1. PROPÓSITO Y ALCANCE

Este documento establece la política de evaluación y gestión de riesgos de Seguridad de Información y Ciberseguridad del Grupo UNACEM frente a las amenazas cibernéticas. Busca brindar un enfoque estructurado para identificar, analizar, evaluar y tratar los riesgos. Aplica a todos los activos de información y de TI de las operaciones del Grupo UNACEM, y que son parte del Sistema de Gestión de Seguridad de la Información (SGSI) y el Marco de Ciberseguridad (CSF).

Esta política es de aplicación al Grupo UNACEM que comprende a UNACEM CORP S.A.A. (en adelante, la "Compañía") y sus Subsidiarias (en adelante, "Unidad de Negocio"), y a sus directores, y gerentes y demás trabajadores (en adelante, "los trabajadores").

2. POLÍTICA

Aplicamos una metodología de gestión de riesgos de Seguridad de Información y Ciberseguridad que incluye la identificación de riesgos mediante la actualización periódica del inventario de activos de información y tecnología, la definición del apetito de riesgo, y la evaluación de los controles existentes. Este proceso de evaluación es contínuo y documentado, prioriza los riesgos para su tratamiento y es supervisado a nivel de unidad de negocio, corporativo y directorio.

3. LINEAMIENTOS

A continuación, se detallan los lineamientos que las Unidades de Negocio deberán implementar, acorde con los roles y responsabilidades descritos en el Capítulo 4.

3.1. Identificación de riesgos de seguridad de Información y ciberseguridad

a) Identificamos y actualizamos periódicamente los inventarios de Activos de Información y tecnología para evaluar los riesgos.

b) Los Activos de Información se categorizan de acuerdo a su naturaleza (instalaciones, servicios, aplicaciones, datos, soportes, equipos informáticos, auxiliares, redes, claves criptográficas, etc).

c) Los Activos de Información se clasifican según la Política de Clasificación y Tratamiento de Información, para su protección y gestión de riesgos.

d) Analizamos las amenazas y vulnerabilidades de los Activos de Información en coordinación con los propietarios de la información, para obtener una visión integral de los riesgos que puedan comprometer los Activos de Información.

3.2. Apetito de Riesgo

a) El apetito de riesgo es aprobado por el Directorio y determina nivel máximo aceptable de impacto y probabilidad de un riesgo, para la toma de decisiones y asignación de recursos.

b) Las Unidades de Negocio cuantifican el impacto potencial en función del EBITDA (en caso de ser cercano a cero, se utiliza otra métrica definida por el Comité de Riesgos y Cumplimiento).

c) El Directorio aprueba umbrales de indicadores clave, que definen el nivel mínimo aceptable, en función de la probabilidad máxima de ocurrencia del riesgo.

3.3. Identificación de controles existentes

a) Evaluamos constantemente si los controles actuales mitigan eficazmente los riesgos, documentando su diseño, operación y mantenimiento.

b) Realizamos auditorías periódicas, incluyendo pruebas de penetración y simulaciones de incidentes para medir su efectividad.

c) Definimos KPIs y KRIs para monitorear el desempeño de los controles, asegurando su contribución a la reducción de riesgos.

d) Revisamos y ajustamos los controles tras incidentes de seguridad, identificando causa raíz, oportunidades de mejora y fortalecimiento de controles existentes.

3.4. Evaluación de riesgos

a) Realizamos una evaluación de riesgos periódica, en donde se analizan los Activos de Información y detectamos nuevos riesgos.

b) Analizamos los riesgos identificados, y determinamos el nivel de priorización en función de su probabilidad e impacto.

c) Clasificamos como críticos los riesgos que superen el apetito de riesgo, establecemos el tratamiento apropiado, y los reportamos al Directorio para su evaluación y supervisión.

d) Estimamos la probabilidad de ocurrencia e impacto utilizando registros históricos o juicio de experto y la documentamos para reportarla a los niveles requeridos.

3.5. Respuesta al riesgo

a) Evaluamos y definimos acciones para tratar todos los riesgos, en coordinación con el CISO Corporativo, propietarios de los Activos de Información y la gerencia.

b) Aplicamos estrategias de respuesta a los riesgos, como aceptar, compartir, mitigar o evitar el riesgo, según corresponda.

c) Cuando establecemos controles y planes de mitigación, detallamos su objetivo, responsable, evidencia y seguimiento para lograr su efectividad y facilitar la auditoría.

d) Supervisamos la implementación de controles y planes de mitigación, presentando avances a la Dirección Corporativa de Riesgos y Cumplimiento.

3.6. Reporte de riesgos

a) Informamos y gestionamos los riesgos de Seguridad de Información y Ciberseguridad, para asegurar decisiones alineadas con la estrategia y apetito de riesgo del Grupo.

b) Establecemos mecanismos de comunicación efectiva para reportar riesgos e impactos a los niveles apropiados de la organización.

c) Utilizamos el reporte de riesgos en la toma de decisiones estratégicas y operativas.

3.7. Monitoreo y revisión

a) Realizamos un monitoreo continuo de la implementación y eficacia de los controles y gobierno en la gestión de riesgos.

b) Analizamos periódicamente cambios en Activos de Información, amenazas, vulnerabilidades y estrategias de tratamiento, incorporándolos en la gestión de riesgos.

c) Revisamos la ejecución de los planes de respuesta a riesgos, asegurando que las acciones implementadas sean efectivas y sostenibles.

d) El CISO Local documenta y presenta el estado de la gestión de riesgos de Seguridad de Información y Ciberseguridad al CIO Local y al Comité Operativo de Seguridad de Información y Ciberseguridad presidido por el CISO Corporativo.

4. RESPONSABLE DE LA POLÍTICA Y SU REVISIÓN

El Director Corporativo de Riesgos y Cumplimiento es el responsable de esta Política y vela por su cumplimiento.

El CISO Corporativo, designado por el responsable de esta Política, es el encargado de garantizar su implementación, liderar la estrategia de seguridad de la información y ciberseguridad, supervisar el cumplimiento de los objetivos establecidos y coordinar la definición y alineación de los presupuestos y recursos a nivel corporativo y local.

Los Gerentes Generales de las Unidades de Negocio deberán garantizar el cumplimiento de esta Política, sus lineamientos y la estrategia de seguridad de la información y ciberseguridad. Para ello, deberán designar y supervisar al CISO Local responsable de su implementación, así como asegurar la disponibilidad de los recursos necesarios para alcanzar los objetivos establecidos en su Unidad de Negocio.

El CISO Corporativo deberá revisar y actualizar esta Política cuando ocurra algún cambio importante en el entorno del Grupo UNACEM o por lo menos cada dos años, sometiendo cualquier cambio a los niveles de aprobación correspondientes.

Los CISOs Locales son responsables de la operación directa de la seguridad de información y ciberseguridad, y deberán adaptar, implementar, mantener las operaciones y desplegar las soluciones tecnológicas acorde a esta política en sus respectivas Unidades de Negocio, y escalar oportunamente las excepciones necesarias al CISO & CDO Corporativo.

5. DOCUMENTOS DE REFERENCIA

Código	Documento
-	Código de Ética y Conducta
-	ISO/IEC 27001
-	Marco de Ciberseguridad de NIST versión 2.0
UC-SI-POL003	Política Corporativa de Clasificación y Tratamiento de Información
-	Política Corporativa de Gestión Integral de Riesgos

Nombre del Documento	**Política Corporativa de Evaluación y gestión de Riesgos de Seguridad de Información y Ciberseguridad**			Versión
Elaborado por	Luis Budge Gerente Corporativo de Ciberseguridad	Fecha de Elaboración	15/05/2025	1.0
Elaborado por	Guillermo Cortijo Supervisor Corporativo de Seguridad de información y Ciberseguridad	Fecha de Elaboración	15/05/2025	1.0
Revisado por	Fernando Dyer Director Corporativo de Riesgos y Cumplimiento	Fecha de Revisión	26/05/2025	1.0
Revisado por	Pedro Lerner Gerente General Corporativo	Fecha de Revisión	26/05/2025	1.0
Revisado por	Comité de Riesgos y Cumplimiento	Fecha de Revisión	18/06/2025	1.0
Aprobado por	Directorio	Fecha de Aprobación	18/06/2025	1.0

6. ANEXO - DEFINICIONES

- **Activo de información.-** Es todo aquello que es o contiene información a la cual la Compañía directamente le atribuye un valor y, por lo tanto, requiere protección.

- **Activo de TI.-** Un componente o recurso, tanto físico como lógico, utilizado en el entorno de Tecnologías de la Información (TI) que aporta valor a la Compañía.

- **Amenaza.-** Causa potencial de un incidente no deseado, que puede resultar en daño a los activos, tales como la información, los procesos y los sistemas y el consiguiente perjuicio a la organización.

- **Apetito de riesgo.-** Es el nivel de riesgo que la Compañía está dispuesta a asumir para cumplir con sus objetivos.

- **Confidencialidad.-** Característica de la información que está disponible solo para personas o sistemas autorizados.

- **Disponibilidad.-** Característica de la información a la cual pueden acceder solo las personas autorizadas cuando sea necesario.

- **Impacto**.- Consecuencias económicas, legales u operativas que sufre la Compañía cuando se materializa un riesgo.

- **Información**.- Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptibles de ser procesada, distribuida y almacenada.

- **Integridad.-** Característica de la información que es modificada solo por personas o sistemas autorizados y de una forma permitida.

- **Probabilidad.-** Es la posibilidad de que un evento se materialice y cause un impacto en la Compañía.

- **Riesgo:** Es un evento, acción u omisión, de fuente interna o externa, que puede ocurrir y afectar de manera adversa el logro de los objetivos.

- **Vulnerabilidad:** La debilidad de un activo (personal, hardware, software, información física o lógica) o un control (política, procedimiento, guía, práctica) que puede ser explotada por una o más amenazas.

- **CISO (Chief Information Security Officer) Corporativo:** La figura de liderazgo encargada de la estrategia de seguridad de la información y la supervisión de su implementación a nivel corporativo.

- **CISO (Chief Information Security Officer) Local:** Responsable de implementar y mantener la estrategia de seguridad de la información definida corporativamente en su respectiva unidad de negocio.