1. Purpose

Establish the criteria for recording, monitoring, and execution of information backups of the IT systems of Grupo Bimbo.

2. Scope

This policy applies to the all personnel of the Global IT Departments and the administrators of Grupo Bimbo, S.A.B. de C.V. applications, and/or any of its affiliates that support Grupo Bimbo applications.

3. Definitions

Business Impact Analysis *(BIA)*: Method that allows the business to estimate the damage in case of loss or interruption of a business process caused by an incident, disaster, or emergency.

Event: Relevant change of configuration and/or IT service.

Monitoring: Process through which it is observed, gathered and studied the data behavior of a computer system, through the thresholds previously defined to alert about a possible event.

Backup: Process of copy generation and digital data backup of company information.

Restoration: Procedures and controls to restore the data and functionality of an application and/or company system.

4. Responsibilities

The administrator of application: Ensure appropriate procedures and controls are operating to comply with the requirements specified in this policy.

IT Risks Committee: Establish requirements for the periodicity of generating backups of critical information contained in the information assets, considering the BIA of each Business Unit.

Global Infrastructure Department: Define the standards for time synchronization in the information assets. Guarantee the information restoration requirements are met, according to the guidelines of this policy.

5. General guidelines

In order to guarantee the information security of the company during the recording, event monitoring, and information backup, the procedures and controls for backup and recovery capability must comply with the following guidelines:

Recording and monitoring

For the recording and event monitoring, the administrator of the application must:

- Monitor daily the applications being monitored to register the failures and events that compromise the security of the information, and conserve these records, for subsequent review and consultation. The logs taken must ensure appropriate time according to the applicable regulations in each locality.
- Make records in *Service Now* and assign them to the IT areas responsible for its attention.

Backups and restoration

For backups management and restoration of IT systems, the Global Infrastructure Department must comply with the following:

- Establish, together with the IT Risks Committee, appropriate backup schedules (dates and times), of the information contained in the information assets.
- In case of any contingency and/or request from a regulatory body, the backup and restoration process include all necessary information contained in the information asset. The backup and restoration standards and requirements are established by the IT Risks Committee.
- Guarantee that the information included in the backups is encrypted in order to ensure its confidentiality.

6. Responsibility / Ownership

The Global IT Department is the assigned owner of this policy and is primarily responsible for its contents, updating, monitoring of its compliance and submission for approval before the Global Internal Control and Risk Management Department, the Steering Committee, and CEO.

7. Updates

The changes implemented in between versions are described below:

Revision / history of the revision				
Version	**Revision date:**	**Updated by:**	**Approved by:**	**Main Changes**
1				