Política de Seguridad de la Información y Continuidad de Negocio

31 de agosto de 2023

1 Introducción

La Política de Seguridad de la Información y Continuidad de Negocio del GRUPO LOGALTY establece los principios y directrices para la protección de la información, la garantía de la continuidad de las operaciones y la supervisión y mejora continuas de la seguridad en todas las áreas de la organización. Esta política es un compromiso fundamental de la alta dirección para salvaguardar la confidencialidad, integridad y disponibilidad de la información, cumplir con los requisitos legales y regulatorios, asegurar la resiliencia del negocio y fomentar una cultura de seguridad sólida.

2 Alcance

Esta política se aplica a todos los empleados, contratistas, proveedores y cualquier otra entidad que acceda, procese, almacene o transmita información en nombre del GRUPO LOGALTY o de cualquiera de las organizaciones que forman parte del grupo.

3 Principios

- **Confidencialidad**: Nos comprometemos a proteger la información confidencial contra divulgaciones no autorizadas. Solo se divulgará información confidencial a personas autorizadas y con un propósito legítimo.
- **Integridad**: Mantendremos la precisión y la integridad de la información a lo largo de su ciclo de vida. Implementaremos controles para prevenir modificaciones no autorizadas o indebidas de la información.
- **Disponibilidad**: Garantizaremos la disponibilidad de la información y los sistemas críticos para respaldar las operaciones comerciales. Implementaremos medidas de redundancia y planes de continuidad para minimizar el impacto de interrupciones.
- **Autenticación**: Estableceremos mecanismos sólidos de autenticación para garantizar que solo las personas autorizadas tengan acceso a la información y los sistemas. Implementaremos métodos de autenticación apropiados, incluyendo contraseñas seguras, autenticación de dos factores y otros controles.
- **Trazabilidad**: Mantendremos registros detallados de actividades y eventos relacionados con la seguridad de la información. Los registros permitirán el seguimiento y la revisión de acciones realizadas por usuarios y sistemas, contribuyendo a la detección y respuesta temprana a incidentes.
- **Cumplimiento legal**: Cumpliremos con todas las leyes, regulaciones y requisitos contractuales relacionados con la seguridad de la información, la continuidad de negocio y la privacidad de los datos.

4 Responsabilidades

- **Comité de Seguridad**: El Comité de Seguridad es responsable de supervisar y aprobar la estrategia de seguridad de la información y continuidad de negocio, revisar los informes de riesgos y desempeño, y proporcionar dirección estratégica en asuntos de seguridad y continuidad.
- **CISO (Chief Information Security Officer):** El CISO es responsable de liderar la estrategia de seguridad de la información de la organización, supervisar la implementación de controles de seguridad, identificar y evaluar los riesgos de seguridad, coordinar las respuestas a incidentes de seguridad y liderar la planificación de la continuidad de negocio.
- **DPO (Data Protection Officer):** El DPO es responsable de garantizar el cumplimiento de las leyes de protección de datos y privacidad, proporcionar asesoramiento sobre cuestiones relacionadas con la protección de datos, supervisar la gestión de los datos personales y actuar como punto de contacto con las autoridades de protección de datos.
- **Empleados y Contratistas**: Todos los empleados y contratistas deben cumplir con las medidas de seguridad establecidas, informar cualquier incidente de seguridad y participar en la formación y concienciación sobre seguridad.

5 Gestión de Riesgos y Continuidad de Negocio

Identificaremos y evaluaremos regularmente los riesgos de seguridad de la información y los riesgos relacionados con la continuidad de negocio. Tomaremos medidas para mitigarlos de manera efectiva y desarrollaremos planes de continuidad para los escenarios críticos.

6 Procesos de Seguridad y Continuidad

Estableceremos controles de seguridad adecuados, basados en una evaluación de riesgos, para proteger los activos de información.

Utilizaremos como marcos de referencia para garantizar la seguridad de la información y la continuidad de negocio, las normas ISO 27001, ISO 22301, el Esquema Nacional de Seguridad (ENS), el Reglamento General de Protección de Datos (RGPD), la Directiva NIS, el Reglamento DORA y el Reglamento eiDAS.

7 Monitorización y Mejora

Revisaremos y auditaremos periódicamente los controles de seguridad y los planes de continuidad para asegurar su efectividad y adecuación.

Mejoraremos continuamente nuestros procesos de seguridad y continuidad en función de los resultados de las revisiones y cambios en el entorno de amenazas.

8 Comunicación y Concienciación

Comunicaremos regularmente los aspectos de seguridad de la información, resiliencia y continuidad de negocio. Brindaremos capacitación para garantizar que todos los involucrados comprendan y cumplan con esta política.

9 Incumplimiento de la Política

El incumplimiento de esta política de seguridad de la información y continuidad de negocio puede dar lugar a acciones disciplinarias.

10 Aprobación y Actualización

Esta política será revisada anualmente y actualizada según sea necesario para garantizar su relevancia y efectividad.