POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, CONTINUIDAD DE NEGOCIO Y PRIVACIDAD

LOGALTY PRUEBA POR INTERPOSICION SL

Firmado digitalmente por LOGALTY PRUEBA POR INTERPOSICION SL
Fecha: 2024.09.12 11:45:23 +02'00'

12 de julio de 2024

INFORMACIÓN GENERAL

Tipo	**Política General** Política Específica Procedimiento Instrucción Técnica Plan Plantilla
Clasificación	**Público** Confidencial Uso Interno
Versión	V.1
Estado	Borrador en curso **Aprobado** Retirado

HISTÓRICO DE VERSIONES

Versión	Fecha de Aprobación	Sección y cambios	Autor
V.1	22.07.2024	Primera Versión	GRC MANAGER

Índice

1 INTRODUCCIÓN

En GRUPO LOGALTY como Prestador de Servicios de Confianza, reconocemos la importancia de proteger la información de nuestros clientes, garantizar la disponibilidad de nuestros servicios en todo momento y cumplir con las regulaciones de privacidad de datos en constante evolución.

El Grupo entiende que junto con las oportunidades y beneficios que ofrece la tecnología, también nos enfrentamos una serie de desafíos y riesgos inherentes a un entorno digital cada vez más complejo y dinámico. Sabemos que es fundamental que adoptemos un enfoque proactivo y holístico hacia la seguridad de la información, la continuidad del negocio y la privacidad de los datos para proteger nuestros activos más valiosos y garantizar la sostenibilidad y excelencia a largo plazo de nuestras operaciones.

Por ello, el Grupo ha adoptado la presente Política que debe servir de referente para la toma de decisiones en todos los niveles y unidades que conforman el Grupo y guiar las conductas de los empleados, directivos y administradores en sus relaciones tanto internas como externas.

2 OBJETIVO

El objetivo de esta política es garantizar la protección, integridad y confidencialidad de la información de la empresa, así como establecer medidas para la continuidad del negocio y el cumplimiento de la privacidad de los datos, en toda la actividad del Grupo.

La Política de Seguridad de la Información, Continuidad de Negocio y Privacidad del Grupo Logalty (en adelante, la “Política”) 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.

3 ÁMBITO DE APLICACIÓN

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.

El ámbito de aplicación también incluye todos los sistemas de información, activos de datos y recursos tecnológicos utilizados por las empresas del Grupo, ya sea internamente en las instalaciones de las mismas o externamente en entornos remotos, como la nube o servicios de terceros. Además, se extiende a todas las ubicaciones geográficas donde opera la empresa, independientemente de las jurisdicciones locales o regionales.

4 NORMATIVA APLICABLE

Para la elaboración de la presente Política así como los demás documentos, procedimientos o instrucciones relacionadas con la seguridad de la información, continuidad de negocio y privacidad, se tendrá en cuenta la normativa vigente aplicable a cada una, así como estándares internacionales de buenas prácticas y normativa interna de aplicación.

5 MARCO DE GOBIERNO

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

5.1 Consejo de Administración

El Consejo de Administración de Grupo Logalty desempeña un papel crucial en la supervisión y dirección estratégica de la empresa, y por tanto es el encargado, en última instancia, de la supervisión del cumplimiento de la presente política. Asimismo, el Consejo participa en la formulación de la visión y la estrategia financiera del Grupo, asegurándose de que esté alineada con los objetivos a largo plazo y considerando los intereses de todas las partes interesadas.

5.2 Comité Ejecutivo

El Comité Ejecutivo, como máximo órgano de ejecución del Grupo, tiene la obligación de supervisar y dar el apoyo necesario para la implementación y cumplimiento de la política.

Es por ello que, entre sus principales funciones se encuentran las siguientes:

- Definir y aprobar los objetivos de seguridad de la información, continuidad de negocio y privacidad.
- Supervisar el cumplimiento normativo en materia de seguridad, continuidad de negocio y privacidad.
- Asignar recursos financieros y humanos necesarios para garantizar su cumplimiento.
- Asegurar que se establecen políticas y objetivos compatibles con la dirección estratégica de la organización en materia de Seguridad de la Información, la Continuidad del Negocio y la Privacidad.
- Asegurar la integración de los requisitos del sistema de gestión en los procesos del Grupo.
- Monitorizar y supervisar la eficacia del sistema de gestión.

5.3 Comité de Continuidad, Riesgos y Seguridad (Comité de CRS)

La organización dispone de un Comité específico para gestionar la Continuidad, los Riesgos y la Seguridad del Grupo Logalty (Comité de CRS), en el que participa el Comité Ejecutivo. El Comité de CRS es el responsable en última instancia del diseño y la estrategia de ejecución del programa de seguridad de la información, continuidad y privacidad y no pude delegar esta responsabilidad a otros roles. Sus principales funciones son:

- Proponer una estrategia de seguridad, continuidad y privacidad, alineada con la estrategia del negocio.
- Aprobar, y revisar de forma periódica las políticas, planes y procedimientos asociados.
- Recolectar y analizar datos relativos al rendimiento y nivel de cumplimiento del sistema de gestión de la seguridad, continuidad y privacidad, del proceso de gestión de riesgos, y de los controles y medidas de seguridad adoptados.
- Monitorizar las principales desviaciones y brechas de seguridad, analizando y proponiendo posibles vías de mejora en los procesos y controles de seguridad.

- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Informar regularmente del estado de la seguridad de la información, continuidad y privacidad a la Dirección, así como de cualquier desviación o brecha de seguridad.
- Promover la mejora continua, comunicación y formación a empleados, a efectos de prevenir riesgos de seguridad, continuidad y privacidad.

El Comité de CRS se deberá reunir con una periodicidad trimestral, y de forma extraordinaria siempre que se requeira.

5.4 Chief Information Security Officer (CISO)

El CISO, junto a su equipo, 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, entre otros.

5.5 Business Continuity Manager (BCM)

El BCM, junto a su equipo, es responsable de garantizar la continuidad de negocio de la organización, identificar los procesos y funciones críticos de la empresa y desarrollar planes para mantener y restablecer o restaurar rápidamente las operaciones en caso de interrupción, gestionando los riesgos asociados y garantizando la resiliencia organizacional.

5.6 Data Protection Officer (DPO)

El DPO es responsable de supervisar el cumplimiento de la normativa sobre protección de datos y privacidad y las políticas de privacidad en el Grupo, proporcionar asesoramiento sobre cuestiones relacionadas con la protección de datos y la evaluación de impacto relativa a la protección de datos, así como cooperar y actuar como punto de contacto con la autoridad de control de protección de datos.

5.7 Otros roles

El Grupo Logalty ha nombrado asimismo determinados roles que tienen una gran importancia dentro de sistema de gestión de la seguridad de la información, continuidad y privacidad:

- **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 auditoría interna anual del sistema integrado de gestión de seguridad y continuidad y presentar los resultados al Comité CRS.

6 PRINCIPIOS DE ACTUACIÓN

Esta política recoge los principios que el Grupo 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:

1. Entendemos la seguridad como un **proceso integral**, constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de información.

2. Realizamos la gestión de la seguridad, continuidad y privacidad basada en los **riesgos**, manteniendo el análisis permanentemente actualizado.
3. Implementamos medidas **de prevención, reacción y recuperación**, para protegernos ante incidentes de seguridad indeseados.
4. **Reevaluamos de forma periódica** las medidas de seguridad, continuidad de negocio y de privacidad adoptadas y su eficacia.
5. Nos tomamos la seguridad como una función diferenciada, dedicando **recursos y esfuerzos adicionales** a los necesarios para la prestación del servicio.
6. Garantizamos la disponibilidad de la información y los sistemas críticos para respaldar las operaciones comerciales, implementando medidas de redundancia y planes de continuidad para minimizar el impacto de interrupciones.
7. **Entendemos el cumplimiento legal como la base de actuación del negocio por tanto, el Grupo realiza todas las acciones necesarias para cumplir con** las leyes, regulaciones y requisitos contractuales relacionados con la seguridad de la información, la continuidad de negocio y la privacidad de los datos.
8. Comunicamos y realizamos formaciones internas de forma continua.

Asimismo, el Grupo se compromete a fijar anualmente objetivos de mejora de los procesos de seguridad de la información, continuidad del negocio y privacidad debidamente documentados y revisados.

7 MARCO DE INFORMACIÓN

Establecer un marco de información adecuado es fundamental para cumplir con los compromisos de seguridad, continuidad y privacidad de Grupo Logalty.

Los principales objetivos del marco de información son:

- Ofrecer a la Alta Dirección y al Consejo de Administración información precisa, clara y adecuada con la antelación necesaria, para facilitar la toma de decisiones y verificar el cumplimiento de los objetivos propuestos.
- Atender los requerimientos de información de organismos supervisores, si los hubiera.
- Proporcionar a los responsables de las distintas áreas y a las áreas de control, los datos necesarios para poder realizar el control del cumplimiento de la estrategia definida en el Grupo en relación a la seguridad, continuidad y privacidad.

En este sentido, el Comité de Dirección recibirá periódicamente información sobre:

- La estrategia adoptada en relación a la seguridad de la información, continuidad de negocio y privacidad.
- Acciones correctivas a realizar o mejoras que afecten a la estrategia de negocio.
- Brechas detectadas o vulnerabilidades, así como el plan de remediación.
- Cambios normativos que afecten de forma significativa a los procesos ya implementados en materia de seguridad de la información, continuidad del negocio o privacidad.

8 REVISIÓN Y MEJORA CONTÍNUA

En cumplimiento del Código Ético aprobado por el Consejo de Administración del Grupo, la presente Política será revisada cuando:

- Exista una modificación de la normativa aplicable.
- Se necesiten adaptaciones a recomendaciones realizadas por una autoridad competente .
- En el caso de que el Grupo quiera hacer mejoras y/o aclaraciones en el documento.
- En todo caso, se realizará una revisión anual del contenido de la Política.

Cualquier revisión y/o actualización deberá ser aprobada por el órgano correspondiente y comunicado de forma efectiva a la plantilla siempre que dicha modificación sea sustancial para la compresión de la presente Política. No se comunicarán las actualizaciones puramente de formato o de corrección de erratas.

9 PUBLICACIÓN, COMUNICACIÓN Y FORMACIÓN

La presente Política deberá ser pública y accesible a todos los empleados del Grupo. La organización realizará una comunicación efectiva a toda la plantilla y la misma podrá publicarse en la Web o Webs de todas las empresas del Grupo Logalty.

Asimismo, aquellos empleados que hagan uso o que entre sus funciones deban atender específicamente a las obligaciones de esta Política recibirán una formación específica con el objetivo de que estén debidamente informados de todos los aspectos del presente documento.

10 APROBACIÓN VIGENCIA

Este texto ha sido aprobado por la Presidenta Ejecutiva en representación del Consejo de Administración y previa ratificación por el Comité Ejecutivo. Esta Política de Seguridad de la Información, Continuidad de Negocio y Privacidad es efectiva desde la fecha de aprobación y hasta que sea reemplazada por una nueva política.