Política de Seguridad de la Información y Continuidad de Negocio

28 de noviembre 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

Esta política recoge los principios que la compañía considera esenciales en la gestión y tratamiento de la información tanto en sus procesos internos como en los servicios y procesos de negocio prestados a sus clientes. Dichos principios son:

- **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.

Adicionalmente a los anteriores, nos adherimos a los siguientes principios alineados con el Esquema Nacional de Seguridad (ENS):

- **La seguridad como un proceso integral,** constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de información.
- **Gestión de la seguridad basada en los riesgos,** manteniendo el análisis permanentemente actualizado.
- **Prevención, reacción y recuperación**, ante eventos no deseados de seguridad.
- **Reevaluación periódica de la seguridad y su eficacia**.

- **La seguridad como función diferenciada**, dedicando recursos y esfuerzos adicionales a los necesarios para la prestación del servicio.

4 Liderazgo

La organización dispondrá de un Comité específico para gestionar la Continuidad, los Riesgos y la Seguridad del Grupo Logalty (Comité CRS). En este comité participará la alta dirección.

A través del Comité CRS, la alta dirección de la compañía demuestra un claro liderazgo y compromiso con respecto al sistema de gestión y a la seguridad de la información,

a) asegurando que se establecen políticas y objetivos compatibles con la dirección estratégica de la organización;

b) asegurando la integración de los requisitos del sistema de gestión en los procesos

c) asegurando que los recursos necesarios para el sistema de gestión estén disponibles;

d) comunicando la importancia de la continuidad y seguridad de la información eficaz

e) asegurando que el sistema de gestión consigue los resultados previstos;

f) dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión; y

g) promoviendo la mejora continua

Respecto a las responsabilidades indicadas en el RGPD, el Comité CRS ejercerá las funciones de responsable del tratamiento para los datos propios y como encargado del tratamiento para los datos de los clientes de los servicios.

5 Roles y Responsabilidades

Será responsabilidad del Departamento de RRHH la asignación de los roles relacionados con la Seguridad de la Información y la Continuidad de Negocio a cada empleado, garantizando el conocimiento y la aceptación de cada rol asignado.

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.

Entre los roles destacados en el ámbito de la Seguridad de Información tenemos:

- **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.
- **Responsable de la Información y el Servicio**: Determinará los requisitos de la información tratada y los requisitos de los servicios prestados.
- **Responsable del Sistema**: Se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

- **Auditor Interno**: Responsable de realizar la auditoria interna anual del sistema integrado de gestión de seguridad y continuidad y presentar los resultados al Comité CRS.

Estos cinco roles definidos por la organización no podrán asignados a las mismas personas ni deberá existir ninguna vinculación jerárquica entre ellos que pueda condicionar la independencia de sus funciones. Estos cinco roles formarán parte del Comité CRS.

6 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.

La apreciación de los riesgos de seguridad de la información y el proceso de tratamiento deben alinearse con los principios y directrices genéricas definidos en la Norma ISO 31000 y la Metodología MAGERIT.

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

7 Marcos de Referencia

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.

8 Prevención

Las distintas áreas deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, se implementarán los controles y medidas de seguridad adecuados. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados. Para ello, se consideran relevantes las siguientes prácticas:

- Establecer mecanismos de autorización ante cambios, asignación de accesos y privilegios o paso de sistemas de información a producción.
- Evaluar regularmente la seguridad.
- Solicitar la evaluación periódica por parte de terceros con el fin de obtener visiones independientes.

9 Detección

Se debe monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia. Para ello, esta política establece la necesidad de establecer mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

10 Respuesta

Se establecerán procesos, y dotará de recursos y herramientas que permitan responder con eficacia a los eventos e incidentes de seguridad.

Los distintos procesos y procedimientos operativos que se desarrollen deberán dar dotar de esta capacidad de forma proporcional a la criticidad de los sistemas e información afectados.

11 Gestión de incidencias de seguridad

Se dispondrá de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información. Estos procedimientos cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema. En particular, se dedicarán recursos para la detección y reacción frente a código dañino.

12 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.

13 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.

14 Incumplimiento de la Política

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

15 Aprobación y Actualización

Esta política será aprobada por el Comité CSR y revisada y actualizada anualmente según sea necesario para garantizar su relevancia y efectividad.