PREPARED BY:
Strategic Management Control Manager

REVIEWED BY:
Audit and Risk Committee
Chief Executive's Office
General Management

APPROVED BY:
Board of Directors

CODE: GE-P001
VERSION: 02
APPROVED ON: May 28, 2026

CORPORATE POLICY OF INTERNAL CONTROL AND INTEGRAL RISK MANAGEMENT

ACEROS AREQUIPA

1. OBJECTIVE

Define our Corporate Internal Control and Enterprise Risk Management Policy, considering the criteria and framework for action to develop, strengthen, and maintain an internal control and enterprise risk management system that supports the Company in achieving its organizational objectives.

2. SCOPE

The application of this policy is applicable to all members of Corporación Aceros Arequipa and Subsidiaries (hereinafter CAASA).

3. RESPONSIBILITIES

Three Lines Model

Internal control and risk management are carried out by all members of the organization, including the Board of Directors, Senior Management, Managers, Deputy Managers, Supervisors, Employees, and the Internal Audit Department. We understand that, according to the COSO framework, internal control is performed through ***Three Lines Model*** [1]***:***

- **First Line:** Process Owners and Employees, who are responsible for maintaining an effective and efficient internal control system.
- **Second Line:** The support areas, such as Quality Management, Environment, Occupational Health and Safety, Legal Services, Asset Security, Quality Control, Budget Control, Inventory Control, among others, supervise compliance with the control guidelines that we have established.
- **Third Line:** The Internal Audit Department, is responsible for evaluating the organization's internal control system and recommending corrective measures or improvements, which may be taken into consideration by the Process Owners Its position is independent from the business areas that will be the subject of its analysis.

[1] The Institute of Internal Auditors, The IIA's Three Lines Model: An Update of the Three Lines of Defense (2020), pages 4-6.

Each of the people that make up our organization fulfills a function within the internal control and comprehensive risk management system, the main responsibilities being the following:

3.1. Board of Directors

It is responsible for approving the internal control and comprehensive risk management policy and defining the corresponding roles, responsibilities and reporting lines. As well as supervising its effectiveness and suitability[2], for this purpose, assigns direct responsibility for risk management and the implementation, maintenance and permanent updating of internal control systems to the Executive Presidency and General Management.

Likewise, it delegates to the Audit and Risk Committee (CAR) the evaluation of the effectiveness of the internal control system[3] and risk management.

3.2. Audit and Risk Committee (ARC)

It is responsible for ensuring that CAASA has an effective internal control system and that policies and procedures are implemented to ensure adequate risk management, ensure compliance with corporate codes and policies approved by the Board of Directors, periodically monitor management of risks and report it to the Board of Directors, and consider the effectiveness of CAASA's internal control over annual and interim financial information, including information technology security and control[4].

3.3. Executive Presidency

In coordination with the General Manager, defines the Corporate Strategic Plan, establishes short-, medium-, and long-term objectives[5], identifies ***strategic and emerging risks that could affect the achievement of the Company's strategy, and promotes*** the implementation of mitigation strategies. The Executive President ***also fosters*** a risk management culture ***throughout the organization.***

Annually, in conjunction with the General Management, presents to ***the*** Board of Directors our strategic plan and the main risks to which the business is exposed,

[2] Code of Good Corporate Governance for Peruvian Companies. 2013 – "Principle 25" / page 14
[3] CAASA's Internal Audit Activity Statute. Sep 2020 – "Scope" / Page 1
[4] Statute of the Audit and Risk Committee / page 4
[5] Aceros Arequipa SA Corporation Statute – "Article 63" / Page 16

considering both current and long-term impacts.

3.4. General Management

It is responsible for designing, implementing, maintaining and supervising the internal control system and managing the risks to which we are exposed. The responsibilities of the General Manager, in relation to internal control and comprehensive risk management include[6]:

- Define the objectives and goals, the structure of the organization, the delegation of powers, the internal regulations (***corporate*** policies, codes, guidelines, among others) and the supervision of the results of the officials and collaborators.
- Supervise internal control activities and comprehensive risk management at the Corporate level, assigning the Macroprocess Owners the responsibility for identifying risks and the design, implementation and evaluation of the effectiveness of the controls established in each of their processes.
- Periodically validate with the Board of Directors the risks at the entity level, the associated control activities and the required action plans.

3.5. Macroprocess Owners

Assigned to Managers who have adequate experience and professional judgment for the management of the operational and support processes for which they are responsible, their responsibilities include:

- Supervise the implementation of internal regulations (corporate policies, codes and regulations), as well as define the procedures, instructions and guidelines for the fulfillment of the objectives of its operational or functional units.
- Guarantee that processes are designed to achieve business objectives, minimizing losses and optimizing the use of resources.
- Ensure the implementation and maintenance of comprehensive risk management in the processes under their responsibility, under the GIRO methodology.
- Supervise the control system defined in its processes.

[6] COSO "Internal Control – Integrated Framework. 2013" / page 149

3.6. Process / Sub-Process Owners

Responsibility for our Processes and Sub-Processes is assigned, depending on the degree of complexity and impact on business objectives, to: Managers, Assistant Managers, Supervisors and Supervisors who have experience and adequate professional judgment, their responsibilities include:

- Strengthen the execution of the processes under their responsibility, seeking efficiency and effectiveness in their operations and the fulfillment of business objectives.
- Measure the performance of the process and be accountable for the results achieved.
- Identify and evaluate the risks inherent to the activities of the processes under their responsibility, and define sufficient controls for their administration, in accordance with the GIRO methodology.
- Execute monitoring activities to ensure the correct design and operation of the implemented controls.
- Keep the documentation of your process updated: i) Flowchart, ii) Matrix of risks and controls, and iii) Matrix of segregation of functions (if applicable).

3.7. All Collaborators

- Comply with internal policies, procedures and standards within the scope of our roles and responsibilities.
- Report the identification of new risks or materialization of any risk to the corresponding Process Owner or Sub-Process.
- Report to your direct boss or manager any breach of internal rules, regulations or laws within the framework of CAASA operations.
- Report, through the Ethics Line, any actual or suspected violation of the Company's Code ***of Conduct and*** Code Against Fraud, Corruption and ***Other Crimes.***

3.8. Strategic Management Control Department

- Define and update the risk management methodology considering the reference frameworks, good practices and standards of the external framework, ensuring its continuous improvement.
- Assist Senior Management, Process Owners and collaborators in the deployment of the risk management methodology to identify, analyze,

control and monitor risks at the entity and process level.

- Report to the Audit and Risk Committee (ARC) on the progress of the implementation, ***monitoring,*** and strengthening of CAASA's risk management system.

3.9. Internal Audit Department

Performs audit work exclusively, has autonomy, experience and specialization in the issues under its evaluation, and independence for monitoring and evaluating the effectiveness of the internal control system.The Internal Audit Manager reports directly to the Audit and Risk Committee (ACR) on its plans, budget, activities, progress, results obtained and actions taken.

The Internal Audit Manager reports organizationally to the Board of Directors, so his appointment and dismissal correspond to the Board of Directors at the proposal of the Audit and Risk Committee (ACR)[7].

4. REGULATORY OR REFERENCE FRAMEWORK FRAMEWORK

4.1. Corporate Framework

The Internal Control and Enterprise Risk Management Policy is framed within ***and aligned with the organization's principles, guidelines, and strategic definitions, which guide risk management, decision-making, and the achievement of objectives:***

- ***The Purpose: "Together we build a better world", guides risk management and the internal control system, ensuring that the organization's decisions and actions are carried out in a manner consistent with the generation of sustainable value and a positive impact on our stakeholders.***
- The Vision, to ***be leaders in the Peruvian steel market,*** positioned among the most profitable in the region and with an active presence in the ***international*** market.
- The Mission, by offering steel solutions to our clients, through innovation, continuous improvement and human development, contributing to the growth of the countries in which we participate and increasing value for our

[7] CAASA's Internal Audit Activity Statute. Set 14 – "Authority and Independence" / Pages 1 and 2

shareholders and interest groups.

- Corporate Values: teamwork, passion for work, focus on what matters, ***and integrity.***
- ***The Code of Conduct, which details*** the philosophy, ***behaviors,*** and principles that govern us and serves as a guiding element in our relationship with the ***stakeholder*** groups.
- The Code Against Fraud, Corruption ***and Other Crimes,*** which communicates the guidelines and ***assigned responsibilities*** for preventing, detecting, investigating, and responding to any act of fraud and corruption, maintaining a culture of zero tolerance toward any ilegal act.
- The corporate policies mentioned in annex 1 that allow us to comply with the sustainable management of the business and the generation of shared value.
- The Good Corporate Governance Practices, that promotes a climate of respect for the rights of shareholders and investors in general; It contributes to generating value, solidity and efficiency in the company.

4.2. Methodological and Conceptual Framework

We adopt the following conceptual frameworks:

- The Internal Control reference framework (2013) and the integrated Risk Management framework – ERM (2017) of COSO (Committee of Sponsoring Organizations of the Treadway Commission). COSO is recognized globally as the leading framework for designing, implementing and developing internal control and evaluating its effectiveness.
- The position statement of the Institute of Internal Auditors – IIA (for its acronym in English): The ***three lines*** for effective risk management and control.

Additionally, for specialized functions, we complement the adoption with other reference frameworks such as ISO 31000, COBIT 5 for the management of Information Technology, the Code of Good Corporate Governance issued by the Superintendency of Stock Market (SMV), etc

4.3. Corporate Policies

The Internal Control and Comprehensive Risk Management Policy is developed and complemented by our Corporate Policies and Codes. These are approved by

the Board of Directors in order to strengthen the internal control environment of the Corporation (See Annex I: List of Corporate Policies and Codes).

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

It is an international initiative that establishes recommendations for companies to disclose climate-related financial information, allowing them to evaluate and manage the risks and opportunities associated with ***the material impacts that climate change may have*** on their operations and strategies.

Our methodology focuses on classifying the risks and opportunities in the face of climate change taking into account what is proposed by the TCFD, which are classified as:

- **Physical risks:** They refer to natural disasters or environmental events caused by climate change.
- **Transition risks:** They refer to changes in policies, legislation, technology and the market for the mitigation of climate change.

5. DEFINITIONS

5.1. Risk

An uncertain event or situation that, if it materializes, may affect the achievement of the organization's strategic or process objectives, impacting its performance and the creation or protection of value.

5.2. Inherent Risk

The level of risk present in an activity or process before applying controls or any risk response, considering its likelihood of occurrence and impact.

5.3. Residual Risk

The level of risk to which the organization is exposed after the implementation of controls or risk responses, considering its likelihood of occurrence and impact.

5.4. Risk Criticality

The result of assessing the likelihood of occurrence and the impact of a risk, which determines its level or severity for prioritization purposes.

5.5. Control

An action, mechanism, or activity implemented as part of a risk response, integrated into operations and decision-making, to reduce its likelihood of occurrence and/or impact. It contributes to the achievement of objectives by ensuring that risk remains within the defined risk appetite and tolerance levels through its prevention, detection, or correction.

5.6. Internal Control

A process composed of policies, procedures, and activities, designed and implemented based on risks, incorporated into operations and decision-making, aimed at providing reasonable assurance regarding the achievement of objectives, the protection of resources, and the reliability and efficiency of operations.

5.7. Risk Appetite

The level of risk exposure that the organization is willing to assume in order to achieve its strategic and process objectives, consistent with its strategy and management capacity, establishing the boundaries within which decisions are made.

5.8. Risk Tolerance

The level of acceptable variation in risk exposure relative to the defined risk appetite, which establishes the boundaries within which the organization can operate without compromising the achievement of its objectives.

5.9. Impact

The magnitude of the adverse consequences that a risk could generate if it materializes.

5.10. Probability

The level of possibility that a risk will occur within a given period.

5.11. Opportunity

A potential positive outcome derived from an uncertain event, which may contribute to the achievement of objectives, the creation of value, or the improvement of the organization's performance.

5.12. Latency

The time elapsed between the emergence of a risk and its detection or materialization.

6. INTERNAL CONTROL GUIDELINES

6.1. By adopting this policy, we seek to achieve the following outcomes:

- Prevention: *Reduce the likelihood of risk occurrence through the implementation of controls integrated into processes.*
- Self-control: The ability of each employee to *manage* and control their *activities,* detect deviations, and *execute* corrective actions in *a timely manner.*
- Effectiveness: *Achievement of objectives and expected results in processes, aligned with risk management.*
- Efficiency: Rational and optimal use of resources in process *execution, considering the associated level of risk.*

6.2. Professional Judgment

The internal control system requires the application of professional judgment *in the design, implementation, and execution of* the control activities under each person's responsibility. *To this end, we ensure that our* employees *possess the appropriate competencies, experience, and profile, especially in* positions involving greater risk and responsibility.

6.3. Documentation of the Internal Control System

We have a process documentation methodology *that establishes* the information requirements *necessary for the management* of each process. These requirements include the *identification, assessment,* and documentation of risk and control *matrices, as well as* the recording of evidence *supporting* the compliance and *effectiveness of the implemented controls, ensuring their traceability.*

7. INTEGRAL RISK MANAGEMENT GUIDELINES

7.1. Risk Classification

Risks may be classified by:

a. *By management level: Distinguishes between risks that impact the strategic direction of the business and those that affect day-to-day operations. These are Strategic Risks and Process Risks.*
b. *By risk type: Risks are classified according to their origin and their potential impact on the achievement of objectives. These may include Strategic Risks, Operational Risks, Information and Reporting Risks, and Compliance Risks.*
c. *By impact type: Describes the nature of the consequences that could arise if a risk materializes. These may include Economic, Operations and Information Systems, Reputation and Image, Regulatory and Legal, Environmental, and Occupational Health and Safety impacts.*

7.2. Risk Assessment

Risk assessment aims to determine the severity and prioritization of risks within the organization, considering standardized criteria that allow for their consistent analysis. For each risk, Inherent Risk (exposure without controls) and Residual Risk (exposure after applying controls) are determined.

For this purpose, minimum criteria such as impact and likelihood of occurrence are used, in accordance with the definitions established in this policy (see Definitions Section and Annex II: Risk Assessment Criteria).

a. *Impact: Assessed by considering the consequences that the materialization of the risk could generate for the organization.*
b. *Probability: Assessed by considering the possibility of the risk occurring within a given period, based on criteria such as* (i) Frequency, (ii) Exposure, and (iii) Occurrence Estimate (based on experience and professional judgment).

Additionally, depending on the nature of the processes or specific regulatory requirements, some areas or subprocesses may consider ***additional*** criteria to strengthen the analysis and assessment of risk impact or likelihood of occurrence, such as risk exposure, reversibility, speed of occurrence (latency), vulnerability, among others.

8. INTERNAL CONTROL COMPONENTS AND COMPREHENSIVE RISK MANAGEMENT

By adopting the COSO framework, we declare compliance with the principles of internal control, ***structured around the following components:***

8.1. Control Environment

Is the set of rules, processes, and structures that ***provide*** the foundation for internal control ***across the Corporation.***

The principles of this component are [8]:

a. ***The organization demonstrates*** a commitment to integrity and ethical values.
b. The Board ***of Directors*** demonstrates independence from Senior Management and exercises supervision of the performance of the internal control system, through the Audit and Risk Committee.
c. The Senior Management, with the oversight of the Board of Directors, establishes the structures, reporting lines, and levels of authority and responsibility ***necessary*** to achieve the Company's objectives.
d. ***The organization demonstrates*** commitment to attracting, developing, and retaining competent professionals in alignment with ***organizational objectives,*** in accordance with the Human Management Policy.
e. ***The*** responsibilities ***of individuals*** and the level of internal control ***are defined*** to achieve ***organizational*** objectives.

8.2. Definition of Objectives

The definition of strategic objectives is a ***prerequisite for risk management, as it enables risk identification, risk assessment, and risk response.*** First, strategic objectives must be defined before identifying the risks that the organization faces and defining the actions necessary to manage them[9].

Within this framework, we define and update our corporate objectives through ***the annual Corporate Strategic Planning process,*** ensuring alignment with ***our strategy and risk apetite.***

[8] COSO "Internal Control – Integrated Framework. 2013" / page 31
[9] Enterprise Risk Management – Integrated Framework / page 21

8.3. Event Identification

The Board of Directors and Senior Management recognize that uncertainty exists, therefore, there is no certainty of when an event with negative or positive effects may occur during the course of operations. During his tenure, Senior Management considers a series of potential events, affected by both internal and external factors. If the event may have a negative impact, it represents a risk, whereas events with a potential positive impact may represent opportunities for us. Management must manage both risks and opportunities and define actions and provide resources to mitigate risks and take advantage of opportunities[10].

8.4. Risk assessment

Risk assessment allows us to take into account the degree to which potential events could have an impact on the achievement of our strategic objectives. This evaluation is carried out ***considering*** the probability ***of occurrence and*** impact[11] ***through the application*** of qualitative and quantitative methods.

a. We define and identify our objectives with sufficient clarity to allow the identification and evaluation of risks.
b. We identify the risks to achieve our strategic objectives and analyze them to determine how they should be managed
c. We consider the probability of fraud, corruption and any other event that violates ethics and integrity when evaluating the risks for the achievement of objectives.
d. We identify and evaluate changes that could significantly affect the internal control system.

8.5. Risk Response

After evaluating the relevant risks and based on the company's risk appetite, Senior Management and Officials determine the response strategy. These strategies can be those of accepting, mitigating, sharing or avoiding. When considering the strategy, its effect on the probability and impact of risk is evaluated, as well as the costs and benefits, and the one that places the residual

[10] Enterprise Risk Management – Integrated Framework – / page 37
[11] COSO "Internal Control – Integrated Framework. 2013" / page 59

risk within the tolerance level established according to the risk appetite of the company is selected [12].

8.6. Control Activities

Control activities are actions established to mitigate identified risks based on their level of criticality. Depending on their nature, controls can be preventive or detective and can include manual, semi-automated, and automated controls.

The principles of this component are[13]:

i. We define and develop control activities in business processes that contribute to mitigating risks to acceptable levels.
ii. We define and develop control activities in information systems that contribute to IT risk management.
iii. We deploy control activities through policies and codes that establish the general lines of internal control and procedures or instructions that put said policies and codes into practice.

Segregation of duties is integrated into the design and ***operational execution, that is,*** the development of control activities. In those areas where it is not practical to carry out a segregation of duties, the Process Owner selects and develops alternative control activities with which compliance is mandatory.

8.7. Information and Communication

We have various internal and external communication channels with interested parties to ensure compliance with business objectives and reinforce internal control systems. According to the COSO framework[14]:

a. We obtain, generate and use relevant and quality information to support the operation of the internal control system.
b. We communicate information internally, including the objectives and responsibilities that are necessary to support the functioning of the internal control system.

[12] Enterprise Risk Management – Integrated Framework / page 81
[13] COSO "Internal Control – Integrated Framework. 2013" / page 87
[14] COSO "Internal Control – Integrated Framework. 2013" / page 105

c. We communicate with external stakeholders about key issues affecting the operation of internal control and ***our Codes of Conduct.***

8.8. Monitoring Activities

Monitoring activities enable the evaluation of whether the components of the internal control system are present and operating effectively. Continuous evaluations (ISO audits, Legal Requirements Compliance Audits, product quality controls, budget control, occupational health and safety supervision, environmental inspections, etc.), ***independent evaluations*** (internal and external audits), or a combination of both, ***enable us to determine whether the components of the internal control system are present and functioning properly. The principles of this component are***[15]:

a. We select, develop and carry out continuous and/or independent evaluations to determine if the components of the internal control system are present and functioning.
b. The results of the evaluations are communicated to us in a timely manner to apply corrective measures.

9. INTERNAL CONTROL LIMITATIONS

Internal control, regardless of how well designed, implemented and developed it may be, can only provide reasonable and not absolute assurance to the Board of Directors and Senior Management regarding the achievement of our objectives. The likelihood that the objectives will be achieved will be affected by the limitations inherent in all internal control systems. These limitations include the fact that professional judgement/judgment may be deficient when making decisions, the impact of external events beyond the control of the company and human errors[16].

10. VALIDITY AND REPEALS

This Policy was initially approved at the Board of Directors meeting held on January 26, 2017 and modified on June 23, 2023 and ***May 28, 2026.*** This Policy is effective from the date of its approval.

[15] COSO "Internal Control – Integrated Framework. 2013" / page 123
[16] COSO "Internal Control – Integrated Framework. 2013" / page 137

ANNEX I:List of Codes and Corporate Policies

Code of ***Conduct***
Code against Acts of Fraud and Corruption ***and other Crimes***
Corporate Investment Policy
Corporate Inventory Policy
Corporate Policy for the Purchase of Goods and Services
Corporate Policy for Internal Control and Comprehensive Risk Management
Corporate Fixed Asset Policy
Corporate Credit and Collection Policy
Corporate Information Policy
Corporate Human Management Policy
Corporate Human Rights and Diversity Policy
Corporate Tax Management Policy
Corporate Tax Strategy Policy
Corporate Occupational Health and Safety Policy
Corporate Environmental Policy
Corporate Social Responsibility Policy

Note: This information is referential. Up-to-date corporate codes and policies can be found on our intranet ***or the digital document control tool.***

ANNEX II: Risk Assessment Criteria

1. Impact

Impact	Very Low	Low	Moderate	Considerable	High
Economic (Operating Profit > 50 MM) *Applicable if the Average Operating Profit of the last 3 years exceeds 50 million soles.*	• ***Less than 0.12% of the average Operating Profit of the last 3 years.***	• ***Between 0.12% and 0.25%*** of the average Operating Profit of the last 3 years.	• Between 0.25% and 0.5% of the average Operating Profit of the last 3 years.	• Between 0.5% and 1% of the average Operating Profit of the last 3 years.	• Greater than 1% of the average Operating Profit of the last 3 years.
Economic (Operating Profit < 50 MM) *Applicable if the Average Operating Profit of the last 3 years is less than 50 million soles.*	• ***Less than 125 thousand soles.***	• Between ***125 thousand and 250*** thousand soles.	• Between 250 thousand and 500 thousand soles.	• Between 500 thousand and 1 million soles.	• Greater than 1 million soles.
Impact on operations and information systems (qualitative)	• ***Interruption of operations for less than 1 hour.*** • ***The integrity and/or timeliness of information is not affected.***	• Interruption of operations ***between 1 and 4 hours.*** • The integrity and/or timeliness of ***non-critical*** information ***is affected.***	• Interruption of operations between ***4 and 8 hours.*** • The integrity and/or timeliness of critical information is affected.	• Interruption of operations between 8 and 24 hours. • Loss of non-critical CAASA or third-party information that cannot be recovered.	• Interruption of operations greater than 24 hours. • Loss of critical CAASA or third-party information that cannot be recovered.
Impact on reputation and image (qualitative)	• ***Minimal public awareness. No perception of company responsibility.***	• Minimal public awareness. ***Low perception*** of company responsibility.	• Moderate public awareness. There may be a ***perception of company responsibility.***	• Wide media coverage. Perception of company responsibility.	• Massive public awareness and wide frequency or permanence in the media. Receives political interest. Perception of company responsibility.

Regulatory and legal impact (qualitative)	• ***Results in non-compliance with internal, legal, sectoral, labor, or tax regulations, but does not generate a sanction.***	• Results in non-compliance with internal, legal, sectoral, labor, or tax regulations, ***generating a written warning without payment of penalties.***	• Results in non-compliance with internal, legal, sectoral, labor, or tax regulations, ***requiring payment of*** penalties ***of less than 100 thousand soles.***	• Non-compliance with legal, sectoral, labor, or tax regulations, requiring payment of penalties ***between 100 thousand and 500 thousand soles.*** • Ethical misconduct ***involving a single employee that*** breaches internal regulations and/or constitutes a crime.	• Severe non-compliance with legal, sectoral, labor, or tax regulations, requiring payment of penalties ***greater than 500 thousand soles,*** may generate criminal sanctions for the entity or representative and/or regulatory intervention. • Ethical misconduct ***involving more than one employee that*** breaches internal regulations and/or constitutes a crime.
Environmental Impact (Nature of the event/impact)	• ***The scope of the impact is specific and limited to the activity level.*** • ***No measurable environmental impact on environmental factors is evident and the impact is fully reversible without formal corrective actions.***	• The scope of the impact ***extends*** beyond the activity level and ***involves part of the process.*** • Impact on company environments and infrastructure located on paved surfaces.	• ***The scope of the impact involves the entire process.*** • Impact on 1 environmental factor (Air, Soil, Water, Flora and Fauna).	• ***The scope of the impact involves other processes.*** • Impact on 2 or more environmental factors (Air, Soil, Water, Flora and Fauna).	• The scope of the impact extends beyond the company's boundaries. • Impact on sensitive natural environments or populations ***(nature reserves, water bodies, or communities).***
Occupational Health and Safety (Nature of the incident and damage)	• ***Very minor injuries, may cause discomfort or inconvenience.***	• Minor injuries without disability, ***requiring first aid treatment.***	• Temporary disability requiring ***restricted work.***	• ***Partial disability requiring medical leave.*** • Reversible damage to health.	• Permanent total disability ***or fatality.*** • Irreversible damage ***to health.***

2. Probability

Probability	Very Low	Low	Moderate	Considerable	High
Frequency	• *The event has never occurred or has not occurred in more than 3 years.* • *Less than 0.25% of cases / transactions.*	• *The event has occurred once in the last 3 years.* • *Between 0.25% and* 0.5% of cases / transactions.	• During the last year, the event has not occurred, but it has occurred *more than once in the last 3 years.* • Between 0.5% and 1% of cases / transactions.	• During the last year the event has occurred once. • Between 1% and 5% of cases / transactions.	• During the last year the event has occurred more than once. • Greater than 5% of cases / transactions.
Exposure	• *Very rare sporadic exposure, occurring at some point during the year.* • *Assessment result below 25% of the acceptable limit.*	• *Unusual exposure, occurring at some point during the work shift. At least once per month.* • Continuous exposure, between 25% and 50% of the acceptable limit.	• *Occasional exposure, occurring at some point during the work shift. At least once per week.* • Continuous exposure, between 50% and 75% of the acceptable limit.	• *Frequent exposure, or several times during the work shift, even for short periods. At least once per day.* • Continuous exposure, between 75% and 100% of the acceptable limit.	• *Continuous exposure or several times during the work shift for prolonged periods.* • Continuous exposure, above the acceptable limit.
Estimation of occurrence (experience and professional judgment)	• *Very low occurrence estimate.*	• Low occurrence estimate.	• Moderate occurrence estimate.	• Considerable occurrence estimate.	• High occurrence estimate.

ACEROS
AREQUIPA