MANUAL DE CONDUCTA

GRUPO SECURITY S.A.

v20171112 1100

A TODOS LOS EMPLEADOS DE GRUPO SECURITY S.A.

"Ser confiables es un sello de todos quienes trabajamos en las empresas de Grupo Security, y por ello es nuestro compromiso el cumplimiento de este Manual de Conducta, manteniendo altos niveles éticos, profesionales y de transparencia en el trabajo diario."

Renato Peñafiel Muñoz
Gerente General
Grupo Security

ÍNDICE

1. Alcance del Manual de Conducta

El presente Manual de Conducta es aplicable a todos los empleados que conforman Grupo Security S.A., siendo un documento complementario al Código de Ética y sujeto al Contrato de Trabajo, Reglamento Interno, Políticas, Normas y Procedimientos emitidos por la empresa y la legislación chilena e internacional correspondiente.

Las obligaciones que impone este Manual han sido establecidas en armonía con los derechos fundamentales de los empleados, y miran a la ejecución de buena fe de las relaciones laborales, evitando que se produzcan conflictos de intereses, utilización de información privilegiada o abuso de una situación de predominio en que puedan encontrarse los empleados por razón de sus funciones, o del área en la cual se desempeñan.

1.1 Nuestra Misión

Satisfacer las necesidades de financiamiento, inversión, seguros y servicios de nuestros clientes, a través de la entrega de un servicio integral, que supere sus expectativas y se distinga por su calidad.

1.2 Nuestra Visión

Ser una referencia en todas nuestras relaciones, tanto en el ámbito de negocios como en el de recursos humanos, de manera de satisfacer integralmente las necesidades de nuestros clientes, accionistas, empleados y entorno social en el cual nos desenvolvemos, impulsando acciones que concilien familia y trabajo.

1.3 Nuestros Valores

Transparencia: privilegio ante todo a la verdad, transparencia en las relaciones y comportamiento honorable.

Profesionalismo: lealtad y compromiso con los objetivos de nuestra compañía, y motivación para desempeñar eficientemente y sin vacilaciones las funciones propias del cargo.

Proximidad: inspirados por una fuerte vocación de servicio hacia terceros - clientes internos y externos y demás actores del mercado - atender a sus requerimientos y dar solución a ellos, en cuanto sea posible.

2. Difusión, Vigencia y Actualizaciones

El presente Manual de Conducta se entiende como conocido desde su aprobación por el Directorio y correspondiente difusión. Por lo tanto, deberá ser entregado a todos los empleados y publicado en la Intranet del Grupo Security S.A.

En relación a su vigencia, ésta será de carácter indefinido y será modificado por el área de Cultura Corporativa en conjunto con Cumplimiento Corporativo, en la medida que se deban incorporar nuevas reglas de comportamiento. Por lo tanto, es responsabilidad de cada empleado conocer las actualizaciones que se realicen al presente Manual.

3. Conducta General

El presente Manual de Conducta establece las siguientes reglas de comportamiento para todos los empleados en el desarrollo de sus actividades:

A) Conocer el presente Manual y ajustar su actuar en todo momento al espíritu, los principios y a las disposiciones establecidas en él, de manera profesional, seria, eficiente y diligente.

B) Conocer y estar actualizados en las prácticas, procedimientos y normativas relacionadas con su cargo y estar concientes de sus responsabilidades.

C) Mantener absoluta objetividad e independencia de juicio en el ejercicio de su actividad profesional.

D) Mantener una actitud amable, digna y respetuosa, tanto con sus clientes internos y externos, como con los demás miembros del mercado (competidores, proveedores, etc.). Especialmente deberán conducirse con honestidad, claridad, precisión, seriedad, lealtad, imparcialidad, probidad, buena fe y de acuerdo a las buenas prácticas, que garanticen la transparencia y seguridad para los clientes, la integridad del mercado y la rentabilidad de la empresa.

E) Mantener una actitud cooperadora y transparente, que fomente la confianza entre las empresas del Grupo (Auditoría, Unidades de Control Interno, el Directorio, Gerentes, Ejecutivos Principales, etc.) como con los reguladores, autoridades bursátiles, administrativas y judiciales en general.

F) No realizar ninguna operación, transacción o actividad con dineros provenientes de actividades reñidas con la ley o que atenten contra las buenas costumbres, tales como: tráfico de drogas, de armas, corrupción, entre otras.

G) Someterse con arreglo de la ley a exámenes médicos y demás procedimientos clínicos que se le exijan con el fin de acreditar una salud física y mental apta para el cargo que desempeña.

H) Se espera que todos los empleados administren adecuadamente sus finanzas personales y que sus niveles de endeudamiento sean compatibles con sus ingresos.

I) Los supervisores deben mantener una conducta apropiada con su cargo y con los estándares establecidos por la empresa, por lo tanto, no deben exigir a sus subordinados la realización de conductas que no sean acordes a los procedimientos establecidos o que sean contrarias a la ética.

Se debe tener presente, que todas las conductas mencionadas anteriormente no representan el universo completo de situaciones de comportamientos. Es por ello, que se espera de cada empleado mantenga una conducta acorde con los valores y principios establecidos en el Código de Ética.

4. Conductas Específicas

Se establecen las siguientes conductas específicas para todos los empleados:

4.1 Ley 20.393: Delitos de Lavado de Activos, Financiamiento del Terrorismo, Cohecho y Receptación.

La Ley Nº 20.393, establece la responsabilidad penal de las personas jurídicas en los delitos de lavado de activos, financiamiento del terrorismo, cohecho y receptación, por lo tanto, la empresa podrá ser responsable de los delitos que los empleados y dependientes cometan dentro del ámbito de sus funciones.

En consideración a lo anterior, la empresa prohíbe expresamente cualquier conducta que pueda dar lugar a una imputación penal de la empresa por los actos cometidos por los dueños, controladores, responsables, ejecutivos principales, representantes, quienes realicen actividades de administración o supervisión y cualquier empleado de la empresa interno o externo.

En conclusión, los delitos detallados a continuación no pueden ser cometidos dentro de ninguna actividad que tenga relación con los negocios de la empresa:

A) Lavado de Activos: Cualquier acto tendiente a ocultar o disimular el origen ilícito de determinados bienes, a sabiendas que provienen de la perpetración de delitos relacionados con el tráfico ilícito de drogas, terrorismo, tráfico de armas, prostitución infantil, secuestro, cohecho

y otros. Asimismo, el que adquiera, posea, tenga o use los referidos bienes, con ánimo de lucro, cuando al momento de recibirlos ha conocido su origen ilícito.

B) Financiamiento del Terrorismo: Persona que, por cualquier medio, solicite, recaude o provea fondos con la finalidad de que se utilicen en la comisión de cualquiera de los delitos terroristas señalados en la Ley 18.314 (artículo 2°).

- Apoderarse o atentar contra un medio de transporte público en servicio.
- Atentado contra el Jefe de Estado u otras autoridades.
- Asociación ilícita con el objeto de cometer delitos terroristas.

C) Cohecho a funcionario Publico Nacional o Extranjero: Consiste en ofrecer o consentir en dar a un empleado público (nacional o extranjero) un beneficio económico, en provecho de éste o de un tercero, para que:

- Realice actos propios de su cargo en razón del cual no le están señalados derechos.
- Omita un acto propio de su cargo.
- Ejecute un acto con infracción a los deberes de su cargo.

D) Receptación: Quien, conociendo su origen o no pudiendo menos que conocerlo, tenga en su poder, transporte, compre, venda, transforme o comercialice especies que provengan de hurto, robo, receptación, apropiación indebida y/o hurto de animales. Asimismo, el delito de receptación sanciona las conductas negligentes de quienes adquieren o poseen dichos bienes.

Todos los empleados deben tener especial cuidado en no cometer actos que puedan configurar su responsabilidad penal y eventualmente vincular a la empresa en tales hechos. Por lo tanto, deben evitar relacionarse con personas naturales o jurídicas de las cuales se sospeche que sus negocios son ilegales o ilegítimos. De este modo, comprometerse a cumplir a cabalidad con el Reglamento de Prevención de Delitos, y reportar al área de Cumplimiento de la empresa las operaciones sospechosas de las que tiene conocimiento en el ejercicio de sus funciones.

4.2 Criterios Generales para los Conflictos de Interés

¿Qué es un conflicto de interés?

El conflicto de interés constituye una incompatibilidad que se produce entre los intereses de la Empresa y los de un empleado (s), cuando en una determinada operación que éste ejecuta como funcionario (s) de aquélla, hace primar sus propios intereses, o los de terceros con los cuales se encuentra vinculado por relaciones de negocio, parentesco, afectividad u otro factor personal relevante. Igualmente, existe conflicto de interés cuando el empleado incursiona en negocios del mismo giro del empleador, que le han sido prohibidos, sea que actúe en forma directa o indirecta. En todos los casos de conflictos de interés, la inobservancia de la incompatibilidad a que dan origen importan una deslealtad hacia la Empresa. Bajo estas consideraciones, un empleado no debe actuar en el ejercicio de su cargo en ningún asunto en el cual tenga un interés (de cualquier naturaleza) directo o indirecto, que pudiere afectar su objetividad o independencia de juicio.

Es claro que una decisión tomada por la Empresa en una situación de conflicto de interés puede ser adoptada sobre la base de razones equivocadas. Pero, aún para el caso de ser correctas tales razones, los conflictos pueden afectar la reputación de una organización y dañar la confianza privada y pública.

Sin perjuicio del marco determinado por su definición, son innumerables todas las acciones que pueden interpretarse como un conflicto de interés, atendida la inobservancia de la incompatibilidad en que ellos se resuelven. Por la vía del ejemplo, cabe mencionar los siguientes casos, en los cuales cabe prestar la mayor atención, para su detección:

Ejemplo 1: El interés económico de un empleado del Grupo Security S.A., o de algún miembro de su familia, que tenga o busque establecer una relación de negocios con dicha empresa.

Ejemplo 2: La vinculación que tenga o adquiera un empleado con una Persona Expuesta Políticamente

(PEP). Debe declarar esta situación a su Jefe, Supervisor o Gerente.

Ejemplo 3: La recepción de algún beneficio u hospitalidad (obsequios) de un tercero a quien pueda afectar una decisión o acción del Grupo Security S.A.

Ejemplo 4: El consejo proporcionado por un empleado a sus parientes u otras personas vinculadas con él, para la compra de valores que figuran en su cartera, con violación del deber de reserva que le compete observar.

Sin perjuicio de las obligaciones y prohibiciones acordadas al efecto en el contrato, o establecidas en la normativa interna de la Empresa, las cuales operan por sí mismas, algunas consideraciones generales para identificar potenciales conflictos de interés son:

• Percepción: ¿La actividad o transacción en la cual participa el empleado podría percibirse como un posible conflicto de interés? Si todos los hechos relacionados se hicieren públicos, ¿Impactarían al Grupo Security S.A. o al empleado?

• Intención: ¿Si la gestión u operación que desarrolla el trabajador hacia un tercero, tendría por objeto influir en el criterio del destinatario o del empleado, en términos que afecten los intereses de la Empresa?

• Impacto: ¿Quedará la compañía, sus accionistas o clientes en situación de desventaja, sin motivos legítimos, si usted participa de la actividad, operación o transacción en que participa?

• Objetividad: ¿La participación en la actividad o transacción afectará el criterio de un cliente, o en el suyo, en relación con cualquier decisión de negocios?

• Consideraciones de tiempo: Si la actividad implica una acción externa, ¿interferirá el tiempo requerido con su habilidad para desempeñar sus responsabilidades con la compañía, sus accionistas o sus clientes en forma eficaz?

¿Qué debe hacer si piensa que podría existir un conflicto de interés?

Deberá consultar a su Jefe, su Supervisor o su Gerente. En el caso de que no pudieran resolverse se deberá comunicar por escrito al Oficial de Cumplimiento de su empresa con copia al área de Cumplimiento Corporativo, al igual que todos los mandatos relacionados con conflictos de interés que sean aceptados.

Es política de la empresa no actuar jamás contra los intereses de sus clientes. Por lo tanto, los empleados deberán revelar a sus superiores la naturaleza y extensión de cualquier conflicto o incluso indicio de ello entre sus propios intereses (personales, sociales, financieros o políticos) y los de un cliente, caso en el cual siempre deberán primar los de estos últimos y darles un tratamiento justo y equitativo. De no ser posible, tienen que abstenerse de realizar la operación.

En caso de conflicto entre clientes, no se perjudicará a ninguno, y se agotarán todas las instancias para llegar al mejor equilibrio y/o acuerdo entre todas las partes.

En este sentido el objetivo es evitar que la empresa se encuentre en una posición de líder en dos lados de una transacción. Es así como, para evitar eventuales conflictos de interés, debemos abstenernos de aceptar mandatos para actuar a nombre de nuestros clientes (salvo en aquellos casos en que el cliente sea el cónyuge del empleado o un hijo/ hija menor de edad de éste). En caso que un mandato de este tipo sea aceptado, los empleados se deberán regir por el principio de independencia, esto es que se deberá velar siempre por los intereses del cliente, por sobre los propios o de terceros.

4.3 Consumo de Alcohol, Drogas y Estupefacientes

Los empleados evitarán en toda circunstancia el consumo de cualquier tipo de droga o estupefaciente no autorizado médicamente, así como la ingesta de alcohol en horarios de trabajo exceptuándose las celebraciones autorizadas. Fuera del horario de trabajo los empleados cuidarán de no sobrepasarse en el consumo de alcohol por los efectos negativos en su salud y en la imagen del Grupo Security S.A.

Cualquier infracción a la prohibición acerca del consumo y tráfico de drogas ilícitas o alcohol, así como la negación al sometimiento de exámenes médicos y demás procedimientos clínicos que se le exijan con el fin de acreditar una salud física y mental apta con el cargo que desempeña, se considerará como un incumplimiento grave al presente Manual y al Código de Ética, así como también respecto del Reglamento Interno de Orden, Higiene y Seguridad del Grupo Security S.A. Los empleados deberán autorizar que sus resultados sean conocidos por el empleador, sujetándose esta materia a las regulaciones legales.

4.4 Actividades Distintas a las Efectuadas en el Desempeño de sus Funciones

Durante el horario de trabajo los empleados no están autorizados para desempeñar actividades laborales distintas a las pactadas en su contrato de trabajo o descripción de cargo. Sin embargo, en cualquier horario distinto al laboral se podrán realizar trabajos o actividades siempre y cuando éstas no sean equivalentes a las funciones desempeñadas en la empresa, esto es, que no se encuentren comprendidas dentro del giro del empleador (art. 160, 2 Código del Trabajo).

En el caso que se realice un trabajo o actividad en un horario diferente al laboral y que pueda estar relacionado a las funciones desempeñadas en la empresa (Clases, charlas, presentaciones, etc. cuyo contenido este vinculado a la empresa) debe ser informado previamente por escrito al supervisor directo, quien solicitará a Cultura Corporativa la autorización y determinará si interfieren, compiten o se encuentran en conflicto con los intereses de la empresa o con su posibilidad de cumplir con sus deberes de trabajo. En la eventualidad de que suceda esto último, los empleados evitarán realizar dichas labores.

4.5 Apremios ilegítimos

Queda estrictamente prohibido a todos los empleados ejercer cualquier tipo de conducta que no sea acorde con un ambiente laboral digno y de respeto mutuo. Por lo tanto, todo tipo de apremio ilegítimo o acoso, sea sexual o de otro tipo, que ejerza cualquier empleado sobre otro, en especial de un jefe hacia un subordinado, deberá ser informado a la brevedad al superior directo de los involucrados, o bien, en la eventualidad de que la situación no se pudiera resolver o se sintiera incómodo al tener que recurrir a personas de su misma unidad, deberán informar a Cultura Corporativa a través de los medios establecidos para ello.

4.6 Bullying Laboral

El bullying laboral es aquel comportamiento abusivo que genera en los empleados incomodidad y que tiene un impacto negativo en la vida de las personas dentro y afuera del lugar de trabajo. Éste incluye principalmente:

- Amenazas personales
- Comentarios despectivos
- Humillación pública
- Tácticas de intimidación
- Abuso verbal
- Excluir al empleado a propósito de reuniones o discusiones
- Demandas excesivas, fechas límite imposibles o peticiones irracionales.

La empresa, en su afán de mantener las buenas relaciones laborales tanto al interior como fuera del lugar de trabajo prohíbe estrictamente

a los empleados ejercer cualquier tipo de comportamiento de bullying tanto entre compañeros, como con proveedores, clientes, etc.

En el caso que cualquier empleado sea víctima o se encuentre en presencia de este comportamiento, deberán reportarlo a la brevedad al superior directo, o bien, en la eventualidad de que la situación no se pudiera resolver o se sintiera incómodo al tener que recurrir a personas de su misma unidad, deberán informar a Cultura Corporativa a través de los medios establecidos para ello.

4.7 Manejo de Información Interna

La información a la que tienen acceso los empleados que pertenecen al Grupo Security S.A., es de carácter confidencial y para uso interno. No podrá salir de la empresa, divulgarse, ser refraseada o revelada, ya sea de modo parcial o total, a nadie, inclusive clientes, familiares, amigos, socios y otros empleados quienes no la necesiten para el desempeño de sus funciones sin la expresa autorización del responsable asignado (Ver Anexo Nº 1).

Es por ello que los empleados manejarán la información proporcionada por sus clientes con la más estricta confidencialidad, haciendo toda clase de esfuerzos para evitar revelarla a terceros, ya sea en forma intencionada o no, sin el consentimiento expreso y por escrito de los clientes y el Supervisor. Por lo tanto, como mínimo todos los empleados deben tener presente:

A) Se prohíbe que cualquier persona que trabaje en la institución use la información para beneficio propio, de un tercero o de familiares.

B) Sólo se debe acceder a esta información en el ámbito de las tareas encomendadas por el cliente o la empresa al empleado.

C) No conversar en público asuntos en que se encuentre involucrada este tipo de información, sea de la empresa, de nuestros clientes o proveedores actuales o potenciales.

D) Las unidades que posean información deberán velar porque nadie fuera de su área tenga acceso a ella, salvo que sea necesario de acuerdo con las normas establecidas en la empresa. En caso que otro empleado, quien no requiere tal información para el desempeño de sus funciones, la solicitara, se deberá informar inmediatamente al superior directo o a quien lo reemplace.

E) Asegurarse que los documentos relacionados con los negocios estén guardados de un modo seguro, resguardando la privacidad del cliente y de la empresa.

F) Guardar bajo llave en escritorios o archivadores todos los materiales relacionados con los clientes y otros materiales de la empresa que sean potencialmente confidenciales.

G) Mantener la documentación de sus computadores personales bajo un estricto control, con claves de acceso a la información contenida en los discos duros y en la red corporativa.

H) Velar por la seguridad y privacidad en las áreas de negocio, controlar el acceso a las zonas de oficinas, que contengan información confidencial y las entradas a las salas de archivo o bodegas en que se almacene información histórica.

I) No realizar transacciones fuera de las áreas establecidas, ni utilizar teléfonos celulares u otros artefactos que no hayan sido autorizados por la empresa para éstas. Para estas transacciones se considerarán áreas establecidas, aquéllas donde se maneja información confidencial, reservada, etc. o se realizan las transacciones como son las mesas de dinero, corredoras de bolsa u otras similares.

J) Abstenerse de realizar grabaciones, filmaciones o fotografías dentro de las dependencias de la empresa sin la aprobación previa del superior o encargado del área.

K) Suscribir un acuerdo de confidencialidad o extender el ya suscrito, a situaciones especiales en que la participación del empleado pueda dar lugar a un conflicto de interés, o su exclusión necesaria o conveniente por razones de interés superior corporativo. Este acuerdo de confidencialidad

debe ser solicitado al Oficial de Cumplimiento o a Cultura Corporativa.

La información confidencial relativa a los clientes, sólo podrá ser revelada a terceros como consecuencia de un estatuto o de una regulación, un proceso legal apropiado o en cumplimiento de las inspecciones realizadas por las entidades reguladoras y/o fiscalizadoras.

Estos requerimientos deben ser informados en forma previa a sus supervisores directos, validados y autorizados por Fiscalía.

Ante cualquier duda relacionada con el manejo de información confidencial e interna se podrá consultar al Manual de Manejo de Información de Interés para el Mercado (MMIIIM), documento que se encuentra disponible en la Intranet, y en el Anexo N° 1 de este documento.

4.8 Manejo de Consultas de Clientes, Terceros y Medios de Comunicación

Respecto de consultas realizadas por los clientes, siempre se deberá verificar que quien realiza la pregunta respectiva corresponda a la persona del cliente. Si éste no es conocido personalmente, se deberá verificar su identidad mediante la presentación de un documento en que se individualice o bien llamar al teléfono que éste tiene registrado en la empresa que es cliente, tratándose de consultas llevadas a cabo por vía telefónica, internet u otro medio. En la eventualidad, de que el cliente no pueda presentarse y envíe un representante, éste deberá proporcionar la documentación legal que lo acredite como tal, la que deberá ser validada con Fiscalía.

En el caso de consultas de terceros, en razón de nuestro deber de confidencialidad, no estamos autorizados para entregar información respecto de nuestros clientes, salvo que dichos antecedentes sean solicitados formalmente por las autoridades locales (Poder Judicial y Reguladores).

Se debe tener presente que todo requerimiento solicitado por las autoridades o terceros deberá ser canalizado por la Fiscalía de la empresa, sin que esté permitido entregar respuesta alguna sin dicho V°B°.

Todo empleado debe abstenerse de anunciar cualquier información a los medios de comunicación, salvo que su cargo lo indique (asumiendo la correspondiente responsabilidad) o bien esté expresamente autorizado para ello. Para todos los efectos, los únicos responsables de entregar comunicados a la prensa son el Presidente del Directorio y el Gerente General.

4.9 Regalos, Incentivos, Actividades Sociales, etc.

Recepción de regalos, incentivos, etc.

Con el propósito de mantener la transparencia en los negocios y evitar cualquier tipo de mala interpretación, es importante tener presente lo siguiente:

A) En relación a los regalos e incentivos queda expresamente prohibido:

• Requerir para sí o para un tercero cualquier objeto/asunto de valor a cambio de una transacción/negocio, servicio o información confidencial relativa a la empresa Grupo Security S.A. Aceptar cualquier objeto de valor (salvo compensación usual autorizada o atenciones y regalos de valor nominal según aparece más adelante) de cualquier persona que diga relación con transacciones/negocios de la empresa.

• Aceptar cualquier tipo de donaciones de parte de clientes (salvo si provienen de algún familiar). En caso que esto suceda o tiene conocimiento de que pueda ocurrir, deberá informar al jefe directo.

• Los empleados no podrán, por sí o por persona interpuesta, solicitar dinero a préstamo o recibir cualquier tipo de facilidad financiera de clientes, proveedores, intermediarios, contrapartes o terceros, salvo que provenga de relaciones familiares o de la vinculación con instituciones

financieras acreditadas para estos fines.

B) Podrán aceptarse las siguientes atenciones:

• Los objetos de propaganda de escaso valor (que no excedan U.F. 3,5). Cualquier regalo, invitación o atención cuyo valor sea superior a U.F. 3,5 deberá ser previamente autorizado por el Gerente General de la empresa.

• Las invitaciones normales o actividades sociales que no excedan de los límites considerados razonables en los usos sociales (que no excedan U.F. 3,5).

• Las atenciones ocasionales por causas concretas y excepcionales que constituyan expresiones de amistad o buena voluntad (como regalos de Navidad o de boda), siempre que no sean en dinero y estén dentro de límites módicos y razonables.

Estas atenciones sólo podrán aceptarse en forma esporádica, quedando vedada su habitualidad, o su reiteración sin causa justificada. En ningún caso podrán exceder al monto máximo fijado precedentemente para ellas.

Sólo con autorización de su Jefatura el empleado podrá participar en eventos puramente ocasionales patrocinados por los proveedores, distribuidores o clientes, en que se sorteen o regalen - mediante criterios de selección impersonales - premios consistentes en artículos, beneficios tales como descuentos, pasajes, estadías, alojamiento, entrada a espectáculos, etc. entre los presentes.

Finalmente, en caso de no ser posible negarse a aceptar una atención que sobrepase los límites establecidos, se deberá informar inmediatamente sobre el regalo o atención recibida a su superior directo a través de algún medio escrito (dependiendo si el monto o características del obsequio es excesivo, también se deberá dar aviso al Gerente General de la empresa) y con copia a Cumplimiento Corporativo.

Entrega de regalos, Incentivos, etc.

Como regla general, tampoco se deberá entregar atenciones, regalos, invitaciones, favores o cualquier otro tipo de compensación vinculada con su actividad profesional en la empresa por iniciativa propia, ya sea a clientes, proveedores actuales o potenciales, intermediarios o cualquier otro tercero. Salvo que se trate de situaciones institucionales como promociones, concursos, etc. y que no estén relacionadas con una transacción en particular.

Adicionalmente, respecto de empleados públicos nacionales y extranjeros, no se aceptarán ni entregarán obsequios de valor significativo que denoten intención del oferente o del cliente de influir con un tipo de compensación por algún negocio, transacción o gestión que realice con la empresa, ya sea antes, durante o después que esa operación se haya llevado a cabo, dando cumplimiento de este modo a la Ley 20.393 (Delito de Cohecho).

4.10 Donaciones

Queda establecido que todas las donaciones realizadas por la empresa deben quedar debidamente documentadas en forma previa a través del Formulario de Donaciones y de Recepción de Donaciones de la empresa (Ver Anexo Nº 2), esto con el propósito de mantener la transparencia, realizar un control y seguimiento de los fondos donados. Todos los formularios deberán ser enviados al área de Cumplimiento Corporativo, la cual se encargará de canalizar esta información y llevar un registro de ello.

4.11 Soborno

El soborno es la entrega de dinero o cualquier otro tipo de compensación con el propósito de influenciar de manera ilegal la conducta de una persona. Por lo tanto, queda estrictamente prohibido el uso de recursos de la empresa por parte de cualquier empleado para propósitos ilegales, carentes de ética como comisiones ilegales o compensaciones ilegítimas. Así como también la aceptación de cualquier compensación por personas o instituciones tanto externas como entre empleados.

4.12 Uso de los Recursos y Activos de la Empresa

Todos los empleados deben mantener una actitud adecuada, realizar un correcto uso y resguardar en forma responsable todos los recursos y/o activos institucionales proporcionados por la empresa, no malgastándolos y buscando el ahorro en todas sus acciones. Esto considera:

A) Propiedad de la empresa y/o servicios: No estarán facultados personalmente ni a través de cualquier pariente para disponer de bienes y/o servicios institucionales sin autorización previa por escrito del Gerente General de la empresa o quién éste designe. Esto se hace extensivo a propiedades o vehículos embargados por cuanto ello puede producirle problemas legales a la empresa. En todo caso, para la enajenación de cualquier bien o servicio institucional, la empresa seguirá un proceso formal e informado que garantice la transparencia.

B) No sacar provecho de una legítima oportunidad de negocio de la empresa: No deberá aprovechar para beneficio personal cualquier oportunidad de negocio que sea de legítima propiedad de la empresa por cuanto haya sido gestionada por la empresa a través de su personal, contactos o su capacidad financiera.

C) Uso de información, recursos tecnológicos y sistemas de la empresa: En conformidad con lo señalado precedentemente, sólo es permitido el uso de Internet en el ámbito de las tareas encomendadas por la empresa a sus empleados. En consecuencia, está prohibido acceder a páginas de Internet cuyos contenidos no se encuentren relacionados con la actividad que el empleado desempeña y/o sean reñidos con la moral (para mayor información ver Política de Seguridad de la Información publicada en Intranet, particularmente Norma de Gestión de Comunicaciones).

La cuenta de correo electrónico que Security asigna a sus empleados tiene por objeto el adecuado desarrollo de su trabajo, por lo que se entiende que es de propiedad de la empresa, siendo sujeto de revisión en conformidad a la ley, y sólo podrá ser utilizada por los empleados durante el ejercicio de sus funciones, no siendo posible conservarla una vez que se ha dejado de trabajar en la empresa.

No se debe utilizar los recursos computacionales u otros bienes de la empresa para realizar negocios externos, ni para actividades ilegales o no éticas.

Mayor información sobre este tema puede ser encontrada en el Anexo N°1, de este documento.

D) Uso de viáticos: Con el propósito de mantener el buen uso de los recursos, los empleados deberán rendir en cada viaje o comisión de servicios el importe de viáticos gastados, los cuales no deberán exceder de un buen criterio de comportamiento. Este último deberá ceñirse a la Política de Viajes Grupo Security o lo que Cultura Corporativa defina.

E) Respaldo de Gastos: Todas las actividades sociales, viáticos, etc. deberán reflejar de manera precisa todos los gastos asociados a ellos, quedando respaldados a través de documentación como boletas, facturas, etc. Adicionalmente, todo empleado que deba realizar la rendición de gastos, deberá completar el formulario (Anexo N° 3), el cual deberá entregar al área de Contabilidad respectiva. En consecuencia, no se podrá:

- Mantener cuentas ocultas dentro de la empresa
- Adulterar los respaldos de los gastos realizados
- Incorporar gastos falsos en los libros de registros
- Realizar transacciones o aprobar pagos con el fin de que sean utilizados para propósitos diferentes a los originales.

F) Propiedad Intelectual: Se debe tener presente que la empresa es dueña de todos los derechos, títulos y participaciones en la propiedad intelectual, incluyendo inventos, mejoras, ideas, procesos, programas de software de sistemas y todo tipo de descubrimientos concebidos o desarrollados por todos sus empleados durante el transcurso de su trabajo dentro de la Organización. Por lo tanto, se espera de los empleados un buen uso de la propiedad de los desarrollos generados durante el desempeño de sus funciones (para mayor información ver Política de Seguridad de la Información publicada en Intranet, particularmente, la Norma de Cumplimiento).

Adicionalmente, todo empleado debe informar a sus supervisores directos cuando sea necesario realizar la protección de dicha propiedad intelectual.

G) Utilización de la marca e imagen (logos) de la empresa o empresas de Grupo Security: Queda establecida la prohibición del uso de la marca o imágenes de la empresa o de las empresas de Grupo Security en cualquier tipo de documentación, registro u otros para fines personales o no oficiales.

4.13 Adquisiciones de Bienes o Servicios Personales de la misma Área de Negocios

Con el objetivo de mantener la transparencia en los negocios, los empleados podrán adquirir bienes o servicios de su misma área de negocios cumpliendo con las siguientes condiciones:

A) Estos deberán ser adquiridos siguiendo los mismos procedimientos regulares que el resto de los clientes (Salvo que exista una política específica para ello en la empresa correspondiente).

B) El empleado deberá informar a su superior directo por escrito y solicitar la autorización correspondiente (Ver Anexo Nº 4) y deberá enviar una copia a Cumplimiento Corporativo.

C) Deberán llevarse a cabo por una persona (autorizado por la jefatura correspondiente) distinta del empleado que adquiere el bien o servicio.

D) Deberán ser adquiridos en las mismas condiciones y a precio equitativo de mercado vigente en el momento de la operación (Salvo que exista una política específica para ello en la empresa correspondiente)

Para el caso de los empleados pertenecientes a las áreas de inversión y en relación a las cuentas personales, deberán además acatar lo dispuesto en punto 5.4.6 de este manual.

4.14 Adquisición de Bienes Reposeídos

Los bienes reposeídos son aquellos bienes recibidos por la empresa por el no pago de obligaciones contraídas por un deudor. Ej.: Vehículos, propiedades, etc.

Los bienes reposeídos deben ser ofrecidos en una primera instancia a través de algún medio público de comunicación (Diarios, Radio, etc.) u ofrecidos a través de Corredores, en el caso de propiedades, en Automotoras o Concesionarias cuando se trate de vehículos u otras empresas similares del rubro. Con el propósito de mantener la transparencia y evitar conflictos de intereses, los empleados no participarán en dicho proceso. Si éstos no son adquiridos, se realizará una segunda oferta, pero esta vez a todos los empleados de la empresa y de las empresas de Grupo Security y se seguirá con el procedimiento establecido por cada empresa.

4.15 Adquisición de Activos Muebles de la Empresa

Dentro de la empresa y de las empresas de Grupo Security existe una serie de activos muebles que son renovados. Estos serán ofrecidos en una primera instancia a los empleados de acuerdo a las políticas y procedimientos establecidos en cada empresa.

4.16 Actividades Políticas

Aquellos empleados que, en el ejercicio de sus derechos, participen en actividades políticas deberán informar su condición por escrito y de acuerdo a los procedimientos establecidos por Cultura Corporativa a sus supervisores directos, y las podrán desarrollar siempre y cuando éstas no afecten sus actividades diarias y la imagen de la empresa y de las empresas de Grupo Security.

4.17 Conductas Prohibidas

Existe una serie de conductas que se encuentran expresamente prohibidas para los empleados, por cuanto afectan gravemente a la imagen y confianza que los clientes han depositado en nosotros. Éstas son:

En el desarrollo de sus actividades

A) Recibir en forma personal, en nombre del cliente, o clientes, la correspondencia que la empresa les envía, por cuanto debemos garantizar que éstos tengan la posibilidad de controlar nuestra gestión, asegurando con ello su adecuada transparencia.

B) Aceptar dineros de clientes, destinados al pago de productos o servicios, en lugares no establecidos y por personal no autorizado para ello.

C) Recomendar, sin advertir previamente a los clientes de los riesgos de invertir en capitales volátiles y por ningún motivo sugerir o inducir la evasión de impuestos.

D) Usar indebidamente y traspasar la información que se maneja en las redes y sistemas de la empresa, a través de cualquier medio, ya sea magnético, electrónico o escrito (notebooks, celulares, papeles, pendrives, cds, etc.). Ver Anexo Nº 1.

E) Preguntar o aceptar que nuestros clientes nos entreguen su clave para realizar operaciones en la empresa.

F) Atraer o conservar clientes, otorgando beneficios no compatibles con las sanas prácticas y buenas costumbres del mercado.

G) Ofrecer productos o servicios a precios inferiores a los costos asociados a ellos, con el propósito de obtener un negocio en desmedro de la competencia.

H) Participar de colusiones de manera de limitar la oferta en perjuicio de los clientes.

I) Generar relaciones de negocios por medio de la desinformación, o el mal entendimiento del cliente o proveedores sobre la transacción específica o el alcance de las responsabilidades de la empresa.

J) Falsificar o adulterar información de propiedad de la empresa o de las empresas de Grupo Security.

Al interior de la organización

A) Actividades ilegales de cualquier tipo.

B) Juegos y toda forma de apuestas.

C) Efectuar colectas, a excepción de aquellas previamente aprobadas por Cultura Corporativa.

D) Actividades con fines de lucro personal dentro de la empresa y/o utilizando los recursos y dependencias de la empresa.

E) Mensajes obscenos, vejatorios o abusivos.

F) Actividades contrarias a lo establecido en el Código de Ética.

G) Envío de correos electrónicos masivos o cadenas de correo.

H) Creación, transmisión o recepción voluntaria de material ofensivo, difamatorio, amenazante o abusivo, que incluye pero no se limita, a comentarios basados en la raza, nacionalidad, sexo, orientación sexual, edad, discapacidad, religión o creencias políticas.

I) Cualquier acción deliberada que dañe o perturbe los sistemas o redes de computación, que altere su rendimiento normal o produzca un desperfecto de los mismos.

J) Introducción voluntaria o negligente de virus u otros programas destructivos en los computadores o estaciones de trabajo, en los sistemas y redes de la empresa o en sistemas o redes externas.

K) El desciframiento no autorizado o intento de desciframiento de cualquier sistema o contraseñas de usuarios o cualquier archivo cifrado de usuarios.

L) Utilizar los canales de denuncias para fines

que no corresponden a los establecidos. Ej.: pitanzas, envío de spam, denunciar sin motivos a un funcionario, etc.

5. Conductas Especiales

5.1 Reglas de Conducta Especial para Empleados de Áreas de Pago y Recaudación

Para evitar conflictos de interés, los empleados que desarrollen sus funciones en áreas involucradas con cajas no podrán cobrar documentos personales, ni de empresas o personas relacionadas en su mismo puesto de trabajo. Estas operaciones deberán ser comunicadas en forma previa a la jefatura directa y deberán realizarse a través de otro funcionario autorizado para ello (Anexo 4).

Así mismo, las jefaturas de estas áreas no deberán valerse de su cargo y exigir a sus subordinados el cobro de documentos personales, de empresas o personas relacionadas, o bien que no cumplan con todos los requisitos exigidos (Ej.: Firmas disconformes, sin endoso, fuera de plazo, documentos deteriorados, etc.).

5.2 Reglas de Conducta Especial para Empleados de Áreas de Adquisiciones

En todos los procesos de adquisición, los empleados involucrados deberán firmar una Declaración, Anexo N° 5, donde se establece que no tienen conflictos de intereses al realizar la operación.

5.2.1 Procesos de compra de bienes o servicios

Para todos los procesos de adquisición de bienes o servicios, los empleados a cargo de la decisión siempre deberán escoger la mejor alternativa que beneficie los intereses de la empresa, de acuerdo al requerimiento hecho por los clientes internos, para lo cual utilizarán criterios de comparación, y deberán respaldar y documentar la evaluación de las distintas alternativas y dejar por escrito la decisión tomada.

5.2.2 Proceso de licitación

Como un modo de mantener la transparencia en los negocios, en los procesos de licitación no podrán participar empresas o personas relacionadas con los empleados. Por ello, se solicitará en forma previa a estas empresas o personas, una declaración firmada donde conste que no tienen vinculación familiar con empleados de la empresa o de las empresas de Grupo Security, y deberán señalar sus socios mayoritarios. En la eventualidad de que exista algún conflicto de interés, este se analizará caso a caso, quedando establecido que serán evaluados bajo las mismas condiciones que el resto de los participantes.

5.3 Reglas de Conducta Especial para Empleados de Áreas Comerciales

5.3.1 Gestión de productos o servicios a personas o empresas relacionadas

Con el objetivo de mantener la transparencia en los negocios y evitar todo tipo de conflicto de interés, los empleados que desempeñen sus funciones en áreas comerciales no podrán ser parte de su cartera de clientes, productos o servicios de la empresa para sí, ni para personas o empresas relacionadas. En consecuencia, todos los empleados que trabajen en áreas comerciales deben realizar una declaración (Ver Anexo Nº 6) donde consten todas sus participaciones en empresas relacionadas. Esta declaración debe ser actualizada al menos una vez al año.

Por lo tanto, en la eventualidad que un familiar o una empresa relacionada al empleado quiera tomar un producto o servicio, podrá hacerlo a través de su familiar, sin embargo la administración de la cartera debe realizarse a través de otro funcionario

no relacionado. Adicionalmente, la adquisición de estos productos y/o servicios deberá seguir los mismos procedimientos regulares que el resto de los clientes y bajo las mismas condiciones y precios de mercado vigentes a la fecha de la operación.

5.4 Reglas de Conductas Especiales para Empleados de Áreas de Inversión

El presente punto incorpora conductas especiales de actuación para los empleados de las áreas de inversión de las empresas de Grupo Security. Estos corresponden a funcionarios de las siguientes empresas: Banco Security, Valores Security S.A. Corredores de Bolsa, Adm. General de Fondos Security S.A., Global Security Gestión y Servicios Ltda., Securitizadora Security S.A., Asesorías Security S.A., Seguros Vida Security Previsión S.A., Factoring Security S.A., Inmobiliaria Casanuestra S.A., Hipotecaria Security Principal S.A. o cualquier empresa a la cual sean aplicables estas reglas de comportamiento. Estas medidas deben ser adoptadas por todos los gerentes, administradores, representantes legales, operadores, ejecutivos y todos los demás empleados que por naturaleza de su cargo, funciones o actividad tengan relación con lo aquí establecido.

5.4.1 Principios Fundamentales

Con el fin de cumplir con lo dispuesto en el Título XXI, de la Ley de Mercado de Valores (LMV), además de mantener un adecuado manejo de la información privilegiada y de evitar en todo momento la ocurrencia de conflictos de interés, se aplicarán los siguientes principios orientadores:

• Transparencia: Un mercado transparente es aquel en el cual es posible una apropiada formación de precios y toma de decisiones, como consecuencia de niveles adecuados de eficiencia, de competitividad, y de flujos de información oportunos, suficientes y claros entre los participantes que en él intervienen.

• Reserva: Se entiende como tal el deber de abstenerse de revelar aquella información considerada confidencial o personal. Con ello deben abstenerse de hacer comentarios respecto de la misma que puedan revelar directa o indirectamente su existencia o contenido.

• Utilización adecuada de la información: Los empleados que intervienen en el mercado debe abstenerse de utilizar información privilegiada para sí o para un tercero.

• Lealtad: Se entiende como tal la obligación que tienen los empleados de obrar simultáneamente de manera integra, franca, fiel y objetiva, con todas las personas que intervienen en los mercados (clientes, competidores, etc.). Son conductas que expresan el principio de lealtad:

1. Abstenerse de obrar frente a conflictos de interés.

2. Abstenerse de dar información ficticia, incompleta o inexacta.

3. Omitir conductas que puedan provocar errores en la compra o venta de valores.

4. Evitar participar en operaciones no representativas de condiciones de mercado.

5. Abstenerse de participar o recomendar en cualquiera operación ejecutada sobre la base en la información privilegiada, confidencial o pública que corresponda a clientes, empleados, proveedores o a cualquier otro tercero perteneciente a empresas externas al Grupo Security y sus filiales.

• Profesionalismo: Los empleados que participan en los mercados, siempre deben operar con fundamento e información seria, completa y objetiva, deben además suministrar consejo para la mejor ejecución del encargo en función de las necesidades del cliente.

• Adecuación a la Ley: Señala la exigencia de dar apropiado cumplimiento a todas las disposiciones legales, en especial a los deberes de información en ellas contenidos, subrayándose la importancia de comunicar al cliente cualquier circunstancia sobreviniente que pudiera modificar su voluntad contractual.

• Equidad: Los empleados vinculados a las áreas de inversión deben abstenerse de realizar operaciones que favorezcan a algunos clientes en desmedro de otros.

• Sana competencia: Mantener una interacción correcta con el resto de las empresas e instituciones que conforman el mercado.

5.4.2 Conductas Específicas para el Área de Inversión

Con el propósito de generar confianza en los negocios, evitar conflictos de interés y establecer criterios claros de conductas sobre las funciones relacionadas con operaciones en los mercados, se han establecido las siguientes reglas de carácter general:

• No provocar movimientos desordenados en los precios de cotización o en las tasas de rendimiento del mercado.

• Actuar con la debida diligencia en la recepción y ejecución de las órdenes de compra y venta de títulos.

• En la propuesta, discusión y cierre de cualquier negocio deben tomarse las precauciones necesarias, con el objetivo de lograr del cliente un correcto entendimiento sobre la naturaleza, alcance y condiciones del negocio, en especial las siguientes:

• El claro entendimiento del producto o clase de negocio que se propone.

• El recíproco conocimiento de todos los elementos necesarios para el cierre de la operación.

• El riesgo inherente a la operación.

• Registrar en los libros exigidos por la ley, todas sus operaciones y entregar oportunamente a las partes interesadas los correspondientes comprobantes oficiales de las transacciones que se celebren.

• No difundir rumores alarmistas o tendenciosos basados en información sobre la que no se tengan suficientes datos.

• Abstenerse de realizar y/o participar en prácticas que directa o indirectamente creen condiciones falsas de oferta o demanda que influyan en los precios de los valores, o que tengan por objeto impedir, restringir o falsear el juego de la libre competencia en el mercado.

• Mantener una posición de independencia en la realización de sus negocios, teniendo libertad para aceptar o rechazar aquellos en que se soliciten sus servicios, sin necesidad de explicar los motivos de su rechazo, si es el caso.

• No divulgar información falsa, a fin de influir en las cotizaciones de los valores.

• No contratar productos o servicios con el único fin de generar comisiones o ingresos y sin un interés efectivo para el cliente.

• Guardar reserva, respecto de terceros, sobre las actividades que se ejecuten en relación con su profesión, salvo que exista autorización expresa del interesado o en los casos determinados por la Constitución y las leyes.

• Realizar negocios de manera tal que no generen error a las partes contratantes.

• Abstenerse de suministrar antecedentes a un tercero que no tiene derecho a recibirlos, o con base en dicha información aconsejar la adquisición o venta de un valor en el mercado.

• Adquirir o negociar títulos emitidos, avalados, aceptados o cuya emisión sea administrada por empresas consideradas en riesgo de quiebra, sus filiales o subsidiarias sin la autorización correspondiente.

• Identificar a sus clientes para prevenir que sus operaciones sean utilizadas en actividades de lavado de dinero, terrorismo, cohecho u otras provenientes de actividades ilícitas, informando al área de Cumplimiento de la empresa o al área de Cumplimiento Corporativo y colaborar con las autoridades competentes para estos efectos.

• Abstenerse de ejecutar instrucciones que sean contrarias a la regulación vigente o a las sanas prácticas del mercado.

• No participar en la toma de decisiones o en funciones de representación, en transacciones de cualquier tipo que estén vinculadas o relacionadas de alguna forma con sus intereses particulares o familiares.

• No abusar de una posición dominante con el fin de obtener mejores condiciones que aquellas que pudieran generarse por la sola intervención del mercado.

• Todas las operaciones de estas áreas deben realizarse en cumplimiento de las normas y regulaciones vigentes, y en aquellas que las deroguen, modifiquen o adicionen, así como de las demás normas que se originen en relación con estos temas.

5.4.3 Manejo de la información privilegiada

De acuerdo al Artículo 165 de la LMV y con el fin de preservar el principio de igualdad en el acceso a la información de los participantes, brindarle transparencia al mercado y evitar conflictos de interés, todo empleado de las áreas de inversión que posea información privilegiada deberá:

A) Abstenerse de utilizar en beneficio propio o ajeno, adquirir o enajenar, para sí o para terceros, directamente o a través de otras personas los valores sobre los cuales posea la información privilegiada.

B) No utilizar esta información para obtener beneficios o evitar pérdidas, mediante cualquier tipo de operación con los valores a que ella se refiera o con instrumentos cuya rentabilidad esté determinada por esos valores.

C) Guardar reserva y no comunicar dicha información a terceros, salvo en el ejercicio normal de su trabajo, profesión o cargo.

D) No recomendar a un tercero que adquiera o ceda valores o que haga que otro los adquiera o ceda basándose en dicha información.

No obstante a lo dispuesto anteriormente los empleados podrán realizar operaciones con información privilegiada, por cuenta de terceros, no relacionados con ellos, siempre que la orden y las condiciones específicas de la operación provengan del cliente, sin asesoría ni recomendación del intermediario, y la operación se ajuste a su norma interna, establecida en conformidad al Art. 33 de la LMV.

Negociación incompatible o aprovechamiento indebido del cargo:

Los empleados deberán abstenerse de utilizar información, recursos, e infraestructura de la Empresa, tales como equipos, sistemas, canales de comunicación u otros, en transacciones que realicen - dentro de los límites permitidos - para beneficio propio o de un tercero, o sean ajenas a los fines institucionales, sea que se expresen en un contrato, transacción, operación o cualquier acción, en forma directa o indirecta.

5.4.4 Actividades contrarias a la ley

Con el fin de cumplir con lo dispuesto en el Art. 52 y 53 del Título VIII de LMV, es que se considerarán contrarias al presente Manual de Conducta, las siguientes actuaciones:

• Efectuar transacciones en valores con el objeto de estabilizar, fijar o hacer variar artificialmente los precios. Sin embargo, podrán efectuarse actividades de estabilización de precios en valores de acuerdo a reglas de carácter general que imparta la Superintendencia y únicamente para llevar adelante una oferta pública de valores nuevos o de valores anteriormente emitidos y que no habían sido objeto de oferta pública.

• Efectuar cotizaciones o transacciones ficticias respecto de cualquier valor, ya sea que las transacciones se lleven a cabo en los mercados o a través de negociaciones privadas.

• Realizar transacciones, inducir o intentar inducir a la compra o venta de valores, regidos o no por la LMV, por medio de cualquier acto, práctica, mecanismo o artificio engañoso o fraudulento.

5.4.5 Operaciones por cuenta propia

Las áreas de inversión no podrán realizar operaciones por cuenta propia en detrimento de los intereses de sus clientes. Por consiguiente, cuando se genere un conflicto entre el interés del cliente y la empresa, prevalecerá el del primero.

En consecuencia, las áreas de inversión no podrán adquirir valores por cuenta propia, cuando a dicha fecha uno de sus clientes le haya impartido una orden de compra que pueda cumplirse adquiriendo dichos valores.

De igual manera el área de inversión no podrá vender o comprar valores de su propia cartera a un cliente, cuando a dicha fecha otro cliente le haya impartido una orden de venta que pueda cumplirse cruzando la orden de compra recibida.

El área de inversión no podrá vender o comprar títulos por cuenta propia en mejores condiciones a aquellas sobre las cuales mantenga órdenes pendientes de compra o venta de títulos de la misma naturaleza por cuenta de sus clientes.

Finalmente, el área de inversión, en desarrollo de las operaciones por cuenta propia, deberá contar con la autorización en forma expresa de los clientes, para comprar para sí los valores que le ordenen vender los clientes, o para vender de su posición lo que le ordenen comprar los clientes. Estas operaciones deberán realizarse a precios de mercado y siguiendo los mecanismos bursátiles establecidos para tal efecto.

5.4.6 Actuación en operaciones personales

Para efecto de los instrumentos financieros como: fondos de inversión, fondos mutuos, instrumentos del Banco Central, tesorería, depósitos a plazo fijo, pactos y otros de similar naturaleza, los empleados de las áreas de inversión podrán realizar estas operaciones por cuenta personal, es decir, para sí mismos o por operaciones equiparadas a estas (Ver 5.4.7) a través de cualquier intermediario financiero.

Sin embargo en el caso de compra y venta de acciones (se consideran todas las acciones transadas en Bolsas de Valores Nacionales) y de instrumentos de deuda (bonos de S.A. no bancarias u otros), los empleados sólo podrán realizar operaciones personales o equiparadas a estas (Ver 5.4.7), a través de una de la empresa o de las empresas de Grupo Security. Esto con el propósito de mantener la transparencia en los mercados, evitar la especulación y el mal uso de la información privilegiada. Adicionalmente, estas operaciones, deben efectuarse a través de un funcionario distinto y en ausencia de este, por el Gerente correspondiente.

Otras operaciones, no relacionadas con la naturaleza propia del cargo que desempeña el empleado, deberán efectuarse bajo las condiciones vigentes del mercado a la fecha de su ejecución.

Las demás operaciones, no relacionadas con la naturaleza propia del cargo que desempeña el empleado, deberán efectuarse bajo las condiciones vigentes del mercado a la fecha de su ejecución. Cuando la transacción, operación o inversión se ejecute en una institución financiera distinta al Grupo Security, el empleado deberá informarla a la respectiva empresa de este último, a través de un formulario disponible en la Intranet, otro canal o bien debe ser solicitado al Oficial de Cumplimiento, con copia al Supervisor directo.

5.4.7 Operaciones equiparadas a las operaciones personales

Se equiparan a operaciones personales, las que se indican a continuación:

• Las que realice el cónyuge del empleado, separado o no de bienes.

• Las de sus hijos menores de edad, sujetos a su patria potestad; y mayores de edad que dependan económicamente del mismo, convivan o no con él.

• Las sociedades de las cuales sea dueño directo o a través de otras personas naturales o jurídicas de un 10% o más de su capital o de sus utilidades.

5.4.8 Conflictos de interés en operaciones personales

Los empleados de las áreas de inversión no podrán realizar operaciones personales en detrimento de los intereses de los clientes de la empresa o de las empresas de Grupo Security. Por consiguiente, cuando se genere un conflicto entre el interés del cliente y los empleados, prevalecerá el del primero.

En consecuencia, los empleados de las áreas de inversión no podrá adquirir valores por cuenta personal, cuando a dicha fecha uno de los clientes de la empresa o de las empresas de Grupo Security haya impartido una orden de compra que pueda cumplirse adquiriendo dichos valores.

Los empleados de las áreas de inversión no podrán vender o comprar por cuenta personal títulos en mejores condiciones a aquellas sobre las cuales mantenga órdenes pendientes de compra o venta de títulos financieros de la misma naturaleza por cuenta de los clientes de la empresa o de las empresas de Grupo Security.

Por lo tanto, con el fin de evitar conflictos de interés en la realización de operaciones y el uso de la información privilegiada, los empleados de las áreas de inversión deberán completar un formulario (Ver Anexo Nº 6), en el que consten su situación patrimonial y las personas naturales y jurídicas que se indican en el punto anterior, y deberá actualizarlo una vez al año o bien cada vez que exista un cambio de estas personas. Este formulario debe ser enviado al Oficial de Cumplimiento de la empresa, de este modo, se mantendrá un control sobre la participación de personas naturales y jurídicas, relacionadas con los empleados en las operaciones efectuadas a través de la empresa o de las empresas de Grupo Security y los cambios patrimoniales que experimenten los empleados de las áreas de inversión.

5.4.9 Liquidación y calce de operaciones

Los empleados no podrán realizar ningún tipo de transacción por cuenta propia, personales u operaciones equiparadas, teniendo como contraparte a la empresa o a las empresas de Grupo Security, sin contar con los fondos y/o valores suficientes para cumplir en forma oportuna con las obligaciones emanadas a la fecha de liquidación de éstas.

Para efectos de lo descrito en el párrafo anterior, los empleados incluyendo las personas relacionadas mencionadas en el punto 5.4.7, en ningún caso, podrán realizar compensaciones de saldos a favor y/o en contra provenientes de operaciones cuyas fechas de liquidación no se encuentren calzadas, caso en el cual las transacciones se deberán pagar en forma íntegra y por el valor total de ésta.

5.4.10 Conducta en las operaciones personales asociadas a los distintos instrumentos

Reglas de conducta para las operaciones personales en el mercado de renta fija y/o acciones y para la realización de operaciones personales en el mercado cambiario (Compra/ Venta de divisas)

Con el propósito de contar con reglas claras en la negociación de operaciones personales de renta fija y/o acciones, facilitar estas transacciones, y darle al mercado la máxima transparencia, seriedad, seguridad y evitar conflictos de interés, los empleados de las áreas de inversión debe cumplir con lo siguiente:

A) En ningún caso los valores adquiridos por los empleados, podrán ser vendidos en la misma sesión o día en el que se hubiere realizado la operación de compra. El Gerente General o quien este designe, podrá excepcionar la prohibición de venta anterior cuando existan razones justificadas. Posteriormente esta transacción deberá ser informada al Directorio.

B) Junto con lo anterior el Gerente General o quien éste designe, podrá establecer que los valores adquiridos por los empleados no podrán ser vendidos durante un plazo mínimo contado desde la fecha de su compra. Posteriormente esta transacción deberá ser informada al Directorio.

C) En todos los casos, el plazo mínimo exigido para la venta de valores será de 10 DÍAS CORRIDOS desde la fecha de su compra.

Reglas de conducta para la suscripción de contratos personales en el mercado de futuros y/o derivados inversiones personales en fondos mutuos

Con el fin de dar al mercado la máxima transparencia, seriedad, seguridad y evitar conflictos de interés, los empleados y las personas relacionadas a estos que se encuentran mencionadas en el punto 5.4.7, que suscriban cualquier tipo de contrato con la empresa o las empresas de Grupo Security a fin de realizar operaciones personales de futuros y/o derivados (simultáneas, contratos forward de renta fija o inflación, ventas cortas, opciones, etc.), deberán contar con la autorización expresa del Gerente General o de quien éste designe y constituir las garantías respectivas de la misma forma requerida a terceros no relacionados a la empresa o las empresas de Grupo Security, y posteriormente informar al Directorio.

Mientras que los empleados de las áreas de inversión y las personas relacionadas a estos y que son mencionadas en el punto 5.4.7, no hayan obtenido la respectiva autorización por escrito, no podrán suscribir contratos personales de operación con la empresa o las empresas de Grupo Security. Adicionalmente, los montos no deben superar los montos máximos definidos por la política de Crédito al empleado definida por Cultura Corporativa y aprobada por el Directorio.

Adicionalmente, las operaciones de futuros y/o derivados que sean realizadas por los empleados de las áreas de inversión y las personas relacionadas a estos que se encuentran mencionadas en el punto 5.4.7, deberán realizarse respetando rigurosamente los plazos establecidos por las respectivas bolsas de valores u otras entidades regulatorias.

Con todo, la vigencia mínima exigida para las operaciones descritas en el párrafo anterior, será de 30 días corridos desde la fecha de su realización y en ningún caso quedarán sujetas a anticipos o prepago durante su vigencia.

Reglas de conducta para las inversiones personales en fondos mutuos

Los empleados de las áreas de inversión y las personas relacionadas a éste, que se encuentran mencionadas en el punto 5.4.7, que realicen inversiones en cualquiera de los fondos administrados por la empresa o las empresas de Grupo Security, deberán ceñirse estrictamente a la normativa, procedimientos y reglamentos vigentes que existan para ellos.

5.4.11 Formalización de órdenes

Las órdenes que se otorguen, tienen que formalizarse, en todos los casos, por escrito o cualquier otro procedimiento legalmente autorizado y reconocido como práctica habitual admisible; serán válidas otras formas de transmitir o formalizar órdenes, siempre y cuando a través de registros electrónicos o informáticos, de voz y datos, se pueda localizar y obtener dicha orden. Estas últimas deberán incorporarse a un archivo de justificantes de órdenes o estar contenidas en los registros o archivos informáticos.

6. Término de la Relación Contractual con la Empresa

Todos los empleados que han dado término voluntaria o involuntariamente a su relación contractual con la empresa deben tener presente lo siguiente:

• La propiedad intelectual de todos los desarrollos realizados durante la permanencia en la empresa son de propiedad de la empresa.

• Los recursos proporcionados por la empresa para el desarrollo de sus actividades diarias son de propiedad de ésta y deberán ser entregados formalmente y por escrito a su supervisor directo o bien a quien lo esté reemplazando en ese momento.

(Ver Anexo Nº 7), incorporar declaración de entrega y guardar copia. Se debe incluir celulares y cuentas vistas, TC, etc.

• La cuenta de correo proporcionada por la empresa tiene como objetivo el buen desarrollo de su trabajo por lo que se entiende que es de propiedad de Security. Por lo tanto, una vez que se ha dejado de trabajar en la empresa no es posible conservarla.

• Toda la información interna o confidencial de la empresa, de los clientes, proveedores, etc. no debe ser revelada una vez que se haya desvinculado de la empresa.

Para mayor información ver Política de Seguridad de la Información, particularmente, la Norma de Seguridad en Recursos Humanos.

7. Comunicación de Eventos e Irregularidades

Todos los empleados debe tener consciencia que es obligación informar de inmediato al superior directo cualquier evento sobre conductas ilícitas, ilegales o fraudulentas que lleguen a su conocimiento, que pudiera razonablemente considerarse un delito, un incumplimiento significativo de la ley o reglamentación, un acto deshonesto (incluyendo la malversación de fondos o cualquier efecto de valor perteneciente a la empresa, o el registro inapropiado de los activos o pasivos de la Institución), el incumplimiento de un fideicomiso, o cualquier otra conducta que pudiera afectar seriamente la reputación de la empresa o incumplimientos del presente Manual.

Así mismo, en caso de que no existan lineamientos específicos en el Manual de Conducta u otras publicaciones institucionales sobre una situación particular, deberá primero contactar a su supervisor directo, el cual deberá recabar todos los antecedentes que existan y que digan relación con la infracción de que se trate, e informar al Oficial de Cumplimiento de la empresa.

En la eventualidad, de que la situación no pudiera resolverse, o se sintiera incómodo teniendo que recurrir a personas de su misma unidad para comunicar los incumplimientos a este Manual, puede contactarse con el área de Cultura Corporativa al mail: culturacorporativa@security.cl o a Cumplimiento Corporativo al mail: cumplimientocorporativo@security.cl, o en la forma que los manuales o políticas establezcan como canales de comunicación.

Cabe señalar, que se harán todos los esfuerzos necesarios para mantener bajo rigurosa reserva la identidad de cualquier colaborador que informe sobre una infracción a las disposiciones de este Manual, y así evitar que dicha acción genere alguna represalia en su contra.

Finalmente, se establece que en la eventualidad de que se deba realizar una investigación al interior de la empresa, todos los empleados deberán colaborar y entregar toda la información solicitada.

8. Control y Seguimiento

Con el propósito de adoptar medidas de control adecuadas y suficientes, se tomarán las siguientes consideraciones

• El área de Auditoría Interna realizará revisiones y seguimiento con el objeto de chequear y verificar el cumplimiento efectivo de este Manual.

• Periódicamente, el área de back office será la encargada de enviar un reporte de todas las transacciones realizadas por las áreas de inversión (propias y personales) al Oficial de Cumplimiento de la empresa correspondiente, la cual será la encargada de revisar y controlar las disposiciones establecidas en el Manual de Conducta, como los plazos mínimos, las condiciones de las transacciones antes señaladas, etc.

• Se establece, como aparato de control interno,

un Comité de Ética que tiene por objeto velar por el cumplimiento de las reglas del Manual y demás normativa complementaria y el análisis de casos de incumplimiento. Este Comité está conformado por representantes de: Cultura Corporativa, Contraloría Corporativa, etc. (Ver punto 8.1)

• Finalmente, es responsabilidad de los Gerentes de las distintas áreas y divisiones asegurarse que sus subordinados firmen la declaración de la recepción y aceptación del Manual de Conducta.

8.1 Comité de Ética

El Comité de Ética tiene como responsabilidad asegurarse de la debida difusión y aplicación del Código de Ética y Manual de Conducta, lo cual significa que debe:

• Promover los valores y conductas que se fomentan en el Código de Ética y/o Manual de Conducta, sus valores y principios fundamentales.

• Facilitar y asistir al Encargado de Prevención de Delitos en el desarrollo, implementación y efectiva operación del Modelo de Prevención de Delitos.

• Ser un órgano de consulta.

• Facilitar la resolución de conflictos relacionados con el incumplimiento del Código de Ética y/o Manual de Conducta.

• Conocer y resolver denuncias de acuerdo a lo indicado en este Manual, respetando los derechos de los trabajadores o empleados, en especial el derecho a ser oídos, a defenderse, y a que las resoluciones dictadas en su contra estén debidamente fundadas.

• Canalizar casos especiales a la instancia apropiada.

• Proponer actualizaciones y modificaciones al Código de Ética y/o Manual de Conducta.

• Revisar las solicitudes de aclaración de situaciones específicas.

• Dictar circulares e instrucciones necesarias para el desarrollo y cumplimiento de lo dispuesto en el Código de Ética y/o Manual de Conducta.

El Comité de Ética esta integrado por los siguientes miembros:

- Gerente Contralor
- Gerente Cultura Corporativa
- Fiscal
- Gerente General de la empresa

Todo empleado podrá, a través de los medios establecidos para ello (Punto N° 7) entregar información respecto del incumplimiento de este Manual y/o del Código de Ética, las cuales en todos los casos deberán ser tratadas con absoluta confidencialidad y reserva.

9. Faltas a las Normativas e Incumplimiento del Manual de Conducta

Todo usuario que viole las normativas aquí descritas, se entenderá que está cometiendo una infracción al Manual de Conducta y estará sujeto a acciones disciplinarias, las que dependiendo de la gravedad de la falta, pueden significar poner término a las relaciones contractuales con la empresa, y si corresponde, incluirá la notificación a las autoridades de justicia pertinentes.

Ante cualquier duda sobre el contenido de este Manual, comunicarse con el área de Cumplimiento Corporativo, cumplimientocorporativo@security.cl.

10. Toma de Conocimiento, Aceptación y Compromiso del Manual de Conducta

Todos los empleados deberán entregar la "Declaración de Conocimiento y Aceptación del Manual de Conducta" (Anexo Nº 8) firmada y deberá ser enviada a Cultura Corporativa.

Anexo Nº 1: Norma de Acuerdo de Confidencialidad

1. Objetivo y Alcance

La empresa es responsable de la información cuyo objetivo es garantizar su disponibilidad, confidencialidad e integridad, normar el uso apropiado de los recursos físicos y/o tecnológicos de la empresa, así como garantizar la protección de la propiedad intelectual cuando corresponda.

Su alcance es cubrir aspectos de la seguridad lógica así como las consideraciones de seguridad física de todas las instalaciones correspondientes a los recursos tecnológicos, incluyendo las empresas externas que apoyan o participan en la entrega de servicios de información.

Esta norma se aplica a todas las personas autorizadas a utilizar los recursos de sistemas de información disponibles en la empresa y se considera como parte integrante del Manual de Conducta.

2. Definiciones

Por "usuario" se entenderá a toda persona autorizada para utilizar recursos de sistemas de información de la empresa. Esto incluye a todo empleado de planta, temporal a plazo fijo, así como a los miembros de las empresas que se subcontratan para prestar servicios al interior o por cuenta de la empresa.

Por "Recursos de Sistemas de Información" o "Recursos de Sistemas de Información de la empresa" se entenderá: computadores, impresoras, redes, teléfonos, paquetes de software, aplicaciones empaquetadas o desarrolladas internamente, acceso a Internet, entre otros, a los que pueda tener acceso un usuario en el normal

desarrollo de sus actividades en la empresa o bien cuando está cumpliendo con alguna comisión de servicio en la empresa.

3. Responsabilidades

Es responsabilidad de todos los "usuarios" el cumplir con las normas indicadas en este Manual.

Los gerentes, subgerentes, jefes, administradores delegados y supervisores son responsables de asegurar que todos los empleados que trabajen en sus unidades organizacionales o departamentos, conozcan y cumplan con lo estipulado en este Código.

En adición, todos los "usuarios" dentro de la empresa comparten la responsabilidad de mantener la seguridad de los recursos de información. Por tanto, si algún usuario sospecha del uso incorrecto de los recursos de los sistemas de información de la empresa o de infracciones a esta normativa, deberá informar de inmediato a la jefatura, administrador delegado de Seguridad, al área de Gestión Normativa (gestionnormativa@security.cl) y a Cultura Corporativa (culturacorporativa@security.cl).

4. Consecuencias del incumplimiento

La empresa a través de Cultura Corporativa y apoyado por el área de Seguridad, se reserva el derecho a calificar el mal uso de los "recursos de sistemas información", así como cualquier otro acto del usuario que no esté en concordancia con lo establecido en el presente Manual.

Todo usuario que viole las normativas aquí descritas, se entenderá que está cometiendo una infracción al Manual de Conducta y estará sujeto a acciones disciplinarias, las que dependiendo de la gravedad de la falta, pueden significar poner término a las relaciones contractuales con la empresa, y si corresponde, incluirá la notificación a las autoridades de justicia pertinentes.

5. Uso de los recursos de sistemas de información

La empresa proporciona sistemas de información y herramientas electrónicas, tales como acceso a Internet, servicio de correo electrónico y acceso remoto al correo de la empresa, con el objeto de facilitar y acelerar las actividades propias del negocio (Para mayor información ver Política de Seguridad de la información publicada en intranet, particularmente, a la Norma de Gestión de Comunicaciones).

Los recursos de sistemas de información de la empresa o a los que esta tenga acceso no se deben emplear para negocios ajenos a ella, ni para organizaciones de caridad, ni con ningún propósito político o religioso sin previa autorización por escrito de Cultura Corporativa.

Asimismo queda estrictamente prohibido:

- Actividades ilegales de cualquier tipo.
- Juegos y toda forma de apuestas.
- Efectuar colectas, a excepción de aquellas previamente aprobadas por Cultura Corporativa.
- Actividades con fines de lucro personal.
- Mensajes obscenos, vejatorios o abusivos.
- Actividades contrarias a la ética.
- Envío de correos electrónicos masivos o cadenas de correo.
- Creación, transmisión o recepción voluntaria de material ofensivo, difamatorio, amenazante o abusivo, que incluye pero no se limita, a comentarios basados en la raza, nacionalidad, sexo, orientación sexual, edad, discapacidad, religión o creencias políticas.
- Cualquier acción deliberada y no autorizada que dañe o perturbe los sistemas o redes de computación, que altere su rendimiento normal o produzca un desperfecto de los mismos.

• Introducción voluntaria o negligente de virus u otros programas destructivos en los computadores o estaciones de trabajo, en los sistemas y redes de la empresa o externas.

• El desciframiento, o el intento, no autorizado de cualquier sistema o contraseñas de usuarios o cualquier archivo cifrado de usuarios.

6. Confidencialidad y seguridad de la información o datos

Todos los usuarios de los recursos de sistemas de información son responsables de proteger la confidencialidad, integridad y la disponibilidad de la información que se maneja en las redes y sistemas de la empresa (Para mayor información ver Política de Seguridad de la información publicada en la intranet, particularmente, la Norma de Gestión de Activos).

Para asegurar que la información de la empresa sea debidamente protegida, el acceso a los sistemas de información sólo será otorgado basándose en las responsabilidades y deberes propios de la función de trabajo de cada usuario.

Se entiende incorporada dentro del concepto de Información Confidencial, sin que la presente enumeración pueda considerarse taxativa, toda información relacionada a los negocios, objeto o giro de la empresa, sus clientes y/o proveedores, sea técnica o no técnica, incluidas las marcas comerciales, patentes de invención, modelos de utilidad, diseños industriales, técnicas, bosquejos, dibujos, know how, procesos, aparatos, equipos y equipamiento, algoritmos, programas y documentos computacionales, y fórmulas, todo ello en relación con los productos y servicios que preste actualmente, o pueda desarrollar la empresa, relativos a la investigación; trabajo experimental; desarrollo, detalles y especificaciones de diseño e ingeniería; información financiera; requerimientos de materiales, compras y manufactura, listados de clientes; y estudios , estrategias e informaciones de mercado, ventas, comercialización y marketing.

Las siguientes acciones están prohibidas:

• Alteración o modificación de la información, excepto aquellas relacionadas con las funciones especificas de trabajo.

• Todo intento para obtener acceso o acceder a información a la que no se está específicamente autorizado.

• Uso de instalaciones de procesamiento de datos o recursos de informática de manera inconsistente con sus obligaciones laborales o incompatibles con el Manual de Conducta.

Los recursos del sistema de información y su contenido son activos de la empresa y se deben proteger contra accesos o divulgación no autorizada, modificación y destrucción. Las Jefaturas son responsables de vigilar y supervisar el uso apropiado de sistemas de información y de las herramientas de tecnologías de información disponibles.

Con excepción de lo expresamente prohibido por Ley, la empresa a través de Auditoría interna y apoyado por el área de Seguridad, se reserva el derecho de monitorear el uso de los sistemas computacionales, de leer y copiar todos los archivos o datos contenidos en las estaciones de trabajo, en cualquier momento, con o sin aviso previo.

El monitoreo se puede producir en conformidad a procedimientos administrativos internos o en el ámbito de auditorias internas o externas o bien por mandato legal.

7. Identificación de inicio de sesión para usuarios

Todos los sistemas, redes y aplicaciones computacionales, incluidos los paquetes adquiridos por la empresa, contarán con funciones de control de acceso que puedan identificar y restringir en forma exclusiva los privilegios de cada usuario (Para mayor información ver Política de Seguridad de la información publicada en la intranet, particularmente, la Norma de Control de Accesos).

Las jefaturas respectivas solicitarán los permisos de uso de los sistemas de información de acuerdo con las funciones de trabajo pertinentes, según procedimiento de creación de cuentas de usuario. Una vez otorgado el acceso, se espera que el usuario utilice estos sistemas de manera responsable en todo momento.

Es responsabilidad de los gerentes, jefes y/o administradores delegados de seguridad iniciar el proceso de "Creación de cuentas de usuario" para el personal de sus departamentos que así lo requieran. Todas las solicitudes de acceso, independiente de su tipo, se deben generar en el formulario respectivo según procedimiento establecido.

UST será responsable de monitorear todas las cuentas de acceso a servicios de cómputo activas, se bloquearán las cuentas sin uso por 60 días y se eliminarán aquellas cuentas que han estado sin uso por 90 días consecutivos.

8. Manejo de contraseñas (password)

Los usuarios deberán tomar conocimiento en la Intranet Corporativa de lo indicado en la Norma de Control de Acceso.

9. Manejo de información confidencial

La Información Confidencial le pertenece de manera exclusiva a la empresa (para mayor información ver Política de Seguridad de la Información publicada en la Intranet, particularmente, la Norma de Gestión de Activos).

Se deja expresa constancia que la titularidad y propiedad de la empresa respecto de la información confidencial, se encuentra especialmente protegida, según el caso, de conformidad con el artículo 8° de la Ley 17.366 sobre Propiedad Intelectual, y 68 y siguientes de la Ley 19.039 sobre Privilegios Industriales y Protección de los Derechos de Propiedad Industrial, sin perjuicio de las demás normas legales y reglamentarias que resulten aplicables.

Se espera que los usuarios tomen las debidas precauciones para evitar que personas no autorizadas puedan leer o modificar datos en una sesión de trabajo activa bajo su cuenta de usuario.

Los usuarios deberán terminar la sesión de trabajo (log out) o bien bloquear las estaciones de trabajo en el caso que vayan a dejar sus equipos desatendidos. Es obligatorio el uso de protector de pantalla corporativo con contraseña.

Todo archivo o documento electrónico que contenga información confidencial de la empresa se almacenará en un área segura idealmente respaldada en UST y puede adicionalmente protegerse del uso no autorizado mediante una contraseña.

Las copias impresas, por cualquier medio, de información clasificada como confidencial para la empresa deben ser identificadas como tales y almacenadas en lugares que aseguren su resguardo de usos no autorizadas. Lo anterior es responsabilidad de su dueño.

Los usuarios recuperarán oportunamente de las impresoras todo el material impreso que contenga información confidencial, para asegurarse que no esté disponible para usos no autorizados.

Toda información de carácter confidencial para el negocio debe ser respaldada periódicamente o bien mantenerse copias de seguridad en forma regular. El usuario es responsable de solicitar y asegurarse que se hagan copias de seguridad de los datos vitales almacenados en sus estaciones de trabajo locales a UST. Por su parte, UST es responsable de proveer los mecanismos necesarios para respaldar y almacenar apropiadamente las copias de seguridad de la información.

Todas las copias sobrantes de información que se generan durante la copia, impresión, microfilmación, micro-fichaje, etc. se deben destruir de forma segura y oportuna conforme a la importancia de la información. Esto se

aplica a copias electrónicas y copias impresas. La eliminación de datos privados y confidenciales requiere la trituración de los documentos físicos.

Las copias electrónicas se deben borrar de los sistemas existentes una vez que se defina que dicha información tiene que ser eliminada.

Se debe borrar toda la información contenida en los dispositivos de almacenamiento magnético de datos (como discos duros, pendrives, u otros) antes de que éstos se envíen para intercambio o servicio de mantención o bien se den de baja. El borrado debe ejecutarse de manera segura ya sea sobrescribiendo o volviendo a formatear el dispositivo, etc.

10. Correo electrónico y teléfonos

El objetivo principal de los servicios de correo electrónico (e-mail) y telefonía es ampliar las posibilidades de comunicaciones comerciales de la empresa (como complemento, revisar la Política de Seguridad de la Información publicada en la Intranet, particularmente, la Norma de Gestión de Activos y Norma de Gestión de Comunicaciones).

Las casillas de correos electrónicos proporcionados por la empresa a los usuarios, son de propiedad de Security y por tanto, independientemente de su contenido, están sujetos a los controles que estime conveniente establecer de acuerdo a lo permitido por ley. Se debe usar un lenguaje apropiado y normas de buenos modales en los contenidos de correos electrónicos, igual que en otras comunicaciones verbales o escritas que se generen en el normal desarrollo de las actividades comerciales propias de los negocios de la empresa.

Se prohíben mensajes ofensivos, degradantes o difamatorios. Los usuarios son responsables del contenido, en cualquier formato: texto, sonido o vídeo, enviado a través de Internet o correo electrónico. Todos los mensajes deben cumplir las regulaciones legales pertinentes en relación con los derechos de autor, marcas registradas y propiedad intelectual. Los mensajes deben incluir la identificación del usuario que los genera.

Según sea el caso, es posible que la ley autorice o no, que el área de Seguridad, su jefe u organismos policiales tengan acceso a correos. El monitoreo o divulgación puede producirse bajo requerimiento de auditorias, legal en un juicio u otras acciones legales vinculadas a acciones incorrectas o ilegales de una persona. La existencia de contraseñas y funciones de "borrar mensaje" no restringen ni eliminan la autoridad de la empresa para acceder a las comunicaciones electrónicas de acuerdo a ley.

Está prohibido el acceso o intento de acceso al correo electrónico de otro usuario sin la autorización por escrito del jefe o gerente inmediato.

11. Uso de Internet

El acceso a Internet se otorga a empleados, proveedores, contratistas y clientes de la compañía conforme lo ameriten las necesidades comerciales o de trabajo. La empresa se reserva el derecho a restringir el acceso a Internet según lo estime conveniente. El acceso a Internet consume recursos de infraestructura que son limitados, por lo tanto debe ser usado para apoyar actividades y responsabilidades propias del giro comercial de la empresa (para mayor información ver Política de Seguridad de la Información publicada en la Intranet, particularmente, la Norma de Gestión de Comunicaciones).

El uso aceptable de Internet para realizar funciones laborales incluye, pero no esta limitado a:

- Comunicación entre empleados y con personas externas a la empresa para fines comerciales.

- Revisión de sitios Web de proveedores para obtener información sobre productos.

- Búsqueda de información de referencia de carácter regulatoria o técnica;

- Actividades de investigación patrocinadas por la gerencia de la empresa o Cultura Corporativa.

Los usuarios deben abstenerse de toda actividad

que sea incompatible con el Manual de Conducta. En adición a lo indicado en la "Norma de Gestión de Comunicaciones" publicado en la Intranet Corporativa, las actividades específicas que están estrictamente prohibidas en el uso de Internet incluyen, pero no están limitadas, a:

• Acceso a información que no se encuentre dentro del ámbito de responsabilidades del trabajo de una persona.

• El uso de cualquier medio para obtener acceso no autorizado a un sistema o red de computación interna o externa.

• Transmisión de información de propiedad de la empresa y clasificada como confidencial, sin los controles adecuados.

• Juegos y toda forma de apuestas.

• Visita de sitios de conversación (Chat), excepto los autorizados según lo ameriten las necesidades comerciales o de trabajo y validados por el área de Seguridad.

• Uso de tecnologías no requeridas para los fines comerciales de la empresa, disponibles en Internet tales como: transmisiones de música, vídeos o televisión, etc.

Todo archivo descargado desde Internet debe revisarse para evitar el contagio de virus computacionales. Por lo general, el software de detección de virus instalado en cada computador puede realizar esta detección en forma automática, es de responsabilidad de cada usuario validar su buen funcionamiento y actualización. El usuario debe solicitar apoyo a soporte@security.cl, antes de descargar archivos si sospecha pueda contener un virus o tiene motivos para creer que el archivo representa riesgos específicos.

Es posible que las leyes sobre derecho de autor protejan información que se envíe, visualice o descargue desde Internet. La reproducción de información protegida sólo se permite si tal acción corresponde a un uso justo y autorizado por la jefatura o se basa en el permiso expreso otorgado por el propietario del derecho de autor.

Bajo ninguna circunstancia los computadores conectados a las redes de la empresa, pueden simultáneamente conectarse a Internet a través de un módem. Para mayor información consulte la sección 1.14, "Norma de Gestión de Comunicaciones" publicada en la Intranet Corporativa.

Toda pregunta sobre usos aceptables del servicio de Internet se debe dirigir al área de Gestión Normativa (gestionnormativa@security.cl).

12. Protección contra virus computacionales (Ver software sin licencia instalados en los equipos Security)

Los virus son programas computacionales que se auto-duplican y se propagan a diversos medios de almacenamiento de datos (disquetes, cintas magnéticas, etc.) o por una red. Pueden causar daños que van desde un tiempo de respuesta más lento, pérdida inexplicable de archivos, hasta una falla total de un sistema computacional. Se deben implementar controles para evitar que los virus ingresen a los sistemas computacionales y a la red de la empresa, reduciendo así al mínimo los daños causados por los virus (para mayor información ver Política de Seguridad de la Información publicada en la Intranet, particularmente, la Norma de Gestión de Comunicaciones).

En general los usuarios de los recursos computacionales deben:

• Abstenerse de instalar programas o software externos que no sean parte de los sistemas autorizados para su uso.

• Eliminar los mensajes de correo electrónico de origen desconocido. Los usuarios no deben abrir los archivos adjuntos que pudieran incluir estos mensajes de correo.

• Asegurarse que el software de protección contra

virus esté operativo en su equipo de escritorio o portátil. El cual, no se debe desinstalar de los computadores de escritorio o portátiles.

• Ante la sospecha de infección por virus, debe dejar de usar el equipo en cuestión e informar inmediatamente a la mesa de ayuda, anexo: 4357.

• Antes de distribuir archivos electrónicos a terceros, debe verificar que el archivo en cuestión no contiene virus, a fin de evitar exponer la imagen de la empresa.

13. Teléfonos de la empresa

La empresa proporciona teléfonos para apoyar la ejecución de las actividades comerciales propias del giro de la empresa. Son permitidas las llamadas para fines personales, con tarifa de llamada local, siempre que su frecuencia y duración sean razonables (como complemento ver Política de Seguridad de la Información publicada en la Intranet, particularmente a la Norma de Gestión de Activos).

Para el caso de llamadas de larga distancia (internacional), la empresa proporcionará el acceso a este servicio a los empleados que lo requieran según las funciones que desempeñan. A los usuarios de telefonía IP, se le asignará un código personal y secreto que les permitirá realizar llamadas de larga distancia en cualquier extensión telefónica de la empresa que utilice esta forma de control.

La empresa se reserva el derecho de monitorear este tipo de llamadas en cuanto al número llamado, fecha, hora y tiempo de duración de la llamada y de pedir reembolso por el costo de aquellas llamadas que considere no correspondan con las actividades del negocio.

14. Teléfonos celulares

La empresa proporcionará teléfonos celulares a aquellos empleados que por su función de trabajo así lo requieran. La empresa se reserva el derecho de auditar este servicio en cuanto al número llamado, fecha, hora y tiempo de duración cuando lo estime conveniente y de solicitar el reembolso del costo de aquellas llamadas que considere no correspondan con las actividades del negocio (como complemento ver Política de Seguridad de la Información publicada en la Intranet, particularmente a la Norma de Gestión de Activos).

15. Acceso remoto

El "acceso remoto" aumenta en forma considerable los riesgos de acceso no autorizado a la red e infraestructura computacional, de modo que se requieren estrictos mecanismos de acceso y de control (para mayor información ver Política de Seguridad de la Información publicada en Intranet, particularmente a la Norma de Gestión de Comunicaciones). Los usuarios deben cumplir las siguientes pautas básicas:

A) No es permitido instalar conexiones externas (vale decir, líneas digitales, análogas o de cable) en los recursos tecnológico de la empresa sin obtener previamente la aprobación de la gerencia respectiva y que conste de la validación del área de Seguridad. Todas las solicitudes de instalación de líneas análogas, de módem o de acceso por módem se deben remitir por escrito al área de Seguridad, unidad que realizará el proceso de aprobación de solicitudes.

B) Bajo ninguna circunstancia los computadores o dispositivos conectados a la red de la empresa, deben simultáneamente conectarse a redes externas a través de un módem. Esta situación provoca una brecha de seguridad que puede permitir el acceso no autorizado o admitir la introducción de programas destructivos a la red e infraestructura computacional de la empresa.

C) El acceso a las redes de la empresa, utilizando una conexión de Red Privada Virtual (VPN por sus iniciales en inglés) a través de Internet, debe contar con los métodos y configuración apropiada para garantizar un nivel de seguridad adecuado, tema que debe ser canalizado a través del área de Seguridad.

Otras conexiones a los sistemas e información de la empresa, requieren de la aprobación del área de

Seguridad. El acceso a las redes de la empresa a través de computadores personales de propiedad de los empleados está prohibido a no ser que se tenga previa autorización por escrito del Gerente, Cultura Corporativa y validación del área de Seguridad.

16. Hardware computacional

Los usuarios no moverán ni trasladarán equipos computacionales (computadores de escritorio, estaciones de acoplamiento, máquinas de fax, servidores de red, etc.). Los usuarios no removerán las etiquetas de "activo-fijo" de los equipos computacionales (como complemento ver Política de Seguridad de la Información publicada en Intranet, particularmente a la Norma de Gestión de Activos).

Cuando los computadores portátiles no se utilicen, se deben guardar en lo posible bajo llave o anclados. Durante viajes de negocios, los empleados deben tomar las medidas adecuadas para asegurar los equipos computacionales (no los deje afuera, ni en las habitaciones del hotel a la mano de cualquier otra persona). Durante los vuelos, los computadores portátiles se deben llevar como equipaje de mano.

Se prohíbe estrictamente a los usuarios modificar, eliminar, agregar o alterar la configuración de hardware de los equipos de la empresa.

En caso de robo o extravío por incumplimiento a las normas definidas, los empleados deberán asumir el costo del equipo.

17. Dispositivos móviles

El acceso a la información en cualquier momento y lugar se ha vuelto hoy en día parte de nuestras acciones cotidianas. Los dispositivos móviles como: iPhone, iPad, Tablets, Blackberry, Smartphone o cualquier otro que exista, en conjunto con algunas funcionalidades corporativas como Acceso al Correo y/o Aplicaciones Corporativas, Sincronización de Calendarios/Contactos y Almacenamiento/Edición de documentos, conlleva a que el negocio se mantenga competitivo en el mundo actual, de tal forma de incrementar la productividad.

Es por esta razón que se establecen los mínimos resguardos de seguridad sobre estos dispositivos (Para mayor información ver Política de Dispositivos Móviles).

Anexo Nº 2 (Parte A): Formulario de Donaciones

Empresa que realiza la donación (Área)

Nombre de quien realiza la donación

Nombre de quién autoriza la donación

Nombre de la institución que recibe la donación

Nombre del funcionario que recibe donación por la institución receptora

Tipo de Donación

- ☐ Tangible (Ej.: Materiales)
- ☐ Intangible (Ej.: HH)

Monto de la donación (Acompañar copia de respaldo: boleta, factura, etc.)

Indicar tipo de Moneda (Pesos, UF, Dólares, etc.)

Otros (Comentarios)

Fecha de la Donación (dd/mm/aaaa)

Firma de quien realiza la donación

Firma de quien autoriza la donación

Anexo Nº 2 (Parte B):
Declaración Recepción de Donaciones

Yo _____ Rut _____,
representante de la institución _____,
declaro haber recibido de parte de _____
la siguiente donación: _____
_____
_____

La cual será destinada para los siguientes fines: _____
_____
_____
_____
_____

En consecuencia, como representante de _____,
me comprometo a que la donación será utilizada para los objetivos antes mencionados.

En _____, _____ de _____ de 20____

_____
Firma representante institución

Anexo Nº 3:
Formulario de Rendición de Gastos

Yo _____, Rut _____, declaro haber recibido de parte de _____ , la suma de dinero _____ para la realización de la siguiente actividad: _____ efectuada desde el día ____ de _____ de 20_____ hasta el _____ de _____ de 20___

A continuación declaro el detalle de los gastos realizados:

Nº Boleta o Factura	**Fecha**	**Detalle**	**Moneda**	**Monto**
TOTAL				
SALDO POR PAGAR				
SALDO POR COBRAR				

Con ello, adjunto todos documentos que respaldan dichos gastos.

En _____, _____ de _____ de 20____

_____

Firma

Anexo Nº 4:
Autorización Cobro/Pago de Documentos o Adquisición de Bienes o Servicios dentro de la misma Área de Negocios

Yo *(Nombre de Jefatura)* _____,
Rut _____ me doy por enterado y autorizo la siguiente operación *(Ej.: compra de pasajes, cobro de cheques personales, etc.)* _____
_____
a favor de *(Nombre de empleado que realiza pago o cobro de documentos o adquiere el producto o servicio)* _____ la cual será realizada por *(Nombre funcionario autorizado en realizar la operación)* _____
_____.

Y declaro, que esta operación se realizará siguiendo los procedimientos establecidos.

En _____ , _____ de _____ de 20____

_____

Firma Jefatura

Anexo Nº 5:
Declaración de Personas Áreas de Adquisiciones

Yo _____, Rut _____, consciente de lo dispuesto en el Manual de Conducta y con el objetivo de mantener la transparencia en los negocios, evitar todo tipo de conflictos declaro no tener ningún tipo de interés al realizar la siguiente operación: _____
_____
_____
_____
_____.

Así mismo, declaro no tener relación de parentesco o propiedad con las empresas y/o personas que participan en este proceso.

En _____, a ____ de _____ de 20__

_____

Firma del declarante

Anexo Nº 6:
Formulario Declaración de Personas y Empresas Relacionadas

Yo _____ Rut _____, conciente de lo dispuesto en el Manual de Conducta y con el objetivo de mantener la transparencia en los negocios y evitar todo tipo de conflictos de interés, declaro tener propiedad o participación en las siguientes empresas:

Nombre	**Razón Social**	**RUT**	**% de participación**

Adicionalmente, declaro tener algún tipo de relación o parentesco en 1er grado de consanguinidad (Cónyuge, padres, hijos, etc.) con las siguientes personas:

Nombre	**RUT**	**Parentesco**

En _____, a ____ de _____ de 20___

_____

Firma del declarante

Anexo Nº 7 (Parte A): Formulario de Recepción de Activos

Yo _____ Rut _____, declaro haber recibido por parte de la empresa _____ para el desarrollo de mis funciones como _____ los siguientes materiales o activos (Celulares, Computadores, Notebooks, Teléfono Fijo, Pantallas de PC, Vehículos, Tarjetas Financieras Corporativas, teclados, credenciales, llaves, claves, etc.):

	Activo	**Cantidad**	**Modelo**
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

Adicionalmente, también declaro realizar un buen uso de estos activos procurando su correcto funcionamiento y emplearlos solo en los fines para cuales me fueron entregados.

En _____, a ____ de _____ de 20___

_____

Firma

Anexo Nº 7 (Parte B):
Formulario de Entrega de Activos

Yo _____ Rut _____, hago entrega formal de todos los activos y materiales entregados por la empresa _____ durante el periodo que me desempeñé como _____ con el propósito de mantener las buenas relaciones y evitar cualquier problema con la pérdida de alguno de estos.

Los materiales y/o activos que dejo por escrito corresponden a (Celulares, Computadores, Notebooks, Teléfono Fijo, Pantallas de PC, Vehículos, Tarjetas Financieras Corporativas, teclados, credenciales, llaves, claves, etc.):

	Activo	**Cantidad**	**Modelo**
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

En _____, a ____ de _____ de 20___

_____
Firma

Anexo Nº 8:
Declaración de Conocimiento y Aceptación del Manual de Conducta

Nombres: _____

Apellidos: _____

Rut: _____

Domicilio profesional: _____

Anexo – Teléfono: _____

Empresa: _____

Cargo: _____

Unidad: _____

Declaro conocer, comprender y aceptar el "Manual de Conducta" que he recibido y tengo en mi poder un ejemplar del mismo. Así mismo, afirmo la veracidad de los datos declarados, comprometiéndome formalmente a cumplir las normas establecidas en él.

Tengo presente, que el "Manual de Conducta" forma parte integral del contrato de trabajo y por lo tanto se entiende que representa una extensión de éste.

En _____, a ____ de _____ de 20___

_____

Firma declarante

Glosario:

Grupo: toda empresa que conforma el Grupo Security, ya sea que se trate de filiales o coligadas de Grupo Security S.A.

Empleado: todas las personas que son parte de las empresas, esto incluye al personal de planta, temporales a plazo fijo, así como a los miembros de las empresas que se subcontratan para prestar servicios al interior o por cuenta de la empresa.

MMIIM: Manual de Manejo de Información Interna de Mercado, documento interno de Grupo Security que fue aprobado por el Directorio el 25 de marzo de 2010 y se encuentra disponible en la intranet.

Operaciones: denominación genérica de los negocios y transacciones que se realizan ya sea dentro o fuera de la empresa, reguladas o no reguladas.

Información Confidencial: toda información relacionada a los negocios, objeto o giro de la empresa o empresas del Grupo Security, sus clientes y/o proveedores, sea técnica o no técnica, incluidas las marcas comerciales, patentes de invención, modelos de utilidad, diseños industriales, técnicas, bosquejos, dibujos, know how, procesos, aparatos, equipos y equipamiento, algoritmos, programas y documentos computacionales y fórmulas, todo ello en relación con los productos y servicios que preste actualmente, o que pueda desarrollar la empresa, relativos a la investigación, trabajo experimental, desarrollo, detalles y especificaciones de diseño e ingeniería; información financiera; requerimientos de materiales, compras y manufactura, listados de clientes; y estudios, estrategias e informaciones de mercado, ventas, comercialización y marketing.

Información Interna: (información de interés para el mercado) toda aquella que no es de conocimiento público y que podría incidir en la respuesta a la siguiente pregunta: ¿Sería dicha información determinante respecto a alguna decisión de negocios?

Conflicto de interés: una situación en virtud de la cual una persona, en razón de su actividad, se enfrenta a distintas alternativas de conducta con relación a intereses incompatibles, ninguno de los cuales puede privilegiar en atención a las obligaciones legales o contractuales. Se considera que hay conflicto de interés cuando existe una situación en la cual se puede decidir si beneficiar:

- La utilidad propia o la de un cliente.
- La utilidad de un tercero vinculado a la empresa o la de un cliente.
- La utilidad de una cartera administrada o la de un cliente.
- La utilidad de un tercero vinculado a un empleado de la empresa o la de un cliente.
- La utilidad de una operación o la transparencia del Mercado.
- La utilidad de una cartera administrada o la propia.

LMV: ley 18.045 del Mercado de Valores.

Valores: (Art. 3 LMV) cualquier título transferible incluyendo acciones, opciones a la compra y venta de acciones, bonos, debentures, cuotas de fondos mutuos, planes de ahorro, efectos de comercio y, en general, todo título de crédito e inversión.

Títulos: valores de oferta pública susceptibles de ser transados en el mercado financiero.

Operaciones personales: todas aquellas transacciones realizadas por los empleados para sí, teniendo como contraparte la empresa o las empresas del Grupo Security, u otra entidad del Mercado.

Operaciones por cuenta propia: todas aquellas transacciones realizadas en el mercado por el área de inversión para sí.

GRUPO | security