseña) asignado a cada colaborador, nunca con el de otra persona, ya que las claves de acceso son PERSONALES y SECRETAS. Por lo tanto, no se admite el acceso y/o uso de estas por parte de otra persona ajena a su propiedad.
- Seguridad Informática aplicará las restricciones y filtros necesarios para el uso correcto de estos servicios. Realizará un monitoreo y registrará toda la actividad del uso de los mismos; cualquier abuso será notificado al responsable del área correspondiente y se aplicarán las sanciones vigentes.
- Seguridad Informática bloqueará la recepción de e-mails o provenientes de Internet con archivos adjuntos que considere peligrosos. En caso de requerirse la recepción de estos archivos para el desempeño de las tareas, deberá consultarse con dicho sector.
- Todos los accesos a Internet deberán realizarse a través de la red corporativa y no deberá haber PC's dentro del Banco conectadas a Internet de otra manera, excepto aquellas destinadas a procedimientos de contingencia (debidamente homologadas por Seguridad Informática).

Acceso remoto

- Los usuarios que requieran acceso remoto deberán estar debidamente justificados y formalmente autorizados.
- Al ingresar a la red del Banco en forma remota, debe en todo momento mantenerse la confidencialidad.
- El acceso a archivos debe limitarse a personas autorizadas en base a la necesidad de conocer, al igual que las personas a quienes se muestra los mismos.
- El acceso a información en dispositivos electrónicos portátiles (notebooks, dispositivos móviles, etc.) deben estar protegidos mediante el uso de contraseña.

Alcance del monitoreo de correo electrónico

- La expresión "monitoreo" incluye el archivo de datos y la examinación de esos archivos en forma manual o electrónica.
- La Entidad examinará los archivos de datos de los activos de información del Banco, si los fines así lo requieren (por ejemplo, si existe la sospecha de un uso no autorizado)

- Banco Sáenz puede continuar monitoreando los archivos de su uso de los activos de información del Banco, luego que el empleado haya dejado de pertenecer a la Entidad, si los fines así lo requieren.
- El Banco cooperará con cualquier autoridad legítima en detectar y prevenir cualquier actividad ilegal o cualquier otra actividad que pueda constituir mala conducta profesional. También cumplirá con los pedidos razonables de dichas autoridades acerca de registros, diarios y archivos de uso de los activos de información del Banco.
- La Entidad también estará obligada a revelar cualquier e-mail ante procesos legales, conformar a las normas relacionadas con la revelación de documentos en juicios.
- Banco Sáenz administra el uso del correo electrónico en dispositivos móviles a través de permisos de acceso y políticas específicas, adicionalmente cuenta con la facultad de borrar los datos de los dispositivos de forma remota.
- No deberán enviarse mensajes a todos los usuarios de la red, excepto los que sean canalizados y autorizados por RRHH
-

Uso de Internet

- Garantizar que la utilización de Internet debe ser de acuerdo con ética y valores de Banco Sáenz. Su utilización solo debe obedecer a necesidades de trabajo en beneficio de la Entidad. El acceso a Internet se restringirá a las personas que por temas laborales requieran su utilización. El acceso a Internet será monitoreado por Protección de Activos de Información, quienes serán responsable del bloqueo de los sitios prohibidos.
- El acceso a sitios prohibidos será bloqueado siempre que sea posible. El acceso a dichos sitios será registrado. Si necesita acceder a un sitio prohibido para fines laborales, deberá contactarse con Protección de Activos de Información.

Ambientes Virtualizados

- Se define como la abstracción de los recursos de una computadora, llamada Hypervisor o VMM (Virtual Machine Monitor) que crea una capa de abstracción entre el hardware de la máquina física (host) y el sistema operativo de la máquina virtual (virtual machine, guest), dividiéndose el recurso en uno o más entornos de ejecución. Para las máquinas virtuales se le aplicaran las mismas políticas de seguridad lógica correspondiente a un servidor físico. Las maquinas físicas (host) se conectarán

en una misma zona de seguridad de la red, a fin de evitar múltiples zonas de seguridad distinta en un mismo equipo minimizando la superficie de ataque en hipervisores. Se encontrarán dos roles en los hipervisores, uno de administración de equipos virtuales y otro de administrador de seguridad permitiendo la segregación de roles.

Cambios a software y aplicaciones

- Todo cambio que afecte la plataforma tecnológica debe ser aprobado formalmente a través de los procedimientos de control de cambios al software de base y a las aplicaciones establecidos por la Entidad. Dicho cambio debe efectuarse de tal forma que no disminuya la seguridad existente. Todo cambio que repercuta en su entorno de seguridad debe ser autorizado por el Gerente de Sistemas y el Gerente dueño del dato.

Es importante que como empleado de la institución tengas plena conciencia de las implicaciones del uso del correo a título personal y de corresponder de forma profesional, aplica independientemente si se accede al correo utilizando las instalaciones y equipos IT de la institución o de otro modo. El incumplimiento de cualquier parte de esta política puede dar lugar a una acción disciplinaria, independientemente si la violación se comete durante o fuera del horario de trabajo, independientemente si se utiliza el equipo de trabajo o personal

Fraude y Robos Internos

Se deberá estar atento ante cualquier comportamiento relacionado a: Fraudes, robos, sobornos y/o otras actividades ilegales dentro del ámbito de trabajo
En pro de la seguridad, la prevención del fraude, tu seguridad y la del cliente, la institución se reserva el derecho de:

- Registrar cualquier bolso o equipaje que lleven los empleados o visitas, incluido de mano y paquetes de cualquier índole

- Cuando un empleado ha cometido un acto de deshonestidad ya sea con el banco o las cuentas de los clientes, la institución informara a las autoridades correspondientes y brindara apoyo en relación con cualquier investigación.
- Llevar a cabo monitoreo telefónico, monitorear el uso de correo electrónico, internet, mensaje de voz o de texto que se hayan originado o recibido a través de Software de la institución.
- No se puede asumir la privacidad cuando se usan equipos de la compañía para comunicaciones personales.

Además, en áreas de la seguridad y prevención del fraude, la institución se reserva el derecho de inspeccionar las cuentas y otras instalaciones que tenga cualquier empleado, incluida la revisión de cualquier transacción realizada.

VIII 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.

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 Banco Saenz (a menos que estés debidamente autorizado para hacerlo)

El uso de las redes sociales aplica tanto para fines comerciales como personales. Además, se aplica independientemente si se accede a las redes sociales utilizando las instalaciones y equipos 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, Banco Saenz se reserva el derecho de supervisar, interceptar y revisar cualquier actividad en las redes sociales publicadas utilizando los sistemas o equipos de la institución

Debes comprender que cualquier mensaje, publicación en las RS conversación o cualquier otro tipo de información o comunicación enviada o recibida utilizando los sistemas del Banco Saenz será monitoreada y no permanecerá privada

Además, también podemos revisar cualquier actividad en las redes sociales publicadas utilizando equipos externos, si el contenido hace referencia (explícita o implícita) alude, 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 si la violación se comete durante o fuera del horario de trabajo, independientemente si se utiliza el equipo de trabajo o personal.

IX DIVERSIDAD E INCLUSION

Una cultura inclusiva nos ayuda a dar respuesta a la base de clientes cada vez más diversa que a la vez permite crear y mantener una fuente segura de colaboradores capacitados y comprometidos.
Todos somos responsables de tratar a nuestros colegas y clientes con dignidad y respeto, así como crear 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, estado civil, discapacidad, sexualidad, raza, color, creencia religiosa o nacionalidad, doctrina política o condición social, todo lo que atente contra la persona en su integridad, su dignidad, su empleo o degrade el clima de trabajo, se debe denunciar, ya sea contra usted o cualquiera de sus pares.
No se aceptará ningún tipo de parcialidad, prejuicio, o burla en ninguna forma y en ninguna circunstancia.

X SOBRE MEDIDAS DISCIPLINARIAS

Se deja expresamente establecido que las medidas disciplinarias relacionadas a la infracción del presente código serán aplicadas por la Gerencia de Recursos Humanos en base a los informes realizados por el Responsable de Prevención y Tratamiento del Fraude y/o los órganos colegiados especializados.
El Banco sancionará a los trabajadores que cometan las siguientes infracciones referidas el presente documento:

- Cuando incumplan deliberadamente lo dispuesto en el presente documento.
- Cuando, teniendo información sobre hechos que afecten al presente Código, no informen acerca de su existencia.
- Cuando, luego de haber hecho una denuncia, se compruebe que esta se hizo con mala fe.

Los artículos 303 y 306 del Código Penal y la Ley 25.246 fijan penas que van desde multa hasta prisión para los directivos, funcionarios y empleados involucrados, e incluso la entidad puede ser condenada por los delitos previstos en los artículos citados (conf. Arts. 304 y 313 del Código Penal). La Entidad también es pasible de sanción a través de multas de hasta diez veces del monto involucrado.

Se hace constar que, según el grado de incumplimiento del presente código, será motivo de la apertura de un sumario interno y/o de su tratamiento en el tribunal de ética según corresponda.

COMPROMISO DE RECEPCIÓN Y CUMPLIMIENTO

En el día de la fecha manifiesto que he recibido el Código de Ética y Conducta de BANCO SAENZ S.A. (Versión 3.2)

Me notifico y presto conformidad de los términos incluidos en el mismo.

Así mismo manifiesto haber sido capacitado en cursos planificados por RRHH en todo lo atinente a la atención a brindar al usuario financiero, conforme a lo dispuesto por el BCRA en la Com. "A" 5.338 y sus modificatorias y complementarias.

El presente código será incluido en la página www.turecibo.com.ar para la notificación y conformidad del empleado o funcionario.