1. PROPÓSITO Y ALCANCE

Este documento establece el modelo y la estructura de gobierno para la protección de la información y de los sistemas del Grupo UNACEM frente a las amenazas cibernéticas. Busca proteger la confidencialidad, integridad y disponibilidad de los datos críticos, la continuidad operativa y facilitar el cumplimiento de los requisitos legales y regulatorios aplicables.

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.

El Grupo UNACEM aplica una estrategia mediante un enfoque integral de ciberseguridad y gestión de riesgos, alineado con NIST, ISO 27001 e IEC 62443, protegiendo los activos que almacenan y procesan información crítica, así como la información crítica en sí misma, aplica el modelo de tres líneas de defensa y supervisa el cumplimiento normativo.

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. Cumplimiento Normativo y Regulatorio

3.1.1. Adhesión a Estándares Internacionales

Adoptamos las directrices del "Cybersecurity Framework NIST" para mejorar la postura de seguridad cibernética del grupo, identificando y priorizando las acciones frente a las amenazas más significativas.

3.1.2. Legislación Nacional y Acuerdos Internacionales

a) Nos adherimos a las leyes de cada país donde el Grupo UNACEM tenga presencia, integrando sus requisitos en nuestros procesos y prácticas de seguridad de las respectivas Unidades de Negocio.

b) Respetamos los acuerdos sectoriales o bilaterales entre países, que afecten el tratamiento y la transferencia de datos en las jurisdicciones que nos apliquen.

c) Desarrollamos capacidades tecnológicas de protección en nuestras Unidades de Negocio, que faciliten el cumplimiento de las leyes de protección de datos personales en las jurisdicciones que nos apliquen.

3.1.3. Establecimiento de las 3 líneas de defensa

El Grupo UNACEM utiliza el modelo de 3 líneas de defensa para asignar los roles de la responsabilidad de la gestión integral de riesgos

a) Primera línea de defensa: Unidad de Negocio

Son responsables de la identificación y evaluación de riesgos (establecer los riesgos asociados a sus procesos), así como la implementación y efectividad de los controles internos para prevenir, detectar y mitigar riesgos, asegurando que las actividades se desarrollen de acuerdo con las políticas y procedimientos establecidos.

b) Segunda línea de defensa: La Dirección de Riesgos y Cumplimiento

Realiza la supervisión y seguimiento en materias relacionadas con el riesgo en su rol de segunda línea de defensa. Esta línea se encuentra a cargo del equipo Corporativo de Ciberseguridad del grupo UNACEM, liderado por el CISO corporativo y se incluyen funciones como la gestión de riesgos, la estrategia de Ciberseguridad, así como el cumplimiento normativo. En este nivel de defensa no se ejecutan las operaciones, pero se supervisan y monitorean los controles de la primera línea, ayudando a mejorar la gestión de riesgos y el cumplimiento de las normativas internas y externas. Esta línea desarrolla y actualiza las políticas, procedimientos, manuales y capacitaciones para abordar los riesgos existentes, nuevos y emergentes.

c) Tercera línea de defensa: Auditoría Interna Corporativa

Realiza el aseguramiento del programa de gestión integral de riesgos en su rol de tercera línea de defensa. La auditoría interna revisa en la primera y segunda línea de defensa la estrategia, el diseño, la implementación y la efectividad del programa corporativo de seguridad de información y ciberseguridad, y emite recomendaciones de mejora.

3.1.4. Relaciones Contractuales

a) Incluimos cláusulas específicas en los contratos con empleados, proveedores, socios comerciales y otras terceras partes, que exigen el cumplimiento de las políticas de seguridad de la información, ciberseguridad y tratamiento de datos personales.

b) Nuestra estrategia de gobierno de seguridad información y ciberseguridad fomenta la evaluación de cumplimiento normativo en las relaciones con terceros que manejen o accedan a la información de uso interno o confidencial del grupo.

3.1.5. Respaldo y Recuperación de la Información

Establecemos planes de respaldo y recuperación de la información acordes con nuestras necesidades y mejoras prácticas internacionales, con el fin de preservar la

continuidad del negocio ante incidentes que puedan afectar la disponibilidad e integridad de los datos.

3.1.6. Registro, documentación y reporte

Registramos, documentamos y reportamos los controles de seguridad de la información y ciberseguridad, cumpliendo con los requisitos de transparencia, integridad y trazabilidad demandados por las mejores prácticas.

3.2. Identificación de Activos y Riesgos

a) Identificamos, documentamos y clasificamos los activos de información y riesgos de ciberseguridad asociados, asegurando su actualización y asignando de responsables para su gestión.

b) Realizamos evaluaciones periódicas de riesgos sobre los activos de información para detectar amenazas y vulnerabilidades, e implementar estrategias de tratamiento.

c) Comunicamos y capacitamos sobre políticas de gestión de riesgos y estrategias alineadas con normativas aplicables.

d) Implementamos mecanismos de identificación continua de activos de información, así como la actualización constante de su inventario.

3.3. Control de Acceso y Gestión de Identidades

a) Gestionamos y restringimos los accesos según necesidad, aplicando mínimo privilegio y revisando permisos periódicamente.

b) Implementamos autenticación robusta (e.g. doble factor de autenticación) y gestión de credenciales de forma segura, con revocación inmediata cuando sea necesario.

c) Utilizamos sistemas de gestión de identidades para controlar el ciclo de vida de los usuarios y responder ante compromisos de seguridad.

d) Monitoreamos los accesos e identidades autorizados de manera continua y ejecutamos auditorías periódicas.

3.4. Gestión de Riesgos de seguridad de información y Ciberseguridad

a) Adoptamos una metodología de gestión de riesgos de seguridad de información y ciberseguridad reproducible, alineada con las mejores prácticas, basada en probabilidad e impacto. Aseguramos su documentación y comunicación para identificar, mitigar y gestionar los riesgos de ciberseguridad que atenten contra la continuidad operativa e información del Grupo UNACEM.

b) Identificamos, analizamos y priorizamos los riesgos de seguridad de información y ciberseguridad, determinando umbrales críticos para facilitar las decisiones y asignación de recursos.

c) Diseñamos e implementamos planes de mitigación adaptados a cada riesgo, reduciendo su impacto o probabilidad a niveles aceptables, considerando eficiencia y costo-beneficio.

d) Desarrollamos reportes, indicadores clave (KPIs) e indicadores de riesgos (KRIs) para medir y reportar la evolución de la probabilidad del riesgo, la efectividad de controles, y determinar los ajustes y mejoras.

e) Mantenemos y reportamos un registro actualizado a la alta dirección y al directorio, para una gestión, supervisión y vigilancia efectivas, promoviendo retroalimentación y mejora continua.

3.5. Monitoreo Continuo

a) Implementamos sistemas para monitorear los activos de información y riesgos de ciberseguridad en el ciberespacio (infraestructura, redes, sistemas, internet), identificando amenazas y generando alertas de seguridad.

b) Analizamos y respondemos a las alertas de seguridad mediante procedimientos que permitan priorizarlas y diferenciar posibles incidentes reales de falsos positivos, con protocolos de acción definidos.

c) Actualizamos periódicamente nuestro sistema de monitoreo y políticas para fortalecer nuestra respuesta ante nuevas amenazas.

3.6. Respuesta ante Incidentes y Continuidad del Negocio

a) Implementamos planes de respuesta ante incidentes, definiendo procedimientos para la detección, evaluación, contención y erradicación de amenazas.

b) Conformamos equipos CSIRT (Cyber Security Incident Reponse Team) en las Unidades de Negocio, los cuales se activan ante incidentes y notifican a las partes interesadas.

c) Establecemos planes de recuperación y continuidad del negocio, efectuamos pruebas periódicas y mantenemos copias de seguridad actualizadas según la necesidad y protegidas para garantizar la restauración de información.

d) Ante incidentes, ejecutamos un análisis de causa raíz, ajustando procedimientos, políticas y planes de respuesta para mejorar la resiliencia ante nuevas amenazas.

3.7. Gestión de Tecnologías y Herramientas de Seguridad

a) Evaluamos tecnologías de seguridad según análisis de riesgos, estándares de la industria y validación del CISO Corporativo, antes de su adquisición.

b) Implementamos y configuramos las herramientas tecnológicas siguiendo lineamientos de seguridad, documentando su uso para garantizar continuidad y consistencia.

c) Establecemos un programa de mantenimiento y actualización constante, aplicando parches de seguridad y revisando periódicamente su efectividad.

d) Monitoreamos el rendimiento y efectividad de las herramientas, realizando pruebas de penetración para detectar fallos y optimizar la infraestructura de ciberseguridad, así como sus capacidades de mitigación de los riesgos.

3.8. Excepción al cumplimiento de las políticas

Frente a eventos que requieran una excepción a la aplicación de las políticas:

a) Identificamos, registramos, evaluamos y reportamos oportunamente al CISO Local, quien evaluará y aprobará formalmente la excepción solicitada, antes de su ejecución, con copia al CISO Corporativo.

b) Seguimos protocolos de comunicación interna y externa para comunicar los impactos pertinentes a las partes interesadas internas y externas afectadas.

c) Mantenemos monitoreo preventivo para detectarlos y prevenirlos, e incluimos la implementación de nuevas tecnologías y prácticas de capacitación.

d) Reforzamos la cultura de seguridad de la información del Grupo para comunicar la importancia de adherirse a las políticas.

e) Cuando las excepciones no se encuentran oportunamente aprobadas y/o soportadas adecuadamente, se aplicarán los procedimientos disciplinarios respectivos.

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.

En el Grupo UNACEM todos tienen la responsabilidad individual de cumplir con las reglas y lineamientos aquí establecidos, así como de buscar orientación ante cualquier duda o necesidad de analizar si una actividad puede violar las normas descritas en esta política.

Se aplicarán medidas disciplinarias y sanciones a aquellos que incumplan lo establecido en la presente política, según lo regulado en los Reglamentos Internos (por ejemplo, Reglamento Interno de Trabajo de cada Unidad de Negocio).

5. DOCUMENTOS DE REFERENCIA

Código	Documento
-	Código de Ética y Conducta
-	ISO/IEC 27001
-	Marco de Ciberseguridad de NIST versión 2.0

Nombre del Documento	Política Corporativa de Organización de la 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

Activos de información relevantes: Activos de información necesarios para que el Grupo UNACEM cumpla con sus objetivos y cuya valoración medida por el perjuicio cuando el activo se ve dañado en términos de la confidencialidad, integridad y disponibilidad de la información es alta, muy alta y extrema.

- **Ciberseguridad:** Es el conjunto de tecnologías, procesos y prácticas diseñadas para proteger redes, dispositivos, programas y datos de ataques, daños o accesos no autorizados.

- **Confidencialidad:** Se refiere a la propiedad que garantiza que la información no esté disponible ni sea divulgada a individuos, entidades o procesos no autorizados.

- **Integridad:** Es la propiedad de salvaguardar la exactitud y completitud de la información y los métodos de procesamiento.

- **Disponibilidad:** Es la propiedad que garantiza que la información esté accesible y utilizable a petición de una entidad autorizada cuando se requiera.

- **Gestión de Riesgos:** El proceso de identificación, evaluación y tratamiento de riesgos que atenten contra el logro de los objetivos de negocio del Grupo UNACEM

- **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.

- **Incidente de Seguridad:** Un evento adverso o una amenaza con la capacidad de impactar negativamente en la infraestructura de la información o en la información misma.

- **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 estratégicos u operacionales.

- **Riesgos estratégicos**: Son eventos que podrían impactar adversamente el logro del propósito u objetivo estratégico, sean por impactos a las iniciativas, capacidades u otros habilitadores. Se incluyen en esta categoría los riesgos de proyectos.

- **Riesgos operacionales:** Son eventos que podrían impactar adversamente el desempeño o eficiencia de las operaciones en marcha. En esta categoría están incluidos, entre otros, los riesgos de producción, logísticos, ciberseguridad, reporte financiero, legales y de cumplimiento