1. INFORMACIÓN GENERAL

Objetivo: Establecer las directrices de seguridad y privacidad para asegurar la protección de la confidencialidad, integridad y disponibilidad de los activos de información que están a disposición de los proveedores para el desarrollo de los acuerdos contractuales establecidos con la organización.

Alcance: Aplica a los proveedores que tiene acceso a la información de la organización y tienen relación contractual directa.

Responsable: Oficial de privacidad y seguridad de la información.

Documentos y registros:

TIPO	CÓDIGO	NOMBRE
Formato	A1.2F12	Acuerdo de confidencialidad
Política	A1.2PO1	Política de tratamiento de datos personales
Manual	A1.1MA3	Manual de definiciones y nomenclatura

2. NORMATIVA

El proveedor es responsable por el conocimiento y debida aplicación de los siguientes lineamientos de seguridad y privacidad de la información:

1. Definir, aprobar, formalizar, publicar y comunicar a los colaboradores la política y directrices relacionadas con la seguridad y privacidad de la información, considerando los requisitos legales aplicables.
2. Establecer los estándares, técnicas o procedimientos necesarios para implementar adecuadamente la política de seguridad y privacidad de la información al interior de la organización.
3. Garantizar la identificación, análisis, evaluación y tratamiento de los riesgos propios y de sus terceros que hacen parte de la cadena de suministro de los servicios prestados a la organización.
4. Firmar el documento A1.2F12 "Acuerdo de confidencialidad" cuando se tenga acceso a información de la organización.
5. Exigir el manejo adecuado y seguro de la información a los terceros, cuando estos tienen acceso a la información de la organización.
6. Informar a la organización por medio del supervisor del contrato, los riesgos que se hayan identificado sobre los servicios prestados, esto con el fin de actualizar el panorama de riesgos y tener el entendimiento de los impactos que estos tendrán sobre la operación.
7. Brindar a los colaboradores vinculados a los servicios que son prestados a la organización, la educación y formación apropiada en seguridad y privacidad de la información, cuyos programas deben dictarse por lo menos una vez al año y ser impartidas en las actividades de inducción/reinducción. Estos programas deben evidenciarse a través de los registros de participación y evaluación.
8. Contar con un proceso formal para la creación, modificación y eliminación de usuarios (cuentas), esto con el propósito de asegurar los derechos o permisos de acceso a las aplicaciones o a los sistemas que manejen o almacenen información de la organización. De igual forma, se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado. Este requisito aplica

para aquellos proveedores que presten servicios de suministro o administración de sistemas tecnológicos de información por fuera de la organización.

9. Restringir el acceso de los terceros a la información y sistemas utilizados por la organización. Estos permisos de acceso deben considerar: la autorización, la necesidad por conocer la información y el nivel de privilegios acorde con las labores realizadas. Los acuerdos contractuales establecidos entre proveedor y los terceros deben contener las obligaciones y responsabilidad en cuanto al manejo seguro de la información de los clientes.
10. El acceso a los sistemas informáticos de los clientes de la organización debe contar siempre con la autorización y acompañamiento de los responsables de dichos sistemas. Los permisos de acceso otorgados deben ser retirados una vez finalizada la prestación de los servicios contratados.
11. Contar con un sistema interactivo de gestión de contraseñas que asegure la calidad de estas cuando son utilizadas en la autenticación de los usuarios ante los sistemas o las aplicaciones. Este sistema puede incluir la verificación de la complejidad, la longitud mínima exigida, la vigencia y la restricción del uso de contraseñas anteriores, entre otros aspectos.
12. Evitar el uso de claves compartidas, genéricas o para grupos. La identificación y autenticación en los dispositivos y sistemas de cómputo de las organizaciones debe ser única y personalizada.
13. Las aplicaciones o sistemas de información utilizados para la prestación de servicios deben contar con herramientas o recursos criptográficos, que permitan cifrar y proteger la información sensible, personal o confidencial de la organización, así como la de sus clientes y colaboradores.
14. Implementar procedimientos para la de gestión de incidentes de seguridad y privacidad de la información, que incluya: la identificación, respuesta, recuperación y la revisión posterior a la implementación de los planes de acción o tratamiento. Los eventos que afecten la operación de los servicios prestados a la organización deben ser notificados a través del supervisor del contrato.
15. Sincronizar todos los relojes de los sistemas de información o aplicaciones utilizadas dentro de los servicios prestados a la organización. Se debe tener como referencia la hora oficial proporcionada por el Instituto Nacional de Metrología.
16. El acceso a las instalaciones y oficinas debe ser controlado para proteger la información sensible o confidencial y prevenir el robo de documentos y equipos.
17. El acceso a las áreas de procesamiento de datos, los centros de cableado y a las zonas de alto uso de información confidencial debe ser restringido y monitoreado.
18. Contar con los mecanismos de seguridad apropiados para evitar el ingreso y la proliferación de software malicioso (malware) proveniente del ciberespacio que puedan llegar a afectar la disponibilidad de la plataforma tecnológica y la confidencialidad de los datos allí almacenados. Estos recursos deben estar actualizados, permitiendo el aislamiento y control de los equipos infectados.
19. Permitir la realización coordinada de revisiones o auditorías gestionadas directamente desde la organización.
20. Contar con procedimientos para el despliegue y la aplicación de los parches o actualizaciones de los sistemas y las aplicaciones.
21. La transferencia de información entre el proveedor y la organización debe realizarse a través de canales seguros de comunicaciones, si es vía correo electrónico se debe hacer a través de cuentas corporativas privadas. En los casos que se transmita información de identificación personal (IIP) o confidencial se aplicarán controles de seguridad y privacidad de la información adicionales, como el cifrado de los mensajes, los cuales serán acordados entre las partes.

22. Cualquier modificación o cambio que se desee realizar en los sistemas informáticos de los clientes de la organización debe ser notificado previamente al responsable de la organización encargado del contacto con el cliente. Además, debe contar siempre con la aprobación y autorización del cliente, siguiendo el procedimiento regular establecido para la aprobación e implementación de cambios en la infraestructura tecnológica.
23. Garantizar la continuidad del servicio, la seguridad y privacidad de la información durante las interrupciones que afecten los servicios prestados a la organización, tales como: las provocadas por fallas o no acceso a la infraestructura física donde se presta el servicio, fallas en el suministro de energía eléctrica, los imperfectos o las fallas en los equipos de cómputo, fallas de los sistemas telefónicos o en los canales de comunicaciones, ausencia de personas críticas para la operación del servicio, ausencia o incumplimiento de los terceros requeridos para la presentación del servicio, entre otros.
24. Cumplir con los requisitos legales en materia de protección de datos personales, derechos de autor y propiedad intelectual, incluido, pero no limitado al uso de información y software.
25. Cumplir con los principios aplicables al tratamiento de datos personales de acuerdo con lo establecido en el documento A1.2PO1 "Política de tratamiento de datos personales" cuando se acceda a información de identificación personal (IIP).

3. CONTROL DE CAMBIOS

VERSIÓN	FECHA DE MODIFICACIÓN	DESCRIPCIÓN DEL CAMBIO
1	17/07/2020	Versión Inicial.
2	3/05/2023	Modificaciones de acuerdo con la nueva versión de la norma ISO/IEC 27001.
3	31/07/2024	1. Se ajusta el objetivo, alcance y normativa en cuanto a la redacción. 2. Se agregó el apartado de documentos y registros. 3. Se eliminan las definiciones y se pasaron al Manual de definiciones y nomenclatura. 4. Se agregó normativa relacionada con la protección de datos personales, derechos de autor y propiedad intelectual. 5. Se agregan lineamientos frente a la ISO/IEC 27701.

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Oficial de privacidad y seguridad de la información	Líder SIG	Gerente administrativa