Gestamp
SOUTH EUROPE DIVISION

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. **La Seguridad de la Información es un objetivo estratégico de nuestra organización.**
La protección y el uso seguro de los activos de la información son prioridades en nuestra organización. Incluye mantener la confidencialidad de la información y no compartirla con terceras partes.

2. **Protección y uso correcto de los activos de información para permitir el intercambio seguro de la misma.**
Es política de la organización que los activos de información estén debidamente asegurados para protegerlos de las violaciones en contra de su confidencialidad, las fallas de integridad o las interrupciones en la disponibilidad de dicha información.

3. **Establecimiento de la evaluación de riesgos.**
Para determinar niveles adecuados de medidas de seguridad a aplicar en los sistemas de información, se lleva a cabo un proceso de evaluación de los riesgos para cada sistema a fin de identificar la probabilidad y el impacto de las fallas de seguridad.

4. **Políticas y pautas de Seguridad.**
Declaración de principios de la Seguridad de la Información:
Los procedimientos de esta política, ISMS (Information Security Management System), deberán cumplir con los requisitos reglamentarios y contractuales.
Se desarrolla un plan de contingencia ante desastres.
Se recuerda de forma periódica a todos los empleados para aumentar su consciencia sobre la Seguridad de la Información.
Todos los empleados tienen el deber de cumplir con esta política y los procedimientos definidos en la ISMS.
Cualquier empleado que viole cualquiera de estas regulaciones se verá involucrado en un proceso disciplinario, de acuerdo a las reglas y regulaciones de los empleados.

Firmas:

Fdo. Sebas Graells
Director IT SED
Fecha: 4 de noviembre del 2021

Fdo. .....
Gerente Jesus SANZ - GMA
Fecha: 05 ABRIL 2022

Gestamp
SOUTH EUROPE DIVISION

INFORMATION SECURITY POLICE

1. Information Security a strategic goal in our company

Protection and secure use of information assets are priorities in our organization. This includes keeping the confidentiality of this information and not sharing it to third parties.

2. Protection and secure use of information assets to enable sharing of information.

It is the organization's policy that the information assets are appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information.

3. Establishing Risk assessment.

To determine the appropriate levels of security measures applied to information systems, a process of risk assessments is carried out for each system to identify the probability and impact of security failures.

4. Security policies and guidelines.

Information security statement of principles:
This policy, ISMS (Information Security Management System) procedures shall comply with regulatory and contractual requirements. Provide all employees with regular information security to increase their information security awareness.
A disaster contingency plan has been developed.
Employees must comply with the policies and procedures of the ISMS. An employee who violates any of these regulations shall be involved in disciplinary process in accordance with the employee rules and regulations.

Signatures:

Signed by: Sebas Graells
SED IT Director
Date: November 04, 2021

Signed by: .....
JESUS SANZ - GMA ..... plant Director
Date: 05 APRIL 2022