Grupo excala	PROCEDIMIENTO PARA EL TRATAMIENTO Y SEGURIDAD DE DATOS PERSONALES (PERSONAS NATURALES Y JURIDICAS)	CODIGO	VERSIÓN
		PD047	2
		FECHA DE APROBACIÓN	
		15/03/2023	

CONSIDERACIONES GENERALES

Política de tratamiento de datos AX454
Política de seguridad de la información AX466
Procedimiento para identificar, clasificar y conservar los activos de la información PD121
Procedimiento para la seguridad de la información PD009
Procedimiento de respaldo de la información PD085
Procedimiento de gestión de incidentes de seguridad PD120
Política de Uso de Recursos Informáticos AX383
Plan de Respaldo de Contingencias TI AX387
Activación del plan de contingencia PD043

QUÉ	QUIEN	COMO	DOCUMENTO / APLICATIVO RELACIONADO	CUANDO	RESULTADO
COMPROMISO DE LA DIRECCIÓN					
Designar Funcionario responsable	Comité de Presidencia	El Comité de Presidencia a través de acta designará cada vez que sea necesario y requerido al funcionario que actuará como responsable de datos dentro de la organización.	Perfil del cargo responsable de tratamiento de datos	Cuando se requiera	Responsable de tratamiento de datos designado
Aprobación de políticas y procedimientos y monitoreo a las		El Comité de Presidencia es el responsable de aprobar las políticas y procedimientos enfocados al tratamiento de datos personales, al igual que sus actualizaciones y/o modificaciones. También será responsable de monitorear el cumplimiento de las políticas y procedimientos periódicamente.	N/A	Cuando se requiera	Políticas y procedimientos aprobados
Comunicación a la Junta Directiva		Informar de manera periódica a la Junta Directiva sobre el seguimiento y cumplimiento de las políticas y procedimientos.		Semestral	Junta Directiva informada
Presupuesto y recursos		Anualmente el Comité de Presidencia designará los recursos requeridos para mantener o mejorar el cumplimiento de las políticas y procedimientos.		Anual	Recursos asignados para tratamiento de datos
Informar sobre la existencia de políticas para el tratamiento de datos	Áreas de Compras (Incluido agrícola, restaurante), Área comercial y marketing, Área de desarrollo organizacional y talento humano, Área de personal, Área de seguridad física.	Antes de recibir la información personal con los datos de los titulares, se les deberá informar que las compañías del GRUPO EXCALA son responsables del tratamiento de sus datos personales, por lo que cuenta con la existencia de políticas internas para el tratamiento de datos, adicional, se les comunicara el aviso de privacidad para el tratamiento de datos personales.	Formato de aviso de privacidad	Casa que se pretenda incluir datos personales	Titulares debidamente informados de la existencia de la política de tratamiento de datos.
	Coordinación de Seguridad Física y de Transporte, la Dirección Agrícola, Dirección Financiera y Administrativa y Coordinación de Operaciones	En las instalaciones físicas de GRUPO EXCALA, siempre se deberá contar con un aviso de privacidad y un aviso de áreas de video vigilancia con la información sugerida por el Funcionario responsable de tratamiento de datos, publicado en las áreas por donde transitan las personas. Se recomienda que el mismo sea ubicado en las entradas de la diferentes dependencias o porterías de las compañías de GRUPO EXCALA y donde se encuentren cámaras de video vigilancia Garantizar la existencia y publicación de estos avisos estará bajo responsabilidad de la Coordinación de Seguridad Física y de Transporte y la Dirección Agrícola en Compañía de Empaque SA, la Dirección Financiera y Administrativa en TEXCOMERCIAL SAS, y por la Coordinación de Operaciones en Compañía de Empaques Internacional SAS.	Formato de aviso de privacidad, aviso de zonas videovigiladas	Permanentemente	
	Dirección de sistemas	Todos los mensajes de salida de los correos corporativos de las compañías de GRUPO EXCALA, deberán contar con el respectivo aviso de privacidad recomendado por el Funcionario responsable de tratamiento de datos, el cual deberá ir al pie de la firma. La Dirección de sistemas será el encargado de garantizar la configuración y existencia de dicho aviso de privacidad en todos los correos corporativos de las compañías de GRUPO EXCALA.	Formato de aviso de privacidad en correos.	Permanentemente	
		Las compañías de GRUPO EXCALA deben contar con una política de uso de página Web actualizada, donde se definan los protocolos de uso y navegación . En esta política se deberá garantizar la publicación del aviso de privacidad para el tratamiento de datos personales suministrados a través de la página web. El Dirección de Sistemas deberá mantener la publicación de dicha política en los portales web de las compañías de GRUPO EXCALA.	Política de uso de página WEB	Permanentemente	
	Dirección de sistemas Área de Marketing	Todas las páginas web de las compañías del GRUPO EXCALA, deberán contar al inicio de la navegación con un banner donde se le informe a todos los titulares las políticas de tratamiento de datos y uso de la página web con respecto a cookies.	Política de uso de página WEB, Política de tratamiento de datos	Permanentemente	

Grupo excala	PROCEDIMIENTO PARA EL TRATAMIENTO Y SEGURIDAD DE DATOS PERSONALES (PERSONAS NATURALES Y JURIDICAS)	CODIGO	VERSIÓN
		PD047	2
		FECHA DE APROBACIÓN	
		15/03/2023	

CONSIDERACIONES GENERALES

Política de tratamiento de datos AX454
Política de seguridad de la información AX466
Procedimiento para identificar, clasificar y conservar los activos de la información PD121
Procedimiento para la seguridad de la información PD009
Procedimiento de respaldo de la información PD085
Procedimiento de gestión de incidentes de seguridad PD120
Política de Uso de Recursos Informáticos AX383
Plan de Respaldo de Contingencias TI AX387
Activación del plan de contingencia PD043

QUÉ	QUIEN	COMO	DOCUMENTO / APLICATIVO RELACIONADO	CUANDO	RESULTADO
Recolectar datos personales	Áreas de Compras (Incluido agrícola, restaurante), Área comercial y marketing, Área de desarrollo organizacional y talento humano, Área de personal, Área de seguridad física.	Los datos personales de los titulares que serán ingresados a las bases de datos de las compañías del GRUPO EXCALA, deberán ser obtenidos única y directamente del titular de los datos personales, los cuales serán consignados en los formatos establecidos para la recolección de datos personales de cada Compañía. Los datos personales también podrán ser recogidos a través de formularios electrónicos en las páginas web, canales Online y redes sociales de las Compañías del GRUPO EXCALA. Cuando se pretenda incorporar datos personales a las bases de datos de las compañías del GRUPO EXCALA, obtenidos a través de terceras personas diferentes al titular, estos deberán contar con la autorización expresa del titular para que sus datos sean entregados a terceros. Para efectos de marketing, mercadotecnia y publicidad, el Área de marketing deberá asegurar que estos terceros: 1. Obtuvieron lícitamente los datos. 2. Están autorizados para suministrar esa información a las Compañías de GRUPO EXCALA para usarlas con fines de marketing, mercadotecnia y publicidad. Por lo anterior, el Área de marketing deberá efectuar una debida diligencia sobre la procedencia de las bases de datos.	Formulario de conocimiento, formato autorización T.D, formato de autorización de uso de imágenes y videos, Clausula de T.D. para contrato de trabajo, formato autorización datos menores de edad, formato planilla control visitantes, check box de autorización en páginas web.	Cada que se pretenda incluir datos personales	Información personal recolectada
Recolectar datos a través de Sistemas de Vigilancia	Área d seguridad	Datos personales de titulares recolectados a través de Sistemas de Vigilancia (Cámaras de seguridad). Los Sistemas de Vigilancia deberán ser instalados en lugares donde no se afecte la imagen, vida privada e íntima de las personas. Sistema de Vigilancia en vías públicas: Solo se podrá instalar cámaras de seguridad en la vía pública para grabar imágenes en el área de porterías y entradas de las compañías del GRUPO EXCALA. Se restringe la grabación a las áreas más próximas al espacio vigilado.	N/A	Permanentemente	Información personal recolectada
Recolectar datos personales de niños, niñas y adolescentes	Áreas de Compras (Incluido agrícola, restaurante), Área comercial y marketing, Área de desarrollo organizacional y talento humano, Área de personal, Área de seguridad física.	El tratamiento de datos personales de niños, niñas y adolescentes solo podrá realizarse, siempre y cuando se cumplan los siguientes requisitos: 1. El tratamiento responde y respeta los intereses superiores de los niños, niñas y adolescentes. 2. El tratamiento asegura el respeto de sus derechos fundamentales. Cumplidos los anteriores requisitos se podrá solicitar la autorización para tratamiento de datos del menor, a través de la autorización otorgada por su representante legal en los formatos establecidos	Formato autorización datos menores de edad.	Cada que se pretenda incluir datos personales de menores	Información personal recolectada
Enviar las políticas para el tratamiento de datos	Dirección de sistemas	Enviar por correo electrónico la política de tratamiento de datos, al correo suministrado por el nuevo titular de datos personales. De no existir correo electrónico del titular, bastara con la entrega del aviso de privacidad. En lo posible se debe tratar de obtener por parte del titular de los datos un correo electrónico. Para los titulares de información personal que ingresa a la base de datos de clientes y proveedores que informen correo electrónico, al momento de su ingreso a la base de datos del sistema de información, de forma automática desde los correos de base de datos se les envía las políticas de tratamiento de datos al correo electrónico informado. Esta actividad está a cargo del área de sistemas de la compañía. La política de tratamiento de datos, el aviso de privacidad y sus formatos complementarios siempre deberán estar publicados y actualizados en las páginas Web de las compañías. El área de sistemas debe garantizar que toda la información relacionada a tratamiento de datos no sea eliminada ni modificada previa autorización del funcionario responsable de tratamiento de datos.	Política de tratamiento de datos. Correo Electrónico	Cada que se pretenda incluir datos personales	Titulares debidamente informados de la existencia de la política de tratamiento de datos.

Grupo excala	PROCEDIMIENTO PARA EL TRATAMIENTO Y SEGURIDAD DE DATOS PERSONALES (PERSONAS NATURALES Y JURIDICAS)	CODIGO	VERSIÓN
		PD047	2
		FECHA DE APROBACIÓN	
		15/03/2023	

CONSIDERACIONES GENERALES

Política de tratamiento de datos AX454
Política de seguridad de la información AX466
Procedimiento para identificar, clasificar y conservar los activos de la información PD121
Procedimiento para la seguridad de la información PD009
Procedimiento de respaldo de la información PD085
Procedimiento de gestión de incidentes de seguridad PD120
Política de Uso de Recursos Informáticos AX383
Plan de Respaldo de Contingencias TI AX387
Activación del plan de contingencia PD043

QUÉ	QUIEN	COMO	DOCUMENTO / APLICATIVO RELACIONADO	CUANDO	RESULTADO
Obtener autorización para el tratamiento de datos por parte del titular	Áreas de Compras (Incluido agrícola, restaurante), Área comercial y Marketing, Área de desarrollo organizacional y talento humano, Área de personal, Área de seguridad física.	Dando cumplimiento al principio de libertad, se deberá obtener la autorización por escrito por parte del titular (PERSONA NATURAL) debidamente firmado o por el representante legal (PERSONA JURIDICA). Sin autorización por parte del titular no se procederá con el ingreso de la información del tercero a las bases de datos de las Compañías del GRUPO EXCALA. Se entiende que la autorización ha sido otorgada, con la firma de los formatos y formularios establecidos para tal fin. Autorizaciones requeridas: Aspirantes a procesos de selección, empleados, uso de imágenes (fotografías y videos), menores de edad, clientes, proveedores y accionistas y visitantes. Las autorizaciones también podrán ser obtenidas por medio electrónico a través de las páginas Web, aplicaciones o canales online, de las Compañías del GRUPO EXCALA por medio del visto bueno o check box de autorización realizado. Por lo anterior, siempre que se recolecten datos por estos medios, se deberá garantizar la solicitud de la autorización de tratamiento de datos y el hipervínculo a la política de tratamiento de datos, dando cumplimiento al principio de transparencia. Se deberá obtener autorización para el uso de datos personales recolectados a través de las cookies de las páginas web de las Compañías de GRUPO EXCALA, para efectos de publicidad, mercadotecnia y marketing, por medio del visto bueno o check box de autorización realizado. Por lo anterior, siempre que se recolecten datos por medio de cookies se deberá garantizar la solicitud de la autorización de tratamiento de datos y el hipervínculo a la política de tratamiento de datos y uso de página Web, dando cumplimiento al principio de transparencia. La autorización de los datos de titulares registrados antes de la expedición del decreto 1377 del 27 junio del 2013, quedaran soportados con la comunicación realizada en diario de circulación nacional solicitando autorización, informando sobre las políticas y derechos de los titulares sobre el tratamiento de datos personales. De acuerdo al artículo 10 numeral 3 del decreto antes mencionado. Datos entregados por terceros en hojas de vida: Las hojas de vida se podrán recibir siempre y cuando cuente con la firma del tercero propietario de la información y no podrá ser usada sino se cuenta con la autorización de tratamiento de datos, la cual debe ser obtenida inmediatamente se comience proceso de selección con el tercero. Si una vez revisada la hoja de vida esta no cumple con los criterios de selección de las Compañías del GRUPO EXCALA, esta deberá ser destruida y la información no será ingresada a la base de datos de las compañías. Fotos obtenidas de internet o redes sociales: Se prohíbe el uso libre sin autorización de fotos obtenidas de internet o redes sociales, a no ser que se determine junto al Funcionario responsable de tratamiento de datos que la foto es un dato público	Formulario de conocimiento, formato autorización T.D, formato de autorización de uso de imágenes y videos, Clausula de T.D. para contrato de trabajo, formato autorización datos menores de edad, formato planilla control visitantes, check box de autorización en páginas Web.	Cada que se pretenda incluir datos personales	Autorización para el tratamiento de datos obtenida correctamente.
Archivar y guardar la documentación de los formatos de autorización de tratamiento de datos.	Áreas de Compras (Incluido agrícola, restaurante), Área comercial y Marketing, Área de desarrollo organizacional y talento humano, Área de personal, Área de seguridad física.	Cada área encargada de recolectar datos, será responsable de archivar y guardar de forma física y/o electrónica según corresponda, la documentación generada durante el proceso de recolección de datos (Formularios, formatos,) en especial las constancias de la autorización por parte del titular para el tratamiento para dar cumplimiento al principio de transparencia. **Datos recolectados de las páginas Web, aplicaciones o canales Online de las Compañías del GRUPO EXCALA:** El área de sistemas será el responsable de guardar y archivar la evidencia de la autorización otorgada por el titular de los datos, garantizando como mínimo la fecha y la identificación del tercero.	Google drive, servidores, ERP	Cada que se pretenda incluir datos personales	Información requerida y autorización de tratamiento de datos debidamente archivada y guardada.

Grupo excala	PROCEDIMIENTO PARA EL TRATAMIENTO Y SEGURIDAD DE DATOS PERSONALES (PERSONAS NATURALES Y JURIDICAS)	CODIGO	VERSIÓN
		PD047	2
		FECHA DE APROBACIÓN	
		15/03/2023	

CONSIDERACIONES GENERALES

Política de tratamiento de datos AX454
Política de seguridad de la información AX466
Procedimiento para identificar, clasificar y conservar los activos de la información PD121
Procedimiento para la seguridad de la información PD009
Procedimiento de respaldo de la información PD085
Procedimiento de gestión de incidentes de seguridad PD120
Política de Uso de Recursos Informáticos AX383
Plan de Respaldo de Contingencias TI AX387
Activación del plan de contingencia PD043

QUÉ	QUIEN	COMO	DOCUMENTO / APLICATIVO RELACIONADO	CUANDO	RESULTADO
Crear y registrar la información personal del nuevo titular que autorizó el tratamiento de sus datos en las bases de datos de la Compañías.	Áreas de Compras (Incluido agrícola, restaurante), Área comercial y Marketing, Área de desarrollo organizacional y talento humano, Área de personal, Área de seguridad física, Dirección de sistemas.	Los datos personales como activos de la información serán clasificados y almacenados de acuerdo al procedimiento interno para identificar, clasificar y conservar los activos de la información. Base de datos física: Los datos personales en documentos físicos se archivan en "única" carpeta física, según corresponda (Carpeta de: Proveedor, cliente, empleado, aspirante a nuevo cargo, etc.) debidamente marcada con el nombre del titular. Los datos personales recolectados en las planillas de control visitantes se almacenarán en única carpeta en forma cronológica. Base de datos Digital y/o Electrónica: Los datos personales escaneados o electrónicos se archivan en "única" carpeta electrónica destinada para esto, debidamente marcada con el nombre del titular. Los datos capturados a través de cámaras de video vigilancia serán almacenados en los DVR y en los servidores administrados por la Dirección de sistemas. Los datos por fotos y videos generados por actividades y/o eventos empresariales, serán almacenados por el área de comunicaciones de tal forma que permita con facilidad la consulta de la titularidad de la imagen y la autorización otorgada. Los datos por fotos y videos generados con fines de publicidad, mercadotecnia y marketing, serán almacenados por el área de marketing de tal forma que permita con facilidad la consulta de la titularidad de la imagen y la autorización otorgada. Todas las fotos deberán ser almacenadas con el nombre o identificación del titular al igual que la autorización brindada con el fin de identificar la autorización del titular de la imagen, con el fin de poder garantizar el derecho al titular y las autoridades de conocer la autorización. Registrar datos personales en el respectivo sistema de información: Todos los datos personales se deben registrar de forma precisa en los sistemas de información (ERP Epicor, UNOE, Midasoft, etc.), garantizando que los mismos sean correctos dando cumplimiento al principio de veracidad o calidad de la información.	Procedimiento interno para para identificar, clasificar y conservar los activos de la información PD121 Sistemas de información: Epicor, Midasoft, UNOE.	Cada creación y/o actualización de datos de terceros en las bases de datos de las compañías.	Datos personales debidamente registrados y almacenados de forma física y electrónica.
Usar y administrar bases de datos físicas y electrónicas	Áreas de Compras (Incluido agrícola, restaurante), Área comercial y Marketing, Área de desarrollo organizacional y talento humano, Área de personal, Área de seguridad física, Dirección de sistemas.	Los datos personales como activos de la información serán clasificados y usados de acuerdo al procedimiento interno para para identificar, clasificar y conservar los activos de la información.Dando cumplimiento al principio de acceso y circulación restringida de los datos personales, se establece: Usar y administrar bases de datos físicas y electrónicas: Solo podrán ser usadas y administradas por los funcionarios que cuenten con la respectiva cláusula de confidencialidad de la información firmada en su contrato de trabajo. En todo caso los funcionarios de las Compañías del GRUPO EXCALA deberán usar las bases de datos personales solo para los fines enunciados en la política de tratamiento de datos. Las bases de datos personales físicas solo podrán ser usadas al interior de la Compañía. En ningún caso podrán ser usadas fuera de esta. Toda información personal retirada del área que la custodia, deberá contar con la autorización y seguimiento por parte del encargado del área respectiva, este implementará los mecanismos de control necesarios para hacer seguimiento de aquella información personal física que salga del área de archivo físico, y para que la información retorne de forma íntegra al espacio físico destinado para almacenarla. Fotocopiar bases de datos físicas: Se limita el uso de "fotocopias de la información personal física" solo para las actividades que estrictamente lo requieran. Bajo ninguna circunstancia ningún funcionario que use las bases de datos físicas, podrá contar con copias físicas de la información personal. Las bases de datos personales electrónicas solo podrán ser usadas desde los equipos de información y comunicación de las Compañías del GRUPO EXCALA, el acceso a los sistemas de información y carpetas electrónicas que contengan datos personales estará limitado para aquellos funcionarios que cuenten con el perfil asignado, debidamente autorizado por el área a cargo de la base de datos y la Dirección de sistemas. Duplicar y extraer bases de datos electrónicas: Se prohíbe duplicar la información personal electrónica. Si para realizar alguna de las actividades enunciadas en la finalidad del tratamiento de datos incluida en la política, se requiere "extraer y/o duplicar información personal electrónica", se debe garantizar que, una vez terminada la actividad, la información extraída y/o duplicada sea eliminada.Consultar bases de datos físicas y electrónicas: Si dentro de las actividades a realizar solo se requiere consultar las bases de datos de información personal, estas deben ser consultadas desde su fuente de origen (sistema Epicor, Midasoft, UnoE, carpeta electrónica en servidor, área física de almacenamiento, etc.) sin extraer información.	Procedimiento interno para para identificar, clasificar y conservar los activos de la información - PD121	Cada que se usen bases de datos físicas y electrónicas	Acceso y circulación restringida a bases de datos personales

Grupo excala	PROCEDIMIENTO PARA EL TRATAMIENTO Y SEGURIDAD DE DATOS PERSONALES (PERSONAS NATURALES Y JURIDICAS)	CODIGO	VERSIÓN
		PD047	2
		FECHA DE APROBACIÓN	
		15/03/2023	

CONSIDERACIONES GENERALES

Política de tratamiento de datos AX454
Política de seguridad de la información AX466
Procedimiento para identificar, clasificar y conservar los activos de la información PD121
Procedimiento para la seguridad de la información PD009
Procedimiento de respaldo de la información PD085
Procedimiento de gestión de incidentes de seguridad PD120
Política de Uso de Recursos Informáticos AX383
Plan de Respaldo de Contingencias TI AX387
Activación del plan de contingencia PD043

QUÉ	QUIEN	COMO	DOCUMENTO / APLICATIVO RELACIONADO	CUANDO	RESULTADO
Uso de datos personales en actividades de, marketing, mercadotecnia y publicidad Uso de datos en comercio electrónico	Área de Marketing Responsable de Comercio electrónico	Siempre que se vaya a realizar un proyecto de marketing, mercadotecnia, publicidad y comercio electrónico el área de marketing y el responsable de comercio electrónico, deberá considerar la privacidad, la ética y la seguridad de los datos personales como un componente esencial del diseño del proyecto. Ver numeral 4 de la guía de sobre el tratamiento de datos personales para fines de marketing y publicidad de la SIC. Ver numeral 5 de la guía sobre tratamiento de datos personales para fines de comercio electrónico de la SIC. **Uso de herramientas de anonimización:** Se prohíbe asociar información o referirse a una persona en proyectos de marketing, mercadotecnia y publicidad. Siempre se deberá utilizar información anonimizada, de tal manera que no se pueda identificar el titular del dato. **Derecho a la tranquilidad en la prospección de clientes:** el uso de los datos personales para actividades de publicidad u ofrecimiento de productos y servicios de las Compañías del GRUPO EXCALA, se deberá garantizar que se realice en días y horarios laborales, buscando no afectar la tranquilidad de los titulares de los datos.	Guía sobre tratamiento de datos personales para fines de marketing y publicidad de la SIC. Guía sobre tratamiento de datos personales para fines de comercio electrónico de la SIC.	Cada que se usen datos para marketing mercadotecnia y publicidad y comercio electrónico	Acceso y circulación restringida a bases de datos personales
Acceso a datos personales recolectados a través de Sistemas de Vigilancia por parte de los titulares	Área de Seguridad física Dirección de sistemas	Cuando un titular ejerza su derecho de acceso a las imágenes recolectadas a través de Sistemas de Vigilancia, las Compañías del GRUPO EXCALA y las empresas de vigilancia deberán adoptar el siguiente procedimiento con el fin de proteger los derechos de los demás titulares: 1. Verificar la calidad de titular de quien solicita el acceso a las imágenes. 2. Requerir al titular la fecha, hora, lugar, y demás, requerida para facilitar la ubicación de la imagen y limitar al máximo la exposición de imágenes de otros terceros. 3. Si en la imagen aparece un (unos) tercero(s) titular(es) de datos personales se deberá contar con la autorización de dicho(s) tercero(s) para la entrega de las imágenes. 4. Si no se tiene la autorización del tercero para divulgar la información contenida en la grabación requerida, las compañías del GRUPO EXCALA deberán garantizar la anonimización del (los) dato(s) del (los) tercero(s) por lo que se deberá hacer borrosa o fragmentar la imagen de dicho(s) tercero(s).	N/A	Cada que se usen bases de datos físicas y electrónicas	Acceso y circulación restringida a bases de datos personales
Circulación de datos personales con terceros	Todas las áreas de la Compañía	En línea con el Código de Ética de GRUPO EXCALA sobre el uso de INFORMACIÓN Y SUMINISTRO DE LA MISMA, se prohíbe la circulación de datos personales con terceros, sin la previa autorización y revisión del funcionario responsable de tratamiento de datos personales y de ser requerido, con autorización del representante legal. Dando cumplimiento al principio de libertad, los datos personales no podrán ser divulgados sin previa autorización del titular, o en ausencia de mandato legal o judicial que releve el consentimiento.	Código de Ética	Cada que se usen bases de datos físicas y electrónicas	Acceso y circulación restringida a bases de datos personales
Compartir datos personales	Todas las áreas de la Compañía	Solo se podrá compartir datos personales sin autorización del titular, a terceros que vayan a actuar como encargados del tratamiento para realizar una actividad por nombre y encargo de las Compañías del GRUPO EXCALA, dicho tratamiento finalizará una vez – finalizado - el encargo. Al contratar con terceros servicios y adquisición de bienes, en los que se requiera para la ejecución del objeto del contrato darle a conocer datos personales de los cuales las Compañías del GRUPO EXCALA son responsables, se deberá diligenciar y firmar obligatoriamente el "Acuerdo para compartir datos personales" y el "Acuerdo de confidencialidad" y será archivado en la documentación de proveedor custodiado por el área responsable. Si no se firma este acuerdo no se podrá compartir información personal de los titulares. Todos los terceros que firmen el acuerdo para compartir datos, serán catalogados como Encargado de datos personales, por lo que serán informados inmediatamente al funcionario responsable de tratamiento de datos, para su control y registro en el Registro Nacional de Base de Datos - RNBD. Se excluye del diligenciamiento del acuerdo para compartir datos personales las compras por internet, como tiquetes aéreos o reservas de hotel ya que los datos suministrados son obligatorios para estructurar la compra y no se considera una actividad de compartir datos personales.	Acuerdo para compartir datos personales Acuerdos de confidencialidad	Cada que se contrate servicios y adquisición de bienes, que requieran dar a conocer al proveedor datos personales	Acuerdo para compartir datos y acuerdo de confidencialidad diligenciado y firmado.

Grupo excala	PROCEDIMIENTO PARA EL TRATAMIENTO Y SEGURIDAD DE DATOS PERSONALES (PERSONAS NATURALES Y JURIDICAS)	CODIGO	VERSIÓN
		PD047	2
		FECHA DE APROBACIÓN	
		15/03/2023	

CONSIDERACIONES GENERALES

Política de tratamiento de datos AX454
Política de seguridad de la información AX466
Procedimiento para identificar, clasificar y conservar los activos de la información PD121
Procedimiento para la seguridad de la información PD009
Procedimiento de respaldo de la información PD085
Procedimiento de gestión de incidentes de seguridad PD120
Política de Uso de Recursos Informáticos AX383
Plan de Respaldo de Contingencias TI AX387
Activación del plan de contingencia PD043

QUÉ	QUIEN	COMO	DOCUMENTO / APLICATIVO RELACIONADO	CUANDO	RESULTADO
Transmisión de datos personales en campañas de marketing, mercadotecnia y publicidad	Área de marketing Área de comunicaciones	Siempre que se contrate terceros para la realización de campañas marketing, mercadotecnia y publicidad, se deberá exigir el respeto a las políticas y procedimientos de tratamiento de datos las compañías del Grupo Excala.	Acuerdo para compartir datos personales Acuerdos de confidencialidad	Cada que se contrate servicios y adquisición de bienes, que requieran dar a conocer al proveedor datos personales	Acuerdo para compartir datos y acuerdo de confidencialidad diligenciado y firmado.
Transmisión de datos personales	Dirección de sistemas Funcionario responsable de tratamiento de datos	Solo se podrán transmitir datos personales a encargados de tratamiento que estén ubicados en los países que cuenten con un nivel adecuado de protección de datos, según información suministrada por la Superintendencia de Industria y Comercio - SIC: Alemania, Australia, Austria, Bélgica, Bulgaria, Chipre, Costa Rica, Croacia, Dinamarca, Eslovaquia, Eslovenia, Estonia, España, Estados Unidos de América, Finlandia, Francia, Grecia, Hungría, Irlanda, Islandia, Italia, Japón, Letonia, Lituania, Luxemburgo, Malta, México, Noruega, Países Bajos, Perú, Polonia, Portugal, Reino Unido, República Checa, República de Corea, Rumania, Serbia, Suecia y los países que han sido declarados con el nivel adecuado de protección por la Comisión Europea (Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay y Nueva Zelanda). Para poder realizar una transmisión de datos personales a un encargado, se deberá realizar un contrato de transmisión de datos por parte de la Dirección de Sistemas de acuerdo a las obligaciones establecidas en el artículo 25 del decreto 1377 de 2013 y este debe contener como mínimo: Alcances del tratamiento, actividades del encargado, obligaciones del encargado para con el titular de los datos y el responsable del tratamiento. El contrato debe ser revisado y autorizado por el funcionario de responsable de tratamiento de datos.	Contrato para transmitir datos personales a otros países	Cada que se trasmita datos a otros países	Contrato para transmitir datos personales elaborado y aprobado.
Eliminar información personal	Áreas de Compras (Incluido agrícola, restaurante), Área comercial y Marketing, Área de desarrollo organizacional y talento humano, Área de personal, Área de seguridad física.	Eliminar información personal de las bases de datos: La información personal deberá ser usada en el tiempo que sea razonable o necesario atendiendo los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información. Una vez cumplida la finalidad del tratamiento se procederá a la supresión de los datos personales. Los datos personales deberán ser conservados cuando así se requiera para el cumplimiento de una obligación legal o contractual. La información personal de terceros, generada a través de Sistemas de Vigilancia (Cámaras de seguridad) será eliminada cuando la capacidad del DVR sea alcanzada y se sobrescriban nuevos datos, lo cual no podrá superar los 3 meses de grabación. Eliminar información personal solicitada por el titular o su causahabiente o apoderado: Una vez recibida la solicitud por alguno de los medios establecidos en la política para esto, se deberá verificar que no exista ninguna obligación legal o contractual que obligue a las Compañías del GRUPO EXCALA a seguir conociendo sus datos, si no hay obligación alguna, se procederá con la eliminación de los datos personales. Solicitud de no envío de publicidad: Cuando un titular de datos personales solicite el no envío de publicidad, esto será atendido inmediatamente y se deberá suprimir sus datos de contacto cuando estos lo soliciten, garantizando que no se le envíe más publicidad. Disposición final (Destrucción) de la información personal física y Electrónica: Los datos personales como activos de la información serán clasificados y destruidos de acuerdo al procedimiento interno para para identificar, clasificar y conservar los activos de la información. La información personal registrada en los sistemas de información de la Compañía deberá ser eliminados de la base de datos por el área de sistemas previa instrucción por el funcionario encargado de tratamiento de datos, garantizando que esta información no pueda ser usada."	Procedimiento interno para para identificar, clasificar y conservar los activos de la información - PD121	Cuando se requiera y cuando el titular lo solicite.	Bases de datos de información personal en uso y depuradas.

Grupo excala	PROCEDIMIENTO PARA EL TRATAMIENTO Y SEGURIDAD DE DATOS PERSONALES (PERSONAS NATURALES Y JURIDICAS)	CODIGO	VERSIÓN
		PD047	2
		FECHA DE APROBACIÓN	
		15/03/2023	

CONSIDERACIONES GENERALES

Política de tratamiento de datos AX454
Política de seguridad de la información AX466
Procedimiento para identificar, clasificar y conservar los activos de la información PD121
Procedimiento para la seguridad de la información PD009
Procedimiento de respaldo de la información PD085
Procedimiento de gestión de incidentes de seguridad PD120
Política de Uso de Recursos Informáticos AX383
Plan de Respaldo de Contingencias TI AX387
Activación del plan de contingencia PD043

QUÉ	QUIEN	COMO	DOCUMENTO / APLICATIVO RELACIONADO	CUANDO	RESULTADO
Actualizar la información personal incluida en las bases de datos	Áreas de Compras (Incluido agrícola, restaurante), Área comercial y Marketing, Área de desarrollo organizacional y talento humano, Area de personal, Area de seguridad física.	Actualizar información personal: La información personal incluidas en las bases de datos de las Compañías del Grupo Excala, deberá mantenerse actualizada dando cumplimiento al principio de calidad de la información. Mínimo una vez al año las áreas que administran bases de datos, deberán facilitar procedimientos de actualización de la información por parte de los titulares. El no recibo de la actualización por parte del titular se entenderá que la información esta actualizada. Cada área mantendrá almacenada o archivada la evidencia del envió y/o recibo de la solicitud de actualización de datos según corresponda (física o electrónica). Una vez recibida la información actualizada por parte del titular, cada área deberá comparar la información recibida contra la registrada en la base de datos y sistemas de información de las compañías del Grupo Excala, y actualizará inmediatamente aquella que no sea exacta o completa. Siempre que un titular solicite la actualización de su información porque esta no sea veraz, completa, exacta o induzca al error esta debera ser atendida de forma inmediata corrigiendo la información.	Formato de actualización de datos personales definido por cada responsable de base de datos (Empleados - clientes - proveedores incluido accionistas)	Una vez al año.	Información personal actualizada en bases de datos.
Proteger la información personal en las bases de datos	Dirección de Sistemas. Áreas de Compras (Incluido agrícola, restaurante), Área comercial y Marketing, Área de desarrollo organizacional y talento humano, Área de personal, Área de seguridad física.	Los datos personales como activos de la información serán clasificados y protegidos de acuerdo al modelo de seguridad de información de las Compañías del GRUPO EXCALA. Política de seguridad de la información AX466 Procedimiento para identificar, clasificar y conservar los activos de la información PD121 Procedimiento para la seguridad de la información PD009 Procedimiento de respaldo de la información PD085 Procedimiento de gestión de incidentes de seguridad PD120 Política de Uso de Recursos Informáticos AX383 Plan de Respaldo de Contingencias TI AX387 Activación del plan de contingencia PD043 Plan de contingencia Compañía de Empaques AX341	Políticas y procedimientos de seguridad de la información	Permanentemente	Información personal con medidas de seguridad apropiadas
Medidas de seguridad en los Sistemas de Vigilancia	Área de Seguridad física Dirección de Sistemas	Las imágenes grabadas a través del Sistema de Vigilancia deberán ser visualizadas en un espacio con acceso restringido que garantice la seguridad de las mismas. El acceso y visualización de las imágenes grabadas deberá estar limitado al personal de seguridad y personal y áreas que por su actividad requieran tener acceso a las cámaras de seguridad. Todas las medidas implementadas para la adecuada recolección, uso y seguridad de las imágenes a través de Sistemas de Vigilancia, serán informadas a la empresa de vigilancia para que las ponga en práctica al operar los Sistemas de Vigilancia.	Políticas y procedimientos de seguridad de la información	Permanentemente	Información personal con medidas de seguridad apropiadas
Medidas de seguridad en el Comercio Electrónico, páginas Web y aplicaciones o canales online	Responsable de Comercio Electrónico Dirección de Sistemas	Seguridad para evitar suplantación de identidad de los clientes en comercio electrónico: Las Compañías del GRUPO EXCALA, deberán establecer procedimientos que permitan establecer la identidad real de los clientes, de manera que se pueda comprobar la veracidad de la información sobre su identificación y, al mismo tiempo, impedir situaciones de suplantación de identidad. Por lo que se deberá establecer mecanismos de firma electrónica o firma digital dependiendo del nivel de riesgo que se considere pueda existir en el proyecto de Comercio Electrónico. Las páginas Web, aplicaciones y canales online deberán garantizar un acceso seguro, por lo que siempre deberán contar con un certificado: Secure Sockets Layer - SSL vigente, que permita mantener segura la conexión a Internet y proteger la confidencialidad.	Políticas y procedimientos de seguridad de la información	Permanentemente	Información personal con medidas de seguridad apropiadas
Atender, dar seguimiento y responder consultas y reclamos	Responsable de tratamiento de datos	Cuando un titular o su causahabiente o su apoderado realice una consulta o reclamo de acuerdo a lo establecido en la política de tratamiento de datos estos deberán ser tramitados y atendidos por las Compañías de GRUPO EXCALA, de acuerdo al procedimiento interno para consultas y reclamos. Solo se podrá brindar información relacionada al titular, a las políticas y procedimientos de tratamiento de datos. Por ningún motivo se suministrará información personal de forma general que afecta la integridad de la información personal de otros titulares. Se deberá mantener prueba de las consultas y reclamos y de las respuestas por parte de las Compañías de GRUPO EXCALA, que sirvan como prueba si en algún momento son requeridas por la Superintendencia de Industria y Comercio (SIC).	Ley 1581 de 2012. Política de tratamiento de datos. Procedimiento interno consultas y reclamos Formatos de respuesta a consultas y reclamos	Cuando se presenten consultas o reclamos	Consultas y reclamos atendidos de acuerdo a la ley y la política interna de tratamiento de datos

Grupo excala	PROCEDIMIENTO PARA EL TRATAMIENTO Y SEGURIDAD DE DATOS PERSONALES (PERSONAS NATURALES Y JURIDICAS)	CODIGO	VERSIÓN
		PD047	2
		FECHA DE APROBACIÓN	
		15/03/2023	

CONSIDERACIONES GENERALES

Política de tratamiento de datos AX454
Política de seguridad de la información AX466
Procedimiento para identificar, clasificar y conservar los activos de la información PD121
Procedimiento para la seguridad de la información PD009
Procedimiento de respaldo de la información PD085
Procedimiento de gestión de incidentes de seguridad PD120
Política de Uso de Recursos Informáticos AX383
Plan de Respaldo de Contingencias TI AX387
Activación del plan de contingencia PD043

QUÉ	QUIEN	COMO	DOCUMENTO / APLICATIVO RELACIONADO	CUANDO	RESULTADO
Registrar, reportar y actualizar información de base de datos ante la SIC	Área de Compras (Incluido agrícola) Área comercial Área de gestión humana (Dirección jurídica y administrativa, dirección de calidad de vida). Área de sistemas y funcionario asignado para el tratamiento de datos	Registro de base de datos: 1. Si para el cumplimiento del objeto social de las Compañías del GRUPO EXCALA fuera necesario la creación de nuevas bases de datos, estas deberán ser informadas al funcionario asignado por las Compañías para tratamiento de datos, para que este actualice el inventario de bases de datos y realice el análisis de riesgos. En lo posible no se deben crear nuevas bases de datos diferentes a las ya registradas en el Registro Nacional de Bases de Datos (RNBD) por las Compañías del GRUPO EXCALA. 2. Se realizará una evaluación de la necesidad de crear una nueva base de datos por las partes interesadas y el funcionario asignado para el tratamiento de datos, de concluir que es necesario se procederá con su registro en el Registro Nacional de Base de Datos (RNBD) y esta nueva base de datos será tratada cumpliendo con la política y procedimientos de tratamiento de datos. Las anteriores actividades se realizarán atendiendo el instructivo "Guía para el inventario de base de datos y registro y actualización en el RNBD". 3. El usuario y contraseña es administrado por el funcionario asignado por la Compañía para tratamiento de datos y por el Jefe de Sistemas, quienes son los únicos con facultades para registrar y actualizar información en el RNBD. Reporte de violaciones a la seguridad de la información y reclamos realizados por titulares: 1. Cuando se presente violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares, los administradores de las bases de datos y el área de sistemas deberán informar por correo electrónico al funcionario asignado por la Compañía para tratamiento de datos de dicha situación, el cual, de forma inmediata sin exceder 15 días hábiles, deberá reportar la situación en el RNBD de la SIC a través de los medios dispuestos para esto. 2. Los reclamos realizados por los titulares durante el primer semestre del año (Enero a junio) se deberán reportar durante los primeros 15 días hábiles de agosto del año en curso, los reclamos realizados durante el segundo semestre del año (Julio - Diciembre) se deberán reportar en los primeros 15 días hábiles de marzo del año siguiente. 3. Para el punto anterior el funcionario asignado para el tratamiento de datos deberá llevar un registro de todos los reclamos realizados por los titulares de forma semestral. Actualización de información de las bases de datos: 1. Se deberá actualizar la información de la base de datos en RNBD en los primeros 10 días hábiles de cada mes siempre y cuando se presenten cambios sustanciales en la información previamente registrada. Los cambios sustanciales están establecidos en el numeral 2.3 de la circular externa de la SIC No. 02 de 2015. 2. Se deberá actualizar de forma obligatoria la información de las bases de datos en el RNBD de la SIC, una vez al año Entre el 2 de enero y el 31 de marzo del año siguiente. Para lo anterior, cada área que administra las bases de datos, deberá enviar hasta el 31 de enero del año siguiente, los cambios en las bases de datos registradas, con el fin que el funcionario asignado pueda realizar la respectiva actualización a tiempo. Las anteriores actividades se realizarán atendiendo el instructivo "Guía para el inventario de base de datos y registro y actualización en el RNBD".	Guía para el inventario de base de datos y registro y actualización en el RNBD. Circular No 02 de 2015 de la SIC	Se registren nuevas bases de datos. Se presenten cambios sustanciales en las bases de datos registradas. Se presenten violaciones de seguridad. Se presenten reclamos.	Registro de nuevas bases. Bases de datos actualizadas en el RNBD. Reporte de violaciones de seguridad y reclamos en el RNBD.
Capacitar y divulgar a los empleados las políticas y procedimientos de tratamiento de datos	Responsable de tratamiento de datos Gestión humana (Dirección jurídica y administrativa, dirección de calidad de vida)	Todos los empleados de las Compañías que usen la información personal de terceros dentro sus actividades cotidianas deberán recibir capacitación referente al cumplimiento estricto de la normatividad y las políticas y procedimientos internos de tratamiento de datos. Todas las políticas y procedimientos internos establecidos para el cumplimiento de la normatividad vigente en materia de tratamiento de datos deberán ser debidamente divulgada al interior de las compañías, a todo el personal que de alguna forma use la información personal de terceros. Capacitación a empleados nuevos: Todo empleado nuevo que ingrese a las compañías que dentro de sus funciones requiera acceso a información personal de terceros, deberá recibir dentro de su inducción y capacitación de ingreso, contenido referente al procedimiento y las políticas internas de tratamiento de datos, de las cuales deberá quedar constancia de asistencia y de recibo de la capacitación. Dicha capacitación deberá ser brindada por el responsable de tratamiento de datos o en su defecto por área de Desarrollo Organizacional. Capacitación a empleados antiguos: Todos los empleados de las compañías que dentro de sus funciones requieran acceso a la información personal de tercero, deberán recibir capacitación y/o actualización 1 vez al año correspondiente a la normatividad, políticas y procedimientos vigentes en materia de tratamiento de datos. De todas las capacitaciones y divulgaciones se debe dejar evidencia de la asistencia y participación de los empleados, dicha evidencia deberá ser archivada por el responsable del tratamiento de datos.	Política de tratamiento de datos.	Una vez al año empleados antiguos. Cuando ingrese personal nuevo.	Empleados debidamente capacitados en tratamiento de datos.

Grupo excala	PROCEDIMIENTO PARA EL TRATAMIENTO Y SEGURIDAD DE DATOS PERSONALES (PERSONAS NATURALES Y JURIDICAS)	CODIGO	VERSIÓN
		PD047	2
		FECHA DE APROBACIÓN	
		15/03/2023	

CONSIDERACIONES GENERALES

Política de tratamiento de datos AX454
Política de seguridad de la información AX466
Procedimiento para identificar, clasificar y conservar los activos de la información PD121
Procedimiento para la seguridad de la información PD009
Procedimiento de respaldo de la información PD085
Procedimiento de gestión de incidentes de seguridad PD120
Política de Uso de Recursos Informáticos AX383
Plan de Respaldo de Contingencias TI AX387
Activación del plan de contingencia PD043

QUÉ	QUIEN	COMO	DOCUMENTO / APLICATIVO RELACIONADO	CUANDO	RESULTADO
Verificar el cumplimiento de la política y el procedimiento interno de tratamiento de datos	Auditoría interna	Anualmente se elaborará un plan de trabajo enfocado a la verificación del cumplimiento por parte de los responsables y funcionarios que usan las bases de datos de las Compañías del GRUPO EXCALA, de las políticas y procedimientos internos para el tratamiento de datos, con el fin de determinar si los controles son efectivos y dan respuesta a los riesgos identificados, considerando la matriz de riesgos - tratamiento datos personales. Se deberá documentar los procedimientos, las pruebas y los resultados obtenidos en las auditorias. Se deberá mantener prueba de los papeles de trabajo de las auditorías realizadas. Se deberá preparar un informe de auditoría para la gerencia de las Compañías del GRUPO EXCALA que incluya los hallazgos, los riesgos y las recomendaciones del caso. Estas actividades se realizarán a cabo atendiendo las instrucciones de la "Guía de auditoria - Informe de gestión".	Guía de auditoria - Informe de gestión". Matriz de riesgos - Tratamiento datos personales.	De acuerdo a lo establecido en la guía de auditoria - Informe de gestión	Informe de gestión de auditoria
Administrar los riesgos de las bases de datos personales	Funcionario responsable de Tratamiento de Datos	De acuerdo a la política interna para la gestión de riesgos de GRUPO EXCALA, se realizarán actividades de identificación, análisis, evaluación, tratamiento y monitoreo por cada una de las bases de datos personales de las Compañías, en sus etapas de recolección, uso o circulación. almacenamiento y supresión de los datos personales. Los riesgos identificados serán base de auditoría de cumplimiento.	Política de gestión de riesgos AX405	Anual	Bases de datos de información con riesgos identificados y tratados
Supervisar y revisar las políticas y procedimientos de tratamiento de datos	Funcionario responsable de Tratamiento de Datos	Anualmente serán revisados y de ser el caso actualizados las políticas, procedimientos y matrices de riesgos enfocados en Tratamiento de Datos Personales. Periódicamente se deberá controlar y actualizar el inventario de base de datos personales para identificar y evaluar nuevas recolecciones, usos y divulgaciones. Periódicamente se deberá revisar y actualizar el contenido de la capacitación impartida a todos los empleados. Se deberá revisar y adoptar los protocolos de respuesta en el manejo de violaciones e incidentes de seguridad sucedidos. Se deberá mantener, revisar y actualizar los acuerdos para compartir datos con los encargados del tratamiento.	N/A	Anual	Programa de tratamiento de datos personales supervisado y revisado.