política de privacidad

Cuando sea necesario distribuir estas políticas o cualquier otra información fuera de la organización, se debe tener cuidado de no revelar información confidencial a la organización, a sus clientes o a sus colaboradores.

En caso de que sea necesario gestionar desviaciones y excepciones, los casos particulares deberán presentarse al Comité de Seguridad de la Información e Inteligencia Artificial para su análisis, en relación con los riesgos relacionados y la aprobación correspondiente, si se considera factible.Entendemos cómo

Es importante que usted sepa cómo utilizamos sus datos, y agradecemos su confianza en que lo haremos con cuidado y sensatez.

Revisión de las políticas de seguridad de la información

InformaLas políticas de seguridad de la información deben revisarse periódicamente o siempre que se produzcan cambios significativos para garantizar su idoneidad, adecuación y eficacia. Esta revisión debe considerar las oportunidades para mejorar las políticas y el enfoque de la organización en materia de gestión de la seguridad de la información, en respuesta a los cambios en el entorno organizacional, las circunstancias comerciales, los requisitos legales o el entorno técnico. Las nuevas versiones o ediciones de estas políticas deben ser aprobadas por el Comité de Seguridad de la Información e Inteligencia Artificial.

acuerdos de transferencia de información

Los acuerdos de intercambio de información que la organización decida establecer incluyen lo siguiente:

Responsabilidades de gestión para controlar e informar sobre la transmisión, el envío y la recepción.

Procedimientos para garantizar la trazabilidad y la no repudiación. NETCOM.PO02.PTI-01 Políticas internas de seguridad de la información – Controles organizativos v1.0, sección 5.14 Transferencia de información. Fecha de aprobación: 5 de mayo de 2025.

Normas técnicas mínimas para el embalaje y la transmisión.

Acuerdos de custodia.

Identificar servicios de mensajería física.

Responsabilidades y compromisos en caso de incidentes de seguridad, como la pérdida de datos.

Utilizar un etiquetado acordado para la información sensible o crítica, garantizando que el significado de las etiquetas se comprenda de inmediato y que la información esté debidamente protegida.

Normas técnicas para el registro y la lectura de información y software.

Cualquier medida de control especial que pueda ser necesaria para proteger los artículos sensibles.

Niveles aceptables de control de acceso. El contenido de cualquier acuerdo debe reflejar la confidencialidad de la información empresarial involucrada.

Acuerdos de confidencialidad o de no divulgación

Hemos firmado acuerdos de confidencialidad con todas las condiciones de esta sección, las cuales quedan incorporadas en las firmas de los contratos.

Nuestro compromiso es mantener absoluta confidencialidad respecto a los objetos de los proyectos que gestionamos, ya sean de consumo privado o público.

No divulgamos información de calificación confidencial, parcial o total, que viole el principio de secreto comercial o bancario o lo que dicta el Reglamento de Operaciones Financieras, Comerciales y de Microcrédito ofrecidas al Consumidor, en su Artículo 38: Sobre prácticas abusivas en los cobros.

En caso necesario, se firmarán acuerdos de confidencialidad con cada miembro del equipo que tenga acceso a la información de nuestros clientes y representantes. Estos acuerdos les obligan a mantener estricta confidencialidad respecto al contenido de la información de nuestros clientes, y su divulgación a terceros o su uso para fines distintos a los establecidos en el contrato está estrictamente prohibido.

La información que generamos para el funcionamiento del servicio prestado será utilizada únicamente por personal autorizado.

La información escrita, verbal y extraída de los sistemas de nuestros clientes en consultas en línea o en soportes magnéticos de sus clientes, bases de datos u otras fuentes, que se nos proporcione, no será divulgada.

Nos comprometemos a cumplir en todo momento con los términos establecidos en el contrato y seremos responsables ante el cliente de garantizar que nuestro personal respete el protocolo de confidencialidad en el manejo de la información. Por lo tanto, en caso de cualquier violación de la confidencialidad por parte de nuestro personal, el contratista será responsable ante el cliente, ya sea en procedimientos administrativos o judiciales, si corresponde.

Nos comprometemos a no duplicar, reproducir ni copiar información confidencial ni ningún dato generado o suministrado a usted, ya sea antes, durante o después de la prestación del servicio contratado por sus subcontratistas o representantes.

Toda la información del cliente contenida en las bases de datos, archivos, soportes de almacenamiento y sistemas del contratista y/o del cliente, ya sean electrónicos y/o impresos, es propiedad exclusiva del cliente y se utilizará únicamente para los fines previamente establecidos en el contrato.

Toda la información relativa a modelos, planes, procesos, regulaciones, guiones, productos crediticios, productos de refinanciamiento, seguridad de la información y estrategias internas para clientes no se utilizará para ningún tipo de divulgación o presentación a otras empresas o personas en ninguna forma.

Los acuerdos de confidencialidad o de no divulgación establecidos por la organización deben abordar el requisito de proteger la información confidencial mediante términos legalmente vinculantes. Estos acuerdos pueden aplicarse a terceros o a los empleados de la organización. Se consideraron los siguientes elementos para identificar los requisitos de los acuerdos de confidencialidad o de no divulgación:

Una definición de la información que se va a proteger (por ejemplo, información confidencial).
Duración prevista del acuerdo, incluidos los casos en los que sea necesario mantener la confidencialidad de forma indefinida.

Acciones necesarias cuando finaliza un acuerdo.

Responsabilidades y acciones de los firmantes para prevenir la divulgación no autorizada de información.

La titularidad de la información, los secretos comerciales y la propiedad intelectual, y cómo esto se relaciona con la protección de la información confidencial.

El uso permitido de la información confidencial y los derechos del firmante para utilizar dicha información.

El derecho a auditar y supervisar las actividades que impliquen información confidencial.

Procedimientos para la notificación y el reporte de la divulgación no autorizada o las violaciones de información confidencial.

Condiciones relativas a la destrucción o devolución de la información cuando finaliza un acuerdo.

Medidas a adoptar en caso de incumplimiento del acuerdo. Los acuerdos de confidencialidad y no divulgación deben cumplir con todas las leyes y reglamentos de la jurisdicción a la que se aplican.

Gestión y mejora de incidentes de seguridad de la información

El Centro de Contacto Empresarial de Netcom ha establecido las responsabilidades y los procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada ante incidentes de seguridad de la información, que incluyen:

Responsabilidades de la dirección para garantizar que los siguientes procedimientos se desarrollen y comuniquen adecuadamente dentro de la organización:

Procedimientos para la planificación y preparación de la respuesta ante incidentes.

Procedimientos para la supervisión, detección, análisis y notificación de eventos e incidentes de seguridad de la información.

Procedimientos para el registro de las actividades de gestión de incidentes.

Procedimientos para el manejo de pruebas forenses.

Procedimientos para la evaluación y la toma de decisiones sobre incidentes de seguridad de la información y la evaluación de las vulnerabilidades en materia de seguridad de la información.

Procedimientos de respuesta que incluyen la escalada del problema, la recuperación controlada tras un incidente y la comunicación a las personas u organizaciones internas o externas pertinentes.

Los procedimientos establecidos garantizan que:

Personal competente se encarga de los asuntos relacionados con incidentes de seguridad de la información dentro de la organización.

Se ha habilitado un punto de contacto para informar sobre incidentes de seguridad.

Se mantienen los contactos apropiados con las autoridades, ext.Partes interesadas externas o foros que se ocupan de asuntos relacionados con incidentes de seguridad de la información.

Los procedimientos de presentación de informes incluyen:

La preparación de formularios para informar sobre incidentes de seguridad de la información, con el fin de respaldar la acción de notificación y ayudar a la persona que informa a recordar todas las acciones necesarias en caso de un incidente de seguridad de la información.

El procedimiento a seguir en caso de un incidente de seguridad de la información consiste, por ejemplo, en observar inmediatamente todos los detalles (como el tipo de brecha o violación, las fallas que se produzcan, los mensajes en la pantalla o el comportamiento extraño) y no tomar ninguna medida por cuenta propia, sino informar inmediatamente al punto de contacto y tomar únicamente medidas coordinadas.

La referencia al proceso disciplinario formal establecido para tratar con los empleados que cometen infracciones de seguridad.

Implementar procesos de retroalimentación adecuados para garantizar que las personas que reportan incidentes de seguridad de la información sean notificadas de los resultados una vez que el asunto haya sido abordado y cerrado, cuando corresponda.

El objetivo es garantizar que todos los incidentes de seguridad se aborden de inmediato.

Solicitud de eliminación de información

Se garantiza el derecho a obtener, cuando proceda, la rectificación de los datos personales y su actualización o supresión cuando estos hayan sido tratados en contravención de las disposiciones legales (véase la legislación y normativa aplicables), en particular debido a la naturaleza incompleta o inexacta de los datos, o cuando hayan sido recogidos sin la autorización del titular.

Cualquier persona interesada podrá solicitar y obtener del responsable de la base de datos la rectificación, actualización, cancelación o supresión y el cumplimiento de la garantía de confidencialidad respecto de sus datos personales.

Por este motivo, Netcom Business Contact Center pone a disposición este medio de contacto para llevar a cabo cualquier trámite indicado en esta sección y garantizar los derechos de las Partes Interesadas.

Correo electrónico: privacidad@netcom.com.pa
Sujeto: Procesamiento de la información

Ley y reglamento aplicables

Se estipula que se cumplirán las disposiciones de la Ley de Protección de la Persona contra el Tratamiento de sus Datos Personales No. 8968, de la República de Costa Rica.

Netcom Business Contact Center asume el rol de administrador de la base de datos.

Control de cambios

Versión	Descripción	Fecha	Responsable
1.0	Creación de documentos	20 de febrero de 2022	Gerente de Tecnologías de la Información, Ingeniero de Procesos
1.0	Aprobación de documentos	2 de junio de 2022	Gerente de Tecnologías de la Información
1.1	Se eliminan los controles relacionados con el desarrollo de software. Se añaden los contactos de las partes interesadas.	13 de junio de 2022	Ingeniero de procesos
1.2	Se modifica la Sección 12.3.1	29 de junio de 2022	Ingeniero de procesos

1.3	Se modifica la dirección de correo electrónico de notificación y se actualizan las políticas internas relacionadas.	30 de julio de 2025	Ingenieros de procesos