Tabla de contenido

A. INTRODUCCIÓN.

El Grupo UNACEM aplica un enfoque formal para la gestión integral de riesgos que le permite establecer un proceso sistemático y sostenible para identificar, mitigar y gestionar los riesgos que atenten contra la estrategia del negocio.

Este manual tiene como propósito asegurar la identificación y respuesta efectiva a los riesgos que enfrenta el Grupo y está alineado con los estándares de Buen Gobierno Corporativo y mejores prácticas. Este documento usa como marco de referencia también los modelos COSO Control Interno 2013, COSO Enterprise Risk Management 2017, NIST CSF (CyberSecurity Framework), la norma ISO 27001:2022 Seguridad de la Información, Ciberseguridad y Protección de la Privacidad y la norma ISO 31000:2018 Gestión de Riesgos.

Las características y beneficios clave de un enfoque formal para la gestión integral de riesgos se pueden resumir en lo siguiente:

- Identificación, evaluación y mitigación sistemática de riesgos, de manera coordinada entre el Centro Corporativo y las Unidades de Negocios y desde múltiples perspectivas, es decir, de una manera integral;
- Disposición de un repositorio central de riesgos con información homologada, revisada y actualizada periódicamente;
- Uso homogéneo de estándares, lenguaje definido y metodología única, adaptada a las necesidades del Grupo;
- Alineación con estándares de Buen Gobierno Corporativo y mejores prácticas de gestión de riesgos;
- Protocolos de priorización, reporte, revisión y aprobación de las matrices de riesgos y planes de mitigación;
- Evaluación de riesgos alineada con el proceso de planeamiento estratégico y al proceso de revisión y aprobación de proyectos de inversión (CAPEX).

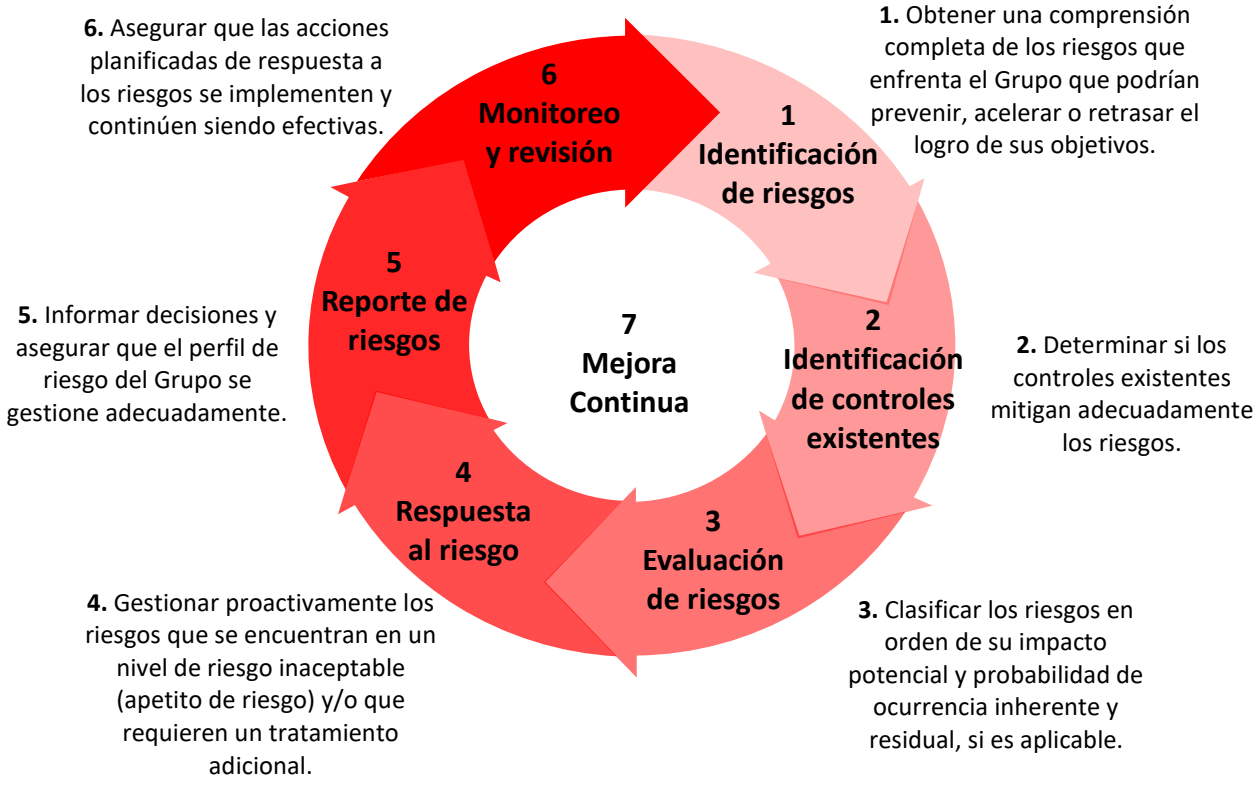
El modelo corporativo de gestión integral de riesgos del Grupo UNACEM ha particionado el universo de riesgos en cinco espacios de riesgo a ser gestionados:

Este manual trata sobre cuatro de los cinco espacios arriba descritos. No se encuentra en el alcance de este manual la gestión de los riesgos de Reporte Financiero (que incluye el sistema de control interno), asunto que será parte de otro documento a ser generado por la función corporativa de finanzas.

B. PROCESO DE GESTIÓN INTEGRAL DE RIESGOS.

El proceso de gestión integral de riesgos tiene como finalidad asegurar de manera estándar la identificación, gestión y reporte de los riesgos en todo el Grupo y se divide en siete etapas, (1) Identificación de riesgos, (2) Identificación de controles existentes, (3) Evaluación de riesgos, (4) Respuesta al riesgo, (5) Reporte de riesgos, (6) Monitoreo y revisión, y (7) Mejora Continua.

Proceso de Gestión de Riesgos



A continuación, este manual detalla cada una de las 7 etapas de la Gestión Integral de Riesgos.

1. Identificación de riesgos.

La identificación de riesgos es la primera etapa del proceso de Gestión Integral de Riesgos y busca visibilidad y comprensión de los eventos que podrían impactar negativamente el logro de los objetivos estratégicos y operacionales del Grupo.

Las actividades a tener en cuenta para la identificación de riesgos son las siguientes:

1.1 Identificación de las personas a involucrar en la identificación de riesgos.

En donde se selecciona a las personas de las Unidades de Negocio y/o del Centro Corporativo con experiencia técnica y gerencial relevante para la identificación de diferentes tipos o categorías de riesgo, así como aquellas personas que tienen conocimiento del negocio para

contribuir en este proceso. Para esta actividad, debemos incluir siempre a los dueños de los macroprocesos de negocio.

1.2 Utilización de las técnicas apropiadas de identificación de riesgos.

Las técnicas usuales incluyen:

a) Entrevistas de identificación de riesgos;
b) Cuestionarios de identificación de riesgos (ver Anexo 1);
c) Talleres de identificación de riesgos;
d) Mapeo de procesos de negocio a Nivel 3 (N3) para identificación de riesgos operacionales (ver Anexo 2);
e) Taxonomía de riesgos operacionales (ver Anexo 3);
f) Revisión de riesgos claves identificados a través de los sistemas integrados de gestión.
g) Análisis FODA/PESTEL;
h) Análisis Bow-tie, este análisis suele usarse como herramienta para explorar las causas y consecuencias de un riesgo;
i) Uso de herramientas tecnológicas que permitan identificar vulnerabilidades y/o debilidades de control basadas en malas configuraciones de los ambientes tecnológicos, los cuales incluyen a las redes IT (Administrativas) o redes OT (industriales).

1.3 Identificación y registro de los riesgos.

Un riesgo es un evento, acción u omisión, de fuente interna o externa, que puede ocurrir, e impactar de manera adversa el logro de los objetivos estratégicos u operacionales.

En el registro de riesgos, para cada riesgo identificado se requiere: (a) un código único de identificación del riesgo, (b) el objetivo estratégico de la unidad de negocio o corporativo impactado por el riesgo -solo para riesgos estratégicos u operacionales top-down- (c) un título que recoja la esencia del riesgo, (d) las causas que generan el riesgo, (e) las consecuencias que se desprenden del riesgo, (f) la categoría a la que pertenece, (g) la probabilidad de que el riesgo ocurra, (h) el potencial impacto – en términos de EBITDA – si el riesgo ocurre, (i) el nivel de riesgo que resulta de la probabilidad e impacto, (j) los controles clave existentes que mitigan el riesgo, (k) el nivel de efectividad de los controles existentes (para riesgos operacionales bottom-up), (l) el nivel potencial de mejora de los controles existentes (para riesgos operacionales bottom-up), (m) la probabilidad de ocurrencia luego de la aplicación de los controles existentes – residual – , (n) el impacto potencial luego de la aplicación de los controles existentes, (o) el nivel de riesgo aplicando la probabilidad e impacto luego de los controles existentes, (p) el nivel de impacto reputacional según la tabla aplicable, (q) la velocidad con la que el impacto del riesgo puede ocurrir, (r) la persona responsable del riesgo, (s) los planes de respuesta o mitigación necesarios para llevar el riesgo a niveles compatibles con el apetito de riesgo del Grupo, (t) el o los dueños del plan de respuesta, (u) las fechas de implementación del plan de respuesta, (v) el estado de implementación de los planes de respuesta, y (w) la fecha en la que el riesgo debe ser revisado para determinar la propiedad de las afirmaciones antes descritas sobre el riesgo (ver Anexo 4).

El registro de los ciber-riesgos se basa en el modelo por capas definido como parte de la estrategia de ciberseguridad, en donde se contemplan los diferentes controles a implementar para gestionar el ciber-riesgo, ello basado en la cobertura de las principales amenazas que pueden generar indisponibilidad en las redes IT / OT del Grupo considerando lo siguiente: (a)

la probabilidad de ocurrencia, (b) el nivel de impacto, (c) la probabilidad de ocurrencia luego de la aplicación de controles existentes – residual – , (d) el nivel de riesgo aplicando la probabilidad e impacto luego de los controles existentes, (e) la persona responsable del riesgo, (f) los planes de respuesta o mitigación necesarios para llevar el riesgo a niveles compatibles con el apetito de riesgo del Grupo, (g) el o los dueños del plan de respuesta, (h) las fechas de implementación del plan de respuesta.

1.4 Considerar todas las categorías de riesgo.

En el Grupo UNACEM hemos dividido los riesgos en dos grandes categorías de riesgo:

a) **Estratégico**: un evento que podría impactar el logro del propósito u objetivos estratégicos (incl. proyectos).
b) **Operacional**: un evento que podría impactar el desempeño o eficiencia de las operaciones del día a día (incl. ciberseguridad y reporte financiero).

El siguiente es un ejemplo de riesgo operacional:

Categoría	Título del riesgo	Causa	Consecuencia
Operacional	Pérdida total o parcial de planta de producción	› Colapso de horno › Falta de suministro de energía	› Daño a los activos › Pérdida de ventas

Los cinco espacios para gestionar (en línea con lo mencionado en la introducción), se encuentran circunscritos dentro de las grandes categorías de Estratégico y Operacional:

1.5 Identificación de riesgos estratégicos

La identificación de los riesgos estratégicos es una actividad fundamental dentro del planeamiento estratégico, así como de los planeamientos anuales subsecuentes que se desarrollan para su implementación.

La identificación de los riesgos estratégicos suele suceder cuando analizamos, por ejemplo, aquellas iniciativas estratégicas, batallas a ganar, adquisiciones, fusiones o proyectos de inversión o CAPEX (en adelante, los llamaremos en conjunto, riesgos de “proyectos”) que fueron propuestos para lograr la implementación de la estrategia.

Su identificación también suele ocurrir cuando, en la ejecución de nuestro trabajo, identificamos riesgos muy importantes en los procesos operacionales existentes o futuros sobre los que se apoya la estrategia del Grupo.

En ambos casos podemos considerar utilizar las técnicas de identificación de riesgos descritas en la sección 1.2 de este Manual.

El responsable del equipo de estrategia o del proyecto o el gerente de proyecto de la Unidad de Negocio es responsable de la identificación de riesgos, mientras que el equipo de riesgos es responsable de la validación del análisis de los riesgos que impactan a los gatilladores del proyecto, la alternativa propuesta, los KPI's, así como retornos y plazos, entre otros; de acuerdo con los cuatro pasos usuales para la identificación de riesgos que se describen a continuación.

a) Cuatro pasos usuales para la identificación de los riesgos estratégicos

Como un primer paso usual en el ejercicio de identificación de riesgos estratégicos, es la identificación de los riesgos que podrían impactar negativamente los objetivos y/o gatilladores de aquellas iniciativas estratégicas, batallas a ganar, adquisiciones, fusiones o proyectos de CAPEX.

Ejemplos de este primer paso de estos incluyen, una recesión económica y/o caída del PBI relacionado al sector construcción, la pérdida de algunos beneficios clave relacionados con las inversiones en CAPEX, el ingreso de nuevos competidores que consumen nuestra cuota de mercado, un cambio en las regulaciones existentes o modificaciones en las reglas de mercado, el impacto de una huella de carbono que genere cargas tributarias, etc.

En segundo lugar, identificamos los riesgos relacionados a los *stakeholders* del proyecto o iniciativa. Por ejemplo, una potencial reacción negativa de las comunidades sobre la instalación de una nueva planta de concreto, los posibles retrasos de las autoridades en el otorgamiento de permisos y licencias, etc.

En tercer paso, podemos situar a la identificación de los riesgos relacionados a la propia ejecución del proyecto que podrían impactar el tiempo, costo, productividad y calidad del propósito final del proyecto, entre otros.

Estos riesgos son aquellos, por ejemplo, que impactan el tiempo de entrega del proyecto, las ratios de productividad, la eficiencia y/o el retorno sobre la inversión, las interferencias en el subsuelo no identificadas en los anteproyectos, las variaciones importantes de tasas de interés o tipo de cambio, y huelgas o conmoción social, entre otros.

En cuarto lugar, podemos también identificar riesgos relacionados a ESG (ambientales, sociales y gobernanza), teniendo énfasis en el medio ambiente.

Ejemplos incluyen el riesgo de no cumplir con los compromisos de ambientales relacionados al proyecto, cambios en las regulaciones ambientales, la poca velocidad del desarrollo de tecnologías que apoyan metas de emisión de carbono, tiempo adicional requerido para concluir las negociaciones con las comunidades y que son requeridas como parte del otorgamiento de licencias ambientales, así como riesgos directos como inundaciones, deslizamientos que afectan accesos a nuestras instalaciones o la red logística, etc.

b) Análisis de escenarios

Otro vector de análisis requerido para identificar los riesgos estratégicos consiste en el análisis de escenarios que es una técnica de evaluación que se utiliza para identificar y medir la aparición potencial de sucesos de riesgo o para evaluar la resiliencia de un proyecto.

En este tipo de análisis se establecen a nivel del *Free Cash Flow* (FCF) del modelo financiero del proyecto, típicamente sobre tres escenarios: (i) Caso base, (ii) Caso optimista, y (iii) Caso pesimista. Estos escenarios se logran a través de la sensibilización coherente del set de los principales gatilladores y/o hipótesis más importantes del proyecto.

c) Otros riesgos que resaltar en los proyectos.

Para la identificación de riesgos en proyectos de inversión o CAPEX, es importante también tener en cuenta las siguientes categorías descritas en la Política Corporativa de CAPEX:

i. Riesgos legales y tributarios:

Son aquellos riesgos que podrían originarse a partir de las líneas grises de cumplimiento legales y/o tributarios como, por ejemplo, reclamos o contingencias y que podrían impactar el proyecto. Estos riesgos incluyen, por ejemplo, una paralización del proyecto al inicio al no disponer de todos los permisos correspondientes, o quizás reclamos que podrían surgir de la autoridad tributaria por la ambigüedad en la interpretación de la legislación relacionada (e. g. pérdidas arrastrables, créditos tributarios).

ii. Riesgos de ejecución

En adición a lo señalado párrafos arriba, para identificar los riesgos de ejecución, debemos revisar la lista de los imprevistos que pudiesen darse en la implementación del proyecto, por ejemplo, las interferencias que se puedan encontrar en la perforación del túnel, los retrasos en la entrega de maquinaria crítica, las huelgas, y los retrasos en una etapa crítica del proyecto o de la ruta crítica.

En la identificación de riesgos de ejecución, es importante tener en cuenta las categorías de riesgos definidas en el procedimiento de gestión de riesgos de proyectos (ver Anexo 5).

iii. Riesgos con las comunidades

En esta categoría se incluyen aquellos riesgos en el relacionamiento con las comunidades, así como sus potenciales esquemas de mitigación. Un ejemplo podría ser la imposibilidad de obtener el *permiso social* debido a oposición al proyecto por parte de los líderes de las comunidades, o quizás la paralización de la obra debido a protestas de las comunidades.

iv. Riesgo de no actuar

Es útil también examinar, de ser factible, cuáles serían las consecuencias de llevar a cabo el proyecto y mantener el *status quo* o situación actual.

Para más detalle sobre la presentación de estos riesgos, por favor refiérase a la Política Corporativa de Proyectos de Inversión (CAPEX).

1.6 Identificación de riesgos operacionales

Entre las formas más usuales de identificar los riesgos operacionales se encuentran el enfoque de arriba hacia abajo (*Top Down*) y el enfoque de abajo hacia arriba (*Bottom Up*).

- Top Down
  Usa técnicas como i) entrevistas de identificación de riesgos, ii) talleres de identificación de riesgos y iii) análisis FODA/PESTEL con la taxonomía de riesgos operacionales para la identificación de los riesgos.

- Bottom Up
  Utiliza técnicas usualmente aplicadas sobre procesos que se encuentran mapeados e incluyen, i) cuestionarios de identificación de riesgos y ii) revisión de riesgos claves identificados a través de los sistemas integrados de gestión con el mapeo de proceso de negocio, por lo menos a nivel 3.

En cuanto a la identificación de los riesgos de ciberseguridad, nos basamos en el marco de referencia NIST CSF (*Cybersecurity framework*), en donde se encuentran detallados los diferentes dominios de ciberseguridad que deben ser evaluados, según las mejores prácticas, así como los controles a considerar para la gestión de los riesgos. Ver la taxonomía de riesgos de Ciberseguridad en el Anexo 6.

La Gerencia de la Unidad de Negocio, en su rol de primera línea de defensa y representada por el líder del área de tecnología de información, es responsable de la identificación, mitigación y monitoreo de los riesgos de ciberseguridad. Los lineamientos, políticas, resolución de consultas, supervisión y seguimiento, como parte del rol de la segunda línea de defensa, son responsabilidad del *Chief Information Security Officer* (CISO) Corporativo.

2. Identificación y evaluación de controles existentes.

Luego de la identificación propia de los riesgos, debemos identificar los controles existentes y establecer si éstos mitigan los riesgos identificados a un nivel de apetito de riesgo aceptable. En adición, la evaluación de controles asegura que las personas estén comprometidas para implementar mejoras en el ambiente de control.

2.1 Identificar los controles existentes para cada riesgo identificado.

Si es posible, con las mismas personas involucradas en la etapa de identificación de riesgos, debemos considerar:

- ¿Cuáles son los controles implementados para reducir la probabilidad que el riesgo se materialice?
- ¿Cuáles son los controles implementados para reducir el impacto de ocurrir el riesgo?

Ejemplo.

Título del riesgo	Control adecuado	Control require mejoras
Pérdida de personal clave.	El Gerente Corporativo de Compensaciones revisa cada seis meses los niveles salariales por categoría definidos en la Política de Compensaciones vs. el promedio de la industria. En caso de identificar desviaciones de +/- 10% solicita al Comité de Compensaciones la aprobación del (de los) ajuste(s) correspondiente(s).	Esta es una buena empresa para trabajar por lo que debería se suficiente para mantener al personal clave.

2.2 Completar una evaluación de los controles identificados.

Luego de identificar los controles existentes, es importante evaluar los controles existentes para saber si son adecuados.

Los controles adecuados mitigan los riesgos identificados, son medibles y pueden ser validados.

La siguiente actividad es decidir si los controles actuales son adecuados. Es importante que los controles especificados en el registro de riesgos sean evaluados y probados en términos de su existencia y efectividad general.

- ¿Quién realiza el control?
- ¿Cómo se realiza el control?
- ¿Qué reportes u otra información son usados para realizar el control?
- ¿Con que frecuencia se realiza el control?
- ¿Cuál es la evidencia de la ejecución del control?
- ¿Qué se hace frente a los casos excepcionales?
- ¿El control cumple con mitigar el riesgo identificado (total o parcialmente)?

Use los criterios de calificación de controles proporcionados en el registro de riesgos para evaluar los controles identificados para cada riesgo en términos de su efectividad (efectivo, parcialmente efectivo, inefectivo) o si tiene potencial de mejora (fácil, moderado, difícil).

2.3 Evaluación de los controles identificados de ciberseguridad.

En cuanto a los controles de ciberseguridad, al utilizar el marco de referencia para la identificación de los riesgos, se seleccionan controles específicos basados en tecnología para mitigar posibles indisponibilidades en la infraestructura tecnológica, así como potenciales fugas de información.

El Marco de Ciberseguridad del NIST (NIST CSF) nos proporciona una metodología efectiva para gestionar el riesgo de ciberseguridad. Consta de cinco funciones principales: identificar, proteger, detectar, responder y recuperar. Al aplicar el NIST CSF, se deben seguir los siguientes pasos: comprender el contexto y los objetivos, realizar una evaluación de riesgos, establecer objetivos de ciberseguridad, desarrollar un plan de acción, implementar controles de seguridad, monitorear y revisar continuamente, y buscar mejoras continuas. Este enfoque flexible y adaptable garantiza una gestión integral del riesgo de ciberseguridad y permite proteger los activos críticos de una organización contra las amenazas en constante evolución.

3. Evaluación de riesgos.

El propósito del proceso de evaluación de riesgos es priorizar los riesgos en términos de su probabilidad de ocurrencia e impacto (financiero o reputacional) potencial. Los riesgos identificados deben evaluarse para poder darles prioridad y asignar con celeridad los recursos a los riesgos de mayor nivel.

El primer criterio de priorización es el nivel de riesgo, sin embargo, ante dos o más riesgos del mismo nivel se considera la probabilidad individual, de ser la misma, el impacto reputacional.

3.1 Decidir cómo cada riesgo será evaluado.

Para priorizar los riesgos, cada riesgo necesita ser evaluado en términos de su probabilidad de ocurrencia e impacto potencial:

- Probabilidad: ¿Qué tan posible es que el riesgo se materialice?
- Impacto: Si el riesgo se materializa, ¿Cuál sería la consecuencia?

3.2 Evaluar cada riesgo en términos de probabilidad e impacto.

Evaluación de riesgos inherentes:

- **Probabilidad inherente**: evaluación de la probabilidad de ocurrencia del riesgo sin tener en cuenta controles.
- **Impacto inherente**: evaluación del impacto potencial financiero, si el riesgo se materializa, sin tener en cuenta controles.

Evaluación de riesgos residual:

- **Probabilidad residual**: evaluación de la probabilidad de ocurrencia del riesgo después de tener en cuenta controles existentes.
- **Impacto residual:** evaluación del impacto potencial financiero y reputacional[1], cada uno de manera independiente, si el riesgo se materializa, después de tener en cuenta controles existentes.

Para estos efectos se definen los siguientes criterios de evaluación:

Impacto Reputacional	Criterio
Alto	Impacto significativo o dramático en la confianza de los *stakeholders* con cobertura mediática nacional o regional e investigación o sanción de los reguladores.
Medio	Impacto moderado en la confianza de los *stakeholder* con cobertura local y/o intervención de los reguladores.
Bajo	Impacto mínimo en la confianza de los *stakeholders* sin cobertura mediática ni intervención de los reguladores.

El impacto potencial financiero y reputacional son independientes, es decir, puede haber un riesgo con impacto financiero mayor o severo e impacto reputacional bajo o viceversa.

La probabilidad de ocurrencia se estima en función a los registros históricos de ocurrencia del evento (ver cuadro a continuación) o a juicio de experto, dependiendo de la naturaleza del riesgo o si nunca ocurrió el evento.

Probabilidad de ocurrencia.	Criterio
Muy Alta	El evento ocurrió en más de una oportunidad en el último año.
Alta	El evento ocurrió en una oportunidad en el último año.
Media	El evento ocurrió en una oportunidad en los últimos 2 años.
Baja	El evento ocurrió en una oportunidad en los últimos 3 años.
Muy Baja	El evento no ha ocurrido en los últimos 3 años.

3.3 Aplicar el apetito de riesgo definido en la Política Corporativa de Gestión Integral de Riesgos.

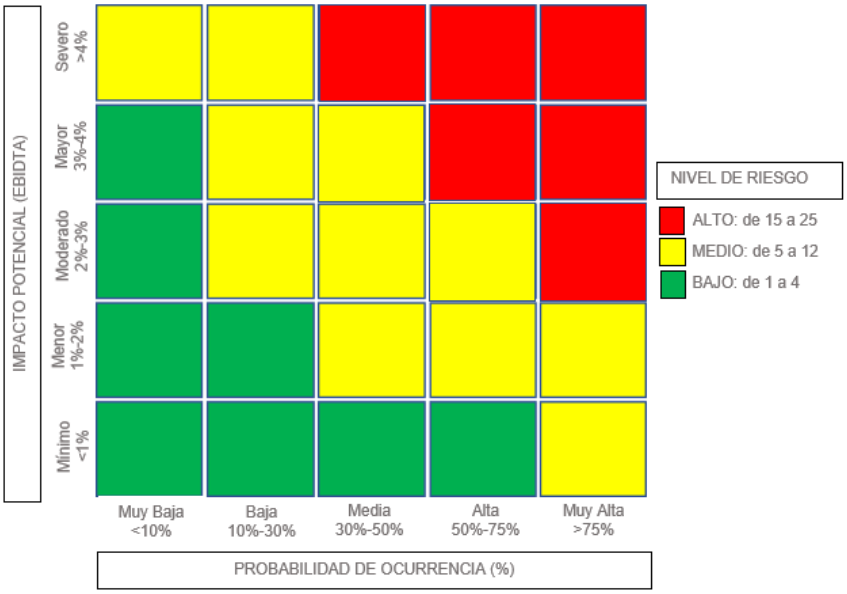
El nivel de riesgo máximo aceptable es el apetito de riesgo que se desea asumir en la consecución de los objetivos del negocio. Sirve de guía para la toma de decisiones y en la

asignación de recursos. En este sentido, en el Grupo UNACEM, el apetito de riesgo se ha definido en la Política Corporativa de Gestión Integral de Riesgos como impacto potencial máximo de pérdida aceptable multiplicado por la probabilidad máxima aceptable de ocurrencia de esta pérdida.

En el Grupo UNACEM, el impacto potencial se estima en términos cuantitativos en función del EBITDA de la Unidad de Negocio pertinente presupuestado del año en curso. En caso el EBITDA sea cercano a cero o negativo, éste se reemplaza por las ventas netas u otra medida que establezca el Comité de Riesgos y Cumplimiento. En adición, el impacto potencial se estima también en términos cualitativos como la afectación en la reputación.

El nivel de riesgo es el resultado de la combinación del impacto potencial y la probabilidad de ocurrencia del riesgo. Cabe señalar que el nivel de riesgo es el principal criterio de priorización en la gestión de los riesgos.

3.4 Mapa de riesgos.



3.5 Evaluación de riesgos estratégicos

La evaluación de riesgos estratégicos tiene que cumplir con los criterios de probabilidad e impacto reputacional descritos en la sección 3.2, sin embargo, los criterios de impacto financiero considerarán los indicadores financieros clave (estos incluyen, el EBITDA incremental, el monto total de la inversión, VPN, etc.) de la iniciativa estratégica para su cálculo.

La evaluación de riesgos estratégicos sigue la línea de los cuatro pasos usuales para la identificación de los riesgos estratégicos de la sección 1.5 subsección a).

Para la evaluación de riesgos relacionados a batallas a ganar, iniciativas estratégicas, adquisiciones o fusiones, los criterios de evaluación se determinarán en función de cómo los

riesgos identificados podrían impactar negativamente sus objetivos y/o gatilladores, siendo usualmente a nivel de *KPI*'s, así como retornos y plazos, entre otros.

Con relación a la evaluación de riesgos relacionados a los *stakeholders* del proyecto, los criterios de evaluación usualmente incorporan a los antes mencionados (i.e. *KPI*'s), como los riesgos identificados podrían impactar negativamente la reputación dado que los *stakeholders* consideran a las comunidades, autoridades, reguladores, clientes y/o consumidores, entre otros.

En el caso de la evaluación de riesgos relacionados a proyectos de CAPEX, los criterios de evaluación estarán relacionados a como estos riesgos podrían impactar negativamente la propia ejecución del proyecto (i.e. costos, tiempo, etc.). Para más detalle ir a la sección 3.6 Evaluación de riesgos de proyectos y al Anexo 5 en dónde se detalla la taxonomía de riesgos que debe aplicarse en el desarrollo del Business Case del proyecto.

Para la evaluación de riesgos relacionados a ESG (ambientales, sociales y gobernanza), teniendo énfasis en el medio ambiente, los criterios de evaluación usualmente también incorporan a los antes mencionados (i.e. KPI's), como los riesgos identificados podrían impactar negativamente la reputación.

En adición, en todos los casos, la evaluación de riesgos estratégicos considera también el análisis de escenarios, es decir, evaluar como los riesgos identificados podrían impactar negativamente cada uno de los escenarios definidos. En este sentido, dependiendo de la probabilidad en cada uno de los escenarios se determinará si el impacto se incorpora al modelo financiero o se considera como una contingencia.

3.6 Evaluación de riesgos de proyectos

En última instancia, la evaluación de riesgos de ejecución de proyectos tiene que cumplir con los criterios de probabilidad de ocurrencia e impacto potencial descritos en la sección 4.2, sin embargo, el procedimiento de gestión de riesgos de proyectos ha definido criterios adicionales de evaluación de impacto potencial, dada la naturaleza de los riesgos.

Estos criterios se homologarán con los criterios de evaluación estándares descritos en la sección 3.2 de la siguiente manera:

- Impacto Financiero: Será el resultado de la suma de los impactos en costos, tiempo, alcance y/o medio ambiente.
- Impacto Reputacional: Será el mayor de los impactos en reputación e imagen, medio ambiente y/o seguridad.

El PMO del equipo de estrategia o del proyecto o el gerente de proyecto de la Unidad de Negocio es responsable de la identificación de riesgos, mientras que el equipo de riesgos es responsable de la validación del análisis de los riesgos que impactan a los proyectos.
Solicitar Tabla de evaluación a la Dirección Corporativa de Riesgos y Cumplimiento.

3.7 Identificación de Cisnes Negros.

Los Cisnes Negros son eventos que normalmente aparecen en la parte superior izquierda del mapa de riesgos. Esto debido a que son altamente improbables, sin embargo, si ocurren tendrían un impacto severo. A pesar de que los cisnes negros tienen un nivel de riesgo medio o bajo, no deben ignorarse, asegurándose de estar preparados por si ocurren.

3.8 Evaluación de riesgos de ciberseguridad.

Los riesgos de ciberseguridad son, en síntesis, indisponibilidad de la infraestructura tecnológica y fuga de información. Si bien en base al marco de Ciberseguridad del NIST (NIST CSF) se deben identificar y evaluar las diferentes amenazas que pueden llevar a materializar estos riesgos em base al impacto y probabilidad, se ha determinado que todo riesgo de ciberseguridad es evaluado como prioritario (crítico) dado el alto impacto y alta probabilidad de ocurrencia debido a: (a) dependencia tecnológica, (b) sofisticación de los ataques cibernéticos, (c) impacto económico y operacional y (d) aumento de ciber ataques a infraestructura crítica.

4. Respuesta al riesgo.

El sólo hecho de identificar y evaluar los riesgos es insuficiente, éstos necesitan ser tratados con una gestión proactiva, por lo que cada riesgo debe tener un tratamiento adecuado de acuerdo con su probabilidad e impacto (ver Anexo 7).

El proceso de respuesta al riesgo o tratamiento del riesgo debería tener prioridad en aquellos riesgos que tienen un nivel de riesgo alto y/o requieren tratamiento adicional. Los siguientes pasos resumen la forma usual de responder al riesgo.

4.1 Definir un dueño del riesgo.

Un dueño del riesgo debe ser definido para cada riesgo. El dueño del riesgo es una persona con conocimiento del riesgo y con suficiente autoridad para asegurar la implementación de las actividades del plan de respuesta, incluyendo la asignación de recursos.

El dueño del riesgo no puede ser un área o grupo de personas, deberá ser una persona individual o un rol en la Unidad de Negocio o en el Centro Corporativo.

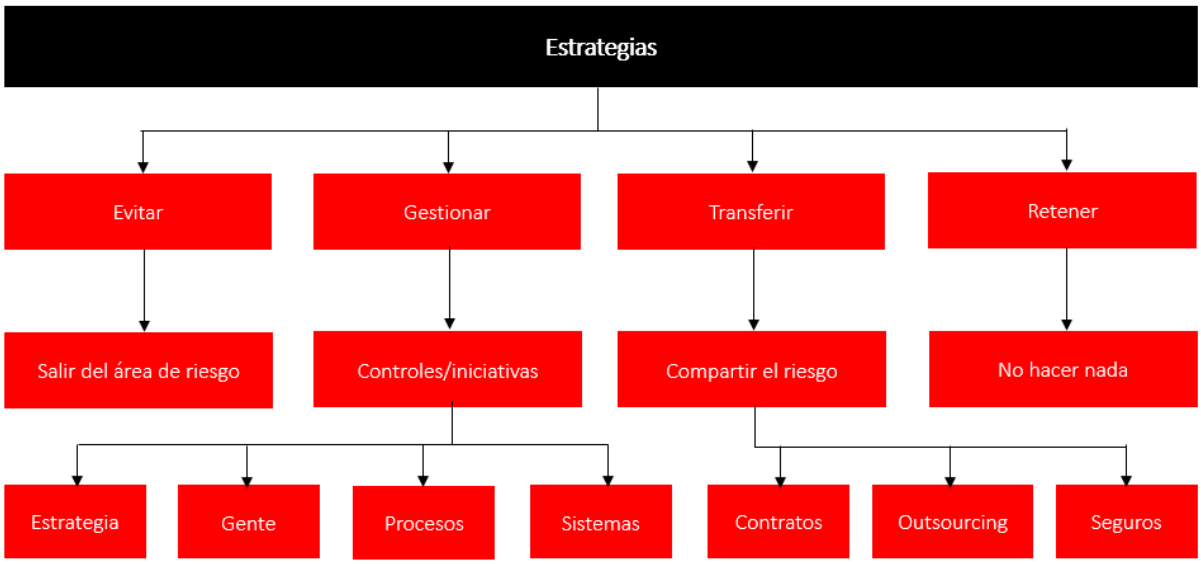
4.2 Determinar la necesidad de respuesta al riesgo.

Decidir si el riesgo requiere tratamiento adicional, considerando los controles actuales. Para aquellos riesgos que lo requieran, el dueño del riesgo definirá que acciones adicionales son requeridas:

- Evitar el riesgo, decidiendo no iniciar o continuar con la actividad que da lugar al riesgo.
- Gestionar el riesgo, por ejemplo, a través de controles o de un plan de mitigación.
- Transferir el riesgo a un tercero o terceros.
- Retener el riesgo mediante una decisión informada y no hacer nada.

La respuesta al riesgo debe apuntar a ubicar el riesgo residual a un nivel aceptable, teniendo en cuenta el apetito de riesgo (ver Anexo 8).

Estrategias de tratamiento de riesgos



4.3 Considerar para los planes de respuesta al riesgo.

- Preferir controles preventivos vs. detectivos y los controles automáticos vs. manuales.
- Evaluar si los controles reducen la probabilidad de ocurrencia o el impacto potencial del riesgo. Usualmente, las acciones de mitigación reducen la probabilidad de ocurrencia.
- Evaluar el costo de las acciones de mitigación vs. el impacto financiero potencial del riesgo, para asegurar la eficiencia de los controles. En adición, evaluar el impacto reputacional.
- Definir un responsable y fecha de cumplimiento del plan de respuesta o de cada una de las acciones de mitigación (controles).
- Evaluar constantemente las fechas de cumplimiento de las acciones de mitigación para evitar retrasos y/o reprogramaciones.
- En caso de un plan de respuesta con un largo periodo (un año o más) de implementación, descomponerlo en acciones de mitigación menores con fechas de cumplimiento independientes, para un seguimiento más efectivo del plan de respuesta.

4.4 La respuesta a los riesgos de ciberseguridad.

Se ha definido una estrategia corporativa de ciberseguridad para el Grupo Unacem, la cual debe ser implementada por todas las áreas de Tecnología de las diferentes Unidades de Negocio del Grupo.

La estrategia de control del riesgo se ha dividido en 4 capas para una adecuada gestión y seguimiento, las capas y sus respectivos controles son:

- Monitoreo y respuesta ante incidentes
  - Capacidades de monitoreo de amenazas en redes IT / OT (*CyberSOC*)
  - Capacidades de inteligencia de amenazas para la identificación de amenazas globales que pudieran afectar la infraestructura IT / OT del Grupo
  - Managed Detection and Response (MDR)
  - Network Detection and Response (NDR)

- Tecnología de Ciberseguridad
  - Seguridad en equipos finales (Servidores, estaciones de trabajo)
  - Parchado virtual
  - Multifactor de autenticación para acceso remoto a redes y entornos de colaboración
  - Gestión del acceso privilegiado (Cuentas administradoras)
  - Protección contra denegación de servicios (DDoS)
  - Gestión de identidades y accesos (IAM)

- Configuración y operación
  - Gestión de vulnerabilidades
  - Gestión de obsolescencia

- Gobierno
  - Políticas
  - Comités
  - *KPI*'s

5. Reporte de riesgos.

Los riesgos identificados y priorizados y los planes de respuesta al riesgo deben comunicarse a los *stakeholders* clave. Esto permite que se tomen decisiones más informadas y asegura que el perfil de riesgo del Grupo se gestione adecuadamente.

En este sentido, la gestión de riesgos busca identificar, mitigar y gestionar los riesgos que atenten contra la estrategia de negocios del Grupo UNACEM.

5.1 El proceso de reporte de riesgos describe los siguientes reportes trimestrales:

- Reporte de riesgos a la Comisión de Riesgos de la Unidad de Negocio.
- Reporte de riesgos consolidado al Comité de Riesgos Corporativo.
- Reporte de riesgos consolidado al Comité de Riesgos y Cumplimiento.

Sin embargo, la gestión de riesgos no debería ocurrir con esta frecuencia. La identificación y gestión de riesgos debería ser constantemente considerada y discutida en los CODIR, Comités de Gerentes y/o reuniones a los que asistan *stakeholders*.

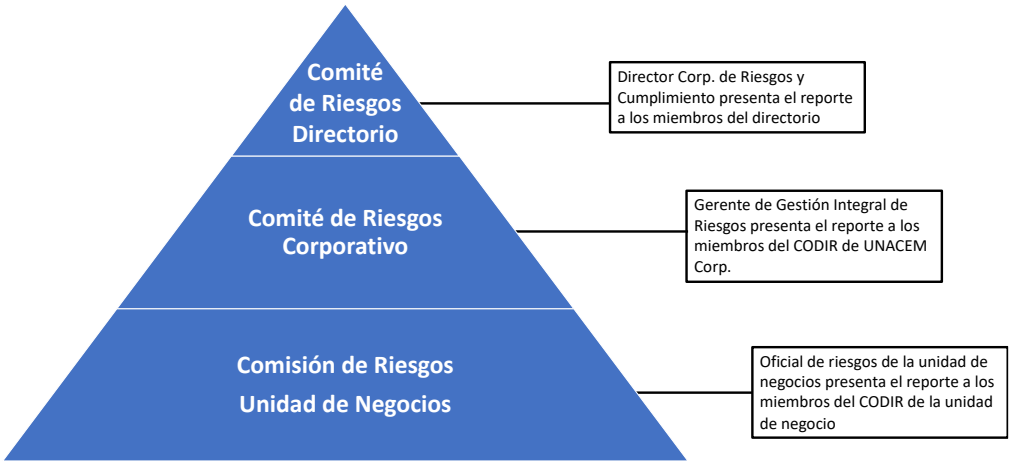
En el reporte de riesgos presentará los principales riesgos, sean estratégicos u operacionales de acuerdo con el criterio de priorización establecido en la sección de evaluación de riesgos. Esta priorización será revisada por la Comisión de riesgos de la Unidad de Negocios y validada por el Comité Corporativo.

En el reporte de riesgos, debe ser incluido un resumen de los cambios más importantes desde el último reporte, así como la información más relevante del registro de riesgos para cada uno, incluido el estatus de implementación, así como la eficacia de los planes de respuesta al riesgo.

El reporte de riesgos de la Unidad de Negocio debe ser presentado a la Comisión de Riesgos de la Unidad de Negocio por el Oficial de Riesgos antes de ser compartido con el Centro Corporativo. En este sentido, el reporte de riesgos consolidado deberá ser presentado al Comité de Riesgos Corporativo por el Gerente Corporativo de Gestión Integral de Riesgos antes de ser presentado al Comité de Riesgos y Cumplimiento por el Director Corporativo de Riesgos y Cumplimiento.

El Presidente del Comité de Riesgos y Cumplimiento reportará trimestralmente un resumen al Directorio.

El proceso se resume en el siguiente diagrama:



5.2 Estructura del reporte de riesgos.

- Resumen ejecutivo (máx. una página).
- Introducción (máx. dos páginas) –
  - Principales cambios vs. el último reporte (i.e. nuevos riesgos o riesgos mitigados y/o materializados, cambios importantes en probabilidades e impactos, etc.).
  - Nivel de cumplimiento de planes de respuesta.
  - Perfil de riesgo actual (i.e. opinión del perfil de riesgo actual vs. cumplimiento de estrategia de negocio u operacional, ¿Qué hacer para mejorar el perfil de riesgo?, etc.).
  - Entre otros (i.e. riesgos emergentes).
- Mapa de calor – de los principales riesgos a reportar.
- Resumen de matriz de riesgos – de los principales riesgos a reportar.
- One page – de cada uno de los riesgos principales a reportar (ver Anexo 10).
- Anexos – (i.e. planes de respuesta detallados).

5.3 Proceso de reporte de riesgos de ciberseguridad.

Se ha establecido un modelo de gobierno basado en la interacción de los principales actores para la gestión del riesgo y el reporte adecuado en los diferentes niveles de la organización.

Los participantes de la estructura de modelo de gobierno definido son:

a) Comité de Riesgo y Cumplimiento del Directorio Corporativo: Instancia superior en donde se presentan los riesgos y se hace seguimiento de su gestión.

b) Vicepresidencia de Finanzas y Dirección Corporativa de Riesgos y Cumplimiento: Sponsors del modelo de gobierno, facilitan el cumplimiento y funcionamiento del modelo.

c) CISO (Chief Information Security Officer) y CIO (Chief Information Officer) Corporativo: Si bien el CISO corporativo es el responsable del modelo de Gobierno de Ciberseguridad, el trabajo en conjunto con el CIO es fundamental para la gestión del ciber riesgo, el cual está soportado 100% en tecnología. Dentro de las principales funciones del modelo destacan:

   i. Definir la política general de ciberseguridad y los lineamientos que las empresas deben seguir.

ii. Presentar al comité de Riesgo y Cumplimiento los avances en la gestión de Ciberseguridad, basada en *KPI*'s.

iii. Implementar Comités de Ciberseguridad Operativos y Ejecutivos con las empresas del grupo UNACEM con el objetivo de:

- Coordinar el despliegue de la estrategia.
- Verificar el estado de proyectos y servicios clave para la gestión del ciber riesgo.
- Revisar niveles de avance en *KPI*'s
- Identificar los riesgo y problemas a gestionar para la implementación de la estrategia y modelo de gobierno

d) Áreas de IT (Sistemas) y OT (planta industrial): Son las encargadas del despliegue de los controles que formen parte de la estrategia de ciberseguridad y asimismo son los responsables de velar por la operación de ciberseguridad.

Como parte del modelo se ha definido un esquema de medición basado en KPI's para poder medir la gestión del riesgo, la madurez en temas de ciberseguridad de la corporación y la evolución mensual de las empresas en cuanto a la cobertura del ciber riesgo.

La frecuencia de medición y reporte de avances en cuanto a indicadores se ha definido de la siguiente forma:

- Mensual: Comités de Ciberseguridad
- Trimestral: Comité de Riesgos y Cumplimiento del Directorio

6. Monitoreo y revisión.

El monitoreo y revisión es una etapa esencial del proceso de gestión de riesgos. Es importante recordar que los riesgos no permanecen estáticos; los riesgos cambian, las prioridades cambian, los planes se completan, las respuestas que eran efectivas pueden volverse menos efectivas, etc. Por lo tanto, es importante continuar monitoreando y revisando los riesgos.

Las siguiente son pautas para la labor de monitoreo y revisión:

6.1 Asegurarse que la revisión del Reporte de Riesgos está en la agenda de las reuniones regulares con la Gerencia.

En adición al proceso de gestión de riesgos descrito, surgen nuevos riesgos a ser identificados y gestionados. Para asegurarse que el proceso de gestión de riesgos es dinámico e identifica esos riesgos emergentes, la gestión de riesgos debería estar en la agenda de las reuniones regulares con la Gerencia.

En estas reuniones, solicitar a los participantes revisar el último reporte de riesgos y hacer las siguientes preguntas:

- ¿Hay algún nuevo riesgo emergente que debería ser incluido en el reporte de riesgos?
- ¿Alguno de los riesgos incluidos en el reporte de riesgos ha cambiado de manera importante en términos de probabilidad y/o impacto, y requiere acciones de respuesta adicionales?
- ¿Hay alguna iniciativa prevista en los próximos 12 meses que pueda dar lugar a un nuevo riesgo clave?

6.2 Monitorear el estatus de los planes de mitigación o de respuesta planeados.

Se debe monitorear periódicamente, por lo menos mensualmente, el estatus de las acciones de respuesta planeadas.

En este sentido, es responsabilidad de los dueños de riesgos y dueños de las acciones el completar los planes de respuesta, deben estar comprometidos y reportar su ejecución.

6.3 Monitoreo del perfil de riesgo.

El monitoreo del perfil de riesgo pretende revisar la gestión de riesgos de manera continua para:

- Identificar alertas de riesgos.
- Identificar diferencias entre el perfil de riesgo y nivel de riesgo aceptable (target o residual acordado).
- Definir indicadores de riesgo (*KRI's*) para monitorear cambios en el perfil de riesgo. Un KRI es una métrica que permite monitorear de manera temprana la potencial ocurrencia de un riesgo para tomar medidas oportunas.
- Identificar factores o situaciones que puedan estar generando dichos cambios.
- Seguimiento a los indicadores de riesgo definidos.

El monitoreo del perfil de riesgo es una acción conjunta de la Gerencia de la Unidad de Negocio.

6.4 Revisar el cumplimiento de los controles y/o efectividad de los planes de respuesta para mitigar los riesgos.

El dueño del riesgo debe revisar y reportar el cumplimiento de los controles y/o efectividad de los planes de respuesta definidos para mitigar los riesgos identificados (incluida la autoevaluación de controles) con el fin de confirmar que se ha reducido efectivamente el nivel de riesgo (probabilidad y/o impacto), a un nivel aceptable.

En caso, de deficiencias de control y/o inefectividad de los planes de respuesta, se deberá definir planes de remediación.

El resultado de la revisión se debe incluir en el reporte de riesgos a la Comisión de Riesgos de la Unidad de Negocio, Comité de Riesgos Corporativo y Comité de Auditoría, Riesgos y Cumplimiento, cuando ocurra.

El Oficial de riesgos deberá encargarse de hacer pruebas selectivas sobre el cumplimiento de los controles y/o efectividad de los planes de respuesta.

7. Mejora continua.

Es una buena práctica definir un proceso de mejora continua de la metodología de gestión de riesgos alineada con las recomendaciones de evaluaciones regulares (internas y/o externas) y a los cambios en el entorno.

En este sentido, se deben realizar las siguientes actividades a fin de identificar oportunidades de mejora concretas sobre la gestión de riesgos:

7.1 Evaluación de los riesgos materializados.

Cuando se materialice un riesgo, debe asegurarse de retroalimentar el registro de riesgos y planes de respuesta con la finalidad de que en el futuro el Grupo esté en una mejor posición para prevenirlo o gestionarlo de una forma más efectiva.

7.2 Evaluación de efectividad del proceso de gestión de riesgos.

Periódicamente (i.e. anualmente), se debe realizar una evaluación o autoevaluación formal que se complemente con el feedback del Comité de Riesgos Corporativo y/o del Comité de Auditoría, Riesgos y Cumplimiento sobre la efectividad del proceso de gestión de riesgos, con la finalidad de identificar posibles oportunidades de mejora para gestionar los riesgos de manera más efectiva y eficiente.

En esta evaluación, se debe evaluar como mínimo el cumplimiento de este manual.

7.3 Evaluación del nivel de madurez de gestión de riesgos

Periódicamente, se debe realizar una evaluación de la madurez del proceso de gestión de riesgos, usando el modelo de madurez adoptado por el Grupo (TBD).

C. DUEÑO DEL MANUAL.

El Director Corporativo de Riesgos y Cumplimiento es la persona responsable del presente manual, el cual estará en constante revisión para asegurar su alineamiento con las mejores prácticas para la gestión de riesgos, así como con respecto a cambios regulatorios, en el Centro Corporativo o en las Unidades de Negocio del Grupo UNACEM.

Nombre del Documento	MANUAL DE GESTIÓN INTEGRAL DE RIESGOS			Versión
Área responsable	Dirección Corporativa de Riesgos y Cumplimiento			
Elaborado por	Javier Carrasco Gerente Corporativo de Gestión Integral de Riesgos	Fecha de Revisión	11/11/2023	1.0
Elaborado por	Fernando Dyer Director Corporativo de Riesgos y Cumplimiento	Fecha de Revisión	11/11/2023	1.0
Revisado por	Pedro Lerner Gerente General Corporativo	Fecha de Aprobación	01/12/2023	1.0
Aprobado por	Comité de Riesgos y Cumplimiento	Fecha de Aprobación	19/12/2023	1.0

ANEXO 1 - Cuestionario de identificación de riesgos

Nombre:	
Área:	
Puesto:	
Fecha:	

EJEMPLO

Riesgo	Causa(s)	Consecuencia(s)
Caída del suministro de energía eléctrica en el predio.	Interrupción en la central eléctrica. Pérdida del transformador. Conexión entrante al predio dañada.	Interrupción de la producción. Pérdida de productos en proceso por falta de refrigeración. Incapacidad para procesar los pedidos de venta debido a la indisponibilidad de TI.

¿Cuáles son los riesgos principales de su unidad de negocio o función?
1.
2.
3.
4.
5.

¿En general, cuál sería la probabilidad de ocurrencia[1] e impacto potencial del riesgo[2]?		
Riesgo 1	i.e. Muy Baja	i.e. Mayor
Riesgo 2		
Riesgo 3		
Riesgo 4		
Riesgo 5		

¿Cuáles son los controles clave actuales que mitigan este riesgo?	
Riesgo 1	i.e. Generador de energía eléctrica de emergencia para asegurar la continuidad de los procesos críticos de manera temporal.
Riesgo 2	
Riesgo 3	
Riesgo 4	
Riesgo 5	

[1] Probabilidad de Ocurrencia: Muy Baja, Baja, Media, Alta, Muy Alta

[2] Impacto Potencial: Mínimo, Menor, Moderado, Mayor, Severo

ANEXO 2 - Niveles de mapeo de procesos de negocio

1. La jerarquía de mapeo de procesos de negocio consta de cuatro niveles.

   N1 - Proceso *end to end*.
   N2 - Proceso.
   N3 - Actividad.
   N4 - Tarea.

2. Ejemplo.

   N1 - *Plan to produce*.
   N2 - Planeamiento de la demanda.
   N3 - Creación de solicitudes de pedido.
   N4 - Creación automática de orden de compra.

ANEXO 3 - Taxonomía de riesgos operacionales

(espécimen para identificación bottom-up)

Clientes, productos y prácticas empresariales	**Eventos externos**	**Riesgo de Liquidez**
Actividades de asesoramiento	Robo y fraude terceros	Capital de trabajo negativo
Adecuación, divulgación de información y confianza	Seguridad de los sistemas	Perdidas por ventas desventajosas (Fire Sales)
Prácticas empresariales o de mercado improcedentes	**Eventos internos**	**Riesgo Regulatorio**
Productos defectuosos	Actividades no autorizadas	Cambio de Regulacion Ambiental
Selección, patrocinio y riesgos	Robo y fraude interno	Cambio de regulacion Credito
Cumplimiento	**Interrupción del negocio y fallos en los sistemas**	Cambio de regulacion de Cumplimiento
Colusiones (internas, de terceros, con terceros)	Interrupccion de actividades por orden administrativa	Cambio de Regulacion Fiscal
Contribuciones inapropiadas a partidos políticos	Interrupción de los sistemas	**Riesgo Tecnico Operativo**
Donaciones o patrocinados inadecuados / Regalos, inv	Interrupción del acceso a la zona de trabajo	Fallas en la gestion de la Calidad
Extorsiones de funcionarios públicos	**Relaciones laborales y seguridad en el puesto de trabajo**	Gestion de subcontratistas
Financiamiento del terrorismo	Alta Rotación de Personal	Producción Clinker
Incumplimientos al codigo de conducta	Bajo Clima Laboral	Riesgo de Contrato (Proyecto/Negocio)
Lavado de Dinero	Diversidad y discriminación	Riesgo de Ingenieria
Perdidas por Incumplimiento de la Regulación Ambier	Higiene y seguridad en el trabajo	Riesgo de Mano de Obra
Perdidas por Incumplimiento de la Regulación Tributa	Reclutamiento de personal inadecuado para el puesto	Riesgo de Seguridad Fisica
Sobornos a funcionarios públicos / Pagos para agilizaci	Relaciones laborales	Riesgo Logistico
Trafico de influencias	**Riego de Mercado**	Riesgo Tecnico de Insumos
Daños a activos materiales	Perdidas cambiarias	Riesgo Técnico de la supervisión
Desastres y otros acontecimientos	Perdidas por tasa de interes	Riesgos Economicos
Ejecución, entrega y gestión de procesos	Riesgo de portafolio	Riesgos Financieros
Aceptación de clientes y documentación	Riesgo de precio	**Riesgos de relacionamiento**
Contrapartes comerciales	**Riesgo de Contraparte**	Alta visibilidad del grupo (Reputación)
Distribuidores y proveedores	Perdidas por incumplimiento de pago o penalidades c	Falla en las Comunicaciones (Mensajes no asertivos
Gestión de cuentas de clientes	**Riesgo de Crédito**	Falla en la comunicación de Indicadores Financieros a
	Perdidas por incapacidad de obtener fianzas necesaria	Fallas en el manejo de Problemas con comunidades/
	Perdidas por incrementos en el costo de financiamien	Fallas en la gestion de Crisis en proyectos

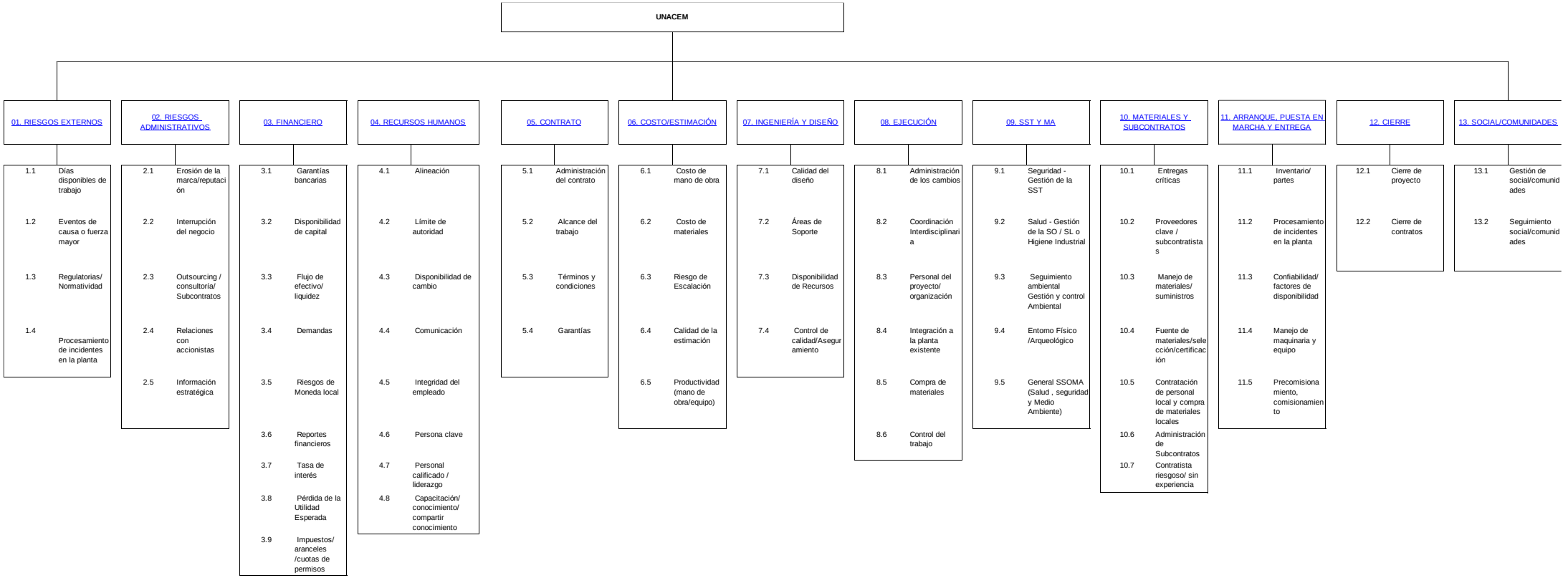
ANEXO 4 - Estructura del registro de riesgos (1/2).

Código	Objetivos UNACEM	Título del Riesgo	Causa del Riesgo	Consecuencia del Riesgo	Categoría del Riesgo	Probabilidad de Ocurrencia Inherente	Impacto Ptencial Inherente (EBITDA)	Nivel de Riesgo (financiero)	Controles Clave actuales	Efectividad del Control	Potencial de Mejora
	Objetivo Estratégico impactado por el riesgo	Definición concisa del riesgo	Lista de la (de las) causa(s) directa(s) del riesgo	Lista de las consecuencias del riesgo, si ocurriera	Categoría a la que el riesgo individual pertenece	Evaluación de la probabilidad que el riesgo ocurra antes de los controles actuales	Evaluación del potencial impacto reputacional del riesgo, si ocurre antes de los controles actuales	Importancia general del riesgo con base en la probabilidad de ocurrencia e impacto potencial	Descripción de los controles clave actuales para mitigar el riesgo	Evaluación de la efectividad de los controles actuales para mitigar el riesgo	Evaluación de la posibilidad de mejorar los controles actuales

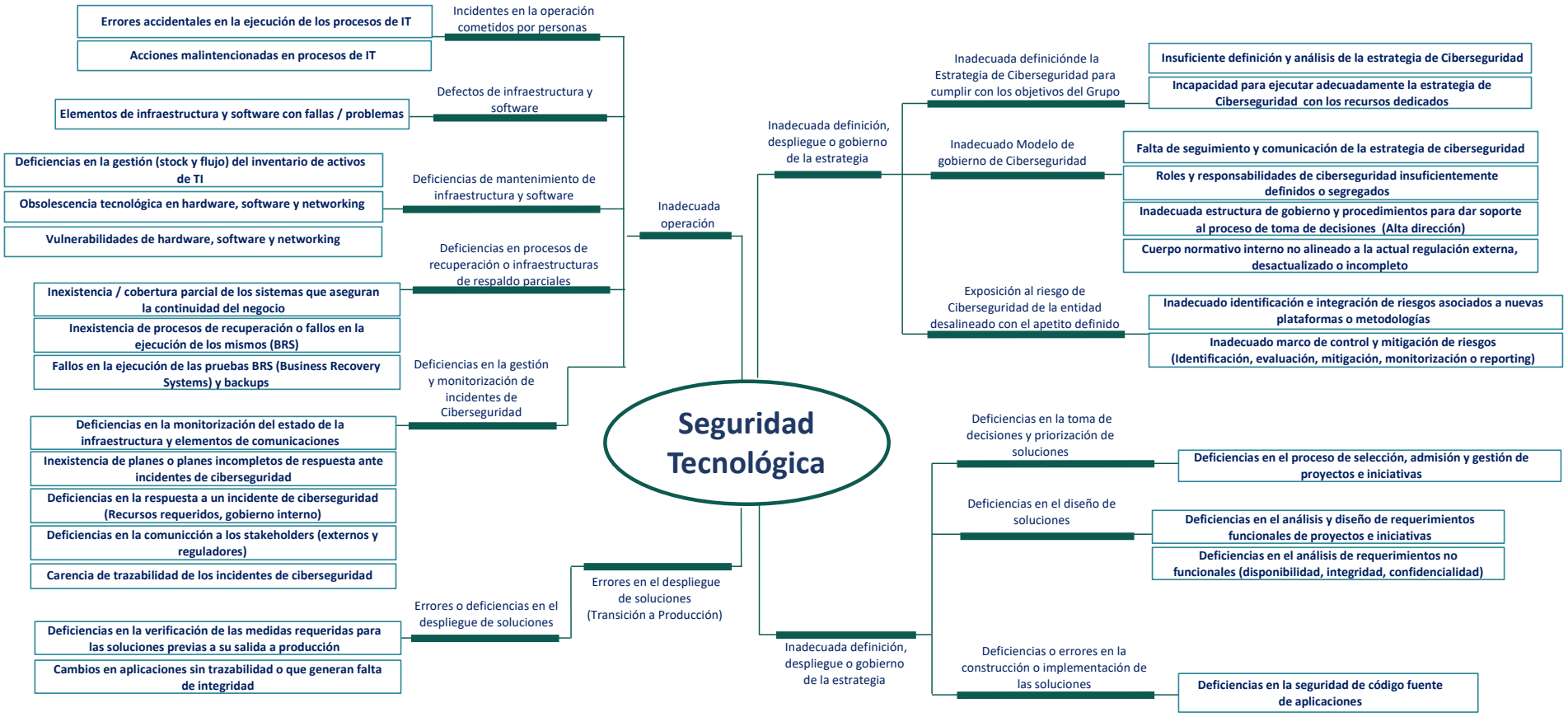
Estructura del registro de riesgos (2/2).

Probabilidad de Ocurrencia Residual	Impacto Potencial Residual (EBITDA)	Nivel de Riesgo (financiero)	Impacto Reputacional	Velocidad del Riesgo	Dueño del Riesgo	Plan de Respuesta	Dueño del Plan de Respuesta	Fecha del Plan de Respuesta	Situación del Plan de Respuesta	Fecha de Revisión	Comentarios
Evaluación de la probabilidad que el riesgo ocurra luego de los controles actuales	Evaluación del potencial impacto financiero del riesgo, si ocurre luego de los controles actuales	Importancia general del riesgo con base en la probabilidad de ocurrencia e impacto potencial	Evaluación del potencial impacto reputacional del riesgo, si ocurre luego de los controles actuales	Velocidad a la cual el riesgo puede manifestarse, i.e. si el riesgo ocurre cuanto toma el impacto máximo en sentirse	Persona responsable del riesgo	Descripción de las acciones adicionales que son requeridas para gestionar el riesgo	Persona(s) responsable(s) de completar el Plan de Respuesta	Fecha(s) cuando las acciones del Plan de Respuesta deben ser completadas	Situación de las acciones del Plan de Respuesta	Próxima fecha cuando el riesgo va a ser revisado.	

ANEXO 5 - Risk Breakdown Structure



ANEXO 6 - Taxonomía de Riesgos de Ciberseguridad



ANEXO 7 - Cuestionario de tratamiento del riesgo

Nombre:	
Área:	
Puesto:	
Fecha:	

Riesgo	**Hecho(s) y/o Posible(s) Causa(s)**	**Consecuencia(s)** (lo que nos dañará)
Pérdida de licencia social debido a accidentes, contaminación del aire, contaminación sonora, etc.	Tránsito intensivo de camiones de clientes y/o proveedores, generado por las operaciones.	Protestas y/o bloqueo de vías.

A. ¿Cuáles son los elementos del riesgo resolver?	
Control 1	i.e. Cronograma de recepción/despacho de camiones de clientes/proveedores
Control 2	
Control 3	
Control 4	
Control 5	

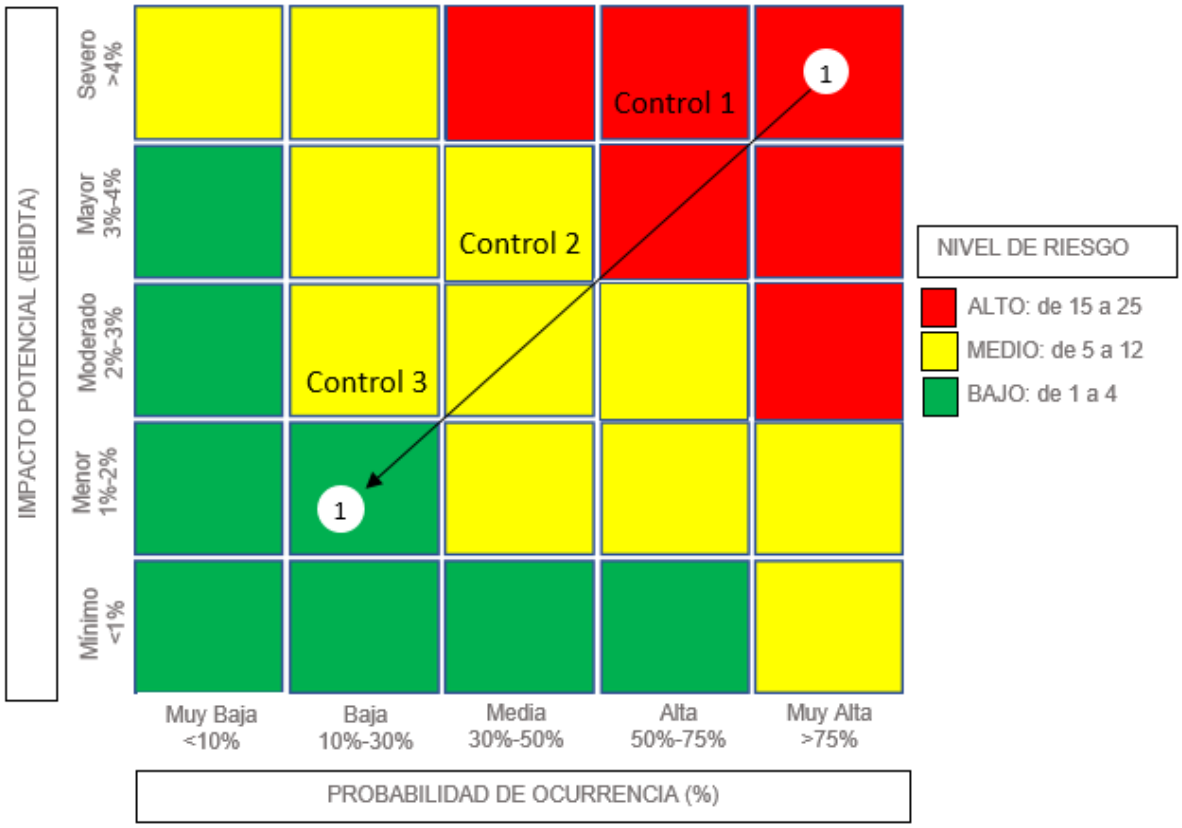
B. ¿Cuáles son los controles clave actuales que mitigan este riesgo?	
Elemento 1	i.e. contaminación del aire, contaminación sonora, etc.
Elemento 2	
Elemento 3	
Elemento 4	
Elemento 5	

C. ¿Cuáles son las acciones adicionales requeridas para mitigar el riesgo?	
Acción 1	i.e. Control de emisiones de camiones de clientes/proveedores
Acción 2	
Acción 3	
Acción 4	
Acción 5	

D. Acciones	**Responsable del Plan de Respuesta**	**Fecha**
Acción 1	i.e. Javier Carrasco, Gerente Corp. de Gestión de Riesgos	10.04.23
Acción 2		
Acción 3		
Acción 4		
Acción 5		

ANEXO 8 – Mapa de Calor

La respuesta al riesgo inherente, es decir el control, debe apuntar a ubicar el riesgo residual a un nivel aceptable. En el ejemplo descrito en este mapa de calor, el Riesgo "1" que se encuentra en un Nivel de Riesgo Inherente Alto (impacto severo, probabilidad muy alta) cuenta con tres controles que atacan tanto el impacto como la probabilidad del riesgo, y que en conjunto llevan al Riesgo "1" a un nivel de Riesgo Residual Bajo (impacto menor, probabilidad baja).



ANEXO 9 - Declaración de Política de Ciberseguridad – Seguridad de la Información

UNACEM S.A.A. reconoce a la información como un activo esencial para el cumplimiento de su misión, visión y objetivos estratégicos, por lo tanto, se compromete a:

- Preservar la confidencialidad, integridad y disponibilidad de los activos de información.
- Adoptar las medidas físicas, técnicas, humanas, administrativas y jurídicas que sean necesarias para proteger los datos personales tratados por el Grupo, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Gestionar los riesgos e incidentes de ciberseguridad y/o seguridad de la información.
- Proteger la información y la plataforma tecnológica que la soporta, como parte de una estrategia orientada a la continuidad del negocio.
- Fortalecer la cultura de seguridad de la información en los empleados, proveedores y clientes.
- Cumplir con la normatividad legal vigente aplicable y otros requisitos contractuales que suscriba la Corporación con terceras partes.
- Garantizar la mejora continua y el desempeño esperado en todos los procesos de la Corporación.

UNACEM S.A.A. se reserva el derecho de iniciar acciones administrativas o legales, según corresponda, hacia las personas o empresas cuyo accionar no se adhiera a la presente declaración de política.

ANEXO 10 - “One page” de riesgo

1. Título del riesgo.

Impacto Inherente EBITDA (PEN)	Probabilidad Inherente	Nivel de Riesgo Inherente	Impacto Residual EBITDA (PEN)	Probabilidad Residual	Nivel de Riesgo Residual	Impacto Reputacional	Dueño del Riesgo	Unidad de Negocio

Descripción

Controles existentes

Plan de respuesta	Estatus	Fecha de finalización	Responsable