

POLÍTICA GLOBAL: SALVAGUARDA DE LOS ACTIVOS Y RECURSOS DE LA EMPRESA.

Esta Política establece los requisitos para la administración responsable de los riesgos y recursos de la Compañía. Nos proporciona un marco de referencia a seguir para las funciones y los responsables al implementar y mantener los controles internos que cubran aspectos financieros, de compras (incluyendo gastos de viaje) y seguridad (incluyendo información, empleados y productos)

¿A QUIÉN APLICA ESTA POLÍTICA?



Todo el personal tiene la responsabilidad de actuar de manera apropiada y responsable










Los gerentes tienen la responsabilidad de asegurarse que los controles internos se encuentren operando.



Para cumplir con esta Política, se espera que todas las áreas SET sigan las directrices y procedimiento globales y que sus directrices y procedimientos locales sean consistentes con esta política.

PRINCIPIOS CLAVE

-  La Compañía está comprometida a salvaguardar los activos y recursos de AZ en nombre de sus accionistas, comprendiendo los riesgos clave relacionados al negocio y estableciendo y manteniendo las responsabilidades y la rendición de cuentas de manera clara para su administración.
-  Debemos operar y mantener un sistema de control interno robusto que esté diseñado para promover la eficiencia, prevenir los fraudes y ayudar a asegurar la confiabilidad de los estados financieros y el cumplimiento de las leyes y regulaciones aplicables.
-  Cada área SET/ funcional debe asegurar que los planes de negocio tienen la flexibilidad para manejar eficientemente las amenazas al negocio
-  También debemos asegurarnos que todas las compras, incluyendo gastos de viaje, están de acuerdo con nuestros objetivos de negocio. Todo el personal tiene la responsabilidad de poner la debida atención al momento de ejercer los recursos de AZ al realizar compromisos financieros en su nombre.
-  Todo el personal tiene la responsabilidad de proteger la información y registros de AZ y de terceros, y los sistemas electrónicos, redes de comunicación y recursos informáticos.
-  La seguridad de las personas, sistemas y productos debe ser salvaguardada.
-  Cada área SET/funcional debe utilizar el marco de referencia especificado en esta política cuando desarrolle e implemente sus controles y políticas.

- 🔗 Cada área SET/ funcional debe designar que gerentes deben desarrollar, implementar y evaluar las normas y procedimientos que cubran el área de la Compañía de la cual son responsables.

RIESGO

Manejo del riesgo

La Compañía esta comprometida a manejar el riesgo de manera efectiva para cumplir los siguientes objetivos.

- 🔗 Salvaguardar la inversión del accionista y proteger el patrimonio de la Compañía.
- 🔗 Ayudar al cumplimiento de los objetivos
- 🔗 Asegurar el cumplimiento de la legislación aplicable.

Para ese fin, esta política y los procedimientos asociados especifican los requisitos mínimos para identificar, priorizar, administrar y reportar los riesgos que enfrenta la Compañía.

El alcance de esta Política de Manejo de Riesgos cubre todo tipo de riesgos, incluyendo riesgos estratégicos, de operación/ejecución y de cumplimiento.

Los resultados de la aplicación efectiva de esta Política de Manejo de Riesgos son:

- 🔗 La comprensión clara de la rendición de cuentas y responsabilidades para el manejo del riesgo y de la supervisión.
- 🔗 La comprensión y el manejo efectivo de los riesgos relacionados a las estrategias corporativas y de negocio.
- 🔗 La comprensión y el control adecuado de los riesgos de no cumplir con las políticas, regulaciones y leyes locales.
- 🔗 El impacto de los riesgos es evaluado midiendo como un riesgo en particular, en caso de que ocurriera, podría afectar negativamente el valor de la empresa.
- 🔗 La mitigación y la fortaleza de los planes de negocio para los riesgos importantes son adecuadamente especificados, ejecutados y monitoreados.
- 🔗 El reporte de los riesgos y como fueron controlados es preciso, relevante y en tiempo.
- 🔗 La escalación adecuada de los riesgos potenciales se cumple utilizando criterios claros, integrados al proceso de negocios.

Los procedimientos y requisitos para el manejo de riesgos y su reporte están detallados en el Procedimiento Global: Proceso y Reporte de riesgos AstraZeneca.

Fortaleza del Negocio

AstraZeneca está comprometida a prepararse lo mejor posible para continuar los procesos críticos de negocio en el caso que ocurriera una importante interrupción en las actividades de negocio, y de manejar el impacto en su reputación en cualquier interrupción potencial con las partes internas y/o externas interesadas.

La Fortaleza del Negocio se basa en tener planes específicos implementados para minimizar el impacto de una interrupción potencial en las actividades de negocio, para esas amenazas clave identificadas durante los procesos de evaluación del riesgo.

La responsabilidad de la rapidez y la planeación de la respuesta, para tener las capacidades adecuadas, y proveer seguridad para la adecuación de los planes a nivel directivo, se deposita en los gerentes en línea del nivel directivo. La responsabilidad de proveer seguridad a nivel directivo para la adecuación de los planes de cada área se deposita en la persona apropiada.

Para asegurar una cobertura coherente de los procesos críticos de negocios, los dueños de los procesos críticos, identificados a través de evaluaciones de riesgos de negocio, están obligados a desarrollar, aprobar y mantener la fortaleza de los planes de negocio apropiados para su parte del negocio.

La fortaleza de los planes de negocio comprende todo o algo de lo siguiente, dependiendo de la naturaleza de la actividad de negocios y las amenazas hacia ellas.

Continuidad del Negocio

La Gestión de Planeación de la Continuidad del Negocio se refiere a la continuidad de los procesos críticos de negocio en el caso de una interrupción a estos que afecten personas, el espacio de trabajo y/o tecnología.

Manejo de Crisis

El manejo de crisis es una serie de actividades dirigidas a los altos directivos diseñadas para dirigir, administrar y resolver o terminar, rápida y efectivamente, cualquier interrupción que tenga el potencial de afectar de manera negativa al negocio y su reputación.

Recuperación en Desastres




El Plan para Recuperación en Desastres se refiere a la recuperación de los sistemas de información críticos que sostienen el negocio.

Respuesta en Emergencias







La Respuesta en Emergencias es el conjunto de acciones que se realizan para estabilizar incidentes que tengan el potencial de lastimar personas, dañar o contaminar la propiedad o interrumpir la operación del negocio.

CONTROLES FINANCIEROS INTERNOS, REGULATORIOS Y OPERATIVOS

Los gerentes dentro de cada área SET/ funcional son responsables por el desarrollo, implementación, la operación en curso y monitoreo de los controles financieros de cada función para asegurar los siguientes objetivos:

-  La operación efectiva y eficiente de las áreas SET/funcionales.
-  Información financiera que opere con integridad, confiabilidad, precisión, transparencia y oportunidad.
-  El cumplimiento de las normas, leyes y regulaciones aplicables.

La Compañía operará sus procesos de control interno de acuerdo a componentes interrelacionados.

-  Un entorno de control que abarque valores, procesos y habilidades que aseguren que las transacciones financieras sean registradas y reportadas de manera precisa y esto incluye:
 - > Un compromiso con la integridad, los valores éticos y la competencia
 - > Filosofía de Dirección y un estilo de funcionamiento
 - > Delegación de autoridad y responsabilidad
 - > Participación y dirección por el Consejo de Directores de AstraZeneca PLC
-  Actividades de control que:
 - > Incluyan el establecimiento de políticas y procedimientos que aseguren que los lineamientos de la administración se lleven a cabo, y
 - > Abarquen un rango de actividades, incluyendo aprobaciones, autorizaciones, verificaciones, conciliaciones, revisiones del desempeño operativo, seguridad de los activos y la separación de funciones.
-  Procesos de información y comunicación que aseguren que la información pertinente fue identificada, procesada y comunicada en una forma y tiempo que permita al personal realizar sus responsabilidades.
-  Sistemas de Información que sean diseñados y establecidos para producir reportes que contengan información operativa, financiera y relacionada al cumplimiento para operar y controlar el negocio.
-  El monitoreo que evalúe la efectividad del sistema de control interno en el tiempo a través de actividades de vigilancia, evaluaciones separadas o una combinación de ambas.
-  Notificación de deficiencias en el sistema de control interno a la alta dirección, al Comité de Auditoría y al Consejo, y acciones correctivas que aseguren el proceso de mejora continua del sistema.

ANTIFRAUDE

La Compañía no tolera el fraude. Tomaremos todas las medidas razonables para prevenir que la Compañía sea víctima de un fraude, y no toleraremos ningún fraude perpetrado en nuestro nombre.

Donde sea detectado un fraude, la Compañía tomará las medidas necesarias para detenerlo inmediatamente, mitigar las pérdidas o daños y evaluar si son necesarias acciones correctivas o controles adicionales para prevenir fraudes futuros (y si es el caso, implementarlos de manera inmediata).

Cuando la Compañía ha sido víctima de un fraude, la Compañía debe tratar de recuperar lo que se ha perdido como consecuencia del fraude. La Compañía debe considerar tomar acciones legales contra los autores del fraude, si son miembros del personal o externos a la Compañía.

Cualquier acción impropia en contra de los recursos de la Compañía debe ser reportada de inmediato a la administración e investigada.

El personal que cometa fraude está sujeto a acciones disciplinarias, incluyendo el despido.

ADMINISTRACIÓN DE RECURSOS Y REGISTROS




Todo el personal es responsable de salvaguardar los activos de la Compañía, incluyendo el dinero, y asegurarse que las transacciones relacionadas con los recursos de la Compañía se registren con precisión y transparencia en los registros de la empresa.






Los gastos deberán ser coherentes con los objetivos de la Compañía y estar sujetos a un escrutinio riguroso en los procesos de proyección y del presupuesto. El personal deberá prestar la debida atención al momento de gastar el dinero de la Compañía y realizar compromisos financieros en nombre de la misma.

Todo el personal debe cumplir con las políticas globales o locales sobre el manejo de registros (por ejemplo, el Procedimiento de Administración de Archivos y Manejo de Registros). Los registros y la información son activos importantes de la empresa, y deben ser protegidos, conservados y eliminados de manera apropiada y en cumplimiento con todas las leyes y políticas de la Compañía.




PRINCIPIOS DE ADQUISICIONES

Cada área SET/funcional debe aplicar criterios para asegurarse que:

-  Las áreas SET/funcionales logren sus objetivos de negocio ejerciendo una mejor administración del gasto de la Compañía congruente con las necesidades y prioridades del negocio con un compromiso adecuado y vinculado a los recursos de la Compañía y utilicen de manera efectiva las capacidades de nuestros proveedores
-  Nosotros protegemos los derechos legales y comerciales de la Compañía.
-  Todas las actividades de compras:

- > Son aprobadas dentro de los límites de autoridad delegados por el corporativo y comité directivo, y
 - > Tengan una adecuada separación de funciones para asegurarse que la requisición, compromiso de adquisición y aprobación de factura tengan controles adecuados en la toma de decisiones.
-  El valor percibido se mide en términos de la calidad de los bienes o servicios adquiridos y el total de los gastos de propiedad
 -  El equilibrio óptimo se logra entre las necesidades de negocio locales o funcionales y que el beneficio corporativo se alcance.
 -  Procesos y procedimientos diseñados para asegurar el cumplimiento de esta política son elaborados, implementados y monitoreados por las áreas SET/funcionales (Ej. Proceso de Compras).
 -  Altas normas de ética profesional e integridad personal se mantienen en línea con el Código de Conducta de AstraZeneca, incluyendo las secciones de “Prevención del soborno y la corrupción” y “Evitar conflictos de intereses”. Debemos operar dentro de un marco ético que cumpla con las políticas de Seguridad, Higiene y Cuidado del Ambiente, Controles Financieros y la Responsabilidad Corporativa dentro de los lineamientos de Adquisiciones.
 -  Los proveedores deben ser tratados con el respeto adecuado.

VIAJES

-  Solo se permiten los viajes estrictamente necesarios
-  Para cada área SET/funcional, la dirección debe implementar políticas de viaje claras, detalladas y accesibles con criterios de aceptación claros.
-  Todos los viajes deben de cumplir con las políticas globales o locales aplicables (por ejemplo, la política mundial de viajes de AstraZeneca)








SEGURIDAD

Manejo de la Seguridad

La Compañía se ha comprometido a crear un entorno global de negocios seguro: protegiendo al paciente, al personal, a los productos, a la propiedad y a la información; minimizando las pérdidas e interrupciones del proceso de negocio, y salvaguardando la integridad de la Compañía y su reputación.

La seguridad es una responsabilidad en línea con la dirección, en donde los individuos tiene responsabilidades específicas. Debe ser manejada como cualquier otra actividad crítica en la propuesta, planeación, dirección y suspensión de las operaciones. La rendición de cuentas y la responsabilidad de la seguridad en AstraZeneca son implementadas cumpliendo con las políticas globales y locales.

Para cada área SET/funcional, la dirección apropiada debe aplicar criterios y procedimientos para asegurarse que:

-  Sus áreas de responsabilidad están sujetas a políticas que incorporan requerimientos locales específicos, sin dejar de ser coherentes con esta Política Global y Políticas y Normas de Seguridad de apoyo.
-  Los riesgos de Seguridad son identificados y entendidos, y medidas adecuadas y en proporción a estos son implementadas para su manejo.
-  Las medidas de seguridad son evaluadas y revisadas periódicamente.
-  Se consideran las implicaciones de seguridad de todos los aspectos de trabajo realizados por terceros en nombre de la Compañía.
-  Los incidentes en la seguridad son reportados, investigados, registrados y comunicados de manera apropiada.
-  Planes de emergencia y respuesta en crisis se han establecido para minimizar el impacto de cualquier incidente o emergencia.
-  No se utilizará seguridad armada a menos que sea un requisito legal o no exista otra alternativa para manejar el riesgo.

Seguridad de la Información

Toda la información de la Compañía y de terceros relacionados, de la cual la Compañía es responsable, debe protegerse para conservar su confidencialidad, integridad y disponibilidad, incluyendo el manejo adecuado por terceros.

Todo el personal debe cumplir con la Política Global de Comunicaciones y las normas locales relacionadas con la información electrónica y sistemas de computo (como la Política de uso de Computadoras). Todo el personal es responsable de manejar la información por las vías adecuadas según su clasificación de seguridad y cualquier requisito específico para su protección.

El personal debe asegurar el cumplimiento de las leyes de derechos de autor siguiendo los procedimientos aplicables globales o locales. (Procedimientos para la utilización de información de terceros (Copyright)).

Cuando se comparta información internamente o con terceros, los procedimientos globales o locales aplicables (como las Guías de Protección a la Información) se deben seguir y deben tomarse medidas – de acuerdo a la confidencialidad de la información – para asegurarse que estará protegida adecuadamente por aquel que la reciba.

Una guía para la protección de la información y la privacidad puede ser encontrada en la Política Global de Privacidad y Protección a la Información.








El procedimiento de la Compañía para la divulgación de información aplica para directores, funcionarios y empleados del Grupo AstraZeneca. Cubre todas las divulgaciones de información privilegiada por parte de la Compañía. La información privilegiada es, información no-pública relacionada al manejo de la Compañía o su

situación financiera que, en caso de hacerse pública, podría tener un impacto en el precio de las acciones de AstraZeneca.

El personal de sistemas debe de seguir todas las normas aplicables, tales como los Principios de Seguridad de Sistemas de la Información y las normas asociadas, los gerentes de sistemas son responsables de asegurarse que estas sean implementadas y respetadas.



Inteligencia Competitiva



Todas las actividades relacionadas con obtener información sobre compañías competidoras y sus productos deben desarrollarse de manera legal y ética.

-  El personal y terceros trabajando en nombre de la Compañía no deben de emplear métodos inadecuados para obtener información
-  El personal y terceros trabajando en nombre de la Compañía no deben buscar información que constituya los secretos comerciales de un tercero sin la autorización de dicha parte.
-  Si son ofrecidos secretos comerciales a un miembro del personal, este debe rehusarse a recibirlos y debe consultar al área Legal para posibles acciones de seguimiento.
-  Si se reciben secretos comerciales no solicitados, el área Legal debe ser consultada y, cuando sea apropiado, el dueño de la información debe ser notificado y la información devuelta.
-  Si de manera accidental se escucha una conversación sobre los secretos comerciales de un tercero, el personal debe informar a su gerente y la información no debe ser utilizada para influir en decisiones sobre el negocio.
-  Al personal de nuevo ingreso no se le debe solicitar, ni ellos deben ofrecer, información que pueda razonablemente ser considerada como secretos comerciales por sus empleadores anteriores.
-  Información originada fuera de AstraZeneca no debe ser utilizada de ninguna manera no autorizada, como es la violación de los derechos de autor o de cualquier acuerdo de confidencialidad.

Medicamentos falsificados

La Compañía utilizará una serie de medidas en contra de la falsificación de medicamentos, y pretende desarrollar su capacidad en esta área:

-  Introduciendo tecnologías que hagan del copiado de un producto más difícil para los falsificadores.
-  Realizando la vigilancia del Mercado y el monitoreo de la cadena de suministros para identificar posibles operaciones de falsificación.

-  Respondiendo rápidamente a cualquier reporte de falsificación de los medicamentos de AstraZeneca, trabajando con los reguladores, profesionales del cuidado de la salud, distribuidores, agencias oficiales y otras organizaciones para asegurar que los intereses del paciente están protegidos.
-  Participando en una variedad de foros contra la falsificación en el sector público y privado.

El personal que tenga conocimiento sobre actividades de falsificación de productos de AstraZeneca debe reportar esto a su gerente de acuerdo con los procedimientos del área local.

La Compañía hará esfuerzos para asegurarse que los pacientes y clientes estén conscientes de los riesgos de utilizar medicamentos falsificados.