ELABORADO POR:
Gerente Control Estratégico de Gestión

REVISADO POR:
Comité de Auditoría y Riesgos
Presidente Ejecutivo
Gerente General

APROBADO POR:
Directorio

Código: GE-P001
Versión: 01
Aprobación: 23 de Junio de 2023

POLÍTICA CORPORATIVA DE CONTROL INTERNO Y GESTIÓN INTEGRAL DE RIESGOS

ACEROS AREQUIPA

1. OBJETIVO

Definir nuestra Política Corporativa para el Control Interno y la Gestión Integral de Riesgos en la compañía, considerando los criterios y el marco de actuación para desarrollar, fortalecer y mantener un sistema de control interno y gestión integral de riesgos que ayude a la empresa a cumplir sus objetivos organizacionales.

2. ALCANCE

La aplicación de la presente política es de alcance a todos los miembros de Corporación Aceros Arequipa y Subsidiarias (En adelante CAASA).

3. RESPONSABILIDADES

Modelo de las Tres Líneas

El control interno y la gestión de riesgos son llevados a cabo por todos los miembros de la empresa; Directorio, Alta Dirección, Gerentes, Subgerentes, Jefes, Colaboradores y el área de Auditoría Interna. Comprendemos que, de acuerdo con el marco COSO, el control interno se realiza a través de tres líneas de defensa[1]:

- **Primera línea de defensa:** Dueños de Proceso y Colaboradores, responsables de mantener un sistema de control interno eficaz y eficiente.
- **Segunda línea de defensa:** Las áreas de soporte, tales como Gestión de Calidad, Medio Ambiente, Seguridad y Salud Ocupacional, Servicios Legales, Seguridad Patrimonial, Control de Calidad, Control Presupuestal, Control de Inventarios, entre otros, supervisan el cumplimiento de los lineamientos de control que hemos dispuesto.
- **Tercera línea de defensa:** El área de Auditoría Interna, es responsable de evaluar el sistema de control interno de la organización y recomendar medidas correctivas o mejoras, que podrán ser tomadas en consideración por los Dueños de Proceso. Su posición es independiente de las áreas de negocio que serán objeto de su análisis.

[1] COSO "Internal Control – Integrated Framework 2013" / pag.147

Cada una de las personas que integran nuestra organización cumple una función dentro del sistema de control interno y gestión integral de riesgos, siendo las principales responsabilidades las siguientes:

3.1 Directorio

Es responsable de aprobar la política de control interno y gestión integral de riesgos y definir los roles, responsabilidades y líneas de reporte que correspondan. Así como supervisar su eficacia e idoneidad[2], para tal efecto, asigna en la Presidencia Ejecutiva y la Gerencia General la responsabilidad directa sobre la gestión de riesgos y la implementación, mantenimiento y actualización permanente de los sistemas de control interno.

Asimismo, delega en el Comité de Auditoría y Riesgos (CAR) la evaluación de la eficacia del sistema de control interno[3] y gestión de riesgos.

3.2 Comité de Auditoría y Riesgos (CAR)

Es responsable de vigilar que CAASA cuente con un sistema de control interno efectivo y que se implementen políticas y procedimientos que aseguren una adecuada gestión de riesgos, velar por el cumplimiento de los códigos y políticas corporativas aprobadas por el Directorio, hacer seguimiento periódico a la gestión integral de riesgos e informarlo al Directorio, y considerar la eficacia del control interno de CAASA sobre la información financiera anual e intermedia, incluyendo la seguridad y el control de la tecnología de la información[4].

3.3 Presidencia Ejecutiva

En coordinación con el Gerente General, define el Plan Estratégico Corporativo, determina los objetivos de corto, mediano y largo plazo[5], identifica los riesgos a nivel de entidad y asiste en la implementación de estrategias para mitigarlos. Es responsable de promover una cultura de gestión de riesgos al interior de nuestra empresa.

[2]Código de Buen Gobierno Corporativo para los Sociedades Peruanas. 2013 – “Principio 25” / pag.14

[3]Estatuto de la Actividad de Auditoría Interna de CAASA. Set 2020 – “Alcance” / Pag. 1

[4]Estatuto del Comité de Auditoría y Riesgos / pag.4

[5]Estatuto de Corporación Aceros Arequipa S.A. – “Artículo 63” / Pag. 16

Anualmente, en conjunto con la Gerencia General, presenta al Directorio nuestro plan estratégico y los principales riesgos a los cuales está expuesto el negocio (riesgos estratégicos a nivel de entidad).

3.4 Gerencia General

Es responsable de diseñar, implementar, mantener y supervisar el sistema de control interno y de gestionar los riesgos a los que nos encontramos expuestos. Las responsabilidades del Gerente General, en relación con el control interno y la gestión integral de riesgos incluyen[6]:

• Definir los objetivos y metas, la estructura de la organización, la delegación de facultades, las normas internas (políticas empresariales, códigos, lineamientos, entre otros) y la supervisión de los resultados de los funcionarios y colaboradores.
• Supervisar las actividades de control interno y gestión integral de riesgos a nivel de Corporativo, asignando a los Dueños de Macroproceso la responsabilidad de identificar los riesgos y el diseño, implementación y evaluación de la eficacia de los controles establecidos en cada uno de sus procesos.
• Validar periódicamente con el Directorio los riesgos a nivel de entidad, las actividades de control asociadas y los planes de acción requeridos.

3.5 Dueños de Macroproceso

Asignada a Gerentes que cuentan con experiencia y juicio profesional adecuado para la gestión de los procesos operativos y de soporte a su cargo, sus responsabilidades incluyen:

• Supervisar la implementación de la normativa interna (políticas corporativas, códigos y reglamentos), así como definir los procedimientos, instructivos y lineamientos para el cumplimiento de los objetivos de sus unidades operativas o funcionales.
• Garantizar que los procesos se encuentren diseñados para alcanzar los objetivos del negocio, minimizando pérdidas y optimizando el uso de recursos.

[6]COSO “Internal Control – Integrated Framework. 2013” / pag.149

• Asegurar la implementación y mantenimiento de la gestión integral de riesgos en los procesos a su cargo, bajo la metodología GIRO.
• Supervisar el sistema de control definido en sus procesos.

3.6 Dueños de Proceso / Subproceso

La responsabilidad sobre nuestros Procesos y Subprocesos se encuentra asignadas, dependiendo del grado de complejidad e impacto sobre los objetivos del negocio en: Gerentes, Subgerentes, Jefaturas y Supervisores que cuentan con experiencia y juicio profesional adecuado, sus responsabilidades incluyen:

• Fortalecer la ejecución de los procesos a su cargo, buscando la eficiencia y eficacia en sus operaciones y el cumplimiento de los objetivos del negocio.
• Medir el desempeño del proceso y rendir cuentas de los resultados alcanzados.
• Identificar y evaluar los riesgos inherentes a las actividades de los procesos a su cargo, y definir controles suficientes para su administración, de acuerdo con la metodología GIRO.
• Ejecutar las actividades de monitoreo para asegurar el correcto diseño y operación de los controles implementados.
• Mantener actualizada la documentación de su proceso: i) Diagrama de flujo, ii) Matriz de riesgos y controles, y iii) Matriz de segregación de funciones (de aplicar).

3.7 Todos los Colaboradores

• Cumplir con las políticas, procedimientos y normas internas dentro del alcance de nuestras funciones y responsabilidades.
• Reportar la identificación de nuevos riesgos o materialización de algún riesgo al Dueño de Proceso o Subproceso correspondiente.
• Reportar a su jefe directo o gerente cualquier incumplimiento de normativa interna, regulaciones o leyes en el marco de las operaciones de CAASA.
• Reportar a través de la línea ética cualquier incumplimiento o sospecha de incumplimiento de lineamientos de nuestro código de ética y código contra actos de fraude y corrupción.

3.8 Gerencia de Control Estratégico de Gestión

• Definir y actualizar la metodología de gestión de riesgos considerando los marcos de referencia, buenas prácticas y estándares del marco externo, asegurando su mejoramiento continuo.

• Asistir a la Alta Dirección, Dueños de Proceso y colaboradores en el despliegue de la metodología de gestión de riesgos para identificar, analizar, controlar y monitorear los riesgos a nivel entidad y procesos.

• Reportar al Comité de Auditoría y Riesgos (CAR) los avances en la implementación y fortalecimiento del sistema de gestión de riesgos de CAASA.

3.9 Gerencia de Auditoría Interna

Realiza labores de auditoría en forma exclusiva, cuenta con autonomía, experiencia y especialización en los temas bajo su evaluación, e independencia para el seguimiento y la evaluación de la eficacia del sistema de control interno.

El Gerente de Auditoría Interna reporta directamente al Comité de Auditoría y Riesgos (CAR) sobre sus planes, presupuesto, actividades, avances, resultados obtenidos y acciones tomadas. El Gerente de Auditoría Interna depende organizativamente del Directorio, por lo que su nombramiento y cese corresponde al Directorio a propuesta del Comité de Auditoría y Riesgos (CAR)[7].

4. MARCO NORMATIVO O DE REFERENCIA

4.1 Marco Corporativo

La Política de Control Interno y Gestión Integral de Riesgos se enmarca en:

• La Visión, en la medida que nos propongamos ser reconocidos como el Grupo Siderúrgico líder en el mercado nacional del acero, ubicados entre los más rentables de la región y con activa presencia en el mercado exterior.

[7]Estatuto de la actividad de Auditoría Interna de CAASA. set 14 – "Autoridad e Independencia"/ Pag. 1 y 2

• La Misión, al ofrecer soluciones de acero a nuestros clientes, a través de la innovación, la mejora continua y el desarrollo humano, contribuyendo al crecimiento de los países en los que participamos e incrementando el valor para nuestros accionistas y grupos de interés.
• Los Valores Corporativos, trabajo en equipo, pasión por el trabajo y foco en lo relevante.
• El Código de Ética, donde se detalla la filosofía y principios que nos rigen, los cuales sirven como elemento rector en la relación con los diversos grupos de interés.
• El Código contra actos de fraude y corrupción, que comunica los lineamientos y las responsabilidades asignadas para prevenir, detectar, investigar y dar respuesta a cualquier acto de fraude y corrupción, manteniendo la cultura de cero tolerancia ante cualquier acto ilícito.
• Las políticas corporativas mencionadas en el anexo 1 que nos permiten cumplir con la gestión sostenible del negocio y la generación de valor compartido.
• Las Prácticas de Buen Gobierno Corporativo, que promueve un clima de respeto a los derechos de los accionistas y de los inversionistas en general; contribuye a generar valor, solidez y eficiencia en la empresa.

4.2 Marco Metodológico y Conceptual

Adoptamos los siguientes marcos conceptuales:

•El marco de referencia de Control Interno (2013) y el marco integrado de Gestión de Riesgos – ERM (2017) de COSO (Committee of Sponsoring Organizations of the Treadway Commission). COSO es reconocido a nivel mundial como el marco líder para diseñar, implementar y desarrollar el control interno y evaluar su efectividad.
•La declaración de posición del Instituto de Auditores Internos – IIA (por sus siglas en inglés): Las tres líneas de defensa para una efectiva gestión de riesgos y control

Adicionalmente, para funciones especializadas, complementamos la adopción con otros marcos de referencia tales como ISO 31000, COBIT 5 para la gestión de Tecnología de Información, el Código de Buen Gobierno Corporativo emitido por la Superintendencia de Mercado de Valores (SMV), etc.

4.3 Políticas Corporativas

La Política de Control Interno y Gestión Integral de Riesgos se desarrolla y complementa con nuestras Políticas y Códigos Corporativos. Estas son aprobadas por el Directorio con el objetivo de fortalecer el ambiente de control interno de la Corporación (Ver Anexo I: Listado de Políticas y Códigos Corporativos).

4.4 TFCD (Task Force on Climate-related Financial Disclosures)

Es una iniciativa internacional que establece recomendaciones para que las empresas divulguen información financiera relacionada con el clima, permitiendo evaluar y gestionar los riesgos y oportunidades asociados al cambio climático en sus operaciones y estrategias.

Nuestra metodología se enfoca en clasificar los riesgos y oportunidades frente al cambio climático tomando en cuenta lo propuesto por el TCFD, los cuales se clasifican en:

- Riesgos físicos: Hacen referencia a desastres naturales o eventos ambientales provocados por el cambio climático
- Riesgos de transición: Hacen referencia a cambios en las políticas, la legislación, la tecnología y el mercado para la mitigación del cambio climático

ACEROS AREQUIPA

5. DEFINICIONES

5.1. Riesgo

Incertidumbre de que un hecho o evento pueda impactar adversamente el logro de nuestros objetivos.

5.2. Control

Medida o actividad adoptada para mitigar el impacto y/o reducir la probabilidad de ocurrencia de los riesgos. El diseño del control debe de contemplar una evaluación del costo y beneficio de su implementación, además cada control debe dejar un mínimo registro o evidencia de que el mismo está operando tal cual fue diseñado.

5.3. Control interno

Es un proceso llevado a cabo por el Directorio, la Alta Dirección, Dueños de Proceso y Colaboradores, diseñado con el objetivo de proporcionar seguridad razonable, no absoluta, en cuanto a la consecución de los objetivos del negocio.

5.4. Apetito al riesgo

Grado de tolerancia o nivel de exposición (criticidad) al riesgo que la organización está dispuesta a aceptar en la búsqueda de valor. Para ello define estrategias de respuesta a los riesgos.

5.5. Oportunidad

Acción o potencial acción que cree o altere los objetivos y/o enfoques para crear, preservar y materializar valor.

6. LINEAMIENTOS DE CONTROL INTERNO

6.1 Al adoptar esta política, buscamos los siguientes resultados:

• Autocontrol: Capacidad de cada colaborador para controlar su trabajo, detectar desviaciones y efectuar acciones correctivas.
• Efectividad: Grado de realización de las actividades planificadas y de obtención de los resultados.
• Eficiencia: Uso racional y óptimo de los recursos.

6.2 Juicio Profesional

El sistema de control interno requiere la aplicación del criterio profesional a la hora de diseñar, implementar y ejecutar las actividades de control bajo su responsabilidad. Es por eso debemos de contar con colaboradores que cumplan con el perfil adecuado para las posiciones de mayor riesgo y responsabilidad.

6.3 Documentación del Sistema de Control Interno

Contamos con una metodología de documentación de procesos donde se describe los requerimientos de información de cada proceso. Esto requerimientos de información incluyen la documentación de una matriz de riesgos y controles y la evidencia del cumplimiento de los mismos.

7. LINEAMIENTOS DE GESTIÓN INTEGRAL DE RIESGOS

7.1 Clasificación de Riesgos

Los riesgos pueden ser clasificados de tres formas: (a) Por los objetivos que afectan, (b) Por su origen y (c) Por el nivel en la organización.

a. Por los objetivos[8] que afectan:

• Riesgos estratégicos: Impactan en el logro de nuestra visión, misión y objetivos estratégicos. Se encuentran relacionados con (a) volatilidad de los precios y variables del mercado, (b) incertidumbre del entorno, (c) cambios regulatorios, (d) capacidad de respuesta a los cambios de la industria, (e) la aplicación indebida de decisiones estratégicas, entre otros. Nuestra principal herramienta para mitigar estos riesgos es el Ciclo de Control Estratégico y el Plan Estratégico Corporativo.

• Riesgos operativos: Impactan en la utilización efectiva de los recursos de la compañía, y que estos estén custodiados apropiadamente, debido a (a) procesos inadecuados, (b) fallas del personal o la tecnología de información, o (c) eventos externos.

• Riesgos de información: Impactan en la integridad de la información financiera y no financiera, tanto interna como externa, usada o emitida a los diversos stakeholders.

• Riesgos de cumplimiento: Impactan en el cumplimiento de las normas externas (normas legales y sectoriales) e internas (p. e. Códigos, políticas corporativas, RIT, entre otros) aplicables.

b. Por su origen:

• Externos: riesgos que provienen del entorno.

• Internos: riesgos que se generan en nuestros procesos.

c. Por el nivel en la organización:

•Nivel Entidad: riesgos que afectan el logro de nuestros Objetivos Estratégicos.

•Nivel Procesos: riesgos que afectan el logro de los objetivos de un proceso específico.

[8]Enterprise Risk Management (2017) – Integrated Framework – / page 11

7.2 Evaluación de Riesgos

Los criterios de evaluación permiten medir y priorizar los riesgos a lo largo de nuestra Corporación y son como mínimo de dos tipos: (a) Impacto y (b) Probabilidad (Ver Anexo II: Criterios de evaluación de Riesgos).

a. **Impacto:** Se refiere a la medida en que un evento de riesgo podría afectarnos. Los criterios de evaluación del impacto incluyen: (i) Pérdida económica, (ii) Impacto en las operaciones y sistemas de información, (iii) Impacto en la reputación e imagen, (iv) Impacto regulatorio y legal (incluye impacto ético y de corrupción), (v) Impacto medio ambiental y (vi) Impacto en la Seguridad y Salud Ocupacional.
b. **Probabilidad:** Se refiere a la cantidad de veces que podría materializarse el riesgo en un periodo. Los criterios de evaluación de probabilidad son (i) Frecuencia, (ii) Exposición y (iii) Estimación de ocurrencia (experiencia y juicio profesional).

8. COMPONENTES DE CONTROL INTERNO Y GESTIÓN INTEGRAL DE RIESGOS

Al adherirnos al modelo COSO declaramos el cumplimiento de los principios de control interno por cada componente:

8.1 Entorno de Control

Es el conjunto de normas, procesos y estructuras que constituyen la base del control interno de la empresa.

Los principios de este componente son [9]:

a. Demostramos compromiso con la integridad y los valores éticos.
b. El Directorio demuestra independencia de la Alta Dirección y ejerce la supervisión del desempeño del sistema de control interno, a través del Comité de Auditoría y Riesgos.
c. La Alta Dirección establece, con la supervisión del Directorio, las estructuras, las líneas de reporte y los niveles de autoridad y responsabilidad apropiados para conseguir los objetivos de la empresa.

[9] COSO "Internal Control – Integrated Framework. 2013" / page 31

d. Demostramos compromiso para atraer, desarrollar y retener a profesionales competentes en alineación con los objetivos de la empresa, de acuerdo con la política de Gestión Humana.
e. Definimos las responsabilidades de las personas y el nivel de control interno para la consecución de los objetivos de la empresa.

8.2 Definición de Objetivos

La definición de objetivos estratégicos es una precondición para la identificación de eventos, la evaluación de riesgos y la respuesta al riesgo. Primero se deberán definir los objetivos estratégicos, antes de identificar los riesgos que la organización enfrenta y definir las acciones necesarias para gestionarlos[10].

Es así que definimos y actualizamos nuestros objetivos corporativos a través de las reuniones anuales de Planificación Estratégica Corporativa.

8.3 Identificación de Eventos

El Directorio y la Alta Dirección reconocen que la incertidumbre existe, por lo tanto, no se tiene certeza de cuándo puede ocurrir un evento con efectos negativos o positivos durante el transcurso de las operaciones. Durante su gestión, la Alta Dirección considera una serie de potenciales eventos, afectados por factores tanto internos como externos. En caso el evento pueda tener un impacto negativo representa un riesgo, en cambio los eventos con un impacto potencial positivo pueden representar oportunidades para nosotros. La Dirección debe gestionar tanto los riesgos como las oportunidades y definir acciones y dotar los recursos para mitigar los riesgos y aprovechar las oportunidades[11] .

8.4 Evaluación de Riesgos

La evaluación de riesgos nos permite tener en cuenta el grado en qué eventos potenciales podrían tener un impacto en el logro de nuestros objetivos estratégicos. Esta evaluación se realiza desde dos perspectivas: la probabilidad y el impacto[12]; utilizando una combinación cualitativa y cuantitativa de métodos.

[10]Enterprise Risk Management – Integrated Framework – page 21
[11]Enterprise Risk Management – Integrated Framework – / page 37
[12]COSO “Internal Control – Integrated Framework. 2013” / page 59
[13]Enterprise Risk Management – Integrated Framework – / page 81

a. Definimos e identificamos nuestros objetivos con suficiente claridad para permitir la identificación y evaluación de los riesgos.
b. Identificamos los riesgos para alcanzar nuestros objetivos estratégicos y los analizamos para determinar cómo deben de ser gestionados.
c. Consideramos la probabilidad de fraude, corrupción y cualquier otro evento que atente contra la ética e integridad al evaluar los riesgos para la consecución de objetivos.
d. Identificamos y evaluamos los cambios que podrían afectar significativamente al sistema de control interno.

8.5 Respuesta al Riesgo

Tras evaluar los riesgos relevantes y en función al apetito al riesgo de la compañía, la Alta Dirección y los Funcionarios determinan la estrategia de respuesta. Estas estrategias pueden ser las de aceptar, mitigar, compartir o evitar. Al considerar la estrategia, se evalúa su efecto sobre la probabilidad e impacto del riesgo, así como los costos y beneficios, y se selecciona aquella que sitúe al riesgo residual dentro del nivel de tolerancia establecido según el apetito al riesgo de la compañía[13].

8.6 Actividades de Control

Según su naturaleza los controles pueden ser preventivos o detectivos y pueden abarcar actividades manuales, semiautomáticas y automáticas. Los principios de este componente son[14]:

i. Definimos y desarrollamos actividades de control en los procesos de negocio que contribuyen a la mitigación de riesgos a niveles aceptables.
ii. Definimos y desarrollamos actividades de control en los sistemas de información que contribuyen a la gestión de riesgos de TI.
iii. Desplegamos las actividades de control a través de políticas y códigos que establecen las líneas generales del control interno y procedimientos o instructivos que llevan dichas políticas y códigos a la práctica.

[13] Enterprise Risk Management – Integrated Framework – / page 81
[14] COSO "Internal Control – Integrated Framework. 2013" / page 87

La segregación de funciones está integrada en el diseño y desarrollo de las actividades de control. En aquellas áreas en las que no es práctico llevar a cabo una segregación de funciones, el Dueño de Proceso selecciona y desarrolla actividades de control alternativas cuyo cumplimiento es obligatorio.

8.7 Información y Comunicación

Contamos con diversos canales de comunicación tanto interna como externa a las partes interesadas para asegurar el cumplimiento de los objetivos del negocio y reforzar los sistemas de control interno. De acuerdo con el marco COSO[15]:

a. Obtenemos, generamos y utilizamos información relevante y de calidad para apoyar el funcionamiento del sistema de control interno.
b. Comunicamos la información internamente, incluidos los objetivos y responsabilidades que son necesarios para apoyar el funcionamiento del sistema de control interno.
c. Nos comunicamos con las partes interesadas externas sobre los aspectos clave que afectan al funcionamiento del control interno y nuestros códigos de conducta.

8.8 Actividades de Supervisión

Para nosotros, las evaluaciones continuas (auditorías ISO, Auditorías de Cumplimiento de Requisitos Legales, controles de calidad de los productos, control presupuestal, supervisiones de seguridad y salud ocupacional, inspecciones ambientales, etc), las evaluaciones independientes (auditorías internas y externas) o una combinación de ambas, se utilizan para determinar si cada uno de los componentes del control interno y los controles para cumplir los principios de cada componente, están presentes y funcionan adecuadamente. Los principios de este componente son[16]:

a. Seleccionamos, desarrollamos y realizamos evaluaciones continuas y/o independientes para determinar si los componentes del sistema de control interno están presentes y en funcionamiento.

[15] COSO "Internal Control – Integrated Framework. 2013" / page 105
[16] COSO "Internal Control – Integrated Framework. 2013" / page 123

b. Los resultados de las evaluaciones se nos comunican oportunamente para aplicar medidas correctivas.

9. LIMITACIONES DE CONTROL INTERNO

El control interno, con independencia de lo bien diseñado, implementado y desarrollado que esté, solamente puede proporcionar una seguridad razonable y no absoluta al Directorio y Alta Dirección con respecto a la consecución de nuestros objetivos. La probabilidad de que se logren los objetivos se verá afectada por las limitaciones inherentes a todos los sistemas de control interno. Entre dichas limitaciones se incluye que el juicio/criterio profesional puede ser deficiente a la hora de tomar decisiones, el impacto de eventos externos ajenos al control de la empresa y errores humanos[17].

10. VIGENCIA Y DEROGACIONES

La presente Política fue aprobada inicialmente en sesión de Directorio del 26 de enero de 2017 y modificada el 23 de Junio de 2023. La presente Política tiene vigencia desde la fecha de su aprobación.

[17] COSO "Internal Control – Integrated Framework. 2013" / page 13705

ANEXO I: Listado de Códigos y Políticas Corporativas

Código de Ética
Código contra Actos de Fraude y Corrupción
Política Corporativa de Inversiones
Política Corporativa de Inventarios
Política Corporativa de Compras de Bienes y Servicios
Política Corporativa de Control Interno y Gestión Integral de Riesgos
Política Corporativa de Activo Fijo
Política Corporativa de Créditos y Cobranzas
Política Corporativa de Información
Política Corporativa de Gestión Humana
Política Corporativa de Derechos Humanos y Diversidad
Política Corporativa de Gestión Tributaria
Política Corporativa de Estrategia Fiscal
Política Corporativa de Seguridad y Salud Ocupacional
Política Corporativa de Medio Ambiente
Política Corporativa de Responsabilidad Social

Nota: Esta información es referencial. Los códigos y las políticas corporativas actualizadas se encuentran en nuestro intranet o la herramienta Goldenbelt.

ANEXO II: Criterios de evaluación de riesgos

Impacto	Bajo	Moderado	Considerable	Alto
Económico (Ut. Oper. > 50 MM) *Aplicable si Utilidad Operativa Promedio de últimos 3 años es mayor a 50 Millones de soles*	• Menor a ***0.25%*** de la Utilidad Operativa promedio de los últimos 3 años.	• Entre ***0.25% y 0.5%*** de la Utilidad Operativa promedio de los últimos 3 años.	• Entre ***0.5% y 1%*** de la Utilidad Operativa promedio de los últimos 3 años.	• Mayor a ***1%*** de la Utilidad Operativa promedio de los últimos 3 años.
Económico (Ut. Oper. < 50 MM) *Aplicable si Utilidad Operativa Promedio de últimos 3 años es menor a 50 Millones de soles*	• ***Menor a 250 mil soles.***	• ***Entre 250 mil y 500 mil soles.***	• ***Entre 500 mil y 1 millón soles.***	• ***Mayor a 1 millón de soles.***
Impacto en las operaciones y sistemas de información (cualitativo)	• Interrupción de las operaciones menor a 1 hora. • No se afecta la integridad y/o oportunidad de la información.	• Interrupción de las operaciones entre 1 y 8 horas. • Se afecta la integridad y/o oportunidad de información crítica	• Interrupción de las operaciones entre 8 y 24 horas. • Pérdida de información no crítica de CAASA o de terceros que no se pueda recuperar	• Interrupción de las operaciones mayor a 24 horas. • Pérdida de información crítica de CAASA o de terceros que no se pueda recuperar
Impacto en la reputación e imagen (cualitativo)	• Mínimo conocimiento público y baja o nula responsabilidad de la empresa.	• Conocimiento público moderado. Puede existir responsabilidad.	• Amplia repercusión mediática. Percepción de responsabilidad de la empresa.	• Masivo conocimiento público y amplia frecuencia o permanencia en medios. Recibe interés político. Percepción de responsabilidad de la empresa.
Impacto regulatorio y legal (cualitativo)	• **Podría generar** el incumplimiento de normativa ***interna o*** legal, sectorial, laboral ni tributaria.	• **Origina** el incumplimiento de la normativa ***interna o*** legal, sectorial, laboral o tributaria, **pero no genera pago** de penalidades.	• Incumplimiento de la normativa legal, sectorial, laboral o tributaria, determina el pago de penalidades. • ***Faltas éticas que incumplen con la normativa interna, no incurre en un delito.***	• Incumplimiento severo de la normativa legal, sectorial, laboral o tributaria, determina el pago de penalidades, **podría generar *sanciones penales para la entidad o representante,*** y/o la intervención del regulador. • ***Faltas éticas de forma sistemática que incumplen con la normativa interna y/o que se incurra en un delito.***
Impacto Medio Ambiental (Naturaleza del suceso/afectación)	• El alcance del impacto es a nivel de la actividad. • Afectación a ambientes e infraestructura de la empresa que se encuentre sobre pavimento.	• El alcance del impacto implica todo el proceso. • Afectación de 1 factor ambiental (Aire, Suelo, Agua, Flora y Fauna)	• El alcance del impacto implica otros procesos. • Afectación de 2 o más factores ambientales (Aire, Suelo, Agua, Flora y Fauna)	• El alcance del impacto sobrepasa los límites de la empresa. • Afectación al ambiente natural sensible o población (reservas naturales)
Salud y Seguridad Ocupacional (Naturaleza del incidente y del daño)	• Lesiones muy leves, pueden causar molestias o incomodidad	• Lesiones leves, sin baja, sin incapacidad, podrían requerir primeros auxilios.	• Incapacidad temporal. • Daño a la salud reversible.	• Incapacidad total o parcial permanente • Daño irreversible/mortal

Probabilidad	Bajo	Moderado	Considerable	Alto
Frecuencia	Nunca ha ocurrido. Menor al 0.5% de los casos / transacciones.	Durante el último año el evento no ha ocurrido, pero ha ocurrido con anterioridad. Entre el 0.5% y 1% de los casos / transacciones.	Durante el último año el evento ha ocurrido una vez. Entre 1% y 5% de los casos / transacciones.	Durante el último año el evento ha ocurrido más de una vez. Mayor al 5% de los casos / transacciones.
Exposición	Exposición continua, por debajo de 50% del límite aceptable.	Exposición continua, entre 50% y 75% del límite aceptable.	Exposición continua, entre 75% y 100% del límite aceptable.	Exposición continua, por encima del límite aceptable.
Estimación de ocurrencia (experiencia y juicio profesional)	Estimación de ocurrencia baja.	Estimación de ocurrencia moderada.	Estimación de ocurrencia considerable.	Estimación de ocurrencia alta.

ACEROS AREQUIPA