Gerencia de Tecnología

Política General de Seguridad de la Información

Registro de modificaciones.

Revisión Versión	Fecha	Tipo de revisión	Identificación de los cambios	Nombre responsable
1.0	12/06/2019	Creación	Creación del documento	Jefe de Riesgo en Sistemas
1.0	28/06/2019	Revisión	Revisión del documento	Subgerente de Gestión de Riesgos
1.0	10/07/2019	Revisión y aprobación	Revisión y aprobación del documento	Gerente de Gobernanza, Gerencia Corporativa de Asuntos Legales y Gobernanza Falabella
1.0	12/07/2019	Revisión y aprobación	Revisión y aprobación del documento	Fiscal
1.0	12/07/2019	Revisión y aprobación	Revisión y aprobación del documento	Gerente Corporativo de Administración y Finanzas
1.0	31/07/2019	Aprobación	Revisión y aprobación del documento	Directorio Plaza S.A.
2.0	28/08/2024	Actualización	Actualización de la estructura, taxonomía y lineamientos de la Política General de Seguridad de la Información.	Especialista de Seguridad de la Información
2.0	23/09/2024	Revisión	Revisión del documento	Jefe de Gobierno de datos y Seguridad de la Información
2.0	21/10/2024	Revisión y aprobación	Revisión y aprobación del documento	Comité de Gobierno de Datos y Seguridad de la Información

2.0	21/10/2024	Revisión y aprobación	Revisión y aprobación del documento	Gerente de Tecnología
2.0	23/04/2025	Aprobación	Revisión y aprobación del documento	Directorio Plaza S.A.

Índice

1. Objetivo

La información es uno de los principales activos de las organizaciones, por lo que la protección de este activo es una tarea esencial para asegurar la continuidad y el desarrollo del negocio, constituyendo también una exigencia legal y una forma de generar confianza en los socios comerciales, proveedores, accionistas, clientes, visitantes y colaboradores de Mallplaza.

Establecer los principios y marco general de trabajo de Mallplaza en cuanto a establecer, implementar, mantener y mejorar de forma continua, el Sistema de Gestión de Seguridad de la Información (SGSI), en concordancia con sus Definiciones Estratégicas (Misión, Visión y Objetivos Estratégicos) y resguardando la confidencialidad, integridad y disponibilidad de los activos de información.

Objetivos Específicos

1. Asegurar el cumplimiento de los requisitos normativos, legales, reglamentarios y contractuales, que estén orientados a la seguridad de la información.
2. Establecer los niveles de acceso apropiados a la información, brindando y asegurando la confidencialidad, integridad y disponibilidad que requiera cada sistema, proceso, actividad crítica y usuario.
3. Implementar un modelo de gestión acorde con el resguardo de la seguridad de la información.
4. Implementar una metodología enfocada en la gestión de riesgo de seguridad de la información en la organización.
5. Definición del ámbito de trabajo y responsabilidades corporativas e individuales respecto al uso de los recursos tecnológicos que provee la empresa y al manejo de la información.

2. Alcance

Esta política tiene alcance regional y es aplicable para todos los colaboradores, servicios externalizados y terceras partes en Mallplaza, sin discriminar el modo de trabajo, ya sea “presencial”, “a distancia”, “teletrabajo” u otra acordada previamente con Mallplaza, en las condiciones que establezca la legislación vigente, los planteamientos de la Dirección del Trabajo.

3. Documentos relacionados

Los documentos internos relacionados con esta política son Estándares, Procesos y Normas que conforman el Sistema de Gestión de Seguridad de la Información de Mallplaza.

4. Generalidades.

4.1 Responsabilidad del documento.

Será responsabilidad del oficial de seguridad de la información difundir y velar por el cumplimiento de esta política

4.2 Mantención del documento

La documentación deberá ser actualizada al menos una vez al año y cada vez que surjan cambios relevantes con afectación al negocio.

4.3 Roles y responsabilidades generales

Los roles y responsabilidades incluidas (pero no limitados) en esta política son:

- Directorio:
  - Garantizar que la política sea compatible con la dirección estratégica de Mallplaza.
  - Garantizar que los requisitos de seguridad de información se integren en los procesos de Mallplaza.
  - Asegurar que los recursos necesarios, para la gestión de seguridad de información, estén disponibles.
  - Comunicar la importancia de una gestión eficaz de la seguridad de información a todo el grupo Gerencial.
  - Velar por el cumplimiento de la presente Política y la correcta implementación del Programa de Seguridad de la Información.
  - Asegurar que las responsabilidades de los roles relevantes para la seguridad de información se asignen y comuniquen dentro de Mallplaza.
- Comité de Gobierno de Datos y Seguridad de la Información:
  - Asegurar que el SGSI sea parte de la agenda del Comité en cada uno de sus aspectos, tanto en el cumplimiento de las cláusulas como en la implementación y cumplimiento de los controles.
  - Validar y asegurar que los requerimientos de Seguridad de la Información sean incluidos en todos los proyectos de Mallplaza.
  - Gestionar nuevos requerimientos o regulaciones locales de Seguridad de la Información y Ciberseguridad que puedan aplicar a Mallplaza.
  - Revisar y aprobar cualquier modificación o actualización que sufra la Política de Seguridad de la Información antes de ser enviada al Directorio.

- Comité de Seguridad: (táctico)
    - Revisar las actualizaciones de la Política de Seguridad de la Información y asegurar que cuente con los puntos necesarios para pasar a su aprobación.
    - Validar que los requerimientos de Seguridad de la Información se apliquen en todos los proyectos de la organización.
    - Establecer un programa anual de actividades de Seguridad de la Información.
- Oficial de Seguridad de la Información
    - Gestionar la ejecución del Programa de Seguridad de la Información.
    - Monitorear y asegurar el cumplimiento de la presente Política.
    - Monitorear que todas las áreas ejecuten y actualicen su inventario de activos, evaluación de su criticidad según la triada CIA (Confidencialidad, Integridad, Disponibilidad).
    - Acompañar y asesorar a las áreas en su evaluación de riesgos basados en la Metodología de Gestión de Riesgos de Seguridad de la Información de Mallplaza.
    - Monitorear que los riesgos que estén sobre el apetito del riesgo de Mallplaza, cuenten con planes de acción y tratamiento.
    - Evaluar anualmente el SGSI y generar propuestas de actualización necesarias, con el objetivo de asegurar el ciclo de mejora continua.
    - Difundir el Marco Normativo Corporativo de seguridad de información.
- Gerencias de Mallplaza
    - Implementar las directrices emanadas de esta política en sus respectivas gerencias garantizando incorporar dentro de sus proyectos y procesos la mirada de Seguridad.
    - Promover el cumplimiento de los requerimientos de Seguridad de la Información a todos sus equipos de trabajo.
    - Generar planes de tratamiento de riesgos para todos aquellos riesgos que se identifiquen por sobre el apetito definido en Mallplaza.
- Gerencia Legal
    - Revisar las normas y regulaciones vigentes de los negocios relacionados a seguridad de información y su aplicabilidad en la organización.
    - Mantener contacto con Oficial de Seguridad de Información Corporativo y Local para mantenerse actualizados de cualquier cambio en las normas o regulaciones relacionadas a Seguridad de la Información y Ciberseguridad.
- Colaboradores

- Deben capacitarse en términos de Seguridad de la Información a través de los cursos dispuestos por la organización.
- Cumplir con los lineamientos de Seguridad de la Información dentro de esta política.
- Conocer los canales de reporte en caso de identificar incidentes o eventos de Seguridad de la Información y Ciberseguridad.
- Asegurar los activos de información según la clasificación definida por Mallplaza.
- Evitar el envío de información a canales de comunicación no autorizados.
- Aplicar los requerimientos de Seguridad de la Información en todas las actividades relacionadas a sus funciones.

4.4 Cumplimiento

Todos los colaboradores de Mallplaza deberán cumplir con esta política, además de Contratistas y empresas externas que tengan relación vigente con Mallplaza y cuenten con accesos a nuestros activos de información de Mallplaza. Cualquier infracción a la normativa anteriormente indicada podrá dar lugar a medidas disciplinarias respecto del Colaborador, de acuerdo con lo establecido en el Código de Integridad, la legislación vigente y el Reglamento Interno de Orden Higiene y Seguridad de la Compañía.

5. Política de seguridad

Los siguientes principios deben guiar el comportamiento de Mallplaza y de los Colaboradores en materia de seguridad de la Información:

a) Mallplaza debe proteger su Información y la de terceros, de forma apropiada según su valor y clasificación, independiente de los medios que la contengan.

b) Mallplaza debe cumplir con todas las regulaciones, leyes y normativas de Seguridad de la Información vigentes en los países en que opera.

c) Mallplaza debe contar con tecnologías de seguridad, procesos, recursos y personal para proteger la Información.

d) Mallplaza debe implementar medidas de control consistentes con su estrategia de Seguridad de la Información.

e) Mallplaza debe realizar, de forma periódica, análisis de riesgos de Seguridad de la Información, de modo que estos se gestionen y traten de forma adecuada mitigando sus impactos.

f) Mallplaza debe elaborar, gestionar y probar todos sus procedimientos de Continuidad del Negocio, a modo de asegurar la operación de todos sus procesos críticos de negocio, ante eventos de desastres o que afecten la Disponibilidad o su correcto funcionamiento.

g) Todos los Colaboradores son responsables por la custodia y protección de los activos de Información que manejan en el desempeño de sus funciones.

5.1 Detalle de la política

Mallplaza deberá velar por la implementación de medidas, requerimientos y procedimientos destinados a proteger la información en los siguientes ámbitos:

a) **Organización de seguridad de información**, en lo relativo a los lineamientos para administrar la seguridad de la información, establecer un marco gerencial de control e implementación, así como definir los roles y responsabilidades de seguridad de la información de Mallplaza.

b) **Gestión de activos de información**, en lo relativo a los lineamientos para mantener una adecuada protección de los activos de información de Mallplaza, para sus procesos críticos, en cada tipo de activo y en cada activo de soporte.

c) **Gestión de riesgos**, en lo relativo a definir y aplicar un proceso de evaluación de riesgos y de tratamiento de riesgos de seguridad de información. Mallplaza debe identificar, evaluar e inventariar sus activos de información periódicamente o cuando un proceso sufra un cambio que impacte en el riesgo sobre los activos.

d) **Gestión de recursos humanos**, en lo relativo a los lineamientos para la selección y contratación; durante la vigencia del contrato de trabajo; y, una vez terminada la relación contractual con los colaboradores, Mallplaza debe asegurar que el colaborador entienda sus derechos y deberes respecto a la seguridad de la información y los activos de información bajo su responsabilidad.

e) **Gestión de criptografía**, en lo relativo a los lineamientos para el uso adecuado y eficaz para proteger la confidencialidad, disponibilidad e integridad de la información procesada, almacenada y compartida. Mallplaza debe asegurar el uso de métodos de encriptación, uso de protocolos seguros y habilitar a los colaboradores los mecanismos.

f) **Gestión de control de acceso lógico**, en lo relativo a los lineamientos para controlar el acceso a los sistemas y aplicaciones de los procesos Core de Mallplaza, para así evitar el acceso no autorizado a la información. Mallplaza deberá aplicar políticas de contraseña, gestión de roles y permisos, así como procesos de revisión de vigencia de las cuentas con acceso a todos los sistemas Core.

g) **Gestión de seguridad física y ambiental**, en lo relativo a los lineamientos para la seguridad física y ambiental, de modo de controlar el acceso de personas a lugares sensibles o restringidos, y evitar daño a las personas y a las instalaciones de Mallplaza. En este ámbito, la organización debe definir protocolos y procedimientos para la

autorización de acceso a instalaciones restringidas, estos deben ser registrados y deben pasar por un proceso de revisión/autorización previa a que se permita el acceso a las instalaciones.

h) **Gestión de las operaciones**, en lo relativo a los lineamientos para la operación correcta y segura de los medios de procesamiento de información de Mallplaza como, asimismo, evitar la divulgación no autorizada, la corrupción de la información y la pérdida de Disponibilidad, debido a procedimientos operacionales insuficientes, inadecuados, o debido al uso de canales de comunicación poco robustos. Para esto Mallplaza debe conocer y formalizar documentalmente los procedimientos asociados a la gestión operacional.

i) **Gestión de las comunicaciones**, en lo relativo a los lineamientos para la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo. Mallplaza debe establecer parámetros de configuración segura para los equipos de comunicación, así como procesos de solicitud, validación y autorización/rechazo de requerimientos de tráfico en la red.

j) **Gestión de adquisición, desarrollo y mantenimiento de sistemas de información**, en lo relativo a los lineamientos para que la Seguridad de la Información sea una parte integral en el diseño y adquisición de aplicaciones o software, y se mantenga hasta el término de su vida útil. Mallplaza debe asegurar que los desarrolladores, internos y externos, cumplan con las buenas prácticas de desarrollo de código seguro, así como implementar procesos de revisión de seguridad previo a su paso a producción.

k) **Gestión de proveedores**, en lo relativo a los lineamientos para la protección de los activos de Mallplaza accesibles a sus proveedores. Mallplaza deberá implementar procesos de revisión del cumplimiento de requerimientos de seguridad en el proceso de contratación de servicios, así como el monitoreo de que los controles y acuerdos contractuales se cumplan a lo largo del período de la prestación del servicio.

l) **Gestión de ciberseguridad**, en lo relativo a los lineamientos para generar mecanismos de seguridad en los aplicativos e infraestructura. Mallplaza debe definir e implementar procesos de evaluación y monitoreo de amenazas, así como aplicar inteligencia de amenazas, que puedan comprometer los activos de soporte tecnológico a través de la explotación de vulnerabilidades conocidas y de día cero.

m) **Gestión de incidentes**, en lo relativo a asegurar una respuesta eficiente y eficaz a los incidentes de seguridad de información y lograr un posterior aprendizaje para reducir la probabilidad o las consecuencias de futuros incidentes. Mallplaza debe contar con una metodología de gestión de incidentes de seguridad de la información y ciberseguridad, que cuente con artefactos actualizados que les permita responder y recuperar la operación en caso de verse afectados por un incidente de clasificación alta o crítica. Además, debe contar con un comité específico con la Alta Gerencia que les permita tomar decisiones frente a incidentes que les genere un riesgo financiero o reputacional.

n) **Gestión de requisitos legales, regulatorios y contractuales**, en lo relativo a identificar, documentar y mantener actualizados estos requisitos que son relevantes para la seguridad de información. Mallplaza debe contar con un proceso periódico para monitorear qué leyes y regulaciones les aplican y cómo pueden implementar controles que les permitan cumplir con dichos requisitos, y por ende proteger los activos de información y a las personas.

6. Referencia de documentos asociados

- NIST CSF 2.0 (Publicada en febrero 2024) – Marco de Ciberseguridad publicado por NIST (National Institute of Standars and Technology).
- NCh-ISO 27001:2022 - Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de gestión de la seguridad de la información - Requisitos.
- NCh-ISO 27002:2022 - Tecnologías de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información.

7. Glosario

Activo de información: Cualquier dato, documento u otro recurso basado en información que es propiedad de una organización, que la administra o mantiene.

Activo tecnológico: Son aquellos recursos para el procesamiento y almacenamiento de datos e información: hardware y software, principalmente.

Confidencialidad: Tiene como objetivo garantizar que la información sea accesible solo para personas autorizadas, protegiéndola contra la divulgación no autorizada y el uso indebido

Integridad: Salvaguarda la exactitud y la exhaustividad de la información y los métodos de tratamiento.

Disponibilidad: Es la garantía de que los sistemas de información y los datos sean accesibles para los usuarios autorizados cuando sea necesario.

Clasificación de información: Define los niveles de criticidad de la información en base a su composición, dependiendo de los datos, el nivel de criticidad puede variar desde: Altamente confidencial, confidencial, interno o público.

Ciberseguridad: Es la práctica de proteger equipos, redes, aplicaciones de software, sistemas críticos y datos de posibles amenazas digitales.