Políticas de seguridad informática.

Claves de acceso

Longitud mínima de las claves de acceso

La longitud de las claves de acceso debe de ser mínima de ocho (8) caracteres y debe de incluir combinación de letras mayúsculas, minúsculas y números.

Claves de acceso difíciles de adivinar.

Todas las palabras claves de acceso escogidas por los empleados para ingresar a los sistemas deben ser difícil de identificar.

En general, no se deben utilizar palabras de un diccionario, derivados del usuario-ID, series de caracteres comunes tales como “123456” o nombres como “PROINGRA”. Así mismo, no se deben de emplear detalles personales como nombre del conyugue, placas de vehículos o fechas de cumpleaños a menos que estén acompañados de caracteres adicionales que no tengan ninguna relación.

Cambio periódico obligatorio de claves de acceso.

Los empleados deben de hacer cambio de sus claves de acceso cada 3 meses.

- Utilización de claves de acceso diferentes cuando se tiene acceso a mas de un sistema.

Si un empleado tiene acceso a varios sistemas de información, se deben de emplear claves de acceso diferentes para cada uno de estos sistemas.

No se deben de compartir claves de acceso.

Bajo ninguna circunstancia los empleados deben de compartir o revelar sus claves de acceso a usuarios no autorizados. Al hacerlo, se expone al usuario autorizado a responsabilizarse de acciones que otras personas hagan con la clave de acceso. Si los empleados necesitan compartir información permanente del computador, ellos deben de usar correo electrónico, directorios públicos, en los servidores de red del área local u otros mecanismos.

Cambio de clave de acceso cuando se sospeche que esta ha sido descubierta.

Todas las palabras claves se deben de cambiar tan pronto como se sospeche que han sido descubiertas o que podrían conocerlas personas no autorizadas.

Los empleados son responsables de todas las actividades involucrando su identificación dentro de la organización.

Los empleados son responsables de todas las actividades llevadas a cabo con su identificación como empleado. Por ejemplo, su correo electrónico empresarial. Los empleados no deben de permitir que otros realicen ninguna actividad con sus sistemas.

Log-off (Fuera del login) de los computadores personales conectados a las redes.

Si los computadores personales (PC) están conectados a una red, cuando no estén en uso se debe de salir siempre de todas las aplicaciones a las que haya ingresado y no exponer el computador a ingresos no autorizados.

Uso de los sistemas

Uso personal del computador y sistemas de comunicación.

El computador que le es asignado a cada empleado en la empresa y los sistemas de comunicación deben de usarse solamente para asuntos de la empresa.

Alteraciones/Expansiones hechas a los computadores dotados por la Empresa.

Los equipos de cómputo asignados por la empresa no deben de ser alterados ni mejorados en ninguna forma (ejemplo: Actualización de procesador, expansión de memoria o adición de otras tarjetas) sin el conocimiento y autorización del responsable del departamento en el cual se labora.

Reporte de los daños de Hardware – Software pertenecientes a la empresa.

Los empleados deben de reportar inmediatamente a los administradores o a sus jefes inmediatos sobre cualquier daño o perdida del equipo, software o información que tengan a su disposición y que sean propiedad de la empresa.

No se deben de almacenar juegos en los computadores de la empresa.

No deben de almacenarse ni usarse juegos en ninguno de los sistemas o del computador de la empresa.

Permiso para uso personal ocasional de los sistemas de la empresa.

Los sistemas de información de la Empresa deben usarse solamente para trabajos relacionados con las actividades de la misma. El uso personal ocasional puede permitirse si:

A. no se consume más que una cantidad mínima de los recursos que podrían, en otra forma, usarse para asuntos de negocios
B. no interfiere con la productividad del trabajador
C. no se apropia de ningún tipo de actividad comercial.

Si esta exploración es para fines personales, debe hacerse en sus horas libres, y no en horas de trabajo de la Empresa. Así mismo, noticias, grupos de discusión, y otras actividades que definitivamente no están dentro de sus obligaciones laborales, deben hacerse en las horas libres del empleado y no en horas de trabajo.

Conceder acceso a correos electrónicos corporativos a extraños de la organización.

No se puede conceder, o dar cierto tipo de prerrogativas con los códigos de identificación de usuarios a individuos que sean colaboradores retirados, proveedores o consultores para usar los computadores de la empresa o de los sistemas de comunicación.

Las prerrogativas de acceso a los sistemas de información se terminan cuando el trabajador se retira de la empresa

Todas las prerrogativas para el uso de los sistemas de información de la empresa deben de terminar cuando se tenga conocimiento que el trabajador se retira de la empresa.

Cambios en la configuración del software instalado en los equipos de computo

No está permitido el cambio en la configuración estándar del software instalado en los equipos de cómputo, tales como:

- Configuraciones de red
- Unidades de red
- Configuraciones de dispositivos (impresoras, scanner).

Administración de control de acceso a la información

Controles de acceso a los computadores principales

Toda la información de los computadores principales (servidores) que sea sensible, critica o valiosa debe tener controles de acceso al sistema para garantizar que no sea inapropiadamente descubierta, modificada o borrada.

Capacidades del usuario para el acceso de archivos y su implicación en cuanto al uso

Los usuarios no deben leer, modificar, borrar o copiar un archivo que pertenezca a otro usuario, sin obtener primero permiso del propietario del archivo. A menos que el acceso general haya sido claramente proporcionado, la habilidad para leer, modificar, borrar, o copiar un archivo que pertenezca a otro usuario no implica que el usuario tenga permiso para realizar estas actividades.

Actividades administrativas

Revisión periódica y reevaluación de los privilegios de acceso del usuario.

La Administración debe reevaluar el otorgamiento de los privilegios de acceso a los sistemas a todos los usuarios como máximo cada seis (6) meses.

Reportes sobre cambios de tareas y responsabilidades.

La Dirección de Gestión Humana y Administrativa o los directores de área, deben informar oportunamente al área de Tecnología sobre todos los cambios de tareas y responsabilidades operativas o administrativas de los colaboradores, retiros e ingresos de nuevos colaboradores, a los administradores de los sistemas de información y del sistema de seguridad para que actualicen, controlen y administren los códigos de identificación de usuarios.

Virus informático

La eliminación de virus informáticos por parte de los usuarios finales requiere ayuda del administrador del sistema

Se prohíbe a los usuarios finales eliminar virus informáticos de los sistemas de la Empresa, cuando éstos están infectados, en razón de que pueden producir más daños en la información o programas o permitir una reinfección sobre éstos, se debe informar a la gerencia.

No se debe bajar y cargar Software de Internet en los sistemas corporativos por parte de terceras personas

Los colaboradores de la empresa no deben de permitir que terceros descarguen softwares en los computadores o sistemas otorgados por la misma. Esta prohibición es necesaria porque dicho software puede contener virus, lombrices, caballos Troyanos y otro malware que puede dañar la información y los sistemas.

Pruebas de virus antes de usar los programas en la Empresa

Para prevenir la infección por virus en los computadores, los colaboradores de la Empresa no deben usar ningún software proporcionado externamente por una persona u organización que no sea un proveedor conocido y confiable. La única excepción a esto, es cuando el software ha sido primero probado y aprobado.

Los medios magnéticos proporcionados externamente deben ser previamente examinados contra la presencia de virus

Cualquier medio magnético proporcionado externamente (como memorias USB o discos duros externos), no pueden utilizarse en ningún computador personal (PC) o servidor de la red local (LAN) de la Empresa, a menos que estos medios hayan sido primero examinados contra virus.

Verificación del software antes de distribuirlo a los usuarios

Antes de distribuir cualquier software a los usuarios, los colaboradores de la Empresa deberán primero someterlo a pruebas exhaustivas, incluso a pruebas que identifiquen la presencia de virus en la computadora.

Manejo del computador

No se debe trasladar los equipos de cómputo

Ningún usuario puede trasladar, desconectar o conectar equipos de cómputo sin la autorización y supervisión de los administradores de TI.

No se debe modificar la configuración del Software Base o de los equipos de computo

Ningún usuario debe modificar la configuración del software base (Sistemas operativos, programas antivirus, programas de Mail) como tampoco modificar la configuración de los equipos de cómputo a través del setup de la máquina.

Apagar los equipos de cómputo al terminar las labores

Todos los equipos de cómputo del área se deben apagar al terminar la jornada laboral. Esto evita el uso indebido de los equipos por parte de personas extrañas o ajenas al área, alarga la vida útil del equipo, evita daños por un apagado incorrecto y contribuye al ahorro de energía.

Problema o funcionamiento anormal que se presente en la operación de un equipo de Cómputo

Los usuarios deben reportar inmediatamente a los administradores de TI cualquier problema técnico que se presente en la operación de un equipo de Cómputo, indicando en la forma más detallada y exacta el tipo de problema presentado.

Apagar correctamente los computadores.

Todos los usuarios deben apagar correctamente los computadores, a través del siguiente proceso: Botón “Inicio/Apagado” > la opción “Apagar”.

Seguridad de los datos

La información se considera el recurso más importante de la Empresa

Es absolutamente esencial que la Empresa proteja la información para garantizar su exactitud, oportunidad y confiabilidad. La información deberá ser manejada adecuadamente y ser accesible sólo a las personas autorizadas, de acuerdo con

los manuales de funciones de cada uno de los colaboradores, las normas, políticas y procedimientos corporativos.

Todos los derechos de propiedad sobre el software y la documentación desarrollada para uso corporativo son exclusivos de la Empresa.

Sin excepción alguna, todo el software (Paquetes Office, sistemas contables) y su documentación generada y desarrollada por colaboradores, consultores, proveedores o contratistas para el beneficio y uso corporativo, es propiedad exclusiva de la Empresa.

Adquisición de software

Siempre que la empresa haya adquirido un software integral, el proveedor deberá proporcionar por escrito la licencia del software y donde certifique la adquisición del mismo.

No se debe copiar, transferir o divulgar software.

Los colaboradores no deberán copiar software proporcionado por la Empresa en ningún medio de almacenamiento magnético o transferir Software de un equipo a otro a través de algún sistema de comunicación, o divulgar software.

No se debe usar herramientas para romper la seguridad de los sistemas.

Los colaboradores de la Empresa no deberán adquirir, poseer, comercializar o usar herramientas de hardware o software que pudieran emplearse para evaluar o comprometer la seguridad de los sistemas de información. Si la Empresa considera

utilizar este tipo de herramientas tecnológicas para la evaluación de la seguridad de los sistemas, deberán ejecutarse en el ambiente de pruebas.

Manejo de la información confidencial de propiedad de terceros.

Toda información confidencial o de propiedad de un tercero, que se ha confiado a la Empresa, deberá ser protegida por una política de confidencialidad corporativa.

No se debe transferir información corporativa a terceros sin la autorización de la Gerencia.

El software de la Empresa, su documentación y otros tipos de información interna, no deben ser enviados o trasladados a sitios o personas que no son de la Empresa, sin la autorización de la Gerencia.

El derecho para examinar los datos guardados en los sistemas de la Empresa

La dirección se reserva el derecho de examinar todos los datos guardados o transmitidos en sus sistemas, como las computadoras y los sistemas de comunicaciones de la Empresa.

Restricción de revelar información particular de los colaboradores.

La Empresa no revelará los nombres, títulos, números de teléfono, localización u otra información particular de sus colaboradores a menos que sea requerido para propósitos del objeto social de la Empresa. Se harán excepciones cuando dicha revelación sea exigida por ley o cuando las personas involucradas hayan consentido previamente tal revelación de la información.

Seguridades para la entrega de información de clientes a terceros

La información recolectada de los clientes, tal como número telefónico y dirección, se debe usar para propósitos internos de la Empresa y se deberá entregar a terceras partes solo si:

- El cliente ha proporcionado su consentimiento anteriormente por escrito

- Por solicitud escrita de Empresas gubernamentales o entes de control.

Confidencialidad de los datos

Confidencialidad de la Información.

Toda la información que tenga carácter confidencial, en los términos establecidos en la ley, deberá enmarcarse en lo establecido en el Código de Ética y Transparencia Empresarial.

Aprobación de la Gerencia General para destruir registros de información

Los colaboradores no deben destruir o disponer de la información que es potencialmente importante para la Empresa sin tener una aprobación específica. El individuo que realice intencionalmente una destrucción no autorizada de los registros o información de la Empresa estará sujeto a acciones disciplinarias incluyendo la terminación del contrato y procesos legales. Los registros y la información se deben conservar sí:

a) Son necesarios en el futuro
b) Las leyes o los estatutos requieren su conservación
c) En caso de que puedan ser necesitados como pruebas en investigaciones de actos ilícitos, no autorizados o abusos.

Información al público

Toda información al público como páginas de inicio, carteleras electrónicas, propaganda en medios escritos y hablados de la Empresa debe ser validada con la Gerencia.

Censura de información divulgada por los medios de comunicación de la Empresa

La administración de la Empresa se reserva el derecho de censurar cualquier tipo de información a través de los medios de comunicación y computadores de la Empresa. Las facilidades de comunicación de la Empresa son privadas y no de dominio público.

Derecho de la administración de la Empresa a remover material de tipo ofensivo o ilegal

La administración de la Empresa se reserva el derecho a remover de sus sistemas de información, cualquier material que pueda ser ofensivo o ilegal.

Persecución étnica, sexual y racial a los colaboradores

La persecución étnica, racial o sexual incluyendo llamadas telefónicas anónimas, números privados y mensajes de correo anónimos está estrictamente prohibidas y pueden causar sanciones e incluso la terminación del contrato de un colaborador. La administración debe hacer que esta política sea clara a todos los colaboradores e investigar en forma inmediata cualquier ocurrencia sospechosa.

Seguridad en comunicaciones

Mecanismos de control de acceso para computadores conectados a la red

Todos los computadores de la Empresa que puedan ser accedidos por terceros a través de mecanismos como: líneas conmutadas, Internet y otros, deben ser protegidos por mecanismos de control de acceso aprobados.

La conexión a Internet requiere implementar un mecanismo de firewall aprobado y certificado

Toda conexión entre los sistemas de comunicación de la Empresa e Internet o cualquier red pública de datos debe incluir un Firewall y otros mecanismos adicionales de control de acceso.

Cualquier comunicación externa vía módems o cualquier otro medio de comunicación debe estar aprobada

Los colaboradores y contratistas no deben llevar a cabo ningún tipo de instalación de nuevas líneas telefónicas o canales de transmisión de datos sin haber sido formalmente aprobados por la gerencia.

Requisitos de seguridad para trabajar desde la casa o sitio de residencia

El trabajo desde la casa es una decisión del jefe del área responsable. Para ello se deben tener en cuenta las siguientes consideraciones: Seguridad física e informática para los recursos de la Empresa, un ambiente de trabajo ameno, procedimientos para evaluar el rendimiento del empleado y mecanismos apropiados para estar en contacto con otros colaboradores.

Divulgación de números de cuentas bancarias

Los números de cuentas bancarias de los clientes son confidenciales y no deben ser divulgadas a terceros sin ser aprobados por la gerencia.

Conexiones remotas a los computadores de la Entidad (por ejemplo, con TeamViewer)

No están permitidas las conexiones remotas a computadores de la entidad a través de herramientas como por ejemplo TeamViewer. Este tipo de conexiones deben ser previamente autorizadas por el área encargada.

Sistemas telefónicos

Uso de teléfonos para uso personal

Los teléfonos de una Empresa tienen la función de facilitar las actividades comerciales, no deben ser utilizados para propósitos personales, a menos de que estas llamadas no puedan efectuarse fuera de las horas de trabajo. En estos casos las llamadas personales deben ser de corta duración con excepciones a ocurrencias de fuerza mayor.

Sistemas de correo electrónico

Asignación y responsabilidades sobre el uso del correo Electrónico

Políticas:

- Los colaboradores de la empresa C.I PROINGRA S.A.S deben emplear las direcciones de correo electrónico corporativas asignadas para atender los asuntos de la Entidad.
- Todos los colaboradores y contratistas de apoyo a la entidad tienen derecho a tener una cuenta de correo institucional.

- Cada usuario debe depurar continuamente su buzón de correo con el fin de mantener espacio disponible para la recepción de nuevos mensajes.
- Cada usuario es responsable de la información enviada y reenviada desde su cuenta de correo.

Restricciones sobre el uso de correos masivos

No está permitido el envío de correos a "Todas las dependencias" o a un grupo de usuarios, cuyo contenido no sea de carácter institucional. En caso de requerirse envío de información institucional a "Todas las dependencias" o a un grupo de empleados, solo se puede realizar con previa autorización de la gerencia o del encargado de comunicados corporativos.

Usando una Cuenta de Correo Electrónico Asignada a Otro Individuo

Los colaboradores no deben utilizar una cuenta de correo electrónico que ha sido asignada a otro individuo ni para enviar ni para recibir información. Si hay necesidad de leer el correo de otra persona (por ejemplo, cuando están en vacaciones), remisión de mensajes a otra dirección u otros métodos pueden ser usados preferiblemente.

Autorización para leer correo electrónico de otros colaboradores

Cuando el jefe de un área y la gerencia estén colectivamente de acuerdo, los mensajes de correo electrónico viajando a través de los sistemas de la Empresa pueden ser monitoreados para cumplir con políticas internas, por sospechar la actividad criminal, y otras razones de sistemas de gerencia. A menos de que este trabajo sea específicamente asignado por los gerentes, el monitoreo de los mensajes de correo electrónico está prohibido por cualquier otro trabajador.

Los mensajes de correo electrónico son registros de la empresa.

El sistema de correo electrónico de la Empresa debe ser usado únicamente para propósitos de trabajo. Todos los mensajes enviados por medio del correo electrónico son registros de la Empresa, quien se reserva el derecho de acceder y revelar todos los mensajes enviados por medio del sistema de correo electrónico para cualquier propósito. Los supervisores deben revisar las comunicaciones de correo electrónico de los colaboradores supervisados para determinar si han atentado contra la seguridad, violado políticas de la Empresa o ejecutado cualquier otra acción no autorizada.

La Empresa también debe revelar los mensajes electrónicos a los oficiales de la ley sin notificación previa a los colaboradores que hayan enviado o recibido este tipo de mensajes.

Autorización para hacer público un mensaje a través del correo electrónico y correo de voz.

La herramienta de envío de mensajes masivos a través de correo electrónico y correo de voz pueden ser utilizadas o aprobadas por la alta gerencia

Propiedad intelectual y seguridad en sitios de trabajo alternos

Protección de la propiedad de la Empresa en sitios de trabajo alternos

La seguridad de la propiedad de la Empresa, en sitios de trabajo alternos es tan importante como lo es en las oficinas centrales. En sitios de trabajo alterno, se deben tomar precauciones razonables que puedan proteger contra robo, daño y/o mal uso a los equipos, el software y la información.

Derechos a Propiedad Intelectual desarrollados en sitios de trabajo alternos

La propiedad intelectual desarrollada o concebida mientras el trabajador se encuentre en sitios de trabajo alternos, es propiedad exclusiva de la Empresa. Esta política incluye patentes, derechos de reproducción, marca registrada y otros derechos de propiedad intelectual según lo manifestado en memos, planes, estrategias, productos, programas de computación, documentación y otros materiales.

Ambientes de trabajo estructurados y telecomunicaciones

Para mantener el privilegio de hacer trabajos por fuera, todas las telecomunicaciones deben estructurar su ambiente remoto, para cumplir con las políticas y estándares de la Empresa.

Conexiones de internet

Restricciones en el uso del internet.

No está permitido el ingreso a páginas de internet que no estén relacionadas con las funciones y responsabilidades de colaboradores o contratistas, tales como:

- Páginas pornográficas, así como aquellas que patrocinen personas u organizaciones al margen de la ley o que tengan algún contenido ilegal (Compra de armas, trata de personas)
- Descargar programas que faciliten conexiones automáticas.
- Páginas de música o videos en línea
- Descargar música y videos, provistos por páginas especializadas para tal fin.
- Utilizar o participar en juegos de entretenimiento en línea.

- Descargar o instalar programas diferentes a los autorizados por la entidad.
- Modificar los paquetes y configuraciones ya instaladas en los computadores de la empresa.

Enviar información de seguridad y pagos a través de internet

Los colaboradores no deben enviar números de tarjetas de crédito, clave de entrada o cualquier otra información de seguridad o pagos por medio del correo electrónico de Internet si esta está en forma legible (no encriptada).

La Empresa bloquea el acceso a ciertas páginas en internet que no tienen que ver con negocios

Los sistemas de información de la Empresa rutinariamente previenen a los usuarios de conectarse a determinadas páginas de Internet no relacionados con las actividades de la misma. Los colaboradores que encuentren que se pueden conectar a páginas de Internet que tengan contenidos sexuales, racistas o cualquier otro tipo de material ofensivo deben desconectarse inmediatamente de ese sitio e informar a la gerencia.

Manejo de software y archivos bajados de Internet

Todo el software y archivos bajados desde fuentes diferentes a la Empresa a través de Internet (o cualquier otra red pública) deben ser protegidos con software de detección de virus. Esto debe realizarse antes de empezar a ejecutar el programa.

Publicación de Material de la Empresa en el Internet

Los usuarios no deben publicar material de la Empresa (software, memos internos, publicaciones de prensa, etc.) en ningún computador que tenga acceso público a

Internet y que pertenezca al sistema, a menos que la publicación haya sido aprobada con anterioridad por el director de servicio al cliente.

Intercambio de Información en Internet

Software, documentación y cualquier otro tipo de información interna de la Empresa no debe ser vendida o transferida a ninguna parte que no pertenezca a la Empresa, para ningún propósito diferente al del negocio expresamente autorizado la gerencia. No se debe dar el intercambio de software y/o datos entre la Empresa y una tercera parte a menos que se haya llegado a algún acuerdo escrito y éste haya sido firmado por el área encargada. Dicho acuerdo debe especificar tanto los términos del intercambio, como las formas en que el software y/o los datos deben ser manejados y protegidos.

Cargar Software a Otras Máquinas por medio de Internet

Los usuarios no deben cargar software que haya sido licenciado por terceros, o software que haya sido desarrollado por la Empresa, a ningún computador a través de Internet a menos que se tenga una autorización previa de la gerencia.

Actualizar Información de la Empresa a través de Internet

Los usuarios que se conecten a los sistemas de la Empresa utilizando Internet no están autorizados a modificar directamente ninguna información de la Empresa.

Reporte de problemas de seguridad

Reporte Interno de Violaciones y Problemas en la Seguridad de la Información

Los colaboradores de la Empresa tienen la tarea de reportar todas las violaciones y problemas con la seguridad de la información a la gerencia en un tiempo prudente para que así se pueda tomar una acción que los solucione prontamente.

Centralización de los reportes relacionados con problemas en la seguridad de la Información

Todas las vulnerabilidades conocidas además de todas las violaciones evidenciadas deben ser comunicadas en forma rápida al área encargada de Tecnologías de la información. Adicionalmente, todas las revelaciones de información de la Empresa no autorizadas, deben ser reportadas a los propietarios de información involucrados.

Está estrictamente prohibido reportar violaciones de seguridad, problemas o vulnerabilidad a cualquier parte fuera de la Empresa (exceptuando auditores externos) sin la previa aprobación escrita.

Interferencia al reporte de problemas en la seguridad de la Información

Cualquier intento de interferir, prevenir, obstaculizar o disuadir a un miembro del personal en su esfuerzo por reportar posibles problemas o violaciones en la seguridad de la información está estrictamente prohibido y es causal de acciones disciplinarias. Cualquier forma de retaliación contra reportes individuales o investigaciones acerca de problemas o violaciones en la seguridad de la información también está prohibida y causa acción disciplinaria.

Reporte externo de violaciones en la seguridad de la información

Si es requerido por la ley o regulaciones, la administración debe informar a las autoridades externas (PONAL, FISCALIA), lo más pronto posible, acerca de violaciones en la seguridad de la información. Si no existe este requerimiento, realizado en conjunto con las Direcciones Jurídica y de Control Interno, la administración debe sopesar las ventajas y desventajas de revelar externamente antes de reportar estas violaciones.

Reporte de mal funcionamiento en el software requerido

Todo el mal funcionamiento aparente en el software debe ser reportado inmediatamente al gerente en línea o al proveedor de servicios del sistema de información.

Investigación requerida por evidencias de delitos

Cuando se demuestren evidencias claras de que la Empresa ha sido victimizada por un delito de computador o comunicaciones, se debe llevar a cabo una investigación. Esta investigación debe proveer información suficiente para que el administrador pueda tomar pasos que aseguren que:

a) Dichos incidentes no se puedan presentar nuevamente,

b) Se hayan restablecido medidas de seguridad efectivas.

Selección de controles

Suministro de Hardware y Software únicamente a través de los canales de compra establecidos.

Brahman S.A.S.
Sabemos darle calidad a sus productos
GRUPO EMPRESARIAL Proingra

Para garantizar conformidad con los estándares de seguridad de información propios, se debe conseguir todo el hardware y software a través de canales estándares de compra.