DOCUMENTO INSTITUCIONAL

SEGURIDAD DE LA INFORMACIÓN

2ª edición

PRESENTACIÓN

La Seguridad de la Información (SI) desempeña un papel cada vez más importante para las empresas del Grupo Senior. Por eso, la necesidad de proteger las informaciones y los activos de información en relación con los riesgos y amenazas que se presentan en este ámbito.

El Grupo Senior, consciente de la relevancia de este asunto, elaboró este documento reforzando la transparencia y patrocinio del tema, con el objetivo de servir de guía para los clientes y el mercado.

Carlenio Castelo Branco

Presidente

RESUMEN

1. SEGURIDAD DE LA INFORMACIÓN

En este ítem se presentarán conceptos relacionados con la Política de Seguridad de la Información, así como temas que demuestren la importancia de su elaboración, implementación y difusión.

1.1 ¿CUÁL ES EL OBJETIVO DE LA SEGURIDAD DE LA INFORMACIÓN?

La Seguridad de la Información tiene un rol estratégico en Grupo Senior y tiene como objetivo garantizar la integridad, confidencialidad, autenticidad y disponibilidad de las informaciones procesadas por la institución. La integridad, confidencialidad, autenticidad y disponibilidad de las informaciones se abordarán en los siguientes puntos.

1.1.1 ¿Qué es la integridad de la información?

Consiste en la confiabilidad de informaciones. Señala la conformidad de los datos almacenados con respecto a las inserciones, alteraciones y tratamientos autorizados realizados. Señala también la conformidad de los datos transmitidos por el remitente con los recibidos por el destinatario. El mantenimiento de la integridad presupone la garantía de no violación de los datos con intención de alteración, grabación o eliminación, ya sea accidental o deliberada.

1.1.2 ¿Qué es la disponibilidad de la información?

Consiste en asegurar que la información sea accesible a las personas y procesos autorizados, en cualquier momento requerido, durante un período previamente acordado. Mantener

la disponibilidad de la información presupone garantizar la prestación continua del servicio, sin interrupciones en el suministro de la información a quienes tienen derecho a ella.

1.1.3 ¿Qué es la confidencialidad de la información?

Consiste en asegurar que sólo las personas autorizadas tengan acceso a las informaciones almacenadas o transmitidas a través de las redes de comunicación. Mantener la confidencialidad presupone asegurar que las personas no tomen conocimiento de informaciones, accidentalmente o intencionalmente, sin contar con la autorización para tal procedimiento.

1.1.4 ¿Qué autenticidad de la información?

Consiste en garantizar la veracidad de la fuente de las informaciones. A través de la autenticación, es posible confirmar la identidad de la persona o entidad que proporciona la información.

1.2 ¿QUÉ ES LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN?

La Política de Seguridad de la Información es un documento formal, aprobado por el directorio del Grupo Senior, que tiene como propósito implementar las mejores prácticas de seguridad de la información, con el fin de asignar responsabilidades, definir derechos, deberes, expectativas de acceso y uso, sancionar y promover una cultura educativa organizacional de seguridad y privacidad de las informaciones del Grupo Senior, clientes, proveedores y socios.

1.3 TEMAS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información del Grupo Senior es un documento completo y organizado por temas. Respetando la Política de Clasificación de la Información, este documento está restringido a empleados y terceros del Grupo Senior. A continuación, se muestra una breve descripción de cada control:

1.3.1 Responsabilidades

Este tema describe todos las funciones y responsabilidades generales de la institución, sus empleados y terceros, incluyendo la alta dirección, en el tema de Seguridad de la Información en el Grupo Senior.

1.3.2 Política de contraseñas

Este tema describe los requisitos mínimos aceptables por parte del negocio para configurar contraseñas de acceso a los ambientes tecnológicos del Grupo Senior. Se implementan controles internos para requerir que las contraseñas

se configuren con un número mínimo de caracteres, bloqueando intentos y frecuencia de cambio, así como bloqueando la reutilización de contraseñas anteriores.

1.3.3 Política de control de acceso

Este tema describe las pautas generales para acceder a los activos y sistemas de información. Los accesos están segregados entre acceso lógico y acceso físico.

1.3.3.1 Acceso Lógico:

La política de acceso lógico define pautas tales como:

• Perfiles de acceso;

• Concesión, Revocación, Revisión y Cancelación de accesos;

• Acceso de terceros;

• Acceso remoto;

• Autenticación de factores múltiples (MFA)

1.3.3.2 Acceso Físico:

La política de acceso físico define lineamientos como:

• Torniquetes;

• Talanqueras;

• Cámaras de seguridad;

• Profesionales de la vigilancia;

• Generadores y UPS;

• Pararrayos;

1.3.4 Política de Uso de Activos y Dispositivos Móviles

Este tema describe las pautas para usar los activos corporativos de manera segura, profesional, ética y legal, así como los requisitos para proteger la información durante el transporte de activos.

1.3.5 Política de Clasificación de la Información

Este tema describe las pautas para clasificar la información en el manejo, etiquetado, transferencia y almacenamiento de activos de información. El documento interno prevé todas las pautas utilizadas para clasificar la información, así como sus categorías.

1.3.6 Política de escritorio despejado y pantalla despejada

Este tema describe las pautas sobre cómo manejar, almacenar y proteger la información durante el uso de las estaciones de trabajo provistas por la empresa, para evitar que las personas no autorizadas accedan a información restringida, manteniendo el principio de confidencialidad. Se implementan controles internos para asegurar el bloqueo automático de las estaciones de trabajo, evitando la exposición indebida de los datos.

1.3.7 Política de Transferencia de Informaciones

Este tema describe las pautas para asegurar que la información de Grupo Senior y sus clientes, terceros y proveedores sea transmitida de manera segura. Se implementan controles internos para garantizar la seguridad durante la transferencia de datos, dentro y fuera de la infraestructura de la empresa.

1.3.8 Política de Trabajo Remoto

Este tema describe las pautas sobre el trabajo remoto. Se implementan controles internos para garantizar que todas las transferencias de información se realicen a través de una red privada (VPN).

1.3.9 Política de Copia de Seguridad

Este tema describe las pautas para administrar las rutinas de copia de seguridad para garantizar la protección de datos contra la pérdida de información. Se implementan controles internos para garantizar que las copias de seguridad se realicen según la política, se prueben periódicamente y se almacenen de forma segura.

1.3.10 Política de Protección de Códigos Maliciosos

Este tema describe las pautas sobre el uso de herramientas para protegerse contra amenazas de malware. Se implementan controles internos para detectar, responder y mitigar la amenaza de forma inmediata.

1.3.11 Política de Gestión de Vulnerabilidades Técnicas

Este tema describe pautas para la gestión de vulnerabilidades internas y externas de Grupo Senior.

Se implementan controles internos para garantizar que las vulnerabilidades se detecten y mitiguen de acuerdo con los niveles de servicio acordados con el negocio. Los testes de invasión se realizan periódicamente para detectar fallas sistémicas, siendo un control secundario para las herramientas de detección de vulnerabilidades.

1.3.12 Política de Gestión de Eventos

Este tema describe las pautas para administrar eventos de seguridad de la información. Se implementan controles internos para asegurar que todos los eventos de seguridad sean centralizados, administrados y monitoreados continuamente.

1.3.13 Política de Desarrollo de Software

Este tema describe las pautas sobre el desarrollo de aplicaciones seguras, siguiendo las prácticas del mercado. Los entornos productivos están segregados de los entornos de homologación y desarrollo, garantizando la modificación sólo por personas previamente autorizadas. Se implementan controles internos para garantizar que las actualizaciones de la aplicación a través de la gestión del cambio y respetando la segregación de funciones. Grupo Senior implementa tecnologías para realizar pruebas estáticas (SAST) y pruebas dinámicas (DAST) durante el proceso de desarrollo.

1.3.14 Política de Respuesta a Incidentes

Este tema describe pautas para prevenir, tratar y responder adecuadamente a los incidentes de seguridad de la información que puedan impactar los servicios o recursos tecnológicos de la

institución. Además, la política describe reglas de priorización y severidad sobre posibles incidentes de seguridad, procedimientos para comunicarse con autoridades y clientes, cuando sea necesario.

1.3.15 Política de Continuidad del Negocio

Este tema describe pautas, procedimientos y estrategias a llevar a cabo ante eventuales escenarios de contingencia alineados con el propósito y objetivos estratégicos de la institución. Las pruebas de recuperación ante desastres se realizan cada seis meses para garantizar que la estrategia esté siempre actualizada.

El Grupo Senior ejecuta su carga de trabajo en proveedores cloud globales que siguen normas y estándares consolidados en el mercado internacional de certificación de Data Centers, en términos de nivel de seguridad y plan de continuidad de negocio. Esta carga de trabajo tiene su copia de seguridad replicada en al menos dos Data Centers, lo que garantiza la prevención del riesgo de pérdida total de datos, basada única y exclusivamente en la capacidad de recuperación de los datos en caso de catástrofe clasificada como ruina, teniendo en cuenta el tiempo de recuperación aplicado por estos actores globales.

Una versión pública está disponible para todos los clientes y mercados: https://www.senior.com.br/politica-de-seguranca-da-informacao

1.4 CÓMO SE REALIZA EL PROCESO DE CONCIENTIZACIÓN SOBRE LA SEGURIDAD DE LA INFORMACIÓN

El Grupo Senior realiza periódicamente eventos de capacitación y concientización en el tema de Seguridad de la Información y Privacidad de Datos, para todos los empleados y terceros. A continuación se muestra una lista de procesos de sensibilización:

• Entrenamiento Interno;

• Semana de la Seguridad de la Información;

• Lives;

• Campañas de phishing;

• Publicaciones en la red social corporativa.

1.5 ¿A QUIÉN DEBE SER DIVULGADA LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN?

La Política de Seguridad de la Información es divulgada a todos los empleados del Grupo Senior, así como a terceros.

Una versión pública está disponible para todos los clientes y mercado: https://www.senior.com.br/politica-de-seguranca-da-informacao

1.6 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA PROVEEDORES

El Grupo Senior gestiona de manera formal y estructurada la gestión de proveedores de la organización. Con ello, es necesario aceptar la Política de Seguridad de la Información para Proveedores, con carácter previo a la firma del contrato de prestación de servicios, para poder suministrar productos/servicios al Grupo Senior.

La Política de Seguridad de la Información para Proveedores está disponible para todos: https://d2nytdlptrqhdi.cloudfront.net/wp-content/uploads/2024/04/25180109/PL011.pdf

1.7 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA CONSULTORES ACREDITADOS

Grupo Senior realiza, de manera formal y estructurada, la gestión de consultores acreditados que actúan en representación de la empresa. Todos los consultores trabajan bajo un contrato de prestación de servicios, con cláusulas de confidencialidad y no divulgación de informaciones a las que puedan tener acceso, así como cláusulas de confidencialidad relacionadas con el tema de privacidad de datos personales. Para asegurar que todos los consultores acreditados actúan de acuerdo con la Política de Seguridad, se realizan auditorías por parte del equipo de Seguridad de la Información, en intervalos acordados con la organización.

2. PRIVACIDAD Y PROTECCIÓN DE DATOS

En este ítem se presentarán conceptos relacionados con la Política de Privacidad de Datos, así como cuestiones que demuestren la importancia de su elaboración, implementación y divulgación.

2.1 RESPONSABLE DE LA PROTECCIÓN DE DATOS

Grupo Senior designó a un profesional como Responsable de Protección de Datos Personales (DPO). Este profesional tiene como función informar y asesorar a la empresa en el tema de privacidad, vigilar el cumplimiento de la LGPD (Ley General de Protección de Datos) y políticas internas, asesorar en cuanto a la evaluación del impacto de la protección de datos y monitorear su desempeño y actuar como puente ante la ANPD (Autoridad Nacional de Protección de Datos) en temas relacionados con el tratamiento de datos personales. Para saber más sobre DPO, visite nuestro sitio web: https://www.senior.com.br/portal-de-privacidades.

2.2 ¿QUÉ ES LA POLÍTICA DE PROTECCIÓN DE DATOS?

La Política de Protección de Datos es un documento formal, aprobado por la dirección del Grupo Senior, que tiene como objetivo implementar las mejores prácticas de privacidad de datos personales, con la finalidad de asignar responsabilidades, definir derechos, deberes, expectativas de acceso y uso, sanciones y promover una cultura educativa organizacional de privacidad de la información del Grupo Senior, clientes, proveedores y socios.

2.3 AVISO DE PRIVACIDAD

El aviso de privacidad es una comunicación clara y objetiva, mediante la cual Grupo Senior, actuando como responsable del tratamiento, aclara al titular cómo se realiza el tratamiento de los datos personales, qué tipos de datos personales son recabados, las finalidades para las cuales son recabados, la hipótesis jurídica que autoriza el tratamiento, los terceros con los que se pueden compartir los datos y las medidas que se adoptan para protegerlos.

Este aviso de privacidad puede ser consultado en la siguiente dirección: https://www.senior.com.br/politica-de-privacidade

2.4 POLÍTICA DE COOKIES

Grupo Senior pone a disposición de los titulares, clientes, proveedores y del mercado, una Política de Cookies, cuya finalidad es conocer cómo interactúan los usuarios con los contenidos, identificar qué recursos son los más buscados, contabilizar los visitantes de una página y mejorar la experiencia del visitante.

La Política de Cookies se puede consultar en la siguiente dirección: https://www.senior.com.br/politica-de-cookies

2.5 CONTACTO CON TITULARES

Grupo Senior pone a disposición en sus sitios web un formulario para que los interesados puedan contactar con la empresa y/o solicitar la ampliación de sus derechos, entre ellos:

• Confirmación de la existencia del tratamiento;

• Acceso a los datos;

• Corrección de datos incompletos, inexactos o desactualizados;

• Anonimización, bloqueo o eliminación de contenido innecesario, excesivo o tratados en violación de las disposiciones de la LGPD;

• portabilidad de datos;

• Eliminación de datos personales tratados con consentimiento del titular, salvo en los casos previstos en el art. 16 de la Ley;

• Informaciones de entidades públicas y privadas con las que Grupo Senior compartió los datos;

• Informaciones sobre la posibilidad de no prestar el consentimiento y sobre la consecuencia de la negación;

• Revocación del consentimiento;

El formulario de contacto con el responsable de Protección de Datos se puede consultar en siguiente dirección: https://www.senior.com.br/portal-lgpd

2.6 MAPEO DE DATOS PERSONALES Y REGISTRO DE ACTIVIDADES DE TRATAMIENTO (ROPA)

El mapeo de datos, o incluso inventario de datos, mapeo de datos o flujo de datos, es un documento que refleja el camino recorrido por los datos personales dentro de la organización, incluyendo procesos, procedimientos y tecnologías a través de los cuales transitan los datos. Grupo Senior mantiene un inventario de datos, actualizándolo constantemente, así como mantiene el Registro de Actividades de Tratamiento (ROPA), con el fin de mostrar cómo se recogen los datos, qué operaciones de tratamiento se realizan y cómo se eliminan los datos personales.

2.7 ANÁLISIS DE IMPACTO DE DATOS PERSONALES (AIPD)

El Análisis de Impacto de Datos Personales (AIPD), o Informe de Impacto de Protección de Datos (RIPD), es un informe cuya función es demostrar cómo el Grupo Senior evalúa los riesgos que implica el tratamiento de datos personales y adopta medidas para mitigarlos.

3. CUMPLIMIENTO Y CERTIFICACIONES

El Grupo Senior, como una forma de demostrar su compromiso con el tema, implementa, mantiene y mejora continuamente el Sistema de Gestión de Seguridad de la Información (SGSI).

3.1ISO 27001

La norma ISO 27001 es el estándar internacional y de referencia para la gestión de la Seguridad de la Información. Su principio general es la adopción por parte de la organización de un conjunto de requisitos, procesos y controles internos, con el objetivo de gestionar y mitigar los riesgos. El Grupo Senior cuenta con su Sistema de Gestión de Seguridad de la Información (SGSI) certificado por la norma ISO 27001, con el siguiente alcance: Sistema de Gestión de Seguridad de la Información que soporta Infraestructura, Desarrollo de Aplicaciones, Entrega y Mantenimiento de soluciones SaaS. A continuación, se muestra la lista de controles implementados por la organización:

3.1.1 Política de Seguridad de la Información

El Grupo Senior mantiene una Política de Seguridad de la Información, divulgada internamente y entrenada por todos los empleados. Este documento está restringido a los empleados y describe todas las prácticas y conductas que deben seguirse durante las actividades profesionales de la empresa.

3.1.2 Organización de Seguridad de la Información

Grupo Senior ha implementado y mejora continuamente una estructura de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la empresa.

3.1.3 Seguridad en Recursos Humanos

Grupo Senior cuenta con procesos internos de recursos humanos para asegurar que los empleados y terceros comprendan sus responsabilidades y cumplan con los roles para los que fueron seleccionados.

3.1.4 Gestión de Activos

El Grupo Senior cuenta con procesos y herramientas adecuadas para identificar los activos de la organización y definir las responsabilidades adecuadas para su protección.

3.1.5 Control de acceso

El Grupo Senior ha implementado, opera y mejora continuamente el proceso de control de acceso a la información y activos de información, con el objetivo de limitar el acceso de personas no autorizadas. La gestión de acceso se realiza respetando el principio de segregación de funciones para los siguientes controles:

• Concesión de acceso;

• Cancelación de accesos;

• Revisión de accesos;

• Revocación de acceso;

3.1.6 Criptografía

El Grupo Senior implementa controles criptográficos para proteger su información y activos de información y asegurarun uso efectivo y apropiado para mantener la confidencialidad, autenticidad e integridad de la información.

3.1.7 Seguridad física y ambiental

El Grupo Senior ha implementado, opera y mejora continuamente los controles de acceso físico para evitar el acceso no autorizado, el daño y la interferencia con los recursos de procesamiento de información y la información de la organización.

3.1.8 Seguridad en las Operaciones

Grupo Senior implementa y mejora continuamente sus procesos internos para garantizar el correcto y seguro funcionamiento de los recursos de procesamiento de información. Se implementan controles técnicos y procesos para garantizar la seguridad de las operaciones de la organización, estos son:

• Gestión del cambio;

• Gestión de Capacidad;

• Protección de malware;

• Copias de Seguridad (Backup);

• Registro y seguimiento de eventos (logs);

• Gestión de vulnerabilidades técnicas;

• Auditorías de cumplimiento operativo.

3.1.9 Seguridad de las comunicaciones

Grupo Senior implementa controles técnicos que aseguran la protección de la información en las redes y los recursos de procesamiento de información que las soportan. Se implementan controles técnicos y procesos para garantizar la seguridad en los servicios de comunicación, estos son:

• Controles de acceso a la red;

• Segregación de redes;

• Políticas de transferencia de información;

• Seguridad en los mensajes electrónicos (emails);

• Cláusulas contractuales de confidencialidad y no divulgación de información.

3.1.10 Requisitos de Seguridad de los Sistemas de Información

Grupo Senior implementa y mejora continuamente los requisitos para garantizar que la seguridad de la información sea una parte integral de todo el ciclo de vida de los sistemas de información. Se implementan controles y procesos técnicos para garantizar la seguridad durante todo el ciclo de vida de la aplicación, estos son:

• Análisis y especificación de requisitos de seguridad de la información;

• Protección de transacciones de aplicaciones;

• Política de desarrollo de software seguro;

• Análisis crítico de cambios operacionales;

• Segregación entre ambientes;

• Pruebas estáticas y dinámicas de aplicaciones.

3.1.11 Relación en la Cadena de Suministro

Grupo Senior ha implementado y mejora continuamente el proceso de relación con los proveedores, con el objetivo de garantizar la protección de la información y los activos de información de la organización. Como buena práctica operativa, la organización elaboró y mantiene actualizada una política de seguridad de la información para proveedores, la cual puede ser consultada en la siguiente dirección: https://d2nytdlptrqhdi.cloudfront.net/wp-content/themes/senior2019/content/pdf/PL011.pdf

3.1.12 Gestión de Incidentes de Seguridad de la Información

El Grupo Senior ha implementado y mejora continuamente un proceso de respuesta a incidentes, con el objetivo de garantizar un enfoque coherente y eficaz para gestionar incidentes de seguridad de la información, incluida la comunicación sobre debilidades y eventos de seguridad de la información.

3.1.13 Continuidad de la seguridad de la información

El Grupo Senior ha implementado y mejora continuamente un proceso de continuidad operativa para entornos tecnológicos, con el objetivo de garantizar que las operaciones se mantengan resilientes después del impacto.

3.1.14 Cumplimiento

El Grupo Senior ha implementado controles internos para garantizar el cumplimiento de las obligaciones legales, estatutarias o contractuales relacionadas con la seguridad de la información y cualquier requisito de seguridad. El certificado ISO 27001 fue emitido por el organismo certificador Bureu Veritas, con aceptación internacional por el sello UKAS (United Kingdom Accreditation Service).

3.2 SOC 1 Tipo II

El informe SOC 1 tiene como objetivo evaluar la estructura de los controles internos de la empresa, enfocados en la auditoría financiera, es decir, aquellos que involucran, de alguna manera, el balance financiero de los clientes. Se mide de tres formas:

• Gestión de Acceso;

• Gestión de Cambio;

• Gestión de Operaciones TI.

El Grupo Senior cuenta con el reporte SOC 1 Tipo II, emitido por Auditoría independiente, para el **producto HCM (Gestión del Capital Humano) en SaaS**.

4. FAQ (Preguntas Frecuentes)

A continuación, se presentan algunas preguntas realizadas por nuestros clientes con respecto a nuestra estructura de seguridad de la información y privacidad de datos:

Pregunta	Respuesta
1. ¿El Grupo Senior cuenta con alguna otra certificación además de la ISO 27001 y SOC 1 tipo II?	Sí. Senior cuenta con un Sistema de Gestión de la Calidad certificado por la norma ISO 9001.
2. ¿El proceso de Respuesta a Incidentes incluye datos personales?	Sí. Incluye datos personales y comunicación con titulares y autoridad nacional, en caso de ser necesario.
3. ¿El Grupo Senior cuenta con un área responsable de Seguridad de la Información?	Sí. El Grupo Senior cuenta con un equipo corporativo de Seguridad de la Información, responsable del tema dentro de la organización.
4. ¿La información confidencial y sensible se transmite de forma segura?	Sí. Toda la información se transfiere de forma segura utilizando los últimos protocolos de criptografía.
5. ¿Existe un proceso de aprobación formal para otorgar y utilizar usuarios privilegiados (administradores)?	Sí. Se implementan controles internos para garantizar la segregación de funciones al otorgar acceso privilegiado.
6. ¿Se realizan pruebas de invasión? ¿Son subcontratados o internos?	Sí. Periódicamente se contratan pruebas de invasión con terceros para los productos en la nube del Grupo Senior. Además, el equipo de seguridad ofensiva interna realiza pruebas diarias en las aplicaciones y redes internas de la empresa.
7. ¿Se registran y almacenan registros para todos los sistemas internos y sistemas en la nube?	Sí. Todos los sistemas de la empresa generan logs. Todos los registros están centralizados en una herramienta SIEM, con tiempo de retención acordado con el negocio.
8. ¿Existe un proceso para eliminación de información, tanto sensible sensible como confidencial?	Sí. El Grupo Senior cuenta con un proceso formal de descarte de información, tanto física como digital, tanto propia como de los clientes.
9. ¿El Grupo Senior cuenta con una política de copia de respaldo implementada y difundida entre todos los ambientes tecnológicos?	Sí. Todos los entornos de tecnología en la nube cuentan con una política de copias de seguridad, con pruebas de integridad periódicas.
10. ¿El Grupo Senior cuenta con una política de gobierno implementada y divulgada internamente?	Sí. Se implementa y divulga una política de gobierno para entornos de nube para todos los productos vendidos por Grupo Senior.
11. ¿El Grupo Senior gestiona a todos los proveedores?	Sí. La organización implementa y adopta una política interna de gestión de proveedores. Los proveedores están registrados, calificados en función del riesgo y monitoreados continuamente.
12. ¿Qué frameworks utiliza Grupo Senior?	Se utilizan controles CIS y NIST.
13. ¿Qué certificaciones profesionales de seguridad de la información tiene el equipo de seguridad de la información?	El equipo de seguridad de la información cuenta con profesionales calificados en sus funciones, y cuenta con las siguientes certificaciones: CISSP, CEH, OSCP, Lead Auditor ISO 27001/27701, Comptia Security+, Data Protection Officer, ITIL Specialist, COBIT, LPI3, DCPT, entre otros.
14. ¿La madurez de la seguridad de la información es evaluada periódicamente por terceros?	Sí. Anualmente se lleva a cabo una evaluación de la madurez de la seguridad de la información con una

	empresa externa, utilizando los marcos CIS Controls y NIST como base.
15. ¿Existen cláusulas contractuales con empleados, terceros y proveedores sobre confidencialidad, seguridad de la información y privacidad de datos?	Sí. Todos los contratos del Grupo Senior cuentan con cláusulas de confidencialidad, seguridad y privacidad.
16. ¿El Grupo Senior cuenta con comités exclusivos para tratar la seguridad y privacidad de los datos?	Sí. Comité de Seguridad en la Nube y Comité de Privacidad de Datos.
17. ¿Cumple el Grupo con el RGPD?	No. Las empresas del Grupo Senior han adaptado sus operaciones para cumplir con la Ley General de Protección de Datos (LGPD).
18. ¿El Grupo Senior alguna vez transfiere datos personales a otros países?	Sí. Para cumplir un contrato con los clientes, en algunos productos, los datos personales pueden ser transferidos fuera de Brasil.