LINEAS EXTREMEAS DE AUTOBUSES S.L.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Código:	D-02
Versión:	00
Fecha de la versión:	02/01/2017
Creado por:	Responsable del Sistema
Aprobado por:	Gerencia

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
02/01/2017	00	Responsable Sistema	Descripción básica del documento

Tabla de contenido

1. Objetivo, alcance y usuarios

El propósito de esta Política de alto nivel **es definir el objetivo, dirección, principios y reglas básicas** para la gestión de la seguridad de la información.

Esta Política se aplica a todo el Sistema de gestión de seguridad de la información (SGSI), según se define en el Documento del Alcance del SGSI.

Los usuarios de este documento son todos los empleados de **LEDA** y las partes externas interesadas.

2. Documentos de referencia

- Norma ISO/IEC 27001, capítulos 5.2 y 5.3
- Documento sobre el alcance del SGSI
- Metodología de evaluación y tratamiento de riesgos
- Declaración de aplicabilidad
- Lista de obligaciones legales, normativas y contractuales
- Procedimiento para gestión de incidentes

3. Terminología básica sobre seguridad de la información*

Confidencialidad: característica de la información por la cual solo está disponible para personas o sistemas autorizados.

Integridad: característica de la información por la cual solo que es modificada por personas o sistemas autorizados y de una forma permitida.

Disponibilidad: característica de la información por la cual solo pueden acceder las personas autorizadas cuando sea necesario.

Seguridad de la información: es la preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistema de gestión de seguridad de la información: parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

4. Gestión de la seguridad de la información

4.1. Objetivos y medición

Los objetivos generales para el sistema de gestión de seguridad de la información son dos.

OBJETIVO Nº1: Crear una mejor imagen de LEDA y,

OBJETIVO Nº2: Reducir el daño ocasionado por potenciales incidentes.

Las metas para la consecución de los mismos están en línea con los objetivos comerciales, con la estrategia y los planes de negocio de la organización. El Responsable del Sistema de Gestión es el responsable de revisar estos objetivos generales del SGSI y de establecer nuevos.

Los objetivos para controles individuales de seguridad o grupos de controles son propuestos por Responsable del Sistema de Gestión y son aprobados por Gerencia en la Declaración de aplicabilidad.

Todos los objetivos deben ser revisados al menos **una vez al año.**

4.2. Requisitos para la seguridad de la información

Esta Política, y todo el SGSI, deben cumplir los requisitos legales y normativos importantes para la organización en el ámbito de la seguridad de la información, la Ley Orgánica de Protección de Datos de Carácter Personal (15/1999) así como como también con las obligaciones contractuales.

En la Lista de obligaciones legales, normativas y contractuales se detalla una lista de requisitos contractuales y legales.

4.3. Controles de seguridad de la información

El proceso de escoger los controles (protección) está definido en la metodología de evaluación y tratamiento de riesgos.

Los controles seleccionados y su estado de implementación se detallan en la Declaración de aplicabilidad.

4.4. Responsabilidades

Las responsabilidades para el SGSI son las siguientes:

- **Gerencia** es el responsable de garantizar que el SGSI sea implementado y mantenido de acuerdo con esta Política y de garantizar que todos los recursos necesarios estén disponibles.
- El **Responsable del Sistema de Gestión** es el responsable de la coordinación operativa del SGSI, como también de informar su desempeño.
- Gerencia debe revisar el SGSI al menos una vez por año o cada vez que se produzca una modificación significativa; y debe elaborar minutas de dichas reuniones. El objetivo de las verificaciones por parte de la dirección es establecer la conveniencia, adecuación y eficacia del SGSI.
- El Responsable del sistema de Gestión implementará programas de capacitación y concienciación de empleados sobre seguridad de la información.
- La protección de la integridad, disponibilidad y confidencialidad de los activos es responsabilidad del propietario de cada activo.
- Todos los incidentes o debilidades de seguridad deben ser informados al Responsable del Sistema de Gestión.

- El Responsable del Sistema de Gestión definirá qué información relacionada con la seguridad de la información será comunicada a qué parte interesada (tanto interna como externa), por quién y cuándo.
- El Responsable del Sistema de Gestión es el responsable de adoptar e implementar el Plan de capacitación y concienciación, que corresponde a todas las personas que cumplen una función en la gestión de la seguridad de la información.

4.5. Comunicación de la Política

El Responsable del Sistema de Gestión debe asegurarse que todos los empleados de **LEDA**, como también los participantes externos correspondientes, estén familiarizados con esta Política.

5. Apoyo para la implementación del SGSI

A través del presente documento, Gerencia declara que en la implementación y mejora continua del SGSI se contará con el apoyo de los recursos adecuados para lograr todos los objetivos establecidos en esta Política, así como cumplir con todos los requisitos identificados.

6. Validez y gestión de documentos

Este documento es válido hasta que se produzcan modificaciones importantes en la actividad de la empresa.

El propietario de este documento es el Responsable del Sistema, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de empleados y participantes externos que cumplen una función en el SGSI pero que no están familiarizados con el presente documento.
- No cumplimiento del SGSI con las leyes y normas, las obligaciones contractuales y con los demás documentos internos de la organización.
- Ineficacia de la implementación y mantenimiento del SGSI.
- Responsabilidades ambiguas para la implementación del SGSI.