

 GRUPO UNACEM	DIRECCIÓN DE RIESGO Y CUMPLIMIENTO	Versión 1.0
	POLÍTICA CORPORATIVA DE CLASIFICACIÓN Y TRATAMIENTO DE LA INFORMACIÓN	
Código: UC-SI-POL-003		Página 1 de 6

1. PROPÓSITO Y ALCANCE

El propósito de la presente política es establecer un marco corporativo dentro del ámbito de Seguridad de Información y Ciberseguridad, que rige la categorización y manejo adecuado de la información dentro del Grupo UNACEM, con un enfoque sistemático y estructurado que busca proteger la integridad, confidencialidad y disponibilidad de los Activos de Información.

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”).

Este documento gobierna a toda la información generada, procesada, almacenada o transmitida por el Grupo UNACEM, así como la infraestructura utilizada para tales fines, sin importar su formato (electrónico o físico). Esto incluye datos en tránsito o en reposo dentro de las unidades de negocio.

La eficacia y ejecución constante de esta política es crucial para minimizar el riesgo de pérdida de información, daño reputacional, y para garantizar la competitividad y eficiencia operacional del Grupo UNACEM. El enfoque de clasificación permite asignar niveles apropiados de protección y estipular controles específicos para diferentes tipos de información, basándose en su valor, requisitos legales y sensibilidad. La gestión apropiada del tratamiento de la información respalda la toma de decisiones informadas, asegura la transparencia y fortalece la confianza de nuestras partes vinculadas.

2. POLÍTICA.

El grupo Unacem establece directrices para proteger y gestionar adecuadamente los datos según su nivel de sensibilidad: pública, interna y confidencial / Crítica. Define responsabilidades en la clasificación, controles de seguridad, auditorías y medidas de almacenamiento, acceso, transferencia y eliminación segura de la información. Además, incluye protocolos de respuesta ante incidentes y un programa de formación continua para concienciar a los empleados sobre la seguridad de la información.

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. Clasificación de Información

El Grupo UNACEM define la siguiente estructura para clasificar sistemáticamente la información, asegurando que sea gestionada de manera que se preserve la confidencialidad, integridad y disponibilidad en consonancia con las políticas corporativas y normativas aplicables.

 GRUPO UNACEM	DIRECCIÓN DE RIESGO Y CUMPLIMIENTO	Versión 1.0
	POLÍTICA CORPORATIVA DE CLASIFICACIÓN Y TRATAMIENTO DE LA INFORMACIÓN	
Código: UC-SI-POL-003		Página 2 de 6

Tabla N° 01: Clasificación de la Información

Clasificación	Descripción	Ejemplos
Pública	Esta categoría incluye información que es accesible por cualquier persona sin que esto represente un riesgo para el Grupo UNACEM. Su divulgación es intencional y puede ser parte de las operaciones normales del Grupo o requerimientos legales. La protección de la información pública se enfoca en garantizar su integridad y disponibilidad.	Reportes anuales, hechos de importancia, comunicados de prensa, contenido del sitio web corporativo, folletos institucionales.
Interna	La información interna está restringida al uso dentro del Grupo UNACEM y su divulgación no autorizada le podría causar impacto negativo. Las políticas de Seguridad de Información y Ciberseguridad están diseñadas para proteger esta información del acceso no autorizado. La información interna es información que no es Pública.	Procedimientos operativos, políticas internas, agendas, informes de seguimiento de proyectos, bases de datos, documentación contable, reportes financieros y no financieros internos y cualquier otra información que no sea definida como pública.
Confidencial / Crítica	La información confidencial / crítica es aquella Interna, cuya divulgación no autorizada o manipulación indebida podría causar un daño significativo al Grupo UNACEM o partes interesadas. Incluye datos personales, financieros, de clientes, y cualquier otro tipo de información que el Grupo dispone y que requiere resguardo con apropiados niveles de seguridad. Los accesos son controlados y se toman medidas para proteger su integridad, confidencialidad y disponibilidad.	Datos personales de clientes o empleados, estrategias comerciales, activos operacionales críticos, datos financieros sensibles.

 GRUPO UNACEM	DIRECCIÓN DE RIESGO Y CUMPLIMIENTO	Versión 1.0
	POLÍTICA CORPORATIVA DE CLASIFICACIÓN Y TRATAMIENTO DE LA INFORMACIÓN	
Código: UC-SI-POL-003		Página 3 de 6

3.2 Manejo y Protección de la Información

- a) Promovemos que cada empleado conozca y cumpla con sus responsabilidades en la correcta clasificación de la información según los criterios establecidos.
- b) Desarrollamos guías detalladas que indiquen cómo clasificar, desclasificar y eliminar información (Pública, Interna, Confidencial / Crítica) según plazos de retención y relevancia.
- c) Implementamos controles de seguridad adecuados, como etiquetado, cifrado de datos, validación, autenticación y autorización de accesos, así como monitoreo constante, para proteger la información de acuerdo al nivel de clasificación asignado.
- d) Realizamos auditorías y evaluaciones periódicas para verificar el cumplimiento y actualizar los criterios de clasificación según su pertinencia y efectividad.
- e) Establecemos protocolos de almacenamiento seguro según el nivel de clasificación, utilizando entornos físicos controlados y datos cifrados.
- f) Implementamos un sistema de acceso controlado basado en mínimo privilegio requerido, limitando el acceso solo a personal autorizado.
- g) Definimos y aplicamos métodos seguros para la transferencia de información, incluyendo cifrado y redes de comunicaciones seguras.
- h) Proveemos métodos validados para la destrucción segura de información Pública, Interna y Confidencial.
- i) Implementamos un proceso de respuesta ante incidentes para mitigar impactos y prevenir recurrencias, con notificación oportuna.
- j) Implementamos un programa de formación continua para capacitar a los empleados en clasificación y manejo seguro de la información, utilizando materiales educativos actualizados.
- k) Realizamos evaluaciones periódicas para medir la comprensión y aplicación de las políticas de Seguridad de Información y Ciberseguridad en la organización.

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

 GRUPO UNACEM	DIRECCIÓN DE RIESGO Y CUMPLIMIENTO	Versión 1.0
	POLÍTICA CORPORATIVA DE CLASIFICACIÓN Y TRATAMIENTO DE LA INFORMACIÓN	Vigencia: [31-12-2026]
Código: UC-SI-POL-003		Página 4 de 6

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.

5. DOCUMENTOS DE REFERENCIA

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

Listar las personas que participaron en la revisión y consenso de un documento de proceso.

 GRUPO UNACEM	DIRECCIÓN DE RIESGO Y CUMPLIMIENTO	Versión 1.0	
	POLÍTICA CORPORATIVA DE CLASIFICACIÓN Y TRATAMIENTO DE LA INFORMACIÓN		Vigencia: [31-12-2026]
Código: UC-SI-POL-003			Página 5 de 6

Nombre del Documento	Política Corporativa de Clasificación y Tratamiento de la Información			Versión
Elaborado por	Luis Budge Gerente Corporativo de Ciberseguridad	Fecha de Elaboración	16/05/2025	1.0
Elaborado por	Guillermo Cortijo Supervisor Corporativo de Seguridad de información y Ciberseguridad	Fecha de Elaboración	16/05/2025	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:** Cualquier dato, información o recursos relacionados con la información que tienen valor para el Grupo y por tanto requieren de protección.
- **Confidencialidad:** Propiedad que tiene la información por ser accesible solo para aquellos autorizados a acceder a ella.
- **Integridad:** Garantía de la exactitud y totalidad de la información y los métodos de su procesamiento.
- **Disponibilidad:** Característica de la información por ser accesible y utilizable por un usuario autorizado cuando se requiera.

 GRUPO UNACEM	DIRECCIÓN DE RIESGO Y CUMPLIMIENTO	Versión 1.0
	POLÍTICA CORPORATIVA DE CLASIFICACIÓN Y TRATAMIENTO DE LA INFORMACIÓN	Vigencia: [31-12-2026]
Código: UC-SI-POL-003		Página 6 de 6

- **Continuidad del Negocio:** Capacidad de continuar con la entrega de productos o servicios a niveles preestablecidos aceptables tras un incidente disruptivo.
- **Gestión de Riesgos:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Usuarios de la Información:** Cualquier empleado o individuo que maneje datos en nombre del Grupo, responsable de adherirse a las políticas y procedimientos de clasificación y tratamiento de la información.
- **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.
- **Niveles de Clasificación:** Categorías asignadas a la información para determinar las necesidades de protección y manejo basadas en su sensibilidad y valor para el Grupo Unacem.
- **Controles de Seguridad:** Medidas de protección implementadas para salvaguardar la información y prevenir accesos no autorizados, alteraciones o pérdidas.
- **Criptografía:** Uso de técnicas matemáticas para cifrar y descifrar datos con el fin de proteger la confidencialidad e integridad de la información transmitida o almacenada.
- **Mínimo Privilegio:** Principio de seguridad por el cual los usuarios reciben el menor nivel de privilegios necesario para realizar sus tareas.
- **Análisis de Impacto de Negocio (BIA):** Proceso destinado a identificar los impactos operativos y financieros resultantes de la interrupción de las actividades y procesos empresariales.