2- ALCANCE

La información es un activo importante para el funcionamiento de las actividades empresariales y para mantener la ventaja competitiva en el mercado. La información debe ser manejada y protegida adecuadamente. Puede estar presente en diversas formas, tales como: sistemas de información, directorios de redes, bases de datos, medios impresos, magnéticos u ópticos, dispositivos electrónicos, equipos portátiles e incluso a través de la comunicación oral.
Este documento contiene un conjunto de reglas que deben cumplir las personas involucradas en el negocio de esta empresa, con el fin de proteger y administrar los activos de información, con base en la "Política Básica de Seguridad de la Información" del Grupo Sumidenso.

Esta Política incluye las reglas del Grupo SWS y también las reglas específicas del Grupo Sumidenso.

3- DEFINICIONES

- **TI**: Tecnología de la Información;

- **Activos de Información**: Un activo es cualquier elemento o dato que agregue valor al negocio, y puede ser información digital o física, cuya violación de la confidencialidad, integridad o disponibilidad traerá un perjuicio a la Organización y/o a sus Clientes. Una filtración que exponga aspectos estratégicos o datos sobre los clientes puede generar una serie de problemas. Además de las pérdidas financieras, las fallas relacionadas con la confidencialidad pueden crear la posibilidad de fraude digital y provocar daños a la imagen de la empresa y pérdida de clientes y oportunidades comerciales. También podemos considerar activos de información a todos los dispositivos para el manejo de la información, tales como: PCs, servidores, cámaras, cámaras de video, grabadoras de voz, almacenamiento externo, etc.

- **Software**: Es la parte lógica, el conjunto de instrucciones y datos procesados en servidores y ordenadores. Toda la interacción de los usuarios de computadoras se lleva a cabo a través de software.

- **Copia de seguridad**: Es la copia de datos de un dispositivo de almacenamiento a otro para que puedan ser restaurados, en caso de pérdida de los datos originales. Ya sea por eliminaciones accidentales o fallas físicas que hacen que los datos se corrompan.

- **Medios extraíbles**: Dispositivos que permiten la lectura y escritura de datos como: CD, DVD, HD Externo, Pen Drive, tarjeta de memoria, entre otros.

- **USB:** Es un tipo de tecnología que permite la conexión de periféricos sin necesidad de apagar el ordenador, además de transmitir y almacenar datos.

- **VPN (Red Privada Virtual):** Un tipo de acceso a la red corporativa, que permite la conectividad, a través de internet, de un equipo corporativo a la red interna de la empresa,

proporcionando funcionalidades y privilegios como si estuviera conectado física y directamente a la red interna.

- **Software de mensajería: Son programas que permiten a los usuarios comunicarse de forma remota (a distancia), a través de** una conexión a Internet. A través de estos programas, es posible enviar mensajes de texto entre dispositivos físicamente distantes. También puede enviar archivos o iniciar sesiones de chat de audio y/o video en tiempo real.

- **Firewall**: Un firewall es un dispositivo de seguridad de red que monitorea el tráfico de red entrante y saliente y decide permitir o bloquear tráfico específico de acuerdo con un conjunto definido de reglas de seguridad. Los firewalls son la primera línea de defensa en la seguridad de la red. Ponen una barrera entre las redes internas e Internet.

- **Módem 3G: Es un dispositivo inalámbrico, con salida USB para la** conexión a otros dispositivos como Tablets (con soporte 3G), notebooks, netbooks, desktops entre otros, con el objetivo de conexión a internet. El módem 3G recibe y decodifica la señal digital de alta velocidad transmitida por los operadores móviles a dispositivos portátiles (teléfonos celulares, teléfonos inteligentes y computadoras portátiles) compatibles con la tecnología 3G.

- **Plazo de Compromiso:** Los Empleados y Proveedores de Servicios contratados directamente por la Compañía y que tengan acceso a la red deben adherirse formalmente a un término, comprometiéndose a actuar de acuerdo con las políticas de Seguridad de la Información. Los contratos de la Institución deben contener una cláusula que salvaguarde la confidencialidad de la información.

- **Descargo de responsabilidad:** El descargo de responsabilidad es el documento que contiene la lista de equipos y/o componentes que están bajo la responsabilidad del empleado. El documento original será archivado ante el Departamento de Informática, pudiendo el usuario solicitar una copia de este para su control. La disponibilidad de cualquier equipo o componente portátil está destinada a empleados con un cargo equivalente o superior al del Coordinador, siempre que sea aprobado por la dirección/junta directiva del área.

3.1- MISIÓN

Asegurar la integridad, confidencialidad y disponibilidad de la información.
La política de seguridad de la información de la empresa, así como las Normas de Medidas de Seguridad de la Información, deben formularse de acuerdo con las Normas Globales de: SWS: IT-0001.

3.1-1. Personas afectadas

- Todas las personas que manejen los activos de información de la empresa;
- Todas las personas que fotografían y graban videos;
- Todas las personas que manipulen el material fotografiado y grabado;

- Empleados y personas de empresas con las que hemos celebrado contratos de externalización.

3.1-2. Alcance de la divulgación

Estas Normas relacionadas con las medidas de seguridad deben ser divulgadas a toda la dirección de la empresa, a los empleados, a los empleados subcontratados y a todas las personas que utilicen los activos de información de la empresa.

3.2- DIRECTRICES

La información de la Organización, de los clientes y del público en general debe ser tratada de forma ética y confidencial y de acuerdo con las leyes y normas internas vigentes, evitando el uso y la exposición indebidos. La información debe ser utilizada de manera transparente y solo para el propósito para el cual fue recopilada.

Según la definición de la norma ISO/IEC 27002 en julio de 2007, la información es un activo que, como cualquier otro activo empresarial importante, tiene valor para la organización y debe protegerse adecuadamente.

La Política de Seguridad de la Información tiene como objetivo proteger la información de diversos tipos de amenazas, para garantizar la continuidad del negocio, minimizando los daños y maximizando el retorno de las inversiones y las oportunidades de negocio.

Para los departamentos que requieren más medidas de seguridad de la información en el curso de los negocios, además de la Política de Seguridad de la Información, se deben crear reglas internas para garantizar la seguridad de los datos.

4. DESCRIPCIÓN DE LAS ACTIVIDADES

4.1- Directrices de seguridad de la información – SWS Group

La información debe recibir una protección adecuada en cumplimiento de los principios y directrices de Seguridad de la Información del grupo SWS, a lo largo de su ciclo de vida, que incluye: Generación, Manipulación, Almacenamiento, Transporte y Eliminación. Todos los activos de información deben almacenarse correctamente en los servidores de la empresa. Los documentos impresos no deben abandonarse después de copiarlos, imprimirlos o utilizarlos.

La seguridad de la información se puede dividir en tres pilares fundamentales. Estos pilares representan un conjunto de principios que sustentan la seguridad de la información y ayudan a definir las mejores prácticas para que las empresas logren sus objetivos de seguridad. Son los siguientes:

a) **Confidencialidad:** La confidencialidad es uno de los pilares fundamentales de la seguridad de la información según la norma ISO 27001. Este pilar tiene como objetivo garantizar que la

información sea accesible solo para las personas autorizadas, protegiéndola de la divulgación no autorizada y el uso indebido. La confidencialidad es especialmente importante para la información sensible, como los datos personales y financieros. Para garantizar la confidencialidad de la información, la norma ISO 27001 establece requisitos como el control de acceso, el cifrado, la implementación de políticas de seguridad de datos y la verificación periódica de los sistemas de seguridad. Además, es importante que las empresas cuenten con un plan de contingencia para hacer frente a incidentes de seguridad que puedan comprometer la confidencialidad de la información.

b) **Integridad:** La integridad se define como la capacidad de garantizar que la información sea confiable, precisa y completa, evitando que se corrompa, se pierda o se modifique indebidamente. Para garantizar la integridad de la información, es necesario adoptar medidas de control para prevenir, detectar y corregir errores y modificaciones no autorizadas, a lo largo de todo el ciclo de vida de la información, desde su creación hasta su eliminación segura. Esto incluye la implementación de procedimientos para garantizar que solo las personas autorizadas tengan acceso a la información, así como la aplicación de mecanismos de verificación para garantizar que los datos sigan siendo consistentes y precisos. Entre los recursos utilizados para este fin, podemos destacar los procedimientos de control de acceso, encriptación y copia de seguridad.

c) **Disponibilidad:** La disponibilidad se refiere a la capacidad de acceder a la información cuando sea necesario, independientemente de dónde se almacene o cómo se procese. Esto significa que la información debe estar disponible siempre que sea necesario, para todos los que tengan acceso a ella. Para garantizar la disponibilidad de la información, es necesario implementar medidas de seguridad para evitar interrupciones o indisponibilidad. Esto incluye la implementación de medidas de redundancia de recursos críticos, tales como: circuitos de internet, dispositivos de red, estructuras de respaldo y recuperación de datos, así como Planes de Contingencia que pueden activarse en caso de fallas o incidentes de seguridad.

La seguridad efectiva de los datos no se trata solo de software específico o procesos bien establecidos. Es fundamental entender que, para que los datos estén realmente seguros, es necesario que los procesos, las personas y las tecnologías estén bien alineados y basados en los Pilares de la Seguridad de la Información.

La Política de Seguridad de la Información de Sumidenso se revisa periódicamente, una vez al año o siempre que sea necesario. Debe ser aprobado por el Comité Ejecutivo del Grupo Sumidenso.

La capacitación en seguridad de la información debe llevarse a cabo en el momento de contratar nuevos empleados, empleados temporales y contratistas.

La capacitación en seguridad de la información debe realizarse periódicamente, una vez al año o siempre que sea necesario. Se llevará a cabo un reentrenamiento para las personas que violen la política o regulación de seguridad de la información. Se debe realizar el registro de la capacitación (participantes aplicables, contenidos de la capacitación, fecha/hora, etc.).

El material de capacitación en seguridad de la información debe crearse sobre la base del material de capacitación de SWS. Debe revisarse periódicamente, una vez al año o tantas veces como sea necesario.

El profesional que recibe información confidencial debe mantenerla y custodiarla, así como limitar su acceso, controlar las copias de documentos, datos y reproducciones que puedan extraerse de la misma. No se podrá transmitir información confidencial a terceros sin el consentimiento del remitente o del área propietaria de la información.

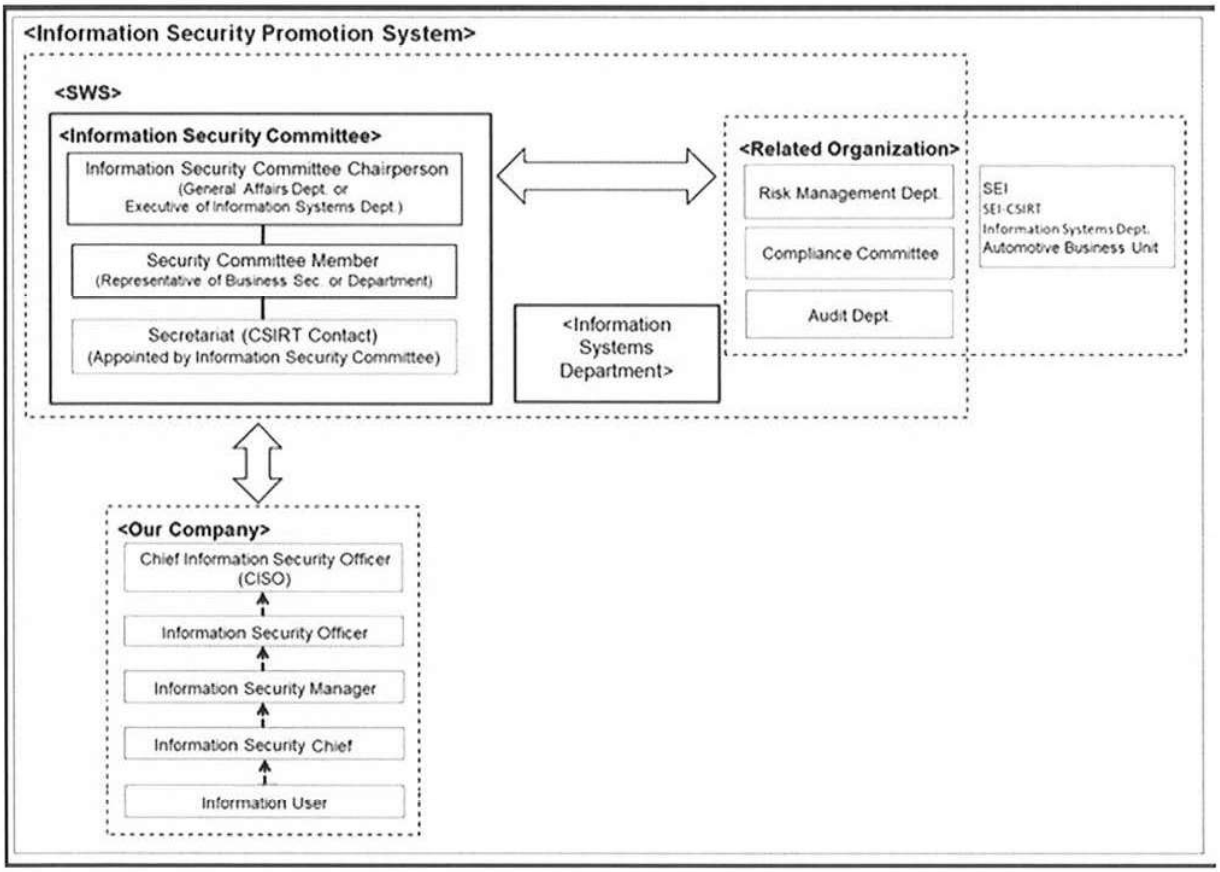
4.1.1- Comité de Gestión de Seguridad de la Información

Para promover la Seguridad de la Información dentro del Grupo Sumidenso, es necesario definir una estructura de gestión de la información, con el objetivo de establecer, controlar e implementar los requisitos de seguridad, siguiendo las reglas globales de nuestra matriz SWS.

Se debe establecer la estructura de gestión de la seguridad de la información, se debe crear un organigrama y se deben definir claramente los responsables.

4.1.1-1. Diagrama de Estructura Organizacional

(Figura 1-1: Marco de Promoción de la Seguridad de la Información)



El uso o divulgación indebida de información confidencial debe registrarse en un formulario de incidente de seguridad y debe informarse al Comité de Gestión de Seguridad de la Información.

Este organigrama define un comité compuesto por representantes de diferentes áreas siguiendo las definiciones y responsabilidades:

(1) CISO: Director de Seguridad de la Información.

Persona responsable de garantizar y promover la Seguridad de la Información desde la perspectiva de toda la empresa y tiene la autoridad necesaria para hacerlo.

Realiza principalmente las siguientes funciones:

- Aprobación de la política de seguridad de la información;
- Confirmación del estado de cumplimiento periódico de la seguridad de la información e instrucciones para la implementación de contramedidas;
- Aprobación de la evaluación de riesgos y contramedidas relacionadas con la seguridad de la información;
- Aprobación de contramedidas para incidentes de seguridad que se hayan producido.

(2) Oficial de Seguridad de la Información (TI)

Empleado designado por el CISO para promover iniciativas que garanticen la seguridad de la información en toda la empresa, monitorear el estado de cumplimiento de la seguridad de la información y promover la evaluación continua de los riesgos y contramedidas sobre la seguridad de la información.

Realiza principalmente las siguientes funciones.

- Creación y revisión de la Política de Seguridad de la Información;
- Comprobaciones periódicas relacionadas con la seguridad de la información;
- Informe periódico del estado de cumplimiento de la seguridad de la información e instrucción de acciones correctivas;
- Evaluación de riesgos y contramedidas en seguridad de la información;
- Manejo de informes de ocurrencias y descubrimientos de incidentes de seguridad;
- Elaboración de materiales educativos sobre seguridad de la información e implementación de capacitación en seguridad de la información.

(3) Gerente de Seguridad de la Información

Son los empleados nombrados por el CISO teniendo en cuenta la estructura organizativa de la Empresa.

Son responsables de velar por el cumplimiento de la política de seguridad de la información en los departamentos bajo su responsabilidad.

Los administradores de seguridad realizan las siguientes funciones:

- Verificar el estado de cumplimiento de las propias medidas de seguridad de la información del departamento e instruir acciones correctivas;
- Ejecutar las instrucciones de contramedidas y guiar las acciones correctivas del oficial de seguridad de la información;
- Aprobar la autoridad para utilizar los activos de información e instruir el control adecuado;
- Implementar la gestión de la seguridad física, incluyendo el control de entrada/salida de personas del propio departamento;
- Controlar y aprobar el envío y/o divulgación de información fuera de la empresa;
- Cooperar en respuesta a las solicitudes relacionadas con la seguridad de la información de los CISO.

(4) Jefes de Departamentos - Persona Clave

Son responsables de velar por el cumplimiento de la Política de Seguridad de la Información en su propio departamento. Realiza principalmente las siguientes funciones.

- Verificar el estado de cumplimiento de las propias medidas de seguridad de la información del departamento e instruir acciones correctivas;
- Fortalecer la conciencia de la seguridad de la información entre los empleados;
- Controlar adecuadamente los activos de información propios del departamento;
- Recopile información sobre incidentes de seguridad e informe al Gerente de Seguridad de la Información o al CISO.

(5) Usuarios de la Información

Los usuarios de información son las personas que participan en negocios relacionados con los activos de información de la empresa.

Los usuarios de la información deben asumir las siguientes responsabilidades:

- Cumplir con la Política de Seguridad de la Información;
- Informar de los incidentes de seguridad y posibles incidentes al jefe o gerente de seguridad de la información.

La estructura de gestión de la información debe ser informada a los empleados, profesionales subcontratados y/o temporales.

El organigrama debe revisarse siempre que sea necesario.

4.1.2- Gestión y Manejo de Activos de Información (Papel y Datos)

El objetivo es gestionar adecuadamente los activos de información de la empresa a proteger y estipular las normas relacionadas con su manejo, reducir los riesgos de seguridad como la divulgación no autorizada, la fuga de información y el uso ilegal, etc. Así como asegurar el nivel de control para obtener protección legal bajo la Ley de Prevención de la Competencia Desleal en caso de que ocurra un incidente de seguridad.

4.1.2-1. Personas afectadas

- Todas las personas que manejen los activos de información de la empresa;
- Todas las personas que fotografían y graban;
- Todas las personas que manipulen el material fotografiado y grabado.

4.1.2-2. Alcance

- Todos los activos de información de la empresa;
- Todos los activos de información obtenidos de clientes y socios comerciales;
- Fotografía y grabación en la empresa o lugar de trabajo del cliente.

4.1.2-3. Reglas de cumplimiento para la gestión de activos de información

4.1.2-3.1. Categoría de Gestión de Activos de Confidencialidad e Información

- El gestor es responsable de definir el período en que la información debe permanecer almacenada en el servidor y de llevar un libro registro que contenga todos los principales documentos de su área, de acuerdo con el modelo proporcionado (anexo 1).
- Cada departamento debe clasificar los activos de información (documentos en papel y datos electrónicos) que su propio departamento gestiona de acuerdo con la Tabla 2-1 <Categoría de Confidencialidad de la Información> para definir su confidencialidad.
- Cada departamento debe crear un "Libro de Control de la Información" para los activos de información (documentos en papel y datos electrónicos) que su propio departamento gestiona para cada tipo y obtener la aprobación del responsable de seguridad de la información (jefe de departamento).
- Es deseable que los documentos en papel se separen de la lista de inventario de archivos, que en principio se define en esta política. Al crearlos por separado de la lista, se debe crear un 'Libro de control de información', en principio, para que coincida con la lista de inventario de archivos.
- Las comprobaciones de inventario deben realizarse con regularidad (una vez al año o más) o según sea necesario.

Tabla 2-1 <Categoría de confidencialidad de la información>

Clasificación de la información	**Definición**	**Información de ejemplo**
Estrictamente confidencial	La información que se filtra podría infringir la privacidad individual o tener efectos graves en las empresas y negocios de los clientes.	- Información proporcionada por los clientes (dibujo o cronograma de desarrollo, etc., del modelo de automóvil antes de la venta); - Hechos graves relacionados con la regulación de los acuerdos; - Información personal que pueda violar la privacidad; - Información de gestión empresarial (estrategia de gestión, información financiera importante); - Información importante relacionada con nuevos productos o investigaciones, etc.;
Persona Autorizada Confidencial	Información que debe divulgarse a personas específicas involucradas, como miembros del departamento o del proyecto, y que puede tener efectos graves en el negocio de la empresa si se filtra. En comparación con la información "estrictamente confidencial", la	- Información del proyecto de la empresa (plan de planificación del desarrollo, etc.); - Conocimientos de diseño, fabricación, exámenes, inspecciones, etc.; - Mediciones, información de planificación de la producción, precios, ventas y compras, etc.;

	precaución asociada con esta categoría de información es menos estricta.	
Confidencial de la empresa (Interno)	Toda aquella información que no sea "Estrictamente Confidencial" y "Confidencial" y que deba ser manejada por la propia empresa y que se deba evitar que sea filtrada a terceros	- Normas Internas / Normas Varias; - Organigrama de la empresa/estructura, etc.;
Público	Es información de Sumidenso o de sus clientes con un lenguaje y formato dedicado a la difusión al público en general, ya sea su carácter informativo, comercial o promocional. Está destinado al público externo o se produce por cumplimiento de la legislación vigente que exige publicidad de esta.	- Manuales Educativos de Capacitación; - Guías del usuario del sistema; - Maquetación de documentos para cumplir con la legislación.

4.1.2-4. Tratamiento de activos de información

Cada departamento debe manejar activos de información (documentos en papel, datos electrónicos) que el propio departamento administra de acuerdo con los niveles de confidencialidad descritos en la Tabla 2-2 <Tratamiento de los activos de información por nivel de confidencialidad>.

- **Indicación**

Los documentos deben contener una indicación acorde al grado de confidencialidad. Las carpetas deben estar identificadas en el reverso y los documentos electrónicos guardados en soportes como DVD y CD deben contener etiquetas con el nombre de los archivos/carpetas junto con el grado de confidencialidad.

Para una mejor comprensión de la identificación correcta, consulte la siguiente tabla:

Categoría (Confidencialidad) / Manipulación	Estrictamente confidencial	Confidencialidad de la persona autorizada	Confidencial de la empresa
1) Indicación	"Estrictamente confidencial": Debe contener una indicación que describa claramente que el asunto es estrictamente confidencial.	"Confidencial", "Persona autorizada confidencial": debe contener una indicación que describa claramente que el asunto es confidencial para la persona autorizada.	"Confidencial de la empresa": Debe contener una indicación que describa claramente que el asunto es confidencial de la empresa.

4.1.2-4.1. Almacenamiento de papel

El almacenamiento de los documentos debe seguir las siguientes reglas, de acuerdo con la confidencialidad:

Estrictamente confidencial	Confidencialidad de la persona autorizada	Confidencial de la empresa
Deben almacenarse en armarios o trasteros cerrados, etc., en zonas donde se controle la entrada/salida (Nota 1).	Deben almacenarse y cerrarse bajo llave en áreas donde se controle la entrada y salida, o en casilleros/trasteros que se puedan cerrar con llave.	Debe seguir las mismas reglas de tratamiento que 'Persona Autorizada Confidencial'. Cuando no se controla la entrada/salida, deben guardarse en armarios.

- La información duplicada o impresa se tratará como equivalente al nivel de confidencialidad del duplicado original o de los datos impresos;
- En principio, está prohibida la eliminación de documentos confidenciales fuera de la Empresa. Si es inevitable por razones comerciales, es necesario obtener la aprobación del gerente del departamento. Si la información se extrae a través de un medio electrónico, es necesario que el dispositivo sea propiedad de Sumidenso y que esté debidamente encriptado. El registro de aprobación también debe llevarse con la fecha, el nombre del documento, el contenido, el destino, el propósito y la información de la persona que lo aprobó. Es necesario mantener el historial de aprobaciones por un período de 1 año;
- El manejo de documentos e información confidencial durante las reuniones debe seguir las mismas reglas y precauciones. Al final, los empleados deben asegurarse de que todos los documentos se hayan recopilado o eliminado.

4.1.2-4.2. Almacenamiento electrónico de datos

- Los documentos electrónicos deben almacenarse en servidores internos de archivos, dispositivos de información o sistemas de información, que son propiedad de la empresa, donde se garanticen los derechos de acceso y seguridad para contramedidas lógicas y físicas;
- El acceso a los servidores de archivos y a los sistemas de información internos debe realizarse mediante una identificación personal (nombre de usuario y contraseña);
- Es deseable que las carpetas de cada departamento estén separadas de acuerdo con los niveles de confidencialidad de los documentos;
- Las personas que pueden acceder y guardar datos en carpetas clasificadas como confidenciales deben estar debidamente limitadas;
- A menos que se utilicen temporalmente, los datos importantes no deben, en principio, almacenarse en un PC;
- Está prohibido el almacenamiento en servicios de Internet (blog, tablón de anuncios, redes sociales, etc.) que no estén autorizados por el CISO;

- En principio, está prohibido el almacenamiento de documentos estrictamente confidenciales en soportes externos. Si es inevitable, por razones comerciales, se debe obtener la aprobación de los responsables y se debe utilizar un dispositivo protegido (encriptado), que es propiedad de Sumidenso;
- Cuando se requiere almacenamiento en medios externos, se debe utilizar un dispositivo proporcionado por la empresa, y el dispositivo debe estar en un formato encriptado, para que no pueda ser decodificado por terceros;
- En principio, se prohibirá guardar la información de la empresa en dispositivos de información (PC personal, dispositivo móvil, servicio externo en la nube, etc.) que no sean los activos de la empresa. Debe seguir la siguiente tabla:

Estrictamente confidencial	Confidencialidad de la persona autorizada	Confidencial de la empresa
El medio de almacenamiento externo en el que se guarda la información debe almacenarse y guardarse bajo llave en armarios o almacenes en áreas donde se controle la entrada/salida.	El medio de almacenamiento externo en el que se guarda la información debe almacenarse en áreas donde se controle la entrada/salida, o en armarios/trasteros que puedan estar bloqueados.	Debe seguir las mismas reglas de tratamiento que 'Persona Autorizada Confidencial'. Cuando no se controla la entrada/salida, deben guardarse en armarios.

4.1.2-4.2.1. Divulgación de documentos

- La divulgación de documentos, incluida la visualización o distribución, debe limitarse a los usuarios autorizados (derechos de acceso) y a los destinos de distribución, tal como se definen en el Libro Mayor de Control de la Información;
- Cuando los usuarios autorizados (derechos de acceso) y los destinos de distribución, según lo estipulado en el libro mayor de control de la información, estén fuera del departamento, el manejo de acuerdo con el nivel de confidencialidad debe acordarse en la creación del libro mayor;
- Cuando los activos de información clasificados como estrictamente confidenciales o confidenciales de personas autorizadas se revelen a otros usuarios o departamentos, que no estén definidos en el libro de control de la información, se debe obtener la aprobación del oficial de seguridad de la información (jefe de departamento) y del gerente de información de seguridad de la información del departamento de origen. mantener el historial de manipulación;
- Cuando los activos de información clasificados como Confidenciales de la Compañía sean revelados a otros usuarios o departamentos, que no estén definidos en el libro de control de información, deberán ser revelados con la aprobación del gestor de la información y se deberá mantener el historial de manejo;
- Cuando se subcontrate a subsidiarias y afiliadas, se deben celebrar acuerdos de confidencialidad con cada departamento según sea necesario;
- En los casos en que sea inevitable revelar información confidencial a terceros por razones comerciales, deben celebrarse acuerdos de confidencialidad por adelantado;

- La información obtenida de fuera de la empresa o de otro departamento debe ser tratada de acuerdo con el nivel de confidencialidad especificado por las fuentes de información correspondientes. No debe utilizarse para nada más que para los fines designados.

4.1.2-4.2.2. Retirada de documentos fuera de la empresa

En principio, está prohibida la retirada de documentos fuera de la empresa. Cuando sea inevitable por razones comerciales, deberán observarse las siguientes reglas:

Estrictamente confidencial	Confidencialidad de la persona autorizada	Confidencial de la empresa
Se requiere la aprobación del oficial de seguridad de la información (jefe del departamento involucrado). (Nota 2) Se debe mantener un historial de recogida/devolución de documentos. El administrador de seguridad de la información o el administrador de la información deben confirmar que se ha devuelto la información que se eliminó. Se debe tener mucho cuidado para evitar fugas a terceros.	Se requiere la aprobación del gerente de dicha información, o del gerente de seguridad de la información, o del oficial de seguridad de la información (jefe de departamento), según sea necesario. Se debe mantener un historial de recogidas/devoluciones. El administrador de seguridad de la información o el administrador de la información deben confirmar que se ha devuelto la información eliminada. Se debe tener mucho cuidado para evitar fugas a terceros.	Se debe tener mucho cuidado para evitar fugas a terceros.

Nota 1: El control de entrada/salida se denominará "4.1.8. Implementación de Seguridad Física".
Nota 2: Los departamentos que necesiten llevar a cabo la eliminación de información estrictamente confidencial inevitablemente debido a las solicitudes de los clientes deben estipular reglas internas basadas en los puntos mencionados en esta norma, y deben obtener la aprobación del oficial de seguridad de la información (jefe del departamento).

4.1.2-5. Categoría de Nivel de Importancia de los Sistemas de Información

Cada departamento debe crear un libro mayor para el activo del sistema de información que el propio departamento gestiona. A continuación, se presentan las clasificaciones de las áreas y elementos que deben incluirse en el inventario que debe realizarse regularmente (una o más veces al año o siempre que sea necesaria una revisión).

Categorización del nivel de importancia de los sistemas de información:

Categoría	Definición
Nivel S	La interrupción de este sistema tiene graves consecuencias para la confirmación de las condiciones de seguridad de los funcionarios y para la transmisión de información. En este caso, cuando se interrumpe el sistema de información, el propósito del tiempo de recuperación es de un día, como el sistema de confirmación de seguridad, el sistema de transmisión de información sobre desastres, el correo electrónico, etc. que funciona en el momento del desastre.
Nivel A	La parálisis de este sistema tiene graves impactos en la gestión de la empresa o en la continuidad del negocio. En concreto, cuando se interrumpe el sistema de información, el objetivo de tiempo de recuperación es de un día. El responsable del departamento determina que la gestión de la empresa o la continuidad del negocio se verán seriamente afectadas porque el alcance afectado es grande, etc.
Nivel B	La interrupción de este sistema tiene un efecto significativo en la continuidad del negocio de la empresa. En concreto, cuando se interrumpe el sistema de información, el objetivo de tiempo de recuperación es de una semana. El jefe del departamento determina que la continuidad del negocio de la empresa se verá afectada significativamente.
Nivel C	La interrupción de los sistemas calificados de nivel C tiene poco efecto en la continuidad del negocio de la empresa porque existen métodos alternativos, etc. Específicamente, el nivel de importancia es diferente de S, A o B, y el objetivo de tiempo de recuperación es de un mes.
Nivel D	La interrupción de los sistemas clasificados de Nivel D no afecta la continuidad del negocio de la empresa porque existen métodos alternativos, etc. Específicamente, el nivel de importancia es diferente de S, A o B, y el objetivo de tiempo de recuperación es de tres meses.

4.1.2-6. Gestión de Sistemas de Información

Cada departamento debe crear un libro mayor para el activo del sistema de información que el departamento utiliza/administra.

Los siguientes son los elementos que deben conformar este documento:

Posiciones del libro mayor del sistema de información:

Nombre del artículo	Contenido

Gerente del Sistema de Información:	Persona que tiene la responsabilidad de administrar el sistema dentro del Departamento de su responsabilidad.
Sistema de Información PIC:	Persona clave que gestiona el Sistema. (Puede ser lo mismo que mánager)
Nombre del sistema:	Nombre del sistema.
Lugar de instalación:	Lugar de instalación.
Nivel de importancia:	Categorización del nivel de importancia relacionado con el sistema. Especifíquelo de acuerdo con el nivel y la importancia mencionados en el punto 4.1.2-2 de este documento (S, A, B, C o D).

Es necesario realizar un Inventario Anual (o siempre que sea necesario).

4.1.3- Normas de cumplimiento para la reparación y eliminación

4.1.3-1. Reparación de equipos

Al reparar PC, servidores y medios de almacenamiento externo, los proveedores deben visitar la empresa y reparar los dispositivos in situ.
Si no es posible efectuar la reparación dentro de la Empresa, se estipula que al enviar o retirar inevitablemente dispositivos fuera de la Empresa, se debe firmar un acuerdo de confidencialidad.

4.1.3-2. Eliminación de equipos o dispositivos de almacenamiento

Al disponer de equipos o medios de almacenamiento dentro de la Empresa, debe existir un Informe, que contenga el análisis técnico del Departamento de TI, justificando el motivo de la eliminación. Este informe debe ser aprobado por el gerente del área, después de completar el proceso de aprobación interna, el equipo de TI debe eliminar toda la información. Esto se puede hacer mediante un software específico para este propósito o mediante la destrucción física de los medios de almacenamiento.

Al subcontratar una desinversión a proveedores, se debe firmar un acuerdo de confidencialidad. Los certificados para completar la eliminación y eliminación de datos (está prohibida la reutilización de dispositivos desechados) deben recibirse del subcontratista.

4.1.3-3. Eliminación de la información en papel

Al desechar la información en papel, es necesario que los empleados destruyan físicamente los documentos a través de trituradoras de papel. Esta precaución es necesaria para evitar la fuga de información confidencial.

4.1.4- Derechos de propiedad

Las tecnologías, marcas, metodologías y cualquier información perteneciente a la Empresa no deben ser utilizadas para fines privados, ni transmitidas a terceros, incluso si han sido obtenidas o desarrolladas por el propio Empleado en su entorno laboral.

4.1.5- Propiedad intelectual

Todos los proyectos, creaciones o procedimientos desarrollados por cualquier empleado durante el curso de su relación laboral con la Compañía son propiedad de Sumidenso.

4.1.6- Reproducción de fotos y grabación de video/voz

4.1.6-1. Prohibiciones y precauciones

Está prohibido fotografiar o realizar grabaciones de vídeo/voz en las instalaciones de la empresa por parte de personas externas.

En principio, la toma de fotografías, grabaciones de información estrictamente confidencial estará prohibida para los empleados o proveedores de servicios. En caso de necesidad específica, en circunstancias inevitables para el negocio de la empresa, es obligatorio obtener la aprobación de la gerencia (preferiblemente) o supervisor local con autorización previa del gerente del área involucrada. El registro también debe conservarse con fecha, lugar, fotógrafo, grado de secreto y finalidad. En caso de permiso, se pondrá a disposición una cámara de la empresa. Se prohíben las cámaras privadas y los teléfonos inteligentes.

En estos casos, se sugiere utilizar una brida para demostrar el permiso para realizar la actividad.

Está prohibido fotografiar y grabar con cámaras personales, teléfonos inteligentes o teléfonos celulares. Solo se pueden utilizar dispositivos de la empresa Sumidenso para este propósito.

4.1.6-2. Trámites y Gestión a la hora de la Fotografía y Grabación

Es necesario conservar el historial de grabaciones aprobadas durante un período mínimo de 3 meses, idealmente 1 año, para que, en caso de necesidad, sea posible analizar el contenido grabado/fotografiado. El historial debe contener: fecha, hora, fotógrafo, ubicación de la foto, motivo de la foto y autorización del responsable del área. Las fotos deben eliminarse de la cámara después de su uso.

Cuando la fotografía o grabación se realice fuera del propio departamento, también se requerirá la aprobación del jefe (jefe del grupo o persona de mayor rango) en el departamento de gestión aplicable a los objetivos/localizaciones de tiro y grabación. El libro de registro debe conservarse durante al menos 1 año.

Cuando la fotografía o grabación se realice fuera de la empresa, como en viajes de negocios, en la oficina del cliente, en almacenes externos, etc., se requerirá la aprobación de la persona responsable del control de los objetivos fotográficos. Deben observarse las normas de fotografía y grabación, estipuladas por el responsable antes mencionado.

Al salir de la empresa con cámaras, grabadoras, etc. y realizar la fotografía o grabación, el historial de mudanzas debe registrarse utilizando libros de contabilidad.

Está prohibido fotografiar y grabar información y fotografías "estrictamente confidenciales" y grabar en el área de seguridad del "Área de nivel A" por parte de visitantes ajenos a la empresa.

Cuando los visitantes de fuera de la empresa fotografían artículos, los datos guardados en sus dispositivos de información, como cámaras, deben verificarse antes de que se vayan para evitar que se eliminen sin autorización o permiso.
Es deseable que los fotógrafos usen una brida para cables mientras toman fotografías.

Al grabar reuniones, se debe obtener el acuerdo de los participantes por adelantado.
Al grabar audio y video de la reunión, consulte "4.1.19 Protección de la información compartida en la herramienta de conferencia/chat web".

4.1.6-3. Gestión después de la fotografía y la grabación

Los materiales fotografiados o grabados deben manejarse de acuerdo con la Tabla 2-2 <Manejo de activos de información por nivel de confidencialidad>, dependiendo de los respectivos niveles de confidencialidad.

Excluyendo los fines de relaciones públicas y contratación, estará prohibido publicar las fotos, películas, datos de audio, etc. fotografiados y grabados en sitios web externos (redes sociales, etc.).

Se debe prestar toda la atención a la pérdida o robo de dispositivos de fotografía y grabación.

Los datos de los dispositivos de fotografía y grabación deben eliminarse después de su uso.
Es deseable comprobar el estado de control de los dispositivos de fotografía y grabación con regularidad (una vez al año o más).

Para el área de seguridad, véase "4.1.8. Implementación de Seguridad Física".

4.1.7- Normas de cumplimiento para la entrada y la salida

El acceso físico a las instalaciones de la empresa se controla a través de directrices de acuerdo con el Control de Acceso de la Empresa.

El Oficial de Seguridad de la Información implementará medidas de seguridad física de acuerdo con la tabla descrita en el punto 4.1.8-1.

Todos deben respetar las áreas de acceso restringido, siguiendo las reglas de seguridad física adoptadas para cada área de seguridad. Estos estándares se definen en el punto 4.1.8-2 <Implementación de la seguridad física> para proteger los activos de información contra entradas ilegales o fugas.

Las normas aplicadas deben estar debidamente controladas mediante el nombramiento de un administrador para garantizar su buen funcionamiento.

4.1.8- Implementación de seguridad física

Cada departamento clasificará las áreas de supervisión del departamento de acuerdo con las definiciones indicadas en la Tabla 4.1.8-1 <Área de Seguridad> para aclarar las áreas de seguridad. La zona de seguridad de las zonas compartidas por otros departamentos se definirá tras las deliberaciones entre los departamentos.

Cada departamento debe crear un libro de áreas de seguridad para las áreas de seguridad del departamento. En el libro mayor del área de seguridad, se deben incluir los siguientes elementos (nombre del sitio, edificio, área y nivel).

Las áreas de seguridad deben revisarse regularmente (una vez al año o más) o según sea necesario.

4.1.8-1. Clasificación del área de seguridad

Área de seguridad	Definición	Ejemplos
Nivel A	Área donde la información estrictamente confidencial se trata regularmente como negocio.	- Salas de servidores; - Salas/áreas donde se procesan los dibujos 3D de los tipos de proyectos; - Ubicaciones con instrumentos de precisión; - Laboratorios, etc.
Nivel B	Área donde los activos de información confidencial de las personas autorizadas se tratan regularmente como negocios.	- Oficinas, etc. (incluyendo las oficinas en fábricas y centros logísticos) etc.
Nivel C	Área en la que los activos de información confidencial de la empresa se tratan regularmente como negocios.	-Plantas; - Centros logísticos, etc.
Nivel D	Área donde no existen límites de seguridad (refiriéndose a fuera de las áreas de Nivel A, B y C) y no hay activos de información controlados por la empresa.	- Entradas/salidas de cada área; - Salas de reuniones/áreas de reuniones compartidas fuera de las oficinas; - Aparcamiento, etc.

4.1.8-2. Implementación de Seguridad Física

○: Esencial, △: Implementar cuando se considere necesario, -: No aplicable

Área de seguridad / Elementos para implementar Requisitos de seguridad		Nivel A	Nivel B	Nivel C	Nivel D
E l	Cerraduras en áreas de seguridad	○	○	○	–
B	Control de entrada y salida				
	- Registrar y mantener el historial de check-in y check-out (personas ajenas a la Empresa)	○	○	○	○
	- Registrar y mantener el historial de check-in y check-out (empleados y contratistas - subcontratados)	○	○	△	△
	- Acompañamiento de guardias de seguridad	△	△	△	△
	- Monitoreo con cámaras	△	△	△	△
C	Contramedidas para fugas electromagnéticas				
	- No se permite la instalación de teléfonos inalámbricos analógicos/micrófonos inalámbricos	○	○	△	△
	- Verificación de escuchas telefónicas (verificación de la existencia del dispositivo, etc.)	○	○	△	△
D	Gabinetes de gabinetes, etc.				
	- Taquillas con cerradura	○	△	△	△
	- Cerraduras de rack (servidores y red)	○	○	○	△
Y	Identificación de UPS para dispositivos de información	○ (*)	△	△	–
F	Instalación de Aire Acondicionado	○	△	△	–
G	Medidas anti-terremoto				
	- Racks (servidores y comunicación, etc.)	△	△	△	–
	- PCs cliente, impresoras, switches, etc.	△	△	△	–
H	Cableado				
	- Medidas de protección de cables (cables bajo el suelo, cubiertas protectoras)	○	○	○	○
	- Implementar etiquetas de identificación	○	○	○	○
	- Separe los cables de alimentación de los cables de comunicación	○	△	△	△
Y o	Medidas contra incendios				
	- Instalación de extintores	○	△	△	△
	- Instalación de detectores de humo y alarma	○	△	△	△
J	Equipos de suministro de energía				
	- Medidas de cortocircuito	○	○	○	△
	- Inspección del cuadro eléctrico y de distribución	○	○	○	△
	- Instalación de sistema de protección contra el rayo	○	○	○	○

4.1.8-3. Control de entrada y salida

Se debe registrar toda entrada de visitantes (personas ajenas a la empresa) a la oficina. Es necesario llevar un libro con la información de entrada con el nombre de la empresa, nombre del visitante, fecha y hora, tema, industria y tiempo de estadía en la empresa. El empleado responsable debe participar en toda la visita.

4.1.8-3.1. Área Nivel A

- Las áreas de nivel A deben permanecer bloqueadas. Se debe realizar un control de entrada/salida.
- Los responsables de los departamentos deben seguir los procedimientos específicos y permitir el ingreso de personas que necesiten ingresar a las áreas con esta clasificación de manera regular.
- El historial de entrada/salida (fecha y hora, nombre, motivo, etc.) debe mantenerse en un libro mayor, y el libro mayor debe conservarse durante 1 año.
- Cuando se produzca el ingreso de un empleado o prestador de servicios no autorizado, se deberán realizar previamente los trámites de registro y autorización.
- La entrada de personas ajenas a la empresa está, en principio, prohibida. Cuando la entrada de personas ajenas a la empresa sea inevitable por motivos comerciales o de soporte, el historial de entrada/salida (fecha y hora, nombre, motivo, etc.) y los permisos de entrada deben ser visibles y se deben mantener registros.
- Se prohíben las discusiones o reuniones con personas ajenas a la empresa.
- Las cámaras de vigilancia deben instalarse según sea necesario. Los registros de imágenes deben guardarse y administrarse durante 3 meses.

4.1.8-3.2. Área Nivel B

- Cuando sea posible, estas áreas deben permanecer cerradas para restringir la entrada de personas no autorizadas.
- Los responsables de los departamentos deben seguir procedimientos específicos para controlar el acceso de las personas que necesitan entrar regularmente en zonas con esta clasificación.
- El historial de entrada/salida (fecha y hora, nombre, motivo, etc.) debe mantenerse en un libro mayor, y el libro mayor debe conservarse durante 1 año.
- Cuando haya un empleado o proveedor de servicios no autorizado, debe estar acompañado por una persona autorizada durante toda la visita.

- En principio, está prohibida la entrada de personas ajenas a la empresa. Cuando la entrada de personas ajenas a la empresa sea inevitable por razones comerciales o técnicas, se deberá conservar el historial de entrada/salida (fecha y hora, nombre, motivo, etc.). El visitante debe llevar una credencial en un lugar fácilmente visible.

- Las discusiones o reuniones con personas ajenas a la empresa deben tener lugar en una sala de reuniones compartida o en un lugar de reunión fuera de las oficinas (Área de Nivel D) en principio.

4.1.8-3.3. Área Nivel C

- Cuando el área no se está utilizando, debe estar bloqueada.

- Cuando personas ajenas a la empresa ingresan a las áreas de clasificación C, se debe mantener el historial de entrada/salida (fecha y hora, nombre, motivo, etc.). El visitante debe llevar una credencial en un lugar fácilmente visible.
- Las discusiones o reuniones con personas ajenas a la empresa deben llevarse a cabo en una sala de reuniones compartida o en un rincón de reuniones fuera de las oficinas (Área Nivel D) en principio.

4.1.8-4. Requisitos de seguridad del centro de datos/sala de servidores

Los equipos (servidores) que almacenan los sistemas ERP de Sumidenso se encuentran en un área protegida – Datacenter ubicada en Santana do Parnaíba/SP. Los demás servidores corporativos (IHS/HBS, firewall, RMX y Mail Server) se encuentran en el centro de datos ubicado en la unidad Mateus Leme/MG. Los servidores de archivos y los servidores que sirven a los sistemas de producción se almacenan en el centro de datos local de cada unidad.
La ubicación donde se encuentran los servidores tiene acceso restringido. El departamento de TI debe designar un propietario principal y secundario para controlar este entorno. En caso de que personas no autorizadas o externas (visitantes, prestadores de servicios, terceros e incluso empleados, sin libre acceso), necesiten tener acceso físico al lugar, siempre deberán ir acompañadas de personas autorizadas. La entrada debe ser previamente aprobada y el historial de entrada y salida debe conservarse durante un período de 1 año.

Las condiciones de la sala de servidores (temperatura/humedad, estado del dispositivo/equipo, etc.) deben comprobarse periódicamente (aproximadamente una vez al día). También se debe verificar el estado de funcionamiento de los dispositivos y equipos.

Todos los equipos instalados en este lugar deben registrarse mediante un libro de control.

En principio, está prohibido transportar dispositivos de información (PC, memoria USB, disco duro externo, teléfono móvil/smartphone, cámara, router móvil, etc.) a la sala de servidores, a excepción de los dispositivos que se vayan a instalar. En el caso de que el dispositivo de información se transporte en circunstancias inevitables para la empresa, el historial de transporte debe registrarse con la aprobación de la persona encargada.

En principio, la fotografía está prohibida. En caso de que se requiera fotografía en circunstancias inevitables en los negocios, el historial de la fotografía debe registrarse con la aprobación de la persona responsable de controlar y almacenar la sala de servidores durante un cierto período (1 año o más).

Las salas de servidores deben contar con un sistema de control de acceso, un sistema de detección de humo y alarma contra incendios, así como medidores de temperatura y humedad.

Las medidas para los cortes de energía deben adoptarse mediante la instalación de UPS, generador de energía y pararrayos.

Se deben instalar luces de emergencia en dicha área para permitir el funcionamiento de los sistemas de información durante el corte de energía.

La aplicación de las medidas de lucha contra incendios debe evaluarse:

- Se deben instalar extintores halógenos o extintores de dióxido de carbono (gas de dióxido de carbono).

Los dispositivos de información instalados en las salas de servidores deben gestionarse mediante la colocación de pegatinas de control, etc. en un libro mayor y en los dispositivos reales.

El tiempo para reemplazar el UPS o las baterías debe registrarse en un libro mayor o adjuntarse a los dispositivos reales.

Cuando los proveedores externos realizan algún trabajo, el informe de trabajo debe recibirse y guardarse durante un cierto período de tiempo (durante más de 1 año).

4.1.9- Compra/Instalación y Control de Servidores

Al comprar/instalar servidores, se deben realizar los procedimientos prescritos.

Se debe instalar un software antivirus, Endpoint Detection and Response (EDR) y un sistema de gestión de activos de TI.

Los medios de instalación deben estar debidamente controlados. Las licencias del software adquirido deben ser gestionadas a través de la creación de un libro de control que debe ser registrado en el Departamento de TI.

Los servidores y el software instalado deben controlarse de la siguiente manera:
Una vez comprado e instalado el servidor (sistema operativo Windows), se debe instalar un sistema de gestión de activos de TI y registrar la información del usuario.

Los servidores (excepto el sistema operativo Windows) en los que no se puede instalar un sistema de gestión de activos de TI (lansweeper), deben controlarse manualmente en un libro mayor, de acuerdo con el modelo definido por el equipo de infraestructura de TI (Server Control Ledger).

La vida útil del Servidor, así como las configuraciones y el control de las licencias deben seguir las reglas descritas en NA-TI-004.

Cuando las licencias de software se transfieran entre empresas debido a la reorganización de la empresa, los procedimientos se basarán en el EULA (End User License Agreement).

El control del número de licencias adquiridas debe realizarse teniendo en cuenta las transferencias. Si hay alguna duda sobre el contenido del acuerdo de licencia, se requiere consultar con el vendedor.

En ausencia de restricciones del sistema, se debe configurar un protector de pantalla protegido por contraseña para que se active cuando el terminal haya estado inactivo durante 15 minutos o menos.

En el momento de la puesta en marcha del servidor, el inicio de sesión debe realizarse con un código de empleado, en principio. Cuando el uso de un ID compartido es inevitable por razones comerciales, es deseable que se registre en un documento con los datos de la persona que inicia sesión y, por razones de seguridad, que la contraseña se cambie cada vez que cambie el administrador del servidor.

4.1.10- Control de entrada y salida de equipos

Está prohibido ingresar a la empresa con equipo personal, excepto teléfonos inteligentes.

Los equipos privados/privados, como computadoras personales, equipos de otras empresas o cualquier dispositivo portátil que pueda almacenar y/o procesar datos, no deben utilizarse para almacenar o procesar información de Sumidenso, relacionada con el negocio, ni deben estar conectados a la red interna de la Organización.

Solo los equipos y software puestos a disposición y/o aprobados por Sumidenso pueden instalarse y conectarse a la red interna. Está prohibido conectarse a la red de Sumidenso, equipos que no sean un activo de la empresa.

Si existe la necesidad de que los proveedores de servicios o los clientes conecten equipos a la red interna, por razones comerciales, es necesario obtener la aprobación del gerente de área responsable de la información y también la aprobación de la gerencia de TI, quien evaluará la necesidad y los riesgos, definiendo la mejor forma de servicio. En caso de que se cumpla con la solicitud, es obligatorio verificar el antivirus antes de liberarlo. Al final del trabajo, el dispositivo debe revisarse nuevamente para asegurarse de que no se registre información confidencial en el equipo.
En caso de que sea necesario conectarse en circunstancias inevitables en el negocio, el historial de conexiones debe registrarse con la aprobación del administrador de la red y almacenarse durante un cierto período de tiempo (1 año o más).

En los casos de ingreso de personas que porten teléfonos celulares o teléfonos inteligentes, se debe informar sobre la política de la empresa que prohíbe fotografías y grabaciones.

Para eliminar los dispositivos de información (PC, Notebooks, etc.) de la empresa, es necesario obtener la aprobación de la Dirección abriendo tickets en el Helpdesk. La llamada debe contener la fecha de salida y también la fecha de devolución del equipo.

4.1.11- Uso de teléfonos celulares y teléfonos inteligentes en el lugar de trabajo

- Está prohibido utilizar la función de anclaje a red (Wi-Fi Router/Docking), ya que la señal inalámbrica puede interferir con el sistema o equipo interno y afectar la producción de la fábrica o negocio. El uso de esta función, sin ninguna restricción, también puede dar lugar a la fuga de información confidencial.

4.1.12- Reglas para el uso de teléfonos celulares y teléfonos inteligentes corporativos

- **Elegibilidad**:
  Los empleados cuyas actividades impliquen el contacto diario con sus superiores, compañeros y/o clientes son elegibles para recibir una Línea Celular Corporativa.
  Entre estos: Directores, Gerentes, Jefes, Coordinadores y otros roles que requieren una comunicación frecuente con clientes, usuarios y personas en las áreas de back-office de la empresa.

- **Cesión:**
  Los Dispositivos y Líneas Telefónicas descritos en esta Política son propiedad de Sumidenso y han sido dimensionados de acuerdo con las necesidades de los usuarios, de cara a la ejecución de sus actividades y en línea con las premisas de la empresa.
  Al recibir la Línea Telefónica + Celular, o Módem del Plan Corporativo Sumidenso, el Usuario firmará un "Término de Responsabilidad", por tiempo indefinido, bajo las condiciones especificadas en el documento.

- **Instalación de la aplicación:**
  La instalación de aplicaciones en Teléfonos Celulares solo se puede realizar con autorización del Departamento de Tecnologías de la Información (TI), o cuando sea el propio que proporcione el software para su instalación/actualización.
  Los procedimientos para la configuración del equipo deben llevarse a cabo de acuerdo con las instrucciones dadas por el Departamento de TI, no permitiéndose al Usuario realizar ningún otro tipo de configuración, que no sea la indicada.

4.1.13- Dispositivos Analógicos

Con el fin de evitar la fuga de información, está prohibido, en principio, la instalación de dispositivos analógicos que puedan dar lugar fácilmente a escuchas telefónicas. En el caso de que se utilicen en circunstancias inevitables, solo deben usarse en áreas restringidas donde no se maneje información confidencial y las conversaciones sobre asuntos confidenciales estén completamente prohibidas pegando el sello que dice "Discusión sobre asuntos confidenciales prohibidos".

4.1.14- Instalaciones / Conexiones de red

Se debe adoptar una infraestructura robusta para las comunicaciones externas (WAN), teniendo en cuenta la seguridad, la calidad del circuito y la redundancia. En el caso de los circuitos de internet, se deben aplicar medidas contra amenazas externas mediante la instalación de un firewall e IPS (Sistema de Prevención de Intrusiones). Se deben realizar pruebas de penetración y monitoreo periódicos.

La estructura de la red debe documentarse a través de diagramas y mapas que contengan toda la información relacionada con las conexiones de todas las unidades del grupo. Este documento debe ser revisado periódicamente por la persona responsable y se debe conservar el historial.

En principio, solo los equipos puestos a disposición y/o aprobados por Sumidenso pueden instalarse y conectarse a la red interna.

La distribución de IP está controlada por DHCP, donde solo los usuarios registrados pueden autenticarse y obtener acceso a la red. La dirección IP se asigna a la máquina a través de la dirección MAC. El rango IP utilizado está de acuerdo con el rango proporcionado por la matriz SWS.

Debe prohibirse el uso de la función de traducción de direcciones IP (NAT) en servidores y ordenadores personales (incluidos los entornos virtuales).

4.1.15- Conexiones de red dentro de la empresa

No se deben enviar ni recibir grandes volúmenes de datos que afecten a las operaciones entre empresas.

Los datos de audio y video no deben transferirse entre las unidades. Cuando sea inevitable debido a fines comerciales, se debe realizar una consulta con el departamento de gestión del sistema de información.

En principio, se prohibirá la instalación y reconexión de dispositivos de red. Cuando se requiera una instalación o un cambio de conexión, siga las Medidas de seguridad para crear e implementar redes.

En principio, debe prohibirse la supervisión de paquetes en la red interempresarial. Al realizar el monitoreo de paquetes, se requerirá una aprobación del departamento de administración de red.

En principio, debería prohibirse la comunicación con las instalaciones externas de la empresa mediante el túnel SSL (Secure Sockets Layer) o tecnologías similares (instalación de software que encapsula los datos de comunicación con HTTPS, etc.) (por ejemplo, software como Team Viewer, etc.). Cuando el uso sea inevitable por razones comerciales, se requerirá la aprobación del departamento de gestión del sistema de información.

4.1.16- Uso de LAN inalámbrica

Está prohibida la instalación de dispositivos LAN inalámbricos (puntos de acceso Wi-Fi) distintos de los proporcionados por el departamento de gestión del sistema de información.

Al instalar, transferir o quitar dispositivos LAN inalámbricos (puntos de acceso Wi-Fi), debe solicitarse al departamento de administración del sistema de información.
Cuando se utiliza una LAN inalámbrica, debe solicitarse con los procedimientos prescritos.

Se deben llevar a cabo los ajustes especificados por el departamento de gestión del sistema de información. Se debe implementar el control por dirección MAC.

- **Acceso a Internet**

  Está prohibido utilizar Internet para cualquier otro propósito que no sea para actividades en interés de la empresa.

  Se debe implementar un control de filtros, con reglas que restrinjan el acceso a sitios dañinos y sitios que no estén relacionados con el trabajo. Se debe implementar la autenticación individual. Las redes sociales deben ser bloqueadas.

  El historial de navegación de acceso web para sitios web externos se guarda durante un cierto período de tiempo y se monitorea. Está prohibida la conexión a Internet mediante el enrutamiento del teléfono móvil o el anclaje a mar.

  Está prohibido, en principio, ver datos de voz o vídeo debido a la sobrecarga del enlace.

  Está prohibido descargar archivos de cualquier tipo (descargar) a través de Internet. Cuando sea necesario, deberá solicitarse al Departamento de Informática, que tras su análisis lo pondrá a disposición del solicitante.

  Se prohibirá el acceso a URLs y banners publicitarios no fiables, etc., que no sean necesarios para el negocio.

  Cuando se utiliza el sistema web en el que el acceso está controlado por una contraseña, la contraseña no debe guardarse en el navegador web. Sin embargo, esto se puede hacer en un PC conectado con AD utilizando el ID personal (conectado con el ID / contraseña del portal SWS).

  Al utilizar sitios web, como sitios de registro de miembros externos, nunca se deben usar contraseñas utilizadas para iniciar sesión en las PC y sistemas internos de Sumidenso.

  Está prohibido publicar cualquier información estrictamente confidencial (documentos, fotos y vídeos) en sitios web externos como Blog, Facebook, Twitter, etc.

  El servidor de correo es el único servidor conectado directamente a Internet y, por esta razón, debe protegerse mediante la implementación de una DMZ.

- **Redes inalámbricas**

Está prohibida la instalación de dispositivos de red inalámbrica que no sean los puntos proporcionados por el Departamento de Informática. Los dispositivos WIFI deben ser seguros y deben garantizar que solo los equipos registrados previamente tengan acceso a la red, a través de la autenticación con Active Directory. El equipo debe estar configurado con cifrado (WPA2, AES) o superior.

- **Uso de Modems**

  En principio, está prohibido el uso de módems 3G/4G en equipos propiedad de Sumidenso, para evitar la invasión/evasión de información, programas y virus. En algunos casos especiales, de acuerdo con una norma específica, se considerará la posibilidad de uso para planes de contingencia previa autorización de los gerentes de las áreas y del área de TI.

  Si existe alguna otra necesidad que no sea una contingencia, es necesario obtener la aprobación del gerente del área de TI, quien evaluará la necesidad y los riesgos, definiendo la mejor forma de servicio.

  Si se autoriza, el historial de autorizaciones debe registrarse con la aprobación de la persona responsable del control y almacenarse durante un período de 1 año.

- **Mantenimiento remoto de proveedores externos**

  Está prohibido el mantenimiento remoto de un proveedor externo.

  En el caso de que se tenga que liberar el mantenimiento remoto, en circunstancias inevitables que afecten al negocio de la empresa, se deben tomar las siguientes medidas contra los riesgos.

  La conexión solo se permite durante el mantenimiento remoto y se prohíbe la conexión constante.

  La operación relacionada con el permiso de conexión (configuración, encendido/apagado, etc.) debe implementarse en el propio lateral cada vez.

  El acceso debe restringirse solo a la información necesaria. El registro de acceso mediante el cual se puede identificar a la persona debe recopilarse y almacenarse durante un cierto período de tiempo (1 año o más).

  Se debe hacer un acuerdo de confidencialidad.

- **Control de fallas de infraestructura de red**

  En caso de un fallo de red a gran escala, es necesario ponerse en contacto con el departamento de administración de redes de Sumidenso. El incidente debe registrarse y el historial debe conservarse durante un período de 1 año o más. Se debe investigar la causa y se deben implementar de inmediato medidas preventivas contra la recurrencia.

- **Monitoreo de seguridad**

  Los cortafuegos siempre deben actualizarse y escanearse constantemente. Se deben registrar los informes con registros.

4.1.17- Reglas para la conexión remota

En principio, la conexión remota dentro de la red Sumidenso está prohibida. Si existe la necesidad de acceso remoto a un equipo dentro de la red Sumidenso, la conexión debe ser monitoreada por el usuario Administrador del Sistema, abriendo un ticket en el Helpdesk, con la aprobación del Administrador de TI.

Al final de la conexión, debe asegurarse de que la sesión haya finalizado o que el dispositivo al que se accede haya sido bloqueado con contraseña.

Si es necesario crear una cuenta específica para el acceso, cuando el acceso remoto ya no sea necesario, los procedimientos especificados para la eliminación deben realizarse inmediatamente.

4.1.18- Medidas de seguridad para dispositivos de información y dispositivos de información portátiles

4.1.18-1. Objetivo

El propósito es estipular reglas de cumplimiento para la instalación y el control de dispositivos de información (PC, medios de almacenamiento externos, cámaras, etc.), dispositivos de información portátiles (teléfonos inteligentes, tabletas, teléfonos móviles, etc.) y software que se utilizan con fines comerciales para que los activos de información de la empresa se puedan utilizar de forma segura.

Es necesario controlar adecuadamente todos los dispositivos de información de la empresa, ya sea hardware o software.

Es necesario mantener un libro de registro de control de Hardware y Software. Este libro debe actualizarse al menos una vez al año o más.

4.1.18-2. Personas afectadas

Todas las personas que utilizan los dispositivos de información, los dispositivos de información portátiles y el software de la empresa.

4.1.18-3. Alcance

Dispositivos de información (PC, medios de almacenamiento externos, dispositivos de fotografía/grabación como cámaras, etc.), dispositivos de información portátiles y software proporcionado por la empresa.

Nota: Los equipos, servidores y medios de almacenamiento externo alquilados también están dentro del alcance.

No se permite el uso de dispositivos privados que no sean proporcionados por la empresa. Cualquier dispositivo en uso, sin autorización, que se encuentre dentro de las instalaciones de Sumidenso, será recogido y devuelto después del análisis del contenido, Sumidenso se reserva el derecho de eliminar archivos, cuando exista sospecha de virus o sospecha de fuga de archivos que contengan información restringida o confidencial.

4.1.18-4. Regla de cumplimiento

- **Compra de Dispositivos de Información**
  Los dispositivos de información estándar de la compañía deben comprarse de acuerdo con las reglas descritas en NA-TI-004.

  En principio, los PC estándar no deben tener medios de almacenamiento externos. Si existe, la unidad de CD/DVD debe tener protección contra escritura. Los puertos USB estándar de PC deben estar bloqueados.

  Con respecto a las unidades USB y los discos duros externos, los dispositivos estándar de la compañía con función de cifrado (128 o más bits AES) deben comprarse con los procedimientos prescritos.
  Al comprar PC no estándar, como PC para CAD o equipos de producción, se debe obtener una aprobación del departamento que decide los dispositivos estándar de la empresa de acuerdo con los procedimientos prescritos.

  Además, los equipos no estándar deben comprarse con las mismas medidas de seguridad (Windows Update, instalación de software antivirus e instalación de software de administración de activos de TI) que los equipos estándar.

  En principio, debería prohibirse la compra de unidades USB y discos duros externos no estándar. Cuando sea inevitable por razones comerciales, se debe obtener la aprobación del departamento que decide los dispositivos estándar de la empresa a través de los procedimientos prescritos.

- **Compra e instalación de software**
  El software estándar debe comprarse e instalarse de acuerdo con los procedimientos prescritos.

  La configuración predeterminada de la empresa debe implementarse de acuerdo con los procedimientos.

El software antivirus y el sistema de gestión de activos de TI deben instalarse en todos los PC conectados a LAN dentro de la empresa. Para conectarse a la 2ª LAN, deben instalarse en principio. (Ver Tabla 4-1).

En el caso de los PC conectados a la 1ª LAN, se debe instalar el software Endpoint Detection and Response (EDR).

Tabla 4-1: Sistemas, etc. que deben instalarse o configurarse en función del destino de la conexión de red:

Sistemas obligatorios	Destino de la conexión de red		
	1ª LAN	2ª LAN (Nota)	Ninguno
Sistema de gestión de activos de TI (Lansweeper)	La instalación es obligatoria.	En principio, debe instalarse. Si no está instalado, es obligatorio el control manual de la gestión de activos de TI.	Es obligatorio el registro manual en el sistema de gestión de activos de TI o la gestión con un libro mayor.
Software antivirus	La instalación es obligatoria.	En principio, debe instalarse. Si una instalación es difícil debido a equipos, etc., ejecute un escaneo periódico (al menos dos veces al año) con una herramienta de búsqueda tipo USB, etc.	La instalación no es necesaria cuando no hay conexiones externas, como USB. Por si acaso, es deseable realizar un escaneo periódico (al menos dos veces al año) con la herramienta de búsqueda tipo USB, etc.
EDR (Software de Detección y Tratamiento de Ataques Cibernéticos)	La instalación es obligatoria.	No es necesario.	No es necesario.
Windows Actualizar	Se requiere la configuración de WSUS.	La configuración de WSUS es imposible.	La configuración de WSUS es imposible.

Nota: En el momento de restablecer la segunda LAN, se requiere una aplicación para SWS.

Implemente medidas de encriptación para PC que se puedan llevar fuera de la empresa, incluidas computadoras portátiles y PC móviles.

No se debe instalar ni utilizar software prohibido por el departamento de gestión del sistema de información. Además, no se debe instalar ni utilizar software que no tenga relación con la implementación del negocio.

El software que se va a comprar siempre debe ser el producto original.

Cuando se compra e instala un software que no está en la lista de software estándar y causa problemas de seguridad y otros problemas en los sistemas de información existentes, el departamento de gestión de sistemas de información puede solicitar que se cambie la configuración de dicho software, se elimine el software y se desconecten los PC de la red dentro de la empresa.

- **Software Aprobado / Gestión de Licencias**

  Todos los usuarios deben utilizar únicamente software licenciado y aprobado por el área de Seguridad de la Información.
  El área de Infraestructura de TI debe establecer los aspectos de control, distribución e instalación del software utilizado.
  Todos los usuarios deben ser informados de la prohibición de instalación de software no aprobado y/o sin licencia.

  Solo se debe instalar software aprobado en las estaciones de trabajo de la empresa.

  El departamento de TI es el sector encargado de aprobar nuevo software o nuevas versiones de software y, posteriormente, permitir su instalación La instalación de cualquier otra aplicación debe solicitarse al Departamento de TI, a través de la apertura de un ticket en el sistema de Helpdesk, que analizará la necesidad.
  Está prohibida la instalación de software sin licencia o software de terceros.

  Con respecto al uso del software, se debe observar estrictamente el contenido de los Acuerdos de licencia de usuario final (EULA) adjuntos o la licencia de software. Deben respetarse especialmente los siguientes puntos;

  a) El software que es gratuito durante un período de prueba no debe usarse después de que finalice el período
  b) El software no debe copiarse fuera del rango permitido en el EULA.

  El EULA del software facturado y los códigos clave (también conocidos como números de serie o números de licencia) para identificar la licencia de software deben gestionarse estrictamente para que puedan verificarse en cualquier momento.

  Al comprar software, verifique la cantidad de licencias requeridas. Si hay alguna deficiencia, es necesario comprar.

  Al actualizar una versión de software, compre los números necesarios por adelantado. Sin embargo, esto no se aplica a un caso en el que el costo de actualización de la versión está incluido en el costo de mantenimiento, etc.

- **Control de acceso a PC**

  Se debe utilizar un único inicio de sesión de usuario para iniciar sesión.

Cuando se utiliza un ID común por razones comerciales inevitables debido a restricciones del sistema, los usuarios deben ser controlados por libros de contabilidad y las comprobaciones de inventario deben implementarse de forma regular.

Cuando se usa un identificador común en un equipo invitado o en un equipo normal por razones comerciales inevitables, los usuarios y el tiempo de uso deben mantenerse y controlarse mediante libros de contabilidad.

Es deseable que no se utilicen identificadores comunes en el mismo turno de trabajo para que los usuarios puedan ser identificados.
Los equipos en los que se pueden usar identificadores comunes deben limitarse al mínimo.

Excepto en los casos en que los datos se guardan temporalmente para viajes de negocios, etc., no se deben guardar datos confidenciales en PC normales.

- **Contramedidas contra virus**

El software antivirus predeterminado de Sumidenso es "F-Secure". Los servidores, computadoras de escritorio, portátiles y teléfonos inteligentes de la empresa deben tener este software antivirus instalado, activado y actualizado permanentemente.

- Se deben observar las siguientes reglas para evitar daños por un bloqueo del sistema o fuga de información causada por virus o gusanos;
- El software antivirus y el sistema de detección y respuesta de endpoints (EDR) especificados por el Departamento de Sistemas de Información deben instalarse en las computadoras;
- El software antivirus debe configurarse de manera que siempre se pueda verificar el acceso a los archivos (escaneo en tiempo real);
- El software antivirus debe configurarse para que el archivo de definición se pueda actualizar automáticamente;
- La versión, el escáner y el archivo de definición del software antivirus deben confirmarse y actualizarse regularmente (1 vez o más en 3 meses);
- El escaneo de todo el disco duro, además del escaneo en tiempo real, debe implementarse al menos 2 veces al año;
- El análisis de virus mediante el software antivirus más reciente debería, en principio, implementarse para los datos o el software traídos del exterior antes de guardarlos en los dispositivos de información de la empresa;
- Al conectar PC que estaban conectados a una red fuera de la empresa (su hogar, otras empresas, etc.) a la red dentro de la empresa, es deseable implementar el escaneo de virus con el software antivirus más reciente antes de la conexión;
- Cuando el departamento de administración del sistema de información o el propio gerente/personal de seguridad de la información del departamento solicita un análisis de virus, el análisis de virus debe implementarse en todos los discos duros;

- Al enviar archivos o aplicaciones a servidores o fuera de la empresa, es deseable enviarlos después de confirmar que un virus no está presente mediante la implementación de un análisis de virus uno por uno con un software antivirus;
- La configuración del software antivirus no debe ser cambiada por una persona sin autorización;
- No se debe enviar un virus o un archivo infectado por un virus. Un virus no debe mantenerse en una computadora a propósito;
- Los archivos desconocidos o que no son de confianza no deben descargarse ni ejecutarse;
- Salvo en los casos inevitables, como el uso de una impresora de red o las especificaciones del sistema de aplicaciones, los archivos no deben compartirse entre PC (PC a PC). Incluso cuando es inevitable, debe prohibirse compartir una unidad de disco completa (por ejemplo, C:/) o compartir con "todos" (todos los usuarios), ya que no solo evita que se detecte la fuente de infección del virus, sino que también provoca la propagación del virus y fugas de información.

- **Contramedidas cuando se sospecha una infección por virus**

Cuando surjan casos sospechosos de infección por virus, las PC deben desconectarse de la red y los casos deben informarse al departamento de administración de antivirus.
<Ejemplos de infección por virus >

- Cuando se muestra un mensaje que muestra una falla de limpieza de virus por parte del software antivirus;
- Cuando se abre un archivo adjunto de un correo electrónico sospechoso y una PC no funciona correctamente;
- Cuando se muestra continuamente un mensaje de detección de software antivirus;
- Cuando se muestra una ventana emergente de advertencia de macro en todos los archivos, etc.

De acuerdo con las instrucciones dadas por el departamento de administración de antivirus, el virus debe eliminarse.

El departamento de administración de antivirus debe confirmar que el archivo de definición de software antivirus en la PC de destino es la última versión. También debe indicar el escaneo en busca de virus en todos los discos duros (incluidas las unidades USB y los discos duros externos) en la PC para ver si el virus se detecta o no.

Cuando el departamento de gestión de antivirus solicite la presentación de dicho informe de contramedidas, el estado de la infección y las futuras contramedidas se indicarán en una hoja específica y se enviarán al departamento de gestión de antivirus.

El departamento de gestión de antivirus debe informar del caso al contacto de notificación de antivirus de SWS.

- **Aplicación de parches de seguridad**

El departamento de infraestructura de TI debe realizar comprobaciones de parches de seguridad para los sistemas operativos. El estado de la actualización debe supervisarse periódicamente.

El programa de actualización debe aplicarse al sistema operativo y al software utilizado para mantenerlos siempre actualizados con un método especificado por el departamento de gestión del sistema de información. Cuando el departamento de gestión del sistema de información emita instrucciones para aplicar el programa de actualización, el programa de actualización debe aplicarse inmediatamente.

El estado de la solicitud de los programas de actualización debe verificarse regularmente (una o más veces en 3 meses).
Los sistemas operativos Windows en los que Microsoft ha interrumpido el soporte tienen, en principio, prohibido conectarse a la red interna de la empresa (excluida la segunda LAN).

Cuando existan circunstancias especiales inevitables y sea difícil actualizar los sistemas operativos, será necesario consultar con el departamento de Sistemas de Información.
Se debe diseñar un plan para actualizar al sistema operativo Windows a una versión compatible con Microsoft.

Las copias de seguridad deben realizarse antes de cualquier aplicación de parches de seguridad.

- **Uso compartido de archivos**

  En principio, está prohibido compartir archivos o unidades de disco de un ordenador a otro. Cuando no se puede evitar el uso compartido, se debe implementar la restricción de acceso mediante autenticación individual.

- **Redes inalámbricas**

  Está prohibida la instalación de dispositivos de red inalámbrica que no sean los puntos proporcionados por el Departamento de Informática. Los dispositivos WIFI deben ser seguros y deben garantizar que solo los equipos registrados previamente tengan acceso a la red, a través de la autenticación con Active Directory. El equipo debe estar configurado con cifrado (WPA2, AES) o superior.

4.1.19- Sistema de comunicación

Es necesario garantizar la seguridad de la información intercambiada en los sistemas de comunicación, como el correo electrónico, y evitar que se produzcan problemas. De esta manera, la empresa ha creado algunas medidas de seguridad destinadas a proteger la información intercambiada a través de los medios de comunicación utilizados.

- **Correo electrónico**

Los sistemas antivirus y antispam deben estar instalados en el servidor de correo. En principio, debería prohibirse la recepción y el envío de archivos adjuntos con extensión .exe, .bat, .com y macros.

Está prohibido el uso del correo electrónico para cualquier propósito que no sea para actividades en interés de la empresa. La dirección de correo electrónico proporcionada por la empresa es un activo de la empresa. La información contenida en las cuentas de correo electrónico del Usuario es responsabilidad del empleado, y le corresponde a él mantener y, si es necesario, crear protecciones para la no violación de estas.

En los correos electrónicos comerciales entrantes, hay muchos casos en los que se incluye información confidencial, información personal de los clientes, etc. que no debe filtrarse al extranjero. Al reenviar correos electrónicos entrantes, se debe prestar toda la atención al contenido y las direcciones de reenvío.

Está permitido unirse a una lista de correo externa utilizando la dirección de correo electrónico de la empresa con fines comerciales. Sin embargo, la seguridad de dicha lista de correo debe considerarse con suficiente antelación y ser revisada por el equipo de TI.

Se prohibirá el reenvío automático de correos electrónicos al servidor de correo electrónico de terceros que no sean grupos SEI y SWS.

Está prohibido registrar el correo electrónico corporativo en sitios de redes sociales, tiendas web o cualquier sitio web que no esté relacionado con el negocio de la empresa.

Reglas para el envío de correos electrónicos internos:

Estrictamente confidencial	Confidencialidad de la persona autorizada	Confidencial de la empresa
Los comentarios a los que hay que prestar atención deben indicarse en el título o en el texto principal. - Los destinos de las direcciones de correo electrónico deben confirmarse para verificar su exactitud. - Los archivos adjuntos deben estar protegidos por contraseñas o encriptación. - La contraseña debe ser notificada por otro método o en un correo electrónico separado.	Es deseable indicar comentarios para prestar atención al manejo en el título o texto principal. - Los destinos de las direcciones de correo electrónico deben confirmarse para verificar su exactitud. - Los archivos adjuntos deben estar protegidos por contraseñas o encriptación. - La contraseña debe ser notificada por otro método o en un correo electrónico separado.	Los destinos de las direcciones de correo electrónico deben confirmarse para verificar su exactitud.

En principio, está prohibido enviar información confidencial fuera de la empresa.

Si el envío es necesario por razones comerciales, se observan las siguientes reglas.

Reglas para el envío de correos electrónicos externos:

Estrictamente confidencial	Confidencialidad de la persona autorizada	Confidencial de la empresa
Los comentarios a los que hay que prestar atención deben indicarse en el título o en el texto principal. Aprobación obligatoria por parte del oficial de seguridad de la información (jefe de departamento), un aprobador debe incluirse en el CC o CCO como destinatario de correo electrónico. Los archivos adjuntos deben estar protegidos con contraseñas o cifrado. La contraseña debe ser notificada por otro método o en un correo electrónico separado. Los destinos de las direcciones de correo electrónico deben estar completamente confirmados para garantizar su exactitud. El contenido, incluida la información estrictamente confidencial, no debe, en principio, describirse en el texto principal del correo electrónico.	Es deseable indicar comentarios para prestar atención al manejo en el título o texto principal. Aprobación obligatoria por parte del oficial de seguridad de la información (jefe de departamento), un aprobador debe incluirse en el CC o CCO como destinatario de correo electrónico. Los archivos adjuntos deben estar protegidos por contraseñas o cifrado. La contraseña debe ser notificada por otro método o en un correo electrónico separado. Los destinos de las direcciones de correo electrónico deben confirmarse para verificar su exactitud.	Los destinos de las direcciones de correo electrónico deben confirmarse para verificar su exactitud. El administrador de dicha información, o el gerente de seguridad de la información, o el oficial de seguridad de la información (jefe de departamento), según sea necesario, deben incluirse en el CC o CCO como destinatario de correo electrónico. Es deseable que los archivos adjuntos que contienen información de la Compañía estén protegidos por encriptación.

El tratamiento de la información en el envío y recepción de correos electrónicos debe ser conforme a las demás normas de tratamiento de la información interna.

Cuando se reciben correos electrónicos sospechosos, como los de remitentes desconocidos, deben informarse (reenviarse) a spam-report@sumidenso.com.br. Después de hacer la denuncia, los correos electrónicos sospechosos deben eliminarse para evitar riesgos. Nunca abra el archivo adjunto ni haga clic en la URL contenida en el texto del correo electrónico sospechoso. La información del "nombre del remitente" se puede modificar fácilmente. De hecho, es posible que el remitente no sea la persona que conoces, por lo que se requiere mucho cuidado.
Está prohibida l distribución voluntaria o involuntaria de mensajes no deseados, como cartas en cadena, material pornográfico u otros que puedan perjudicar el trabajo y causar un tráfico excesivo en la red o sobrecargar los sistemas informáticos.

En los casos de mal uso del recurso, el empleado recibirá una notificación por correo electrónico del administrador de la red, informando sobre el mal uso del recurso. En caso de reincidencia, el empleado puede tener su cuenta bloqueada.

Los correos electrónicos deben respetar el límite de tamaño de 20 Mb. Se bloquearán los mensajes con archivos adjuntos mayores que el tamaño proporcionado. Si el envío es absolutamente necesario, se debe activar el soporte informático local.
Antes de enviar un correo electrónico, debe verificar que la dirección del destinatario sea correcta.

Para enviar archivos grandes (más de 20 MB), debe consultar con el Departamento de Sistemas cuál es el método más adecuado.

Todos los empleados de la empresa deben recibir instrucciones de no abrir archivos sospechosos adjuntos a correos electrónicos recibidos de remitentes, conocidos o desconocidos.

Está prohibido configurar el reenvío de correo electrónico al sistema de correo externo que no pertenezca al grupo Sumidenso.

Está prohibido el correo web externo proporcionado por Yahoo!, Google y MSN, etc.

- **Uso compartido de archivos con clientes**

Se debe utilizar el servicio de intercambio de archivos especificado por el Departamento de Sistemas de Información. Cuando los clientes especifican herramientas de uso compartido, esto no debe aplicarse.

- **Uso compartido de archivos con socios comerciales**

Al utilizar el servicio de intercambio de archivos, en principio, se debe obtener un permiso del Departamento de Sistemas de Información.

- **Envío de documentos por correo o valija diplomática (correo dentro de la empresa)**

Al enviar información clasificada como estrictamente confidencial o confidencial, utilice un sobre no transparente. Utilice la opción de envío: CORREO CERTIFICADO C/AR: correspondencia con acuse de recibo y acuse de recibo.

- **Buenas prácticas de comunicación verbal dentro y fuera de la empresa**

Tenga cuidado al tratar asuntos de la empresa dentro y fuera del entorno laboral, en lugares públicos o alrededor de visitantes, ya sea por teléfono o con un colega, o incluso con proveedores.

Evite nombres y asuntos confidenciales, en estas situaciones, fuera de la empresa o cerca de personas desconocidas.

Si es extremadamente necesario comunicar asuntos confidenciales en lugares públicos, esté atento a las personas que lo rodean que pueden usar la información para dañar la imagen de la empresa.

- **Acceso remoto para empleados (VPN)**

El uso del acceso VPN debe estar restringido y solo para fines relacionados con el negocio de la empresa, y su uso para cualquier otra actividad está prohibido.

Se debe implementar la función de autenticación individual.

Está prohibido compartir las credenciales de acceso a la VPN con nadie.

Nunca deje sesiones de VPN abiertas. Cada vez que el usuario deja su dispositivo conectado a la VPN, el dispositivo debe dejarse bloqueado con una contraseña.

Permanezca conectado a la red a través del acceso VPN solo durante el tiempo que sea necesario para realizar la tarea o el servicio.

El acceso remoto a los usuarios de las zonas operativas debe concederse únicamente en casos de riesgo inminente de interrupción de la operación y/o compromiso del servicio al cliente.

La solicitud de acceso remoto deberá ser registrada por el responsable de Área con la debida justificación. La aprobación debe ser realizada por el Área de TI, que debe analizar las justificaciones y riesgos. El historial de aprobación debe mantenerse durante un período de 1 año.

  - **Elegibilidad**:

Los empleados que usan computadoras portátiles corporativas y que ocupan una posición de confianza son elegibles para el acceso VPN. Entre estos se encuentran: directores, Gerentes,

Jefes y Coordinadores. Para los empleados que no cumplan con estas condiciones, se requerirá autorización previa del Departamento de Recursos Humanos.

No se permite el acceso remoto a través de equipos que no sean un activo de la Compañía.

Si es necesario, en circunstancias que son inevitables para el negocio de la empresa, es necesario obtener la aprobación de la Dirección de TI y del Consejo de Administración.

- **Web/Conferencias y Chat**

Queda prohibido el uso que no sea para fines de la empresa.

Queda prohibido el uso de sistemas y herramientas distintos a los aprobados por el departamento de gestión de Sistemas de Información.

La herramienta aprobada para su uso dentro de la Empresa es Teams. Herramientas aprobadas para reuniones con Clientes y Partners: Teams, Zoom, Web-EX, Skype for Business y Google Meeting.

Las reuniones deben realizarse utilizando dispositivos proporcionados por la Compañía. Está prohibido el uso de dispositivos privados.

Cuando se utiliza el sistema fuera de la empresa, está prohibido utilizarlo en lugares donde terceros puedan verlo u oírlo.

Al compartir documentos con personas externas, como clientes, proveedores, etc., solo se permitirá la visualización en la ventana y se prohibirá el envío de archivos.

Al utilizar una cámara web, se debe tener cuidado de no mostrar la información que no tiene relación con la reunión en segundo plano para evitar la fuga de información.

Al grabar una conferencia web, solicite la filmación y la grabación interna. También es una buena idea informar a los asistentes antes de empezar a grabar la reunión.

- **Protección de la información compartida en la herramienta Web/chat**

Cuando se utilice el sistema fuera de la empresa, debe prohibirse su uso en lugares donde terceros puedan ver u oír.

La información que se maneja en una conferencia web debe manejarse siguiendo las reglas descritas en esta Política.

Al compartir documentos con personas externas, como clientes, proveedores, etc., solo se permitirá la visualización en la ventana y se prohibirá el envío de archivos.

Al usar una cámara web, se debe tener cuidado de no mostrar la información que no tiene relación con el encuentro de fondo para evitar la fuga de información.

Al grabar una reunión web organizada por la empresa, la grabación debe realizarse después de que los participantes hayan llegado a un acuerdo.

Al grabar una reunión web organizada por socios comerciales, la grabación por parte de socios comerciales estará prohibida en principio. Cuando los socios comerciales llevan a cabo la grabación, se debe tener cuidado de no incluir la información de nuestra empresa.

Los miembros registrados en grupos de chat (equipos de Teams) deben mantenerse actualizados.

4.1.20- Control de acceso

La concesión de acceso se llevará a cabo sobre la base de la regla de acceso mínimo necesario para el desempeño de la función.

El acceso debe concederse mediante una identificación personal y los derechos de acceso deben definirse adecuadamente. Todos los accesos deben concederse mediante la apertura de un ticket en el sistema de asistencia técnica, con la aprobación del responsable del departamento.

La identificación de cualquier Empleado debe ser única, personal e intransferible, calificándolo como responsable de las acciones realizadas.

Si es necesario utilizar un inicio de sesión común, se debe registrar un documento de control que contenga la firma de la persona responsable del inicio de sesión. La autenticación individual debe implementarse en todos los sistemas, excepto en los sistemas de fábrica. La función de autenticación protegida por seguridad debe implementarse en el sistema interno y en la aplicación.

La concesión de acceso debe cumplir con el criterio de mínimo privilegio, en el que los usuarios tienen acceso únicamente a los recursos de información que son esenciales para el pleno desarrollo de sus actividades. Periódicamente, los accesos otorgados deben ser revisados por el responsable del área.

Es deseable que el equipo de control de cuentas del servidor revise la necesidad de cuentas y derechos de acceso cada trimestre.

Las solicitudes de revocación de acceso deben registrarse en el sistema de soporte técnico. La suspensión o eliminación debe llevarse a cabo inmediatamente después del registro del ticket.

Se requerirá la configuración para evitar que un equipo que haya iniciado sesión con un ID compartido (incluidos los ID compartidos establecidos en AD) acceda a los servidores de archivos.

Los registros de acceso deben obtenerse y guardarse durante un cierto período de tiempo (al menos 1 año o más).

La presencia o ausencia de acceso ilegal debe ser monitoreada según sea necesario.

4.1.21- Gestión de cuentas privilegiadas

Las cuentas que tienen derechos administrativos del sistema, como root o administrador, no deben usarse en las operaciones habituales del sistema y los registros de operaciones deben mantenerse cuando se usan, y es deseable que se realice una auditoría regularmente.

La contraseña de las cuentas del sistema con derechos administrativos del sistema debe estar estrictamente definida y controlada.

La divulgación de dicha contraseña se limitará al número mínimo de personas necesarias.

La contraseña debe seguir las reglas descritas en esta Política.

Es deseable modificar la contraseña cada vez que cambia un administrador del servidor.

Al asignar una cuenta con privilegios, se requiere la aprobación de la administración de TI.

4.1.22- Autenticación y configuración de contraseña

El usuario es el único responsable de la confidencialidad de su contraseña, y de toda la información que proporcione, pudiendo cambiarla en cualquier momento o, en caso de olvido, deberá solicitar el cambio abriendo un ticket con el visto bueno de la Dirección del área.

Para los usuarios que utilicen dispositivos móviles como notebooks, pendrives y/o discos duros externos, la contraseña o clave de cifrado, generada en el momento de su implementación, por parte de TI, deberá ser transmitida a través del correo corporativo, únicamente al usuario, con las instrucciones de uso.

Está prohibido que el usuario revele o comparta su contraseña. La contraseña es personal e intransferible.

Las contraseñas de root y de administrador deben ser restringidas y controladas por el administrador de TI.

Se debe evitar el acceso a los servidores mediante una cuenta de root o de administrador.

El acceso del usuario a los servicios de infraestructura y/o sistemas de información podrá ser bloqueado o cancelado en las siguientes situaciones:

- Rescisión o rescisión del contrato del usuario con la empresa;

- Traslado del lugar de trabajo del usuario;
- El usuario ya no tiene la necesidad de utilizar servicios de infraestructura y/o sistemas de información;
- Después de que se le haya denegado el acceso por intentos consecutivos fallidos;
- En caso de sospecha de violación o amenazas a la seguridad;
- Por decisión del Consejo de Administración de la sociedad.

En caso de bloqueo, el desbloqueo del acceso deberá ser solicitado por el usuario, previa autorización de la Dirección, a través de la apertura de una convocatoria al área de TI, que deliberará la decisión caso por caso.

En principio, el Departamento de Sistemas de Información debe establecer un sistema de autenticación utilizando la infraestructura de autenticación estándar.

Para que el sistema de información esté conectado a la red interna, teniendo en cuenta la importancia y el nivel de dificultad del método para realizar la seguridad, se debe considerar el uso de la autenticación multifactorial.

Se deben usar los siguientes elementos para la autenticación.

a) Contraseña de un solo uso;
b) Certificado electrónico;
c) Autenticación biométrica;
d) Restricción de conexión mediante dirección IP;

El sistema de información que esté abierto fuera de la empresa debe tener implementada la autenticación multifactorial especificada por el Departamento de Sistemas de Información.

- **Reglas para establecer contraseñas**

  La contraseña debe cumplir con las reglas de seguridad específicas establecidas:
  - Longitud mínima de la contraseña: 8 caracteres (la contraseña no debe tener menos de 8 caracteres);
  - La contraseña debe ser compleja, es decir, no debe contener partes significativas del nombre de la cuenta del usuario o el nombre completo;
  - Es recomendable que los usuarios utilicen una contraseña segura, con letras, números y al menos 1 carácter especial. Si no es posible registrarse con este nivel de dificultad, la contraseña debe tener al menos 4 (cuatro) letras y 4 (cuatro) números.
  - La contraseña debe cambiarse cada noventa (90) días y no se puede establecer la misma contraseña de forma continua.
  - Cambie la contraseña siempre que exista alguna sospecha de compromiso;
  - Informe inmediatamente al departamento de TI sobre cualquier sospecha de intento de violación de la seguridad.

4.1.23- Alquiler de equipos

En principio, está prohibido alquilar equipos informáticos, portátiles y servidores. Si es necesario, se debe obtener la autorización del Gerente del Departamento de TI. En este caso, será necesario preparar un Acuerdo de Usuario que contenga temas relacionados con la confidencialidad y el equipo debe estar de acuerdo con las especificaciones (IT-TI-008).

Después de la terminación del uso o la terminación del contrato, el equipo debe ser inspeccionado por el Departamento de TI, y es obligatorio limpiar/eliminar todos los datos/información relacionados con la Compañía.

4.1.24- Gestión de vulnerabilidades

- **Recopilación de información sobre vulnerabilidades**

  El departamento de Sistemas de Información recopilará regularmente información sobre vulnerabilidades del software y hardware utilizados en los "sistemas de información" que se utilizan en nuestra empresa y en el grupo de nuestra empresa según sea necesario.

- **Manejo de información de vulnerabilidad**

  Si los administradores de sistemas identifican información de vulnerabilidades graves, deben implementar inmediatamente medidas de seguridad, como la aplicación de parches.

4.1.25- Medidas de seguridad de la red

El objetivo es mantener y mejorar la seguridad y confiabilidad de la red de la empresa mediante la clarificación de la gestión de la operación al construir y expandir la red de la empresa.

4.1.25-1. Personas afectadas

- Usuarios de la red

4.1.25-2. Alcance

- Dispositivos de red (conmutadores, puntos de acceso, convertidores, etc.)
- Dispositivos que se conectarán a la red interna de la empresa (incluidos los dispositivos inalámbricos)

4.1.25-3. Reglas de cumplimiento para la construcción de redes

La construcción e instalación de la red, así como el cambio en la infraestructura, no deben llevarse a cabo sin la aprobación previa del departamento de gestión de la red. Los siguientes servicios forman parte del ámbito de red:

- Red de acceso remoto (VPN);
- LAN inalámbrica;
- Segunda LAN (VLAN o separación física);
- Mantenimiento remoto;
- Líneas de Internet;
- Línea exclusiva.

La dirección IP que se asignará a cada dispositivo debe fijarse en principio sin utilizar el servidor DHCP. Cuando se utiliza el servidor DHCP por razones comerciales inevitables, se deben identificar los usuarios y conectar los dispositivos y se debe investigar el tiempo.

La dirección IP debe ser proporcionada por el departamento de administración de red. Solo después de la liberación se puede utilizar la IP.
Debe prohibirse la conexión directa a la red interna mediante la función de traducción de direcciones IP (NAT).

Al construir una LAN inalámbrica, para evitar escuchas telefónicas y fugas de información de terceros, se deben tomar medidas como el cifrado.

4.1.25-4. Gestión y operación de redes

La estructura de red debe gestionarse mediante un diagrama de configuración de red o registros de control de dispositivos de red.

Cuando hay un cambio en el diagrama de configuración de red o en los dispositivos de red, el historial de cambios debe registrarse y guardarse.
Además, el diagrama de configuración de la red debe revisarse regularmente (1 vez o más al año).

4.1.25-5. Gestión de fallos de red

Cuando los usuarios detectan un fallo en la red, deben ponerse en contacto con el departamento de gestión de la red.

4.1.25-6. Construcción de redes y uso de dispositivos de comunicación

- **Se requerirá la aprobación previa del departamento de gestión de la red en los siguientes casos:**
- Construcción inicial o modificación de una red dentro de la empresa (incluido el cambio de diseño);
- Construcción de un nuevo edificio y ampliación de un cambio de edificio/distribución;
- Instalación de la segunda LAN (incluidas las LAN inalámbricas);
- Conexión de dispositivos de red de la empresa, etc. a dispositivos de comunicación (enrutador, conmutadores, puntos de acceso, etc.);
- Inclusión o transferencia de dispositivos de comunicación (Switches, APS, routers, etc.) gestionados por su propio departamento según cambio de layout, etc.

- **Al instalar la línea de Internet, se deben tomar medidas contra amenazas externas.**
  - Instalación de dispositivos (firewall, IPS, etc.) para evitar accesos ilegales;
  - Reconocer la configuración del firewall de forma regular (una vez al año o más) y eliminar la configuración de filtrado innecesaria;
  - Aplicación de medidas para impedir el acceso ilegal;
  - Separación de una red que no es conectable desde fuera de la empresa y una red conectable (instalación DMZ);
  - Realización de pruebas de penetración periódicas por parte de instituciones especializadas;
  - Protección contra virus, etc. (Instalación de un sistema antivirus tipo puerta de enlace, etc.);
  - Aclaración de las medidas de emergencia cuando se produce un acceso ilegal;
  - El uso del acceso a la web debe ser restringido, con autenticación personal y reglas de filtro;
  - Gestión del contenido de configuración y del historial de cambios de los dispositivos de comunicación;
  - Obtención y almacenamiento de registros de comunicaciones (aproximadamente un mes).

- **Al contratar líneas de Internet para fines específicos, se deben observar los siguientes ítems.**
  - Se debe obtener una aprobación por parte del administrador de la red SWS;
  - El acceso debe restringirse a ubicaciones (bancos o ubicaciones relacionadas con el gobierno) que no se puedan conectar a través de la red interna;
  - El número de PC que pueden conectarse debe restringirse al mínimo necesario;
  - El ID personal/contraseña se utiliza para iniciar sesión en los equipos conectados para restringir a los usuarios.

- Al colocar la línea WAN en una empresa no respaldada por capital, se debe instalar un firewall en el lado del grupo de la empresa para controlar las comunicaciones por el destino de la conexión y el puerto de comunicación.

4.1.26- Uso de servicios externos (servicios en la nube)

Mediante el uso de servicios externos (almacenamiento en la nube), la información confidencial se almacenará fuera de la empresa y se introducirán nuevos sistemas de información importantes, lo que se espera que suponga un riesgo operativo. Aquí, se definen las medidas de seguridad de la información para que estos servicios externos puedan utilizarse de forma segura.

4.1.26-1. Personas afectadas

Personas que seleccionan, contratan y utilizan servicios externos

4.1.26-2. Alcance

Información almacenada en servicios externos (almacenamiento en la nube) y sistemas empresariales que utilizan esa información para la implementación.

4.1.26-3. Política de Uso

- El uso de los activos de la empresa o de las empresas del grupo debe tener prioridad sobre los servicios externos, ya que generalmente presentan los siguientes riesgos:
- Dificultades en la investigación de las causas de los incidentes de seguridad de la información, ya que no es posible realizar investigaciones directas o auditorías a proveedores de servicios externos.
- Riesgo de cambiar, interrumpir o suspender el contenido del servicio, de forma unilateral, por circunstancias de proveedores de servicios externos.
- El uso de servicios externos debe limitarse únicamente a los sistemas utilizados en operaciones generales sin requerir exclusividad por parte del grupo SWS, y una introducción puede beneficiar significativamente el negocio de la empresa.
- Cuando el uso de servicios externos es necesario debido a una solicitud de los socios comerciales de la empresa, se requiere consultar con el departamento de gestión de sistemas de información.
- Cuando se trata del almacenamiento de información confidencial, se limita a los casos en que la seguridad de la gestión de la información (identificación de riesgos, evaluación y otras medidas) se haya confirmado de antemano.
- Cuando se utilizan servicios externos, se debe obtener la aprobación del administrador de la información que se almacenará en los servicios externos y del jefe del departamento de gestión del sistema de información, y el acuerdo del jefe del departamento del sistema de información SWS.
- El jefe del departamento de gestión del sistema de información debe confirmar la disponibilidad, confidencialidad e integridad de los servicios externos y, a continuación, decidir si utiliza el servicio externo.

4.1.26-4. Evaluación de Riesgos y Contrato

- **Evaluación de riesgos antes de la firma del contrato**
  Los departamentos que consideren la posibilidad de recurrir a servicios externos deben consultar con el departamento de gestión del sistema de información con suficiente antelación para disponer de tiempo suficiente para realizar una evaluación de riesgos.

  El departamento de gestión del sistema de información confirmará la disponibilidad, confidencialidad, integridad, etc. de la utilización del servicio externo y llevará a cabo una evaluación de riesgos correspondiente al nivel de confidencialidad. Sobre la base de los resultados de la evaluación del riesgo, deben adoptarse las medidas adecuadas contra el riesgo confirmado.

  Los departamentos que consideren el uso de servicios externos deben obtener la aprobación del administrador de la información almacenada, el jefe del departamento de sistemas de información

y el jefe del departamento de sistemas de información de SWS sobre la base del resultado de la evaluación de riesgos.

El departamento de gestión de sistemas de información debe preparar un libro de contabilidad para los servicios externos, de modo que se pueda evaluar fácilmente la influencia de la empresa cuando se produzca un problema en los proveedores de servicios externos y se revele al público.

Se puede considerar el apoyo de un asesor legal.

- **Acuerdo de Servicios Externos**
  Los contratos corporativos deben firmarse cuando se utilizan servicios externos. La cláusula de confidencialidad debe incluirse en el contrato.

- **Evaluación de riesgos después de la firma del contrato**
  Los departamentos que firman un contrato de servicios externos deben comunicar los detalles al departamento de gestión del sistema de información cuando se produzca un cambio en el contenido del contrato o de los servicios, o cuando se rescinda el contrato.

  Cuando el departamento de gestión del sistema de información sea notificado de cualquier cambio contractual, debe realizar de nuevo una evaluación de riesgos según sea necesario.

  Los departamentos que firman un contrato de servicios externos deben proporcionar la información necesaria para la evaluación de riesgos si así lo solicita el departamento de gestión del sistema de información.

  Se puede considerar el apoyo de un asesor legal.

- **Posiciones de gestión en los departamentos de control**
  Los departamentos de control (departamentos que firman un contrato de servicio externo) deben designar al gerente/personal de control.

  El gestor debe gestionar adecuadamente el alta/baja de usuarios de servicios externos y derechos de acceso, etc.

  Cuando la información de la empresa se guarda y almacena en servicios externos, se debe seguir la "Gestión y Manejo de Activos de Información (Papel/Datos)".

- **Gestión del uso de servicios externos**
  El Departamento de Gestión de Sistemas de Información mantiene un libro de servicios externos, evalúa rápidamente el impacto en la Compañía cuando se produce un problema o es anunciado por un proveedor de servicios externo, e informará al gerente del departamento responsable del asunto e instruirá para que deje de usar el servicio, cambie a un servicio alternativo, y así sucesivamente.

El Departamento de Gestión de Sistemas de Información hará un inventario periódico del libro mayor de servicios externos al menos una vez al año y reflejará los nuevos o descatalogados de la lista.

4.1.27- Medidas de seguridad para equipos de producción

Los equipos de producción a menudo están conectados a redes, y es necesario fortalecer las medidas de seguridad de la información para reducir el riesgo de infección por virus, etc. Sin embargo, los PC instalados como parte de los equipos de producción son en muchos casos diferentes de los PC de oficina o los PC para sistemas empresariales, por lo que el software antivirus es difícil de instalar o la autenticación individual es difícil de realizar. Por lo tanto, la atención se centra en la implementación de medidas contra las amenazas de los dispositivos de conexión externos, Internet y los sistemas empresariales.

4.1.27-1. Personas afectadas

Personas que se dediquen al control y funcionamiento de los equipos de producción y de los dispositivos de inspección conexos, etc. (en lo sucesivo denominados "equipos de producción, etc.")

4.1.27-2. Alcance

PCs y dispositivos de red instalados como parte de los equipos de producción, etc. y la información que manejan.

4.1.27-3. Rol del Gerente de Seguridad de la Información del Departamento con Equipos de Producción

El responsable de seguridad de la información debe promover y gestionar las medidas de seguridad de la información en el propio departamento.

Configure el administrador de seguridad de equipos de producción para administrar las PC utilizadas en los equipos de producción, etc., y promueva la administración de PC, la introducción de software antivirus, etc., y actualice a la última versión.

Cuando se producen incidentes de seguridad de la información, el gerente de seguridad de la información debe tomar medidas rápidas y apropiadas en cooperación con los departamentos relacionados.

4.1.27-4. Reglas de cumplimiento para equipos de producción, etc. cuando se planifica la instalación

Cuando se planifica la instalación de un equipo de producción, se debe evaluar la instalación de software antivirus y medidas de seguridad como restricciones de acceso, etc.

4.1.27-5. Normas de cumplimiento para la conexión a la red de equipos de producción

Al conectar el equipo de producción a la red dentro de la empresa, se debe realizar el sistema de administración de activos de TI, el software antivirus y la configuración de Windows Update, como se indica en la Tabla 4-1.

En principio, se prohibirá la conexión de los equipos de producción a Internet, con el fin de recibir mantenimiento remoto de proveedores externos. Cuando dicha conexión sea inevitable por razones comerciales, se debe consultar con el departamento de gestión de sistemas de información.

Es deseable confirmar regularmente que no se intenta el acceso ilegal, etc., al equipo de producción.

En principio, se prohibirá la conexión de PC del sistema operativo Windows, cuyo soporte por parte de Microsoft haya finalizado, en la primera LAN de la red interempresarial. Cuando la conexión se realice inevitablemente por razones comerciales, el departamento de administración será responsable del uso seguro de la restricción de conexión de red.

4.1.27-6. Medidas antivirus para equipos de producción

El software antivirus debe instalarse en las PC y servidores utilizados en los equipos de producción, y es deseable permitir el escaneo en tiempo real. Si la instalación no es posible, se prohíbe la conexión a la primera LAN. La conexión a la segunda LAN debería requerir en principio la instalación de un software antivirus, pero si la instalación es difícil en el equipo, el escaneo debe implementarse regularmente (al menos dos veces al año) con una herramienta de escaneo de virus, etc. y mantener el registro con el resultado del escaneo.

En el caso de los equipos utilizados en equipos de producción, cree una lista de inventario, instale la configuración de WSUS, el software antivirus y el sistema de administración de activos de TI (lansweeper). Es necesario mantener la gestión de los equipos. La lista debe actualizarse al menos 1 vez al año.

4.1.27-7. Reglas de cumplimiento cuando se conectan PC, unidades USB, etc. a equipos de producción

En principio, está prohibido el uso de memorias USB o memorias USB en equipos de producción. Si es necesario, es deseable utilizar los medios de grabación estándar de la empresa. Cuando esto no sea posible por razones comerciales, se deben comprar y utilizar medios de grabación no estándar, como PC y unidades USB de empresa no estándar, de acuerdo con los procedimientos prescritos. Antes de conectarlos a los equipos de producción, deben ser escaneados por un software antivirus para confirmar que no hay ningún problema.

- Para PC
  Confirme que no hay ningún problema de infección de virus con una herramienta de búsqueda de virus, etc., y administre el libro mayor para los resultados de confirmación.

4.1.27-8. Copias de seguridad de equipos de producción

Suponiendo que el equipo de producción esté dañado, se deben realizar las siguientes acciones para

recuperar los datos (configuración).

El sector responsable debe adquirir recursos para proporcionar copias de seguridad, organizar los procedimientos de recuperación e implementar pruebas de recuperación.

Se deben mantener registros de operación sobre el software y los datos cambiantes.

4.2. Plan de contingencia de TI

Una estrategia de contingencia es un conjunto de medidas capaces de asegurar la continuidad de los sistemas vitales de una empresa cuando se produce un problema. Esta planificación debe garantizar que el departamento de TI actúe con rapidez, siguiendo una seguridad predeterminada paso a paso para reducir los daños causados y recuperar la mayor cantidad de datos posible.

La tecnología forma parte de prácticamente todos los procesos de una empresa hoy en día, por lo que los equipos de TI siempre deben contar con medidas preventivas, pero como pueden ocurrir imprevistos, es necesario estar preparados y tener una respuesta inmediata y efectiva ante las amenazas.
El plan de contingencia debe estar bien preparado y tener en cuenta las vulnerabilidades y posibles riesgos que pueda correr la empresa, además de los recursos disponibles para resolver problemas técnicos, controlar ciberataques y otros fallos.

Para que el plan sea efectivo, debemos considerar el siguiente enfoque:

- ✓ Involucrar a todas las áreas en el proceso;
- ✓ Definir un equipo para la gestión de crisis;
- ✓ Realizar análisis de riesgos;
- ✓ Clasificar lo que es prioritario;
- ✓ Definir estrategias de recuperación;
- ✓ Documentar el plan de contingencia (IT-TI-016);
- ✓ Realizar pruebas.

4.3. Tratamiento de la información personal

4.3.1- Objetivo

El propósito es aclarar los elementos que deben observarse cuando se recopila, mantiene, destruye, etc., la información personal, etc., y observar la Ley de Protección de Información Personal.

Información personal se refiere a la información sobre una persona viva que puede identificar a la persona específica por su nombre, fecha de nacimiento u otras descripciones contenidas en dicha información (incluida la información que se puede verificar fácilmente con otra información y, por

lo tanto, identificar a la persona específica) o información que incluye códigos de identificación individual.

4.3.2- Personas afectadas

Empleados de la empresa y empleados contratados que manejan información personal

4.3.3- Alcance

Todos los sistemas que manejan información personal.

4.3.4- Reglas de cumplimiento

- NA-AG-019 – Política de Privacidad Interna
- Política de Privacidad Interna
- NA-AG-020 – Política de Retención y Eliminación de Datos

4.4. Entrenamiento y simulaciones

4.4.1- Objetivo

El objetivo es que los empleados de la empresa y los empleados contratados puedan reconocer la importancia de la seguridad de la información y mejorar su conciencia mediante la implementación sistemática de actividades de capacitación y mejora de la seguridad de la información.

4.4.2- Personas afectadas

Los departamentos que gestionan la formación en seguridad de la información y los responsables de seguridad de la información de cada departamento.

4.4.3- Alcance

Usuarios a los que se aplica la Política de Seguridad de la Información.

4.4.4- Planificación de la formación en seguridad de la información

- **Los departamentos que administran capacitaciones sobre seguridad de la información deben hacer planes para las siguientes capacitaciones:**
  - Capacitación para los nuevos empleados cuando se incorporan a la Compañía;
  - Capacitación periódica (una vez al año o más) para los usuarios;
  - Capacitación periódica (una vez al año o más) para los miembros de la gerencia;
  - Capacitación periódica (una vez al año o más) para los empleados de la clase gerencial y los miembros del comité de Seguridad de la Información;

- Reentrenamiento (Actualización Formativa);
- Capacitación para empleados transferidos de una empresa a otra;
- Capacitación de Empleados Subcontratados, cuando corresponda;
- Capacitación para el manejo de la información, según sea necesario;
- Capacitación para pasantes y trabajadores temporales;
- Ejercicios para hacer frente a incidentes de seguridad;
- Simulaciones para tomar medidas de acuerdo con estos estándares de medición cuando ocurre un incidente de seguridad;
- Ejercicios para tomar las medidas apropiadas de acuerdo con estos estándares de medición cuando se recibe un correo electrónico dirigido o un correo electrónico sospechoso una vez al año o más).

- **Requisitos para la educación y la formación en las Directrices de ciberseguridad de JAMA/JAPIA Ver.2.0**

  El contenido de la formación debe cubrir los siguientes requisitos:
  - Prevención de la infección por virus por correo electrónico;
  - Prevención de la infección por virus causada por el uso de Internet (navegación web);
  - Procesamiento de la información en función de un grado de confidencialidad;
  - Realización de cursos de formación específicos por correo electrónico;
  - Actividades de sensibilización para evitar errores en la transmisión de correos electrónicos;
  - Seguridad de la información y medidas de gestión en cada departamento;
  - Realización de actividades de sensibilización en cada lugar de trabajo;
  - Implementación de actividades de mejora de la concienciación en toda la empresa;
  - Medidas para dar a conocer las normas de entrada y expulsión;
  - Crear oportunidades para que los gerentes entiendan sus roles y responsabilidades relacionados con la seguridad de la información;
  - Manejo cuando ocurre un accidente.

4.4.5- Implementación de la capacitación

El departamento de gestión de la formación en seguridad de la información debe formar a los empleados de recursos humanos, que tengan suficientes conocimientos sobre la seguridad de la información, y nombrarlos profesores de formación.

Los departamentos que gestionan la formación en toda la empresa deben implementar la formación en seguridad de la información para los usuarios proporcionando materiales de formación, basados en los planes de formación.

Siempre que sea posible, se debe utilizar la formación en formato e-learning.

Cuando los empleados son transferidos dentro de la empresa o los empleados contratados se unen al departamento, se deben realizar capacitaciones en seguridad de la información.

Es necesario mantener la siguiente información como historial de capacitación en relación con la capacitación en seguridad de la información realizada:

- Fecha de realización (año, mes y fecha);

- Nombre del curso (contenido de la formación);
- Materiales de capacitación;
- Nombre del departamento de destino;
- Nombre y número de personas que reciben la capacitación;
- Nombre del instructor/ministro.

Es **obligatorio** realizar la formación para la que se invita a los empleados.

4.4.6- Revisión de Planes y Materiales de Capacitación

El departamento de gestión de la formación en seguridad de la información debe revisar el programa de formación con regularidad (una vez al año o más).

El departamento de gestión de la formación en seguridad de la información debe considerar la posibilidad de revisar los planes de formación y el contenido cuando se revise la política de seguridad de la información o se produzca un incidente importante de seguridad de la información.

El departamento de gestión de la capacitación en seguridad de la información debe revisar los materiales de capacitación según sea necesario.

4.4.7- Actividades de mejora de la concienciación

Es deseable que el departamento de gestión de la formación en seguridad de la información lleve a cabo actividades de mejora de la concienciación, como el mes de la mejora de la seguridad de la información.

Durante el mes de mejora de la seguridad de la información o la implementación de diagnósticos del sistema, es necesario considerar las reglas y los riesgos relevantes. Cada departamento debe recordar los contenidos que deben ser conducidos, mantenidos y continuados de forma regular. Cada departamento debe difundir el contenido recordado a sus empleados dentro del departamento.

4.4.8- Informes y confirmación de la implementación de la capacitación

El departamento de gestión de la formación en seguridad de la información debe comprobar el estado de la implementación.

El departamento de gestión de la formación en sistemas de información y cada departamento deben evaluar el nivel de comprensión y competencia de la formación en los ejercicios realizados.

4.5. Directrices internas del Grupo Sumidenso

Todo acceso a la información, a los recursos tecnológicos y a los entornos lógicos debe ser controlado, con el fin de garantizar el acceso únicamente a las personas autorizadas. Las autorizaciones deben ser revisadas periódicamente por el responsable de cada área.

La persona responsable de la autorización o confirmación de la autorización debe estar claramente definida y registrada. Los datos, la información y los sistemas de información de las entidades deben estar protegidos contra amenazas y acciones no autorizadas, ya sean accidentales o no, con el fin de reducir los riesgos y garantizar la integridad, confidencialidad y disponibilidad de los datos.

Se prohíben las conversaciones sobre cualquier asunto relacionado con la empresa en cualquier lugar donde terceros puedan escuchar.

4.5.1- Concesión de accesos suspendidos

La concesión de acceso a la información y a los sistemas se autorizará sobre la base de la norma de acceso mínimo necesaria para el desempeño de la función. La solicitud de acceso debe estar registrada en el sistema de Helpdesk y autorizada por el responsable del área. Periódicamente, los accesos concedidos deben ser revisados por el responsable de cada departamento.

El acceso y uso de todos los sistemas de información, directorios de redes, bases de datos y otros recursos estará restringido a las personas explícitamente autorizadas y según sea necesario para el desempeño de sus funciones. El acceso innecesario o excesivo debe eliminarse de inmediato.

4.5.1-1. Bloqueo/inactivación de la cuenta

Los empleados que no accedan al Sistema Oracle, Sistema de Nómina y/o Sistema de Sincronía Fiscal por un período superior a 90 días tendrán el acceso bloqueado automáticamente, y es necesario abrir una llamada técnica, con el sistema HelpDesk, con autorización del Gerente de Sector para su liberación.

4.5.1-2. Revisión del acceso a los sistemas básicos

1 – Periódicamente, se debe realizar una revisión de los accesos otorgados a los sistemas Oracle/Inventiva. De esta forma, se emitirá un listado de todos los usuarios activos en el sistema por parte del sector IT, con sus respectivos accesos. Esta lista se generará y remitirá a los responsables de cada departamento, quienes deberán verificar que los accesos otorgados a los usuarios sean correctos. Después de la revisión, el documento debe ser devuelto a TI, que realizará los cambios necesarios.

2 – Los empleados que no accedan a ningún módulo del Sistema Oracle por un período superior a 90 días tendrán el acceso a la responsabilidad automáticamente desactivado. Para que el acceso vuelva a ser liberado, será necesario abrir un ticket en el servicio de asistencia, solicitando la liberación. La llamada debe ser autorizada por el responsable del sector para que se realice el servicio.

4.5.2- Normas específicas

4.5.2-1. Reglas de cumplimiento para la construcción del sistema

- **Diseño / Instalación del sistema**

Se debe aclarar el nivel de importancia del sistema y el grado de confidencialidad de la información que maneja el sistema.

En cuanto a los sistemas de información que manejan información sensible, es deseable que la base de datos esté encriptada.

En los niveles de importancia S, A y B, se debe llevar a cabo un proyecto para reducir al máximo el tiempo de suspensión del sistema, como la redundancia de la fuente de alimentación, la CPU y el disco, la ubicación del espejo, etc., dependiendo de un nivel de importancia, en caso de problemas.

Para gestionar la información con un alto grado de secreto, de acuerdo con el apartado "2 Gestión y Manejo de Activos de Información (Papel/Datos)", se debe diseñar un derecho de acceso a la información.

Se deben establecer los derechos de acceso mínimos requeridos para todas las cuentas.

Se debe implementar una función para recopilar y guardar registros de acceso, etc.

Se debe implementar una función para las medidas de acceso ilegal mediante autenticación personal o restricciones de acceso, como el área disponible (dirección IP), el tiempo disponible (tiempo de conexión, tiempo de espera de la sesión), etc.

- **Segregación de los entornos de producción/desarrollo/prueba del sistema**

Se deben tener en cuenta los siguientes elementos para la separación de los entornos de producción, desarrollo y pruebas:
En principio, se debe utilizar un hardware diferente entre el entorno de prueba y el entorno oficial.
Para evitar el uso indebido de los sistemas, el entorno oficial y el entorno de prueba deben ser distinguibles.

En principio, debería prohibirse el acceso al entorno de producción por parte de una persona encargada del desarrollo. Cuando sea inevitable acceder al entorno oficial, se debe obtener la aprobación del administrador del servidor/administrador de bases de datos y se debe obtener un permiso solo para el derecho de 'Solo lectura'.

Se deben tener en cuenta los siguientes elementos para una implementación de prueba:
Al realizar pruebas con los datos oficiales o con los datos de prueba que incluyen 'Estrictamente confidencial', 'Persona autorizada confidencial' y 'Confidencial de la empresa', se debe obtener la aprobación del administrador de datos de destino y se debe prestar toda la atención al manejo de los datos.

Cuando se copian datos acreditados en el entorno de prueba, se debe obtener el permiso del administrador de datos de destino.

Cuando se utilizan datos acreditados como datos de prueba, deben eliminarse inmediatamente del entorno de prueba una vez completada la prueba.

Cuando se proporcionen datos oficiales o datos de prueba, incluidos "Estrictamente confidencial", "Confidencial de la persona autorizada" y "Confidencial de la empresa", a empresas externas, se debe observar la gestión de subcontratación.

También se deben implementar restricciones de acceso para el entorno de prueba.

Para garantizar la integridad de los datos, las pruebas realizadas deben ser coherentes para que se puedan validar los cambios realizados en los programas.

Para asegurarse de que el contenido de la salida de datos de una aplicación es preciso, se debe realizar la siguiente prueba:

- Coherencia de los datos de salida;
- Aclaración de las personas responsables relacionadas con la salida de datos

El cambio o la liberación del programa oficial en el entorno de producción debe controlarse estrictamente para minimizar el riesgo de interrupción de las operaciones. El procedimiento detallado se describe en el documento:
IT-TI-020_Gerenciamento_de_Mudancas_Ambiente_Producao.

Los programas fuente deben ser administrados por herramientas de control de versiones, etc. Es deseable administrar el módulo oficial de la misma manera.

- **Construcción del servidor del sistema**

El administrador de TI, junto con el administrador del sistema, debe evaluar y definir una configuración de servidor de acuerdo con el proyecto.
Solo se deben instalar las aplicaciones/servicios mínimos necesarios que correspondan al propósito del sistema.

La contraseña de la cuenta con derechos de administrador debe estar estrictamente definida y controlada de la siguiente manera:

- Se debe establecer una contraseña de inicio de sesión de acuerdo con el contenido estipulado en "7.7 Autenticación de usuario";
- La divulgación de dicha contraseña se limitará al mínimo;
- Cuando se reemplazan los administradores del servidor, la contraseña debe cambiarse según sea necesario.

Los sistemas divulgados fuera de la empresa (como el EDI) deben tener mensajes cifrados (comunicación de datos) o firmas digitales.

El responsable del sistema/personal de control debe verificar e implementar algunos requisitos antes del inicio de las operaciones en Producción:

- No se han iniciado servicios innecesarios.
- No hay cuentas innecesarias disponibles.

- En principio, no se debe utilizar el ID de usuario predeterminado. Además, se debe cambiar la contraseña inicial.
- El control de acceso es adecuado y está validado.
- Las contramedidas contra las amenazas esperadas son apropiadas.
- Pruebas de implementación de acuerdo con el contenido de los procedimientos de operación/control.
- Verificación de copia de seguridad y restauración

4.5.2-2. Reglas de cumplimiento para la operación y el mantenimiento del sistema

- **Operación y mantenimiento del sistema**

  La persona a cargo del sistema debe crear un manual de procedimientos para la operación y el mantenimiento.

  El manual de procedimientos debe incluir lo siguiente:
  - Procedimientos seguros de reinicio y recuperación del sistema cuando se producen problemas en los dispositivos del sistema;
  - Requisitos para el cronograma del proceso y la orden de ejecución;
  - Información de contacto cuando se producen problemas operativos o técnicos inesperados;
  - Soluciones a errores del sistema u otras situaciones excepcionales.

  El departamento de gestión de operaciones del sistema debe crear un libro mayor de control del servidor y una lista de contactos de las personas relacionadas con cada sistema (se debe proporcionar la información de contacto de los administradores del servidor y de las emergencias).

- **Mantenimiento de hardware**

  El departamento de gestión de hardware debe realizar una verificación periódica de acuerdo con el intervalo de mantenimiento y las especificaciones recomendadas por el proveedor para garantizar la disponibilidad del hardware.

  Al subcontratar la verificación y reparación de hardware, se debe utilizar el proveedor o la agencia de mantenimiento designada por el proveedor.

  Se deben conservar todos los registros de mantenimiento de hardware (incluidos los fallos).

  Al retirar el hardware de las instalaciones de la empresa para su mantenimiento, se debe hacer y celebrar un acuerdo de confidencialidad.

- **Obtención y aplicación de parches de seguridad y modificaciones**

En principio, aplique el parche de seguridad al servidor de Windows en un plazo de 3 meses. Sin embargo, si no se puede aplicar debido a circunstancias comerciales inevitables, consulte con el Departamento de Sistemas de Información.

Si el Departamento de Sistemas de Información le indica que aplique un parche de emergencia, etc., aplíquelo de inmediato.

Para los sistemas operativos que no sean Windows (Linux, Unix, etc.), el gerente/personal de control del sistema de destino debe obtener los parches de seguridad y las modificaciones necesarias de cada proveedor e implementar las actualizaciones necesarias de manera adecuada.

El gerente/personal de control del sistema de destino debe obtener los parches de seguridad y la modificación de cada aplicación de cada proveedor e implementar las actualizaciones necesarias de manera adecuada.

El personal de control/administrador de red debe obtener los parches de seguridad y la modificación de los dispositivos de red de cada proveedor e implementar las actualizaciones necesarias de manera adecuada.

La conexión del sistema operativo Windows, cuyo soporte de Microsoft ha finalizado, a la red interna (que no sea la segunda LAN) estará prohibida en principio.

- **Confirmación del estado de la solicitud de medidas de seguridad**

Cuando se implementa el cifrado de certificados de servidor, se debe administrar una fecha de caducidad del certificado y el certificado debe actualizarse antes de la expiración.

El personal de gestión/control del sistema de destino debe implementar inmediatamente las medidas de seguridad, como la aplicación de parches, distribuidas por el departamento de gestión del sistema de información.

Cuando se producen algunos problemas mientras se toman medidas de seguridad, los operadores deben informar los detalles de los problemas al departamento de gestión del sistema de información.

Cuando el departamento de gestión del sistema de información recibe los informes de problemas, debe confirmar los detalles notificados, considerar contramedidas y difundir la información a los departamentos relacionados según sea necesario.

- **Contramedidas de virus del servidor**

Se deben observar las siguientes reglas para evitar daños por un bloqueo del sistema o fuga de información causada por virus.

El personal de control del servidor debe instalar el software antivirus especificado por el departamento de gestión de sistemas de información en los propios servidores del sistema operativo Windows.

El software antivirus debe configurarse de modo que siempre se pueda comprobar el acceso a los archivos (análisis en tiempo real).

El software antivirus debe configurarse para que el archivo de definición se pueda actualizar automáticamente.

Se debe confirmar que la versión, el motor de análisis y el archivo de definición del software antivirus se actualizan periódicamente.

El escaneo de todo el disco duro, además del escaneo en tiempo real, debe implementarse al menos dos veces al año.

El análisis de virus mediante el software antivirus más reciente debería, en principio, implementarse para los datos o el software traídos del exterior antes de guardarlos en los dispositivos de información de la empresa.

Cuando el departamento de gestión de sistemas de información o el propio responsable de seguridad de la información del departamento solicitan un análisis de virus, el análisis de virus debe implementarse en todos los discos duros.

La configuración del software antivirus no debe ser cambiada por una persona sin autorización.

- **Copia de seguridad del servidor**

Las reglas de operación de copia de seguridad (tiempo de recuperación, período de almacenamiento, etc.) para los servidores deben decidirse de acuerdo con el nivel de importancia del sistema o los requisitos del usuario. Los procedimientos operativos de copia de seguridad, así como el software utilizado y las políticas aplicadas, se describen cn IT-TI-001.

Al aplicar algunos cambios, como la aplicación de parches de seguridad y la modificación de servidores y sistemas, se debe realizar una copia de seguridad con anticipación. Se debe volver a realizar una copia de seguridad después de que se confirme el funcionamiento estable.

Se debe realizar una copia de seguridad en la fecha y hora en que el negocio no se vea afectado.
Una vez completada la copia de seguridad, se deben verificar los resultados de la ejecución (normal/anormal) y se deben obtener y mantener los registros.

En el momento de la instalación inicial o actualización de los servidores, se deben crear procedimientos de recuperación y se debe implementar una prueba de recuperación de los datos de copia de seguridad para confirmar que los servidores se pueden recuperar normalmente.
Los medios necesarios para una restauración del sistema (CD de instalación, DVD, etc.) deben almacenarse y administrarse.

4.5.2-3. Monitorización

- **Monitoreo de seguridad**

El historial de trabajo para las operaciones del servidor y del sistema debe registrarse y guardarse (1 o más años).

El historial de fallos de los registros del sistema y los registros de acceso debe registrarse y guardarse (1 o más años).

Los estándares de gestión para el rendimiento del sistema, los fallos de recursos y hardware, etc., deben establecerse y supervisarse periódicamente.

- **Supervisión del rendimiento**

El equipo de infraestructura de TI debe verificar regularmente el estado de funcionamiento del sistema para mantener operaciones estables. En principio, deben vigilarse los siguientes elementos:

- Carga de hardware y comunicación;
- CPU/memoria;
- Capacidad de la unidad de disco duro;
- Tráfico de red;
- Advertencias del sistema o registros de fallas;
- Advertencias o mensajes de visualización de la consola;
- Registros del sistema (mensajes de error o registros excepcionales);
- Mensajes de advertencia del sistema de gestión de red.

Cuando se detectan anomalías o recursos insuficientes en el sistema o hardware como resultado de la supervisión, se deben tomar medidas inmediatas y adecuadas. Es deseable que el equipo de Infraestructura siga el crecimiento para detectar con anticipación la necesidad de ampliar la capacidad de los equipos en el futuro, y así evitar problemas y ampliar los recursos, según sea necesario.

4.5.2-4. Reglas de cumplimiento para servidores públicos de Internet,

El equipo de Seguridad de la Información debe analizar las amenazas esperadas desde el extranjero (Internet) y considerar las siguientes contramedidas para evitar el acceso ilegal.

- Instalación de dispositivos (firewall, IPS, etc.) para evitar accesos ilegales;
- Contramedidas (ataques, etc.) para suspender los servicios;
- Contramedidas contra la amenaza de convertirse en un servidor trampolín utilizado para acceder ilegalmente a otras organizaciones;
- Distinguir una red conectable de la red no conectable de la empresa externa
- Protección contra virus, etc.;
- Implementación de escritorio y pantalla limpios (el bloqueo de pantalla debe configurarse dentro de los 15 minutos de forma predeterminada);
- Aclaración de las medidas de emergencia cuando se produce un acceso ilegal;

- Recopilación y análisis de ejemplos de acceso ilegal en otras organizaciones;
- Implementación de medidas de seguridad en las comunicaciones, como el cifrado.

4.5.2-5. Instalación

Al instalar un servidor web externo, se debe instalar un certificado de servidor SSL y se debe realizar una comunicación cifrada.

Se debe realizar un diagnóstico de vulnerabilidad una o más veces antes de que comience la operación para confirmar que, en principio, no hay problemas con la vulnerabilidad. Además, tras el inicio de la operación, el diagnóstico de vulnerabilidad debe realizarse de forma periódica (una o varias veces al mes y en el momento de la modificación del sistema).

Cuando se detecta vulnerabilidad como resultado del diagnóstico de vulnerabilidad, se deben tomar medidas en función del grado de urgencia, grado de importancia, etc.

Cuando hay un problema con la vulnerabilidad, se pueden tomar acciones como desconectarse de la red.

Se debe construir y mantener un sistema que pueda responder adecuadamente cuando se detecta una vulnerabilidad o un ataque.

En caso de accidente de seguridad, es deseable que el administrador del sistema y el responsable puedan ponerse en contacto con el usuario individual del servidor. Además, si así lo solicita el Comité de Seguridad de la Información, la información confidencial y la información personal almacenada en el servidor deben estar preparadas para ser enviadas con prontitud.

4.5.2-6. Sistemas

- Los sistemas deben clasificarse según su grado de importancia y deben controlarse mediante un sistema o un libro de control. La información debe ser revisada periódicamente (1 vez al año o cuando sea necesario).

- Los sistemas deben tener control de acceso para garantizar su uso solo por parte de usuarios autorizados. La persona responsable de la autorización debe estar claramente definida y haber registrado la aprobación otorgada, a través de la apertura de una Convocatoria en el sistema de Helpdesk.

- La copia de seguridad debe probarse y mantenerse actualizada para la recuperación ante desastres.

- Se deben implementar pruebas de recuperación de los datos de copia de seguridad y se debe verificar que los datos se recuperaron correctamente después de que se estableció el sistema

- Los medios para la recuperación/restauración del sistema deben controlarse adecuadamente y almacenarse en bóvedas ignífugas.

- En la implementación de nuevas funcionalidades o nuevos sistemas, se deben adoptar buenas prácticas en el desarrollo del proyecto, asegurando que las aplicaciones estén bien diseñadas, probadas y aprobadas.
- No ejecute programas que tengan el propósito de decodificar contraseñas, monitorear la red, leer datos de terceros, propagar virus informáticos, destruir parcial o totalmente archivos o hacer que los servicios no estén disponibles.

- No ejecutar programas, instalar equipos, almacenar archivos ni promover acciones que puedan facilitar el acceso de usuarios no autorizados a la red corporativa de la empresa.

- No envíe información confidencial (autorizada) a correos electrónicos externos sin protección. Como mínimo, el archivo debe estar protegido por una contraseña "robusta".

4.5.2-7. Operación de Sistemas

La estructura de la operación y la lista de contactos en caso de dificultades en los sistemas deben definirse y divulgarse a todos los empleados.

El área de TI debe crear manuales para el mantenimiento y operación de los sistemas. Estos documentos deben incluir procedimientos de inicio y parada, copia de seguridad/restauración y un plan de contingencia en caso de fallas.

Periódicamente, se deben revisar los accesos y eliminar las cuentas innecesarias. El departamento de RRHH debe comunicar al departamento de TI cada vez que un empleado sea despedido o transferido, para que el acceso pueda ser cancelado o revisado.

4.5.2-8. Máquinas – Estación de trabajo

Se pone a disposición de cada profesional una estación de trabajo, compuesta por equipos y software, para que pueda realizar sus funciones. Usted es responsable de la información almacenada en su estación de trabajo. Para ello, debe seguir las directrices y prácticas de Seguridad de la Información para minimizar y evitar la exposición de información considerada sensible para la organización, los clientes y los socios. Las computadoras a disposición de los empleados son propiedad de la empresa, y corresponde a cada uno usarlas y manejarlas correctamente para actividades de interés para la empresa.

La maquinaria y el equipo deberán ser devueltos en el momento de la salida de la empresa por los siguientes motivos: renuncia del empleado, renuncia por parte de la Empresa, jubilación o por cualquier otro motivo definido por la empresa.

Los archivos personales y/o los archivos que no sean pertinentes para el negocio de Sumidenso, como fotos, música, vídeos, etc., no deben copiarse/moverse a unidades de red, ya que pueden sobrecargar el almacenamiento de los servidores. Si se identifica la existencia de estos ficheros, se podrán suprimir definitivamente mediante comunicación previa al usuario.
Los documentos importantes para las actividades de la empresa siempre deben guardarse en unidades de red. Dichos archivos, si se registran solo localmente en las computadoras, no se garantizará que se

realice una copia de seguridad y pueden perderse en caso de falla de la computadora y, por lo tanto, son responsabilidad del propio usuario.

4.5.2-9. Buenas prácticas de seguridad para su entorno de trabajo

- Está prohibido copiar cualquier información en medios externos;
- Está prohibido que el usuario abra, altere o cambie la configuración y/o el equipo de su puesto de trabajo por su cuenta;

- Las estaciones de trabajo cuentan con herramientas de protección contra malware, y es deber del usuario mantenerlas actualizadas.

- Los usuarios deben bloquear el dispositivo con una contraseña siempre que estén ausentes (tecla de Windows + tecla L). Además, se debe configurar un protector de pantalla protegido por contraseña para que se active cuando el terminal haya estado inactivo durante 15 minutos o menos.

- Se deben obedecer los estándares de estilo definidos (fondo de pantalla, pantalla de inicio de sesión, protector de pantalla, colores y estilos), y no se pueden colocar fotos u otras imágenes que no sean las determinadas por el departamento de TI. El fondo de pantalla y el protector de pantalla (5 minutos) se configuran en AD, a través de GPO;

- En la sede o sucursales, el movimiento de cualquier equipo debe realizarse solo con la ayuda de la Coordinación del departamento de Infraestructura de TI de las unidades, y es necesario abrir una solicitud de servicio a través del servicio de asistencia. El control del movimiento de mercancías lo realiza el sector Contable a través de MAF – Movimiento de Activos Fijos.

- Las estaciones de trabajo están sujetas a inspección y deben estar disponibles para este fin por los respectivos usuarios cuando así lo soliciten;

- Los documentos impresos y los medios electrónicos, cuando no estén en uso, no deben mostrarse sobre la mesa. Manténgalo siempre en un lugar seguro;

- Los documentos con información considerada confidencial deben mantenerse en un lugar restringido y con control de acceso;

- Las notas con información confidencial no deben dejarse a la vista;

- No escribas información confidencial en pizarras, Post-its, etc.

- No almacene documentos restringidos y confidenciales en un lugar de fácil acceso;

- Triture los documentos impresos antes de tirarlos;

- No imprimas documentos solo para leerlos;

- Imprima siempre de forma segura, cuando no sea posible extraer el documento de la impresora inmediatamente al imprimir;

- Siempre que salga de la parte frontal de la computadora, mantenga la pantalla bloqueada;
- Solo los equipos de producción no deben tener bloqueo automático;

- Apagar las estaciones de trabajo al final de la jornada laboral, asegurando la desconexión de los servicios o aplicaciones de red;

4.5.2-10. Laptops y dispositivos móviles para empresas

Como regla general, los recursos como computadoras portátiles, teléfonos inteligentes y discos duros externos deben estar disponibles solo para "puestos de confianza", incluso entonces, cuando existe una necesidad real del recurso, como un riesgo inminente de interrupción de la operación y/o compromiso del servicio al cliente.

En los casos en que se otorgue el (los) dispositivo(s) corporativo(s), además de la justificación del Gerente del área que está solicitando el recurso, también será necesario involucrar al Departamento de Recursos Humanos, quien evaluará y ponderará los riesgos legales.

Por lo tanto, los dispositivos móviles solo se liberarán a pedido formal del administrador del área que necesita el recurso. Los teléfonos inteligentes se lanzarán después de instalar el antivirus y configurar el bloqueo de pantalla. La solicitud debe realizarse abriendo un ticket en el sistema de asistencia técnica. El departamento de TI debe analizar la necesidad y, junto con el departamento de recursos humanos, debe emitir una nota a los gerentes informándoles de los riesgos.

Cada empleado debe hacer periódicamente una copia de seguridad de los datos en su computadora portátil. Esta copia debe conservarse en el servidor de archivos. Excepto los correos electrónicos, porque el correo electrónico tiene una copia en el servidor con una retención de 1 año.

Se debe implementar una medida de encriptación en los PC que se puedan sacar de la empresa, para evitar la fuga de información por pérdida o robo.

Las computadoras portátiles sin medidas de encriptación no deben salir de la empresa y deben protegerse con un cable de seguridad o guardarse en un cajón o armario cerrado con llave antes de salir de la oficina.

Al retirar los PC de las instalaciones de la empresa, se debe obtener la aprobación del gerente de seguridad de la información o del administrador de dichos dispositivos y se debe mantener un historial de eliminación.

Si es necesario llevar el PC con frecuencia debido al trabajo desde casa o a viajes de negocios, se debe obtener la aprobación abriendo un ticket en el servicio de asistencia.

Después de traer una PC normal, los datos guardados deben eliminarse y las PC móviles normales deben devolverse a la ubicación de almacenamiento especificada.

4.5.2-11. Mejores prácticas de seguridad para su computadora portátil

Cuando viaje en automóvil, colóquelo en el maletero o en un lugar discreto.

A la hora de desplazarse con el portátil, si es posible, no utilice bolsas convencionales para portátiles, sino mochilas o maletas discretas.

No coloque su computadora portátil en los carritos del aeropuerto ni la facture con su equipaje.

En lugares públicos (recepciones de hoteles, restaurantes y aeropuertos, entre otros), mantenga la computadora portátil cerca y siempre a la vista, sin alejarse del equipo.

Evite usar la computadora portátil en lugares públicos.

En los hoteles, preferiblemente, guarde la computadora portátil en la caja fuerte de su apartamento.

Evalúe si realmente es necesario llevar la computadora portátil en viajes cortos.

4.5.2-12. Acceso al correo electrónico

Como regla general, se realiza una copia de seguridad de todas las cuentas de correo electrónico durante un período de 12 meses. En el caso de las cuentas de la junta directiva, la dirección y el liderazgo, se mantiene una copia de seguridad durante un período de 5 años.

En situaciones específicas, cuando es necesario mantener una copia de seguridad de la cuenta de un empleado por un período de más de 12 meses, es necesario registrar una solicitud a través del sistema de Helpdesk informando el motivo de la necesidad.

Esta solicitud debe ser aprobada por la gerencia del área y será evaluada por el departamento de TI.

4.5.2-13. Medios extraíbles y puerto USB

Los medios extraíbles son dispositivos que permiten la lectura y escritura de datos como: CD, DVD, Disquete, Pen Drive, tarjeta de memoria, HDs portátiles, teléfonos celulares, entre otros.
El puerto USB es el principal punto de vulnerabilidad de seguridad y se puede utilizar para filtrar información corporativa confidencial. Dicha vulnerabilidad no puede ser contenida con firewalls o programas antivirus, ya que los dispositivos están conectados directamente al equipo por los propios usuarios.

Para minimizar los riesgos de exposición y pérdida de datos confidenciales en poder de la empresa y reducir los riesgos de proliferación de malware en las computadoras, los puertos USB deben bloquearse en todos los equipos de la empresa.

Esta regla se aplica tanto a los equipos de sobremesa como a los portátiles.

La liberación de puertos USB en computadoras de escritorio y portátiles se realiza solo si el uso es inevitable, justificado por la Junta de Área y aprobado por la Junta Directiva y de TI. En este caso, se debe llevar un libro de registro para controlar los equipos y los usuarios que tienen este acceso liberado.

Los medios de almacenamiento externo deben controlarse en los libros de control de activos.

Al retirar los medios de almacenamiento externos de las instalaciones de la empresa, se debe registrar una aprobación del responsable de seguridad de la información o del gestor de dichos dispositivos y un historial de retirada utilizando los libros de control de retiradas.

Una vez que devuelva el medio de almacenamiento externo, los datos guardados deben eliminarse. También deben devolverse al lugar de almacenamiento especificado.

Las comprobaciones de inventario deben realizarse con regularidad (1 vez al año o más). El control ledger de calidad debe compararse con objetos reales para verificaciones de inventario.
Cuando se encuentra una discrepancia en el inventario, se deben confirmar las ubicaciones de los medios de almacenamiento externo reales y se deben tomar medidas correctivas, como guardarlos en la ubicación de almacenamiento adecuada o actualizar el libro mayor de control.

Al guardar la información de la empresa en medios externos, como CD/DVD, se debe implementar el cifrado.

4.5.3- Incidentes de seguridad de la información

Un incidente de seguridad puede definirse como cualquier evento adverso, confirmado o sospechoso, que afecte la disponibilidad, integridad, confidencialidad o autenticidad de un activo de información, así como cualquier violación de la Política de Seguridad de la Información de la Compañía.

Es necesario definir las medidas para minimizar los daños y volver a la normalidad con tranquilidad cuando se produce un incidente de seguridad de la información. Con este fin, cada departamento debe actuar de manera inmediata y adecuada en cooperación con el Departamento de Seguridad de la Información.

4.5.3-1. Definiciones de incidentes de seguridad de la información

Los incidentes de seguridad de la información en la empresa se pueden definir mediante los siguientes casos e indicadores;

- Gestión de la información
  a) Filtración de información interna (información personal e información que no debe divulgarse al público);
  b) Quejas sobre la seguridad de la información recibidas de clientes, socios comerciales, etc.;
  c) Robo o Hurto de dispositivos de información como PCs, Notebooks o memorias USB, etc.;
  d) Pérdida o robo de documentos confidenciales;

e) La información "estrictamente confidencial" o "confidencial de la empresa" se envió por error.

- Sistemas de Información
  a) Apagado o suspensión de sistemas causados por infecciones de virus o ataques cibernéticos, el sistema de información, que afecten el negocio de la Compañía;
  b) Fuga de información interna debido a infecciones de virus o ciberataques;
  c) Uso ilícito del sistema de información o falsificación de información;
  d) Uso ilegal de una cuenta por parte de un tercero o suplantación de sitios web, etc.;
  e) Ataques cibernéticos a terceros (incluidos los casos en los que los activos de información de la Compañía se han utilizado ilegalmente para atacar a otras empresas sin el conocimiento de la Compañía).

  Hay muchos casos en los que el estado de los incidentes de seguridad de la información es difícil de reconocer (no está claro si el programa es ilegal o no). Por lo tanto, los incidentes de seguridad de la información incluyen en términos generales indicios de incidentes que pueden ser sospechosos y/o deficiencias del sistema que pueden conducir a un incidente.

4.5.3-2. Conducta cuando se producen incidentes de seguridad de la información

- La persona que genere/detecte incidentes de seguridad de la información deberá presentar un reporte con cada ruta de gestión de la información o sistemas de información, de acuerdo con el sistema interno de reporte;
- El CISO o la persona a la que se solicita el informe debe comunicarlo al Comité de Seguridad de la Información de SWS, que es la ventanilla de contacto del CSIRT;
- Los departamentos en los que se produzcan incidentes o el CISO deben idear y preparar medidas preventivas contra la repetición de incidentes de seguridad y divulgar minuciosamente las medidas a las personas internas;
- Cuando se produzca o se sospeche el uso no autorizado de un sistema de información o la falsificación de información (como el uso no autorizado de una cuenta por parte de otra empresa o la falsificación de un sitio web), indique inmediatamente a todos los usuarios del sistema de destino que cambien sus contraseñas. Además, es deseable tomar medidas para suspender el uso hasta que se confirme el cambio.

- La información más detallada relacionada con la gestión de incidentes se describe en IT-TI-017.

4.5.3-3. Medidas preventivas contra la recurrencia de incidentes de seguridad de la información

Los jefes de los departamentos en los que se producen los incidentes o el CISO deben idear y preparar medidas preventivas contra la repetición de incidentes de seguridad y difundir plenamente las medidas a los departamentos relacionados.

El CISO debe asegurarse de que todos los empleados sean plenamente conscientes del informe posterior a los hechos y de las medidas preventivas de recurrencia según sea necesario.

4.5.3-4. Manipulación cuando se ha producido o se sospecha de un uso no autorizado

Cuando se produzca o se sospeche el uso no autorizado de un sistema de información o la falsificación de información (como el uso no autorizado de una cuenta por parte de otra empresa o la falsificación de un sitio web), indique inmediatamente a todos los usuarios del sistema de destino que cambien sus contraseñas. Además, es deseable tomar medidas para suspender el uso hasta que se confirme el cambio.

4.5.4- Penalidades

El incumplimiento de las normas establecidas en este documento ya sea de forma individual o acumulativa, puede ocasionar, según la infracción cometida, las siguientes sanciones:

- **Comunicación de incumplimiento:** Se enviará al empleado por correo electrónico una comunicación informando del incumplimiento de la norma, con indicación precisa de la infracción cometida. Una copia de esta comunicación permanecerá archivada en el departamento de recursos humanos, en la carpeta respectiva del empleado;
- **Apercibimiento o suspensión:** La sanción de apercibimiento o suspensión se aplicará, por escrito, únicamente en casos de carácter grave o en caso de reincidencia en la práctica de infracciones leves;
- **Despido por justa causa:** En los casos previstos en el artículo 482 de la Consolidación de las Leyes del Trabajo.

4.6. Contratos

Se pueden celebrar contratos con empresas de subcontratación. En principio, está prohibido proporcionar información confidencial. Está prohibida la recontratación de contratos.
Todos los contratos firmados por el Departamento de TI deben incluir los siguientes elementos:

- Confidencialidad;
- Nombramiento de una persona para llevar a cabo la gestión del contrato;
- Cumplimiento de las medidas de seguridad y evaluaciones de riesgos;
- Cumplimiento del procedimiento de incidencia a la seguridad;
- Análisis anual o cuando sea necesario de los servicios prestados;
- Cláusulas de penalidades.

4.7. Auditorias

El director de Seguridad de la Información o CISO debe realizar auditorías periódicas para verificar que los activos de información de la empresa se gestionan correctamente.

4.8. Pandemias y desastres a gran escala

En principio, está prohibido el uso de dispositivos ajenos a la empresa. Los activos fijos de la empresa se pondrán a disposición, en la medida de lo posible, para otorgar acceso en la modalidad de Home Office.
Cuando se requiere una acción urgente y si los dispositivos propiedad de la empresa no son suficientes, el uso de dispositivos personales debe ser evaluado por el equipo de seguridad de la información.
Sin embargo, se deben observar las "Medidas de seguridad para la información y los dispositivos portátiles de información". En este caso, se puede utilizar un software antivirus no especificado por la empresa, sujeto a evaluación por parte del equipo de seguridad de la información.
Está prohibido almacenar los activos de información de la empresa en dispositivos de información personal.

5. RESPONSABILIDADES

- **Consejo de Administración, Dirección, Liderazgo y Coordinación**

Es responsabilidad de la Junta Directiva, Administración, Liderazgo y Coordinación, cumplir y hacer cumplir esta Política; asegurarse de que sus equipos tengan acceso y conocimiento de esta Política de Seguridad de la Información; y reportar inmediatamente cualquier caso de violaciones de seguridad de la información a través del canal de denuncias.

- **Área de Tecnologías de la Información - Corporativo**

Corresponde a esta área proponer ajustes, mejoras, ampliaciones y modificaciones a esta Política. Convocar, capacitar, coordinar, levantar actas y brindar apoyo a las reuniones en las que se discuta esta Política.
Proporcionar toda la información de gestión de seguridad de la información solicitada por los Gerentes.

- **Todos los empleados**

Es responsabilidad de todos mantenerse al día con este documento, procedimientos y normas relacionadas. En caso de dudas, el empleado debe buscar orientación del gerente inmediato y/o del gerente de TI.

6. DOCUMENTOS

- ISO/IEC 17799:2005
- ABNT 21:204.01-010
- Ley 9.609/98 – Ley de Software
- Sitio GIC – Directriz
- Política básica de seguridad de la información de 0001B_ de TI

7. REGISTROS

No se aplica.

8. ACCESORIOS

No se aplica.