GRUPO EL COMERCIO
Directorio

El Comercio

POLÍTICA CORPORATIVA DE PROTECCIÓN DE DATOS V3

Aprobada en la Sesión de Directorio del 30 de Junio del 2022

Elaborado por:	**Cargo**	**Firma**
Miguel Angel Arriola Morales	Subgerente de Asesoría Contenciosa y Cumplimiento	
Revisado por:	**Cargo**	**Firma**
Antonio Horacio Román Calzada	Gerente Central Legal y de Cumplimiento	
Guillermo Paredes Carbajal	Gerente Corporativo de Auditoría y Riesgos	
Aprobado por:	**Cargo**	**Firma**
Directorio Corporativo	Firma por encargo, el Presidente del Directorio, señor Gabriel Miro Quesada Bojanovich	

1. Introducción

En el Grupo El Comercio (en adelante "GEC" o "el Grupo") cumplimos con las leyes, los reglamentos y las normas aplicables, en especial las relacionadas con la protección y tratamiento de datos personales. En este sentido, es inaceptable, sin excepción, tratar información de tal manera que no se incumplan con la normativa nacional e internacional aplicable.

De esta manera, reconocemos que debemos desarrollar todas nuestras actividades que involucren el tratamiento de datos personales de todos nuestros grupos de interés bajo los más estrictos lineamientos de honestidad e integridad en los negocios, manteniendo altos estándares éticos y fomentando la preservación de los principios que rigen para la protección de los datos personales.

GEC se encuentra comprometido con la protección y el tratamiento adecuado de los datos personales que las empresas del GEC podrían obtener y tener acceso. Dicho compromiso incluye la revisión y mejora continua de los procedimientos de todo el ciclo de vida de datos personales de las empresas que conforman GEC a fin de garantizar una adecuada protección de los mismos.

En este sentido, la presente política brinda herramientas a todos los que formamos parte del GEC para proteger la privacidad, confidencialidad y el tratamiento deseado por los titulares de los datos que maneja el GEC, dando así adecuado cumplimiento a la normativa y estándares internacionales de protección de datos personales.

2. Objetivo

El objetivo de la presente Política es establecer los lineamientos generales y específicos que deben seguir todos los directores, funcionarios y trabajadores del Grupo, para garantizar el tratamiento adecuado, la reserva de información, así como la seguridad de los datos personales de nuestros distintos grupos de interés y terceros autorizados con los que interactuamos, de acuerdo con los valores y principios establecidos por el GEC.

Cualquier acto que perjudique la protección de los datos personales en los bancos de datos que manejamos no será tolerado. En esa línea, toda empresa del GEC debe garantizar el irrestricto cumplimiento de la legislación de protección de datos personales que le sean aplicables de acuerdo con la jurisdicción donde operan.

3. Alcance

La presente política es de cumplimiento obligatorio para todos los directores, funcionarios y trabajadores de GEC, así como para cualquier socio de negocios que lo represente y/o proveedor que se contrate o encargue el tratamiento específico de datos.

4. Base Legal

Para la aplicación de la presente Política se deberá tener en cuenta la siguiente legislación:

- **Ley N° 29733** – Ley de Protección de Datos.
- **Decreto Supremo N° 003-2013-JUS** – Reglamento de Ley de Protección de Datos.
- **Decreto Legislativo N° 1353** – Decreto Legislativo que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, Fortalece el Régimen de Protección de Datos Personales y la Regulación de la Gestión de Intereses.
- **Decreto Supremo N° 017-2019-JUS –** Reglamento del Decreto Legislativo N° 1353
- General Data Protection Regulation de la Comunidad Europea.

5. Principios

Esta Política se rige por los siguientes principios:

- **Principio de legalidad:** Se prohíbe la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos.
- **Principio de consentimiento:** Para el tratamiento de los datos personales debe mediar el consentimiento previo, explícito e informado de su titular.
- **Principio de finalidad:** Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización.
- **Principio de proporcionalidad:** Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.
- **Principio de calidad:** Los datos personales que vayan a ser tratados deben ser veraces, exactos y, en la medida de lo posible, actualizados, necesarios, pertinentes y adecuados respecto de la finalidad para la que fueron recopilados. Deben conservarse por el tiempo necesario para cumplir con la finalidad del tratamiento.
- **Principio de seguridad:** el GEC debe adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.
- **Principio de nivel de protección adecuado:** Para el flujo transfronterizo de datos personales, se debe garantizar un nivel suficiente de protección para los datos personales que se vayan a tratar o, por lo menos, por los estándares internacionales en la materia.

6. Responsabilidades

Todas las personas incluidas en el alcance de esta Política tienen la responsabilidad individual de cumplir con los lineamientos y compromisos aquí establecidos, así como de buscar orientación en caso sea necesario.

Sin que la lista sea taxativa, las siguientes áreas tienen a su cargo las responsabilidades que a continuación se detallan:

- **Gerencia Central Legal y de Cumplimiento:**
    - Efectuar el trámite para la inscripción los bancos de datos personales y flujos transfronterizos, así como la actualización respectiva ante la Autoridad nacional competente.
    - Elaborar y mantener actualizada la Política de Privacidad y el Opt-in.
    - Gestionar con la **Gerencia de Data & Analytics** las solicitudes de opinión a la Autoridad Nacional de Protección de Datos Personales.
    - Proporcionar la información relativa al tratamiento de datos personales a la Autoridad Nacional de Protección de Datos Personales cuando esta lo requiera en coordinación con el área respectiva, así como permitirle el acceso a los bancos de datos personales que la compañía administra.
    - Atender, en primera instancia, las inspecciones que la Autoridad Nacional de Protección de Datos Personales realice en los locales del GEC, en coordinación con el área respectiva.

- Atender las solicitudes de derechos ARCO y coordinar con los responsables de los datos de cada empresa/unidad de negocios para el cumplimiento de las mismas dentro de los plazos establecidos
- Guardar toda la información respecto a las solicitudes de los derechos de los titulares en medios físicos o digitales.
- Incorporar las cláusulas sobre protección de datos personales en los contratos con trabajadores y proveedores, según corresponda.
- Dar soporte a los responsables de los datos de cada empresa/unidad de negocio.

- **Gerencia de Tecnología:**

  - Asegurar la implementación de las medidas de seguridad para el adecuado resguardo de los datos personales almacenados en las bases de datos de producción de las empresas del GEC, de acuerdo a las recomendaciones del Chief Information Security Officer.
  - Coordinar con la Gerencia Central Legal y de Cumplimiento la solicitud de opinión a la Autoridad Nacional de Protección de Datos Personales sobre la transferencia de información transfronteriza e inscribirla, de corresponder.

- **Gerencia de Data & Analytics:**

  - Asegurar la implementación de las medidas de seguridad para el adecuado resguardo de los datos personales almacenados en el Datalake de las empresas del GEC.

- **Gerencia Corporativa de Auditoría y Riesgos:**
  - Coordinar y velar por la implementación y adecuado desarrollo de la presente política en las empresas del Grupo.
  - Asegurar que los responsables de los bancos de datos diseñen e implementen controles para resguardar los datos personales y sensibles.
  - Revisar periódicamente la efectividad de los controles de seguridad adoptados para la protección de los bancos de datos personales y generar acciones de mejora, en coordinación con las Gerencias de Negocio Digital y Data & Analytics, en caso corresponda.

- **Responsable de cada empresa/unidad de negocio:**

  - Designar los recursos humanos, técnicos y presupuestables para el cumplimiento de la presente política.
  - Verificar que los responsables de los datos de cada empresa/unidad de negocio cumplan con sus funciones.

- **Responsable de los datos de cada empresa/unidad de negocio:**

  - Informar a la Gerencia Central Legal y de Cumplimiento la existencia de bases de datos y flujos transfronterizos, así como las actualizaciones de las mismas.
  - Coordinar y monitorear las actividades para la implementación, el adecuado desarrollo, y cumplimiento de lo establecido en la presente Política en cada empresa/unidad de negocio.
  - Asegurar el cumplimiento de la Política de Privacidad y el Opt-in.
  - Adaptar la Política de Protección de Datos Personales a cada empresa en particular de acuerdo con la naturaleza e industria, a los objetivos estratégicos del negocio, la legislación y la normativa vigente y coordinar su publicación y difusión.

- Asegurar el cumplimiento y la difusión de la Política de Privacidad de Datos entre los clientes, proveedores y terceros que interactúan con las empresas que conforman al Grupo.
- Apoyar el proceso de implementación de los controles de seguridad necesarios.

- **Directorio del GEC**:
  - Supervisar la ejecución de lo establecido en la presente Política.
  - Aprobar la presente Política Corporativa de Protección de Datos Personales.

7. Definiciones

- **APDP:** Autoridad Nacional de Protección de Datos Personales.
- **Autorización**: Consentimiento previo, expreso, libre e informado emitido por el titular de datos personales para que el GEC, o alguna de las empresas que lo conforma, lleve a cabo el tratamiento de sus datos.
- **Base o Banco de Datos**: Conjunto de datos personales almacenado por el Grupo que sea objeto de tratamiento.
- **Bloqueo:** Es la medida por la que el encargado del banco de datos personales impide el acceso de terceros a los datos y éstos no pueden ser objeto de tratamiento, durante el periodo de bloqueo.
- **Cancelación:** Es la acción o medida que en la Ley se describe como “supresión”, cuando se refiere a datos personales, que consiste en eliminar o suprimir los datos personales de un banco de datos.
- **Dato:** cualquier tipo de código que representa información concreta sobre hechos, elementos, etc., que permite describirlos, estudiarlos, analizarlos o conocerlos, cualquiera sea su forma de almacenamiento.
- **Dato Personal**: Cualquier información que directa o indirectamente se refiere a una persona natural y que está asociada a su identidad (v.g. nombre, condición demográfica, física, fisiológica, psíquica, psicológica, económica, cultural, fecha de nacimiento, número de documento de identidad, domicilio, dirección de correo electrónico, número telefónico, entre otros).
- **Datos sensibles**: Datos personales referidos al origen racial o étnico de una persona, ingresos económicos, datos relacionados a la salud, opiniones o convicciones políticas, religiosas, filosóficas o morales, estado mental, afiliación sindical, e información relacionada a la salud o a la vida sexual entre otros**.**
- **Procedimiento de anonimización:** Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es irreversible.
- **Procedimiento de disociación:** Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es reversible.
- **Titular**: Persona natural cuyos datos o información son objeto de tratamiento del GEC.
- **Política de Privacidad:** Comunicación escrita por el Titular del Banco de Datos Personales y dirigida a los usuarios sobre el tratamiento general de sus datos personales en caso sean recopilados.
- **Términos y condiciones de uso:** Opt-in que el Titular del Banco de Datos Personales solicita al titula de los datos personales para el tratamiento de sus datos.
- **Tratamiento de datos personales**: Operaciones y/o procedimientos que permitan la recopilación, almacenamiento, conservación, elaboración, modificación, bloqueo y cancelación, así como cualquier otra forma de procesamiento que facilite el acceso, o resulte de la comunicación, difusión o interconexión de los datos personales.
- **Transferencia de datos personales**: Transmisión, suministro o manifestación de datos personales objeto de tratamiento del GEC, a cualquier tercera persona distinta del titular de datos personales.

8. Lineamientos generales

GEC ha establecido los siguientes lineamientos generales para el adecuado cumplimiento de la normativa relacionada con la Protección de datos personales en las empresas del Grupo:

- En caso la legislación local de algunas de las empresas del GEC considere mayores restricciones o actividades a las planteadas, se debe aplicar las más exigentes para cada empresa.
- Las empresas del GEC, a través del responsable de datos de cada empresa/unidad de negocio deberán realizar actividades continuas de capacitación y difusión de la presente política.
- Las empresas del GEC gestionarán la implementación de actividades para la evaluación y monitoreo continuo de los controles y señales de alerta diseñados para el adecuado tratamiento de datos personales de nuestros grupos de interés.
- Todos los directores, funcionarios, colaboradores y proveedores encargados de datos personales del GEC deben asegurarse de procesar los datos personales con el debido cuidado, de forma exclusiva para la finalidad definida en su recopilación y cumpliendo la legislación aplicable, así como los lineamientos definidos en la presente política.
- Las Empresas del GEC procurarán: i) que se cumpla lo dispuesto en la presente Política; ii) hacer conocer, observar y respetar la presente Política por cada trabajador; iii) publicar la presente Política en lugares de fácil acceso; y, iv) suscribir obligaciones de confidencialidad con los directores, funcionarios, colaboradores, usuarios, contratistas y terceros que accedan a los datos personales incluidos en los bancos de datos.
- Las empresas del GEC cumplirán con las exigencias de auditoría interna establecidas en la Ley y su reglamento.
- Las empresas del GEC no podrán revelar datos personales salvo que sea ordenado por mandamiento motivado del juez o con autorización de su titular y con las garantías previstas en la Ley.
- Cualquier excepción relacionada con el cumplimiento de la presente política deberá ser canalizada a la **Gerencia de Tecnología, Gerencia de Data & Analytics**, al Gerente Central Legal y de Cumplimiento Corporativo, al responsable de los datos de cada empresa/unidad empresarial o comunicada a través de los canales disponibles.

9. Lineamientos específicos

Debido a la naturaleza de las operaciones de las empresas del GEC, el uso de datos personales de nuestros distintos grupos de interés es indispensable para entender sus necesidades y realizar nuestras actividades comerciales, promocionales, entre otras.

En este sentido, es necesario que, al procesar datos personales, los que formamos parte del GEC cumplan con los debidos cuidados exigidos por la ley y esperados por los titulares de los datos.

A continuación, se detallan las principales consideraciones a ser tomadas en cuenta al gestionar o trabajar con datos personales:

9.1 Recopilación, finalidad y legalidad:

- Los datos personales de una persona natural pueden estar contenidos en distintas formas, tanto físicas como digitales. En este sentido, la recopilación de datos personales deberá encontrarse limitada a aquella que es, actualmente, probable de ser requerida

para una finalidad determinada. No se recopilarán datos que sean irrelevantes para la finalidad establecida.

- Los datos recopilados deben ser almacenados en los dispositivos habilitados por el GEC, tales como: Servidor de Archivos y/o almacenamiento en nube a través del One Drive Corporativo.
- Se encuentra prohibido el almacenamiento de datos personales en dispositivos ajenos a los brindados por la organización.
- El GEC prohíbe la recopilación de datos personales por medios fraudulentos, desleales o ilícitos.

9.2 Autorización y Consentimiento

Las empresas del GEC se comprometen a tratar datos personales que:

- Al no tener el consentimiento inicial del titular, sean recopilados a través de la primera llamada de contactabilidad.
- En caso se recopilen datos personales y/o sensibles, el área encargada de hacerlo deberá coordinar con la Gerencia Central legal y de Cumplimiento, la elaboración de un documento para obtener, de manera escrita, la conformidad de la persona, cuyos datos se están recabando.
- Al ser suministrados, el titular de los datos personales haya manifestado previa, libre, expresa e inequívocamente su consentimiento de uso para la finalidad establecida que le haya sido comunicada.
- El consentimiento podrá ser revocado en cualquier momento de acuerdo con lo dispuesto en los derechos del Titular de la normativa aplicable.
- De acuerdo con lo establecido por la Ley, no se requerirá autorización únicamente en los siguientes casos:
    - Se trate de información de naturaleza pública y de libre acceso.
    - El tratamiento de los datos personales esté autorizado por la ley para fines históricos, estadísticos o científicos, siempre que se utilice un procedimiento de disociación o anonimización.
    - La información sea requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por una orden de una entidad autorizada.
    - Cuando el dato personal haya sido transferido a cualquier empresa del GEC en virtud de un consentimiento previo, expreso e informado por parte de su titular.
    - Cuando los datos personales sean necesarios para la ejecución de una relación contractual en la que el titular de datos personales es parte,
    - Otros establecidos por ley o por el reglamento de Datos Personales.

En este sentido, es obligación de las empresas del Grupo el solicitar y conservar, en las condiciones previstas en la legislación aplicable, una copia física o digital de la respectiva autorización otorgada por el Titular. En caso de datos sensibles, las empresas del Grupo conservarán el consentimiento en físico y por escrito.

9.3 Tratamiento de Datos Personales

- Los datos personales recolectados en las bases de datos de las empresas del Grupo serán considerados información confidencial, y solo podrán ser accedidos, transferidos y utilizados para los fines establecidos, siempre que medie el consentimiento del titular.
- Las áreas de Tecnología de las empresas del GEC deberán tomar medidas específicas para asegurar la debida conservación de la información bajo las condiciones de seguridad, de modo que se pueda evitar, en la medida de lo posible, su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

- Las empresas del GEC son responsables de contar con controles específicos para verificar que la información de las bases de datos a ser registrada frente a las autoridades sea completa, exacta, se encuentre actualizada, sea comprensible y comprobable.

9.4 Transferencia de información

- El GEC podrá transferir los bancos de datos con los que cuente de forma local, o internacional, a las empresas que lo conforman, siempre que esto haya sido informado y aceptado, expresa y previamente por el titular de los datos personales, como parte de su finalidad determinada.
- Las empresas del GEC podrán transferir datos personales a entidades públicas legalmente facultadas dentro del ámbito de sus funciones cuando así sea dispuesto por la legislación aplicable, o por orden o requerimiento de una entidad autorizada.
- Cualquier transferencia transfronteriza, así como nuevos bancos de datos se deben comunicar a la Gerencia Central y de Cumplimiento para su debido registro en el Ministerio de Justicia.
- Todo requerimiento, acceso, transferencia y/o solicitud de datos personales y/o sensibles, deberá ser realizado, mediante correo dirigido al área encargada de los bancos de datos personales indicando el motivo del acceso.
- Todos los bancos de datos personales o sensibles que se transfieran o compartan en formato Excel o Word por correo u otro medio digital a otras áreas del GEC y/o a partes externas (proveedores, clientes) deben ser protegidas con una contraseña, la cual debe ser enviada a través de una vía alterna como SMS o una aplicación de mensajería instantánea.

9.5 Accesos a los Bancos de Datos Personales:

- Se debe limitar el acceso a los Bancos de Datos Personales solo a las personas involucradas en el proceso de tratamiento de los datos personales o sensibles.
- Cada área es responsable de coordinar, de manera directa, con la Gerencia de Data & Analytics, los accesos para las referidas personas.
- Si por algún motivo, una persona natural o jurídica externa, tuviera acceso a los repositorios de datos personales, producto de un servicio contratado por las empresas del GEC, el área responsable de la contratación deberá asegurarse que dicho tercero cuente con un contrato, en donde se encuentre incorporada una cláusula de Protección de Datos Personales y confidencialidad de la información.

9.6 Derechos de los Titulares de la información

El GEC respetará y acatará los derechos de los titulares de datos personales, implementando mecanismos para que el Titular de los datos pueda ejercerlos:

9.6.1 Derecho de Acceso e información

Ante cualquier solicitud de un titular de datos personales, se le deberá:

- Dar acceso:
  - A obtener sin costo alguno toda la información perteneciente a sus datos personales que sea objeto del tratamiento de las empresas del Grupo.
  - Al detalle y las razones que generaron la necesidad de recopilar esta información, la forma en la que se recopiló, a solicitud de quien se recopiló, y las transferencias de dicha información que se han realizado o se tienen previstas realizar.

- El plazo para la atención de este derecho es de 20 días calendarios.

- Informar:
  - La finalidad del tratamiento de sus datos.
  - Quiénes tienen acceso o pueden ser destinatarios de dicha información.
  - El detalle de los datos recopilados del titular.
  - Las transferencias de los datos personales.
  - Tiempo de conservación de los datos.
  - El plazo para la atención de este derecho es de 8 días calendarios.

9.6.2 Derecho de rectificación, actualización e inclusión

- Se rectificará, actualizará o incluirá mayor detalle de los datos personales de los titulares cuando se advierta omisión, error, o falsedad en los mismos.
- Toda rectificación de datos personales deberá ser justificada a través de documentación sustentatoria.
- Se denegará la rectificación de la información cuando exista algún impedimento legal o material para hacerlo.
- El plazo para la atención de estos derechos es de 10 días calendarios.

9.6.3 Derecho de Cancelación o Supresión

- Se suprimirán los datos cuando: (i) estos hayan dejado de ser necesarios; (ii) se haya agotado la finalidad para la cual fueron recopilados; (iii) el titular solicite la cancelación; o, (iv) se haya vencido la vigencia del plazo establecido para su tratamiento.
- El plazo para la atención de este derecho es de 10 días calendarios.

9.6.4 Derecho de Oposición

- En caso no se hubiera prestado consentimiento, el titular de datos personales puede oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. Esta solicitud podrá ser denegada cuando se cuente con una debida justificación contractual o legal para mantener esta información en las bases de datos.
- El plazo para la atención de este derecho es de 10 días calendarios.

9.7 Fuga de Información

- Gestionar, adecuadamente, cualquier incidente relacionado a la fuga de información de datos personales, de acuerdo con el Procedimiento establecido y que se encuentra como anexo al presente documento.
- Informar, inmediatamente a la Gerencia de Auditoría y Riesgos, así como la Gerencia Central Legal y de Cumplimiento, cualquier incidente relacionado a fuga de información de datos personales.

10. Sanciones

Los incumplimientos o infracciones a la presente política podrán ser consideradas faltas graves. En los casos que corresponda, la Empresa tomará las medidas disciplinarias que considere pertinentes en los casos de incumplimiento de las obligaciones aquí estipuladas por parte de los que resultaran responsables. Asimismo, en lo que respecta a incumplimientos por parte de

proveedores, el Grupo aplicará las penalidades o consecuencias correspondientes de acuerdo a la Ley o el contrato respectivo, como, por ejemplo, la resolución del contrato.

11. Verificación del cumplimiento de la presente Política

La revisión del cumplimiento de la presente política se realizará de manera Trimestral y estará a cargo de la Gerencia de Auditoría y Riesgos, en coordinación con la Gerencia de Tecnología, Gerencia de Data & Analytics y Gerencia Central Legal y de Cumplimiento.

El encargado coordinará con el responsable a cargo de los datos personales la revisión de la efectividad de los controles implementados como, por ejemplo:

- Formatos Digitales/Físicos con la conformidad de usuarios para la recolección y tratamiento de los datos personales.
- Usuarios con accesos a los repositorios de bancos personales o sensibles.
- Revisión del equipo asignado al colaborador, para garantizar que no existan banco de datos personales y/o sensibles almacenados de manera permanente, con el apoyo de Mesa de Ayuda y previa autorización del colaborador.
- Correos enviados a otras áreas o colaboradores del GEC que incluyan transferencias de datos personales o sensibles, previa autorización de los colaboradores involucrados.
- Realizar el seguimiento y cumplimiento correspondiente del Procedimiento de Gestión de Fuga de Datos Personales.

12. Reporte de incumplimientos a la presente Política

Si tiene conocimiento o sospecha de un posible incumplimiento a esta Política, deberá informarla de manera inmediata a través de los diferentes canales de reporte que existen:

- Grupo el Comercio Te Escucha
- Comité de Auditoría y Riesgos
- Jefe inmediato superior
- Gerencia Central Legal y de Cumplimiento
- Gerencia de Tecnología
- Gerencia de Data & Analytics

Los procedimientos están establecidos para asegurar que estos reportes sean investigados y que las acciones tomadas sean las apropiadas. El GEC tiene una política de “no represalias” contra ningún denunciante por reportar algún incumplimiento potencial o real de esta Política.

Todos los reportes serán tratados de manera confidencial y se concederá el anonimato a la persona que reporta si es que éste lo solicita.

Anexo 1: Procedimiento de Gestión de Fuga de Datos Personales.

I. OBJETIVO

Definir el plan de tratamiento y gestión de incidentes relacionados a la fuga de información de datos personales, para que se tomen las decisiones y medidas adecuadas para minimizar su impacto.

II. ALCANCE

El presente procedimiento aplica a todas las empresas del Grupo El Comercio.

III. BASE LEGAL

- Ley N° 29733, Ley de Protección de Datos Personales y su Reglamento aprobado por Decreto Supremo N° 003-2013-JUS.
- Política de seguridad de información del grupo el comercio, aprobada en octubre del 2020.

IV. DEFINICIONES

Datos personales: Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.

Datos sensibles: Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual.

Titular de datos personales: Persona natural a quien corresponde los datos personales.

Fuga de información: Llamamos fuga de información a la pérdida de la confidencialidad, de forma que información privilegiada sea accedida por personal no autorizado. El impacto y las consecuencias posteriores a un incidente de fuga de información son negativos. Por un lado, la filtración de información puede dañar la imagen pública del GEC y por tanto impactar negativamente en el negocio, generando desconfianza e inseguridad en clientes. Asimismo, la publicación de información puede generar consecuencias a terceros: grupos externos de usuarios y otras organizaciones cuyos datos se hayan hecho públicos.

V. LINEAMIENTOS GENERALES Y RESPONSABILIDADES DE SEGURIDAD DE INFORMACIÓN

La información del Grupo el Comercio (GEC) es un activo que tiene valor: y, por lo tanto, requiere de una protección adecuada. En ese sentido, para lograr este objetivo, es necesario proteger apropiadamente la información, mediante una evaluación permanente de los riesgos a la que se encuentra expuesta, de manera que se mantenga la confidencialidad, integridad y disponibilidad de la información.

En tal sentido se deben considerar el cumplimiento los siguientes lineamientos de seguridad:

Lineamientos generales: Personal GEC y Terceros

- Toda Persona (Natural o Jurídica: proveedores y su personal) que labore, preste o reciba servicios en el GEC debe manejar adecuadamente la información, de acuerdo con los parámetros definidos por la Empresa.
- Toda Persona (Natural o Jurídica: proveedores y su personal) que labore, preste o reciba servicios en GEC debe comunicar cualquier incidente o debilidad de la seguridad de la información.
- Toda la información o dato de la organización debe ser procesada, transmitida y almacenada en los activos del GEC; en caso el tratamiento de la información o dato sea realizado por un tercero, estas deben cumplir con las políticas de seguridad que el GEC demande.
- No debe divulgar información del GEC ni de sus clientes, que haya sido clasificada como “Secreta”, “Confidencial” o de “Uso Interno”, salvo que hayan sido expresamente autorizados por el Propietario de la Información quien deberá hacerse responsable de esta divulgación.
- Está prohibido que los usuarios extraigan información de las dependencias del GEC si no han sido específicamente autorizados.
- Debe cumplir con todos los requisitos legales, contractuales y normativos relativos al uso de activos de información, incluyendo las políticas de seguridad y protección de datos personales, las cuales deberán mantenerse alineadas con las leyes vigentes.
- Debe proteger sus elementos de control de acceso, como contraseñas, dispositivos y otros, ya que son individuales, intransferibles y de responsabilidad única de cada empleado.
- Debe reportar a un nivel apropiado y lo antes posible, cualquier incidente que ponga en riesgo la seguridad de la información para que se tomen las medidas necesarias

Protección de activos

- Almacenar bajo llave y con restricción de accesos a personas autorizadas, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
- Eliminar los datos cuando dejen de ser útiles para la empresa o de acuerdo con lo informado a los clientes.

Uso de contraseñas

- Mantener las contraseñas en secreto.
- Seleccionar contraseñas de calidad.
- Utilizar contraseñas robustas y modificarlas cada sesenta (60) días, o cuando la gerencia de IT lo requiera, a fin de evitar reutilizar o reciclar viejas contraseñas.
- Cambiar las contraseñas provisorias en el primer inicio de sesión.
- Notificar cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

Equipos desatendidos

- Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla protegido por contraseña.
- Proteger las PC's o terminales contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ejemplo, contraseña de acceso cuando no se utilizan.

Software malicioso

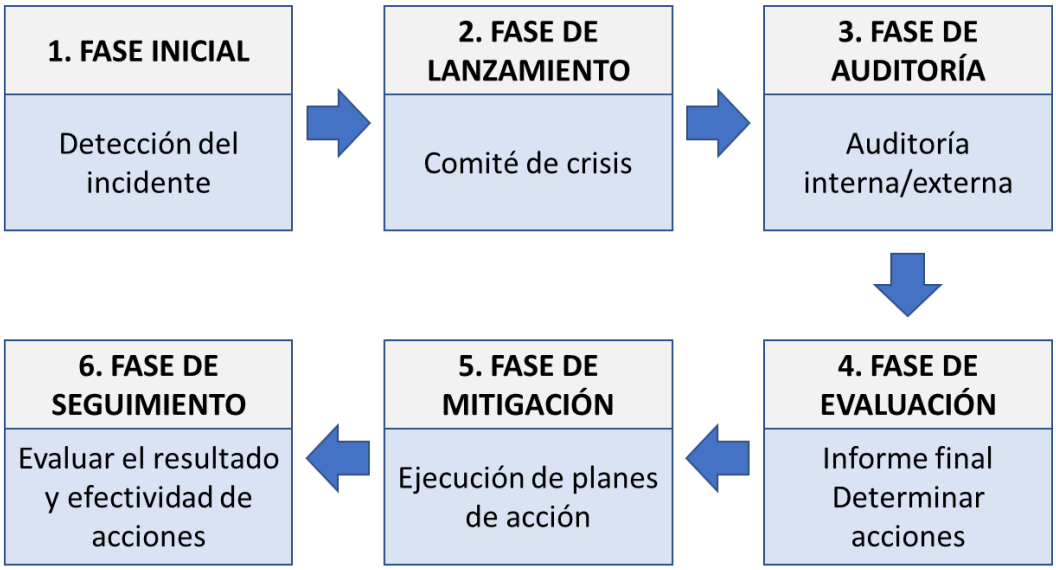
- Está prohibido el uso de software no autorizado por la Gerencia de TI.
- Verificar siempre el remitente de los mensajes de correos electrónicos.
- Entender al correo electrónico como una herramienta de trabajo provista al empleado a fin de ser utilizada conforme el uso al cual está destinada.
- Notificar inmediatamente a la Gerencia de TI y Riesgos en caso se identifiquen mensajes de procedencia sospechosa.
- Guardar la información en la nube o drive autorizados por el GEC.
- Cuando se envíe información de clientes o información sensible, se debe considerar el uso de contraseña que sólo debe ser compartida con el destinatario.

Acceso a internet

- El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto.

VI. PROCEDIMIENTO

Para el tratamiento de incidentes de fuga de información de datos personales se han determinado las siguientes 06 fases:



En función del escenario y los recursos de la organización, las actividades indicadas podrán realizarse de forma simultánea o secuencial. En cualquier caso, establecer la prioridad de las tareas será responsabilidad del Comité de Crisis.

N°	Fase / Actividad	Responsable
1	**Fase Inicial** • Detección e informe del incidente mediante el canal de reporte: ciberseguridad_gec@comercio.com.pe. • Informar internamente sobre el incidente.	Área Legal/Área usuaria Área Legal/TI/Riesgos
2	**Fase de Lanzamiento** • Convocar el Comité de Crisis de fuga de datos personales (Legal, Auditoría y Riesgos, TI, Recursos Humanos). Todas las decisiones y las acciones relativas al incidente deberán ser tomadas y coordinadas por el Comité de crisis. • Informe inicial de la situación y coordinación de primeras acciones.	Área Legal/Unidad de Riesgos Comité de Crisis
3	**Fase de Auditoría** • Inicio de Auditoría Interna para obtención de información sobre el incidente: - Determinar la cantidad de información que ha podido ser sustraída. - Establecer el tipo de datos que contiene la información que ha podido ser sustraída. - Determinar si la información es relativa a la propia organización o es externa. - Establecer y acotar la causa principal de la filtración. Si el origen es técnico, determinar los sistemas que están afectados o en los cuales se ha producido la brecha. Si es humano, iniciar el proceso para identificar como se ha producido la fuga y responsables de esa información. - Determinar el alcance de la publicación de la información sustraída. - Informe preliminar.	Auditoría y Riesgos
4	**Fase de Evaluación** • Contener la filtración y evitar nuevas fugas de información. Identificar los activos de la organización afectados, y su alcance, en relación con los activos de información, infraestructuras, otros.	Tecnología de Información

N°	Fase / Actividad	Responsable
	• Entrevistar a los afectados por la fuga de información, ya sean internos o externos. • Tareas para la mitigación de las consecuencias legales: posibles incumplimientos de normativa en materia de protección de datos personales. También aquellas tareas encaminadas a la preparación de toda la información necesaria ante posibles denuncias por los afectados. • Planificación de comunicación e información del incidente, tanto a nivel interno como externo, a medios de comunicación, y afectados, en caso de ser necesario. • Evaluar posibles sanciones al personal involucrado. • Determinar las consecuencias económicas, que puedan afectar a la organización y su posible mitigación.	Auditoría Interna Área Legal Área Legal Área Legal y RRHH Auditoría y Riesgos
5	**Fase de Mitigación** • Analizar la posibilidad de desconectar un determinado servicio o sistema de Internet. • Contactar con los sitios que han publicado información y solicitar su retirada/eliminación. • Informar sobre el incidente a los terceros afectados, como clientes o usuarios de un servicio, además de los datos que han sido sustraídos a fin de que puedan tomar las acciones oportunas para su seguridad, como puede ser el cambio de contraseñas, revocación de números de tarjetas, otros. • Informar sobre el incidente a la Autoridad Nacional de Protección de Datos Personales.	Comité de Crisis Área Legal Área Legal y Comercial Área Legal
6	**Fase de Seguimiento** • Evaluar el resultado y la efectividad de las acciones realizadas, en relación con las consecuencias y su impacto. • Implantar las medidas definitivas para evitar nuevas fugas y restablecer el normal funcionamiento de los servicios e infraestructuras que pudieran haberse visto afectadas.	Auditoría y Riesgos Tecnología de la Información