Política General de Seguridad de la Información

Gestamp Automoción, S.A.

27 de febrero de 2023

INDICE

1. Introducción

Conforme a lo dispuesto en el artículo 249 bis de la Ley de Sociedades de Capital (la "**LSC**") y en el artículo 8 del Reglamento del Consejo de Administración de Gestamp Automoción, S.A. (la "**Sociedad**"), corresponde al Consejo de Administración la aprobación de las políticas generales de la Sociedad.

En virtud de lo anterior, el Consejo de Administración de Gestamp, por medio de la presente Política General de Seguridad de la Información (la "**Política**"), pretende poner de manifiesto el compromiso de la Sociedad y de las sociedades de su grupo ("**Gestamp**" o el "**Grupo**") con el cumplimiento de los mejores estándares en materia de seguridad de la información.

2. Objetivo y alcance

El objetivo principal de esta Política es proporcionar un marco regulatorio aplicable al Grupo, para la implementación de medidas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de aquella información propia y de terceros que se encuentre a disposición de Gestamp.

En este sentido, el alcance de la presente Política comprende tanto la seguridad física como la seguridad tecnológica o digital, garantizando la aplicación de medidas de seguridad de tipo organizativo, personal y técnico a fin de mantener la continuidad del negocio, prevenir el fraude, minimizar el riesgo de potenciales actuaciones maliciosas, así como proteger la información frente a potenciales daños.

3. Ámbito de aplicación

Esta Política es de aplicación global para el Grupo Gestamp. Por tanto, es de aplicación a todas las sociedades del Grupo (sin perjuicio de las particularidades derivadas de la legislación aplicable a cada una de ellas), así como a su infraestructura, redes, sistemas, equipos industriales, dispositivos y proyectos en todos los ámbitos de su actividad. Asimismo, esta Política es de obligado cumplimiento para todos los empleados, así como para el personal y colaboradores externos de Gestamp, que, para el desempeño de sus funciones, necesiten tratar información o utilizar sistemas de Gestamp.

La presente Política debe ser, por tanto, accesible para todos los empleados del Grupo, así como para el personal y colaboradores externos del mismo, que se relacionen con éste a través de alguno de sus procesos.

4. Principios

A continuación, se enumeran los principios fundamentales en materia de seguridad de la información asumidos por el Grupo:

Seguridad desde el diseño y por defecto. Se declara el compromiso de la dirección de Gestamp y de cada una de las sociedades del Grupo, de que desde el diseño y por defecto, se lleve a cabo el establecimiento, operación, monitorización, mantenimiento, revisión y mejora continua de las medidas de seguridad de la información, con especial foco en la ciberseguridad dentro del Grupo. En este sentido, se encomienda al Área de Ciberseguridad la definición de los objetivos y metas de la seguridad de la información, de cara a la protección de la confidencialidad, integridad y disponibilidad de esta.

Legalidad, eficiencia, corresponsabilidad, cooperación y coordinación. Gestamp deberá cumplir con lo establecido en la presente Política, con todos aquellos requerimientos legales, regulatorios y estatutarios que le sean de aplicación, con los requerimientos contractuales, así como con los requisitos demandados por clientes, socios, entidades gubernamentales, inversores, y resto de partes interesadas.

Responsabilidad proactiva. Las sociedades del Grupo, sus empleados, así como sus colaboradores externos estarán en disposición de poder acreditar el cumplimiento del Cuerpo Normativo de Seguridad, de forma que siempre existan pruebas o evidencias suficientes para poder demostrar dicho cumplimiento.

Prevención y mejora continua. Gestamp establece una estrategia preventiva de análisis sobre los riesgos que pudieran afectarle, identificándolos, implantando controles para su mitigación y estableciendo procedimientos regulares para su reevaluación. En el transcurso de este ciclo de mejora continua, Gestamp mantendrá la definición tanto del nivel de riesgo residual aceptado (apetito al riesgo), como de sus umbrales de tolerancia.

Registro de incidentes. Todo incidente o debilidad que pueda comprometer o haya comprometido la confidencialidad, integridad y / o disponibilidad de la Información deberá ser registrado y analizado para aplicar las correspondientes medidas correctivas y / o preventivas.

Clasificación de la información. Gestamp clasifica la información para facilitar los procesos de control de acceso, custodia y monitorización. Según el nivel de clasificación de la información, se establecen medidas y controles preventivos. Cuanto más sensible se considere la información, más restrictivos son dichos controles.

Minimización de la información. La cantidad y el tipo de información compartida se restringirá al mínimo necesario para la finalidad para la que sea solicitada. Asimismo, el uso de la información facilitada se restringirá a la finalidad para la que haya sido autorizada.

Limitación de acceso a la información. Se limitará al máximo posible el acceso a la información, de manera que no sea accesible a un número indeterminado de personas. La información de la que Gestamp es propietaria y / o depositaria deberá ser únicamente accesible para las personas debidamente autorizadas, pertenezcan o no al Grupo.

Confidencialidad e integridad. La información será tratada y compartida de tal manera que se garantice una seguridad adecuada de la misma, incluida la protección contra el acceso y uso no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

Disponibilidad. La disponibilidad de la información deberá garantizarse mediante las medidas adecuadas de respaldo y continuidad de negocio.

Formación y concienciación. El personal con responsabilidades en materia de seguridad de la información deberá disponer de la adecuada formación para ello. Asimismo, Gestamp realizará tareas para concienciar a todo su personal en el debido uso de la información y en el cumplimiento de las medidas de seguridad para ello.

5. Estructura del Cuerpo Normativo de Seguridad de la Información

El Cuerpo Normativo de Seguridad se configura como todas aquellas políticas, normas, procedimientos e instrucciones internas en materia de seguridad de la información aplicables al Grupo, y su estructura jerárquica es la siguiente:

- Nivel 1. Política General de Seguridad de la Información. Se trata del presente documento, el cual es el principal del Cuerpo Normativo de Seguridad. Establece una declaración a alto nivel de objetivos y el compromiso de Gestamp para la gestión de la seguridad de la información, así como los principios y los controles clave para asegurar la misma. Los demás componentes del Cuerpo Normativo se basan y desarrollan a partir de esta Política.
- Nivel 2. Normas y procedimientos de seguridad. Conjunto de documentos que soportan los objetivos recogidos en la Política. En este nivel se especifican los requisitos de seguridad con mayor detalle para cada sección o ámbito reflejado en la Política.
- Nivel 3. Instrucciones de trabajo. Estos documentos recogen el conjunto de tareas específicas que soportan la operativa diaria. Estas tareas están alineadas con los requisitos de seguridad establecidos en los procedimientos anteriores.

La presente Política junto con los requisitos establecidos en los diferentes procedimientos e instrucciones de trabajo de seguridad de la información que forman el Cuerpo Normativo de Seguridad de Gestamp serán de obligado cumplimiento por todos los empleados, así como por el personal y colaboradores externos del Grupo.

Este Cuerpo Normativo de Seguridad del Grupo está basado en normas y buenas prácticas de seguridad de la información tales como ISO/IEC 27001, NIST y marcos de ciberseguridad (*Cyber Security Frameworks*) y el mismo se somete a un proceso de revisión y actualización anual.

6. Gobierno de la Seguridad de la Información

Estrategia y modelo operativo

Gestamp formaliza su plan estratégico de seguridad de la información, que ha de estar alineado con su plan estratégico de negocio.

Se definen y se asignan las funciones y responsabilidades del personal del Grupo en materia de seguridad de la información para una correcta organización y desarrollo de la estrategia de Gestamp, así como para el adecuado cumplimiento del Cuerpo Normativo de Seguridad. De esta forma, se garantiza la segregación de funciones y se evitan conflictos de interés. En este sentido, podemos distinguir las siguientes áreas:

- IT Corporativo de Gestamp. Es el área encargada de cuidar, mantener, dar soporte y mejorar los sistemas e infraestructuras centrales y corporativos, además de la conectividad entre todos ellos, aplicando siempre los más altos estándares de calidad y seguridad. Es primordial el alineamiento con el negocio y con las necesidades de cada una de las fábricas y divisiones, asegurando la mayor calidad en los servicios

- Área de Ciberseguridad. Es el subárea dentro de IT Corporativo Gestamp encargada de definir los objetivos y metas de la seguridad de la información, de cara a la protección de la confidencialidad, integridad y disponibilidad de esta y de supervisar la ejecución de la estrategia para gestionar la seguridad de la información, a través de la implementación de iniciativas que permitan mejorar la protección de los procesos e infraestructuras de las crecientes ciber amenazas, siguiendo las normas, estándares y guías internacionales para los ámbitos de Gobierno, Protección, Vigilancia y Resiliencia.

- Comité Táctico de Ciberseguridad. Es el Comité encargado de la toma de decisiones, gestión de la estrategia de ciberseguridad y escalado de la información a la alta dirección. Está compuesto por el

Chief Information Officer (CIO) responsable de IT Corporativo de Gestamp y por los siguientes responsables de subáreas de IT Corporativo de Gestamp: el Director de IT Producción, el Responsable de Ciberseguridad y el Responsable de GRC IT.

Gestamp cumple con todos aquellos requerimientos legales, regulatorios y contractuales que le son de aplicación, para lo cual dispone de un marco de control asociado al Cuerpo Normativo de Seguridad para verificar y realizar un seguimiento de su cumplimiento.

Para el correcto desarrollo de las funciones del personal de Gestamp, se dispone de una estrategia de formación y concienciación en materia de seguridad de la información.

Cultura cibersegura

Gestamp fomenta la cultura de seguridad frente al ciber riesgo a todos los niveles y realiza comunicaciones periódicas sobre la estrategia y objetivos generales de ciberseguridad.

Todo el personal del Grupo recibe formación en materia de ciberseguridad de manera regular y genérica durante su vida laboral en Gestamp.

Gestión del ciber riesgo, indicadores y reporte

Gestamp dispone de una metodología de gestión de los ciber riesgos para poder implementar planes de acción cuando sea necesario. Asimismo, realiza evaluaciones y análisis con el fin de detectar los ciber riesgos a los que está sometido y así ser capaz de gestionarlos y reportarlos correctamente.

Con el objetivo de reducir la subjetividad y mejorar la precisión del seguimiento y la respuesta a los ciber riesgos, Gestamp dispone de medidas cuantitativas de ciber riesgos (KPIs) que están incluidas dentro de los riesgos operacionales.

7. Controles implementados para la Seguridad de la Información

7.1. Control de accesos

El acceso por parte del personal interno o externo a los sistemas de información de Gestamp, así como a la información que tratan o almacenan, se debe regular sobre la base de las necesidades de información y operación de cada usuario, de acuerdo con el principio *need-to-know*, otorgando acceso exclusivamente a aquellas funciones y a aquella información que cada usuario requiera para el correcto desempeño de su actividad laboral, acorde con su función y/o perfil operacional.

Los usuarios deben ser únicos y no deben ser compartidos. Todos ellos deben ser inicialmente asignados mediante el principio de Mínimo Privilegio, el cual establece que se den a un usuario los niveles (o permisos) de acceso mínimos necesarios para desempeñar sus funciones laborales.

Los responsables del tratamiento de la información deben ser los responsables de definir los niveles de acceso y de autorizar cualquier acceso extraordinario, de acuerdo con las directrices de los autorizantes o responsables de la información, o, en su caso, de los propietarios del proceso o negocio.

7.2. Seguridad en el desarrollo de software

Los requisitos de seguridad son aplicados durante todo el ciclo de vida de desarrollo del software de Gestamp, tanto en software de desarrollo propio como en aquel desarrollado por terceros, desde las fases de análisis de requerimientos y viabilidad, en las que se particularizan y evalúan dichos requisitos, hasta las fases de diseño, pruebas, implantación, aceptación y su posterior mantenimiento.

Para el correcto desarrollo de software, Gestamp dispone de un plan de pruebas de seguridad que incluye revisiones de código seguro, protección de datos, etc. Asimismo, se podrán realizar pruebas de penetración y escaneo de vulnerabilidades sobre los desarrollos de software antes de su paso a producción.

Gestamp tiene en cuenta la seguridad de la información en sus procesos y procedimientos de selección, desarrollo e implementación de aplicaciones, productos y servicios.

Gestamp realiza comunicaciones a los desarrolladores de software sobre la presente Política y sus objetivos, así como sobre otras normativas internas que forman parte del Cuerpo Normativo de Seguridad.

7.3. Seguridad de los sistemas

Gestamp establece formalmente responsabilidades y procedimientos documentados para asegurar una correcta configuración, administración, operación y monitorización de los sistemas de información.

Asimismo, Gestamp emplea medidas de protección para los sistemas de información que previenen ataques y fugas de información, y que garanticen la segregación de funciones en la asignación de responsabilidades con el objetivo de prevenir un uso no adecuado de los sistemas de información.

Para garantizar la seguridad de los sistemas, Gestamp dispone de un proceso de gestión de parches que contiene las siguientes fases basándose en los activos identificados: software base, disponibilidad, aplicabilidad, adquisición, validación y despliegue.

Gestamp realiza bastionados de sistemas para la correcta implantación del Cuerpo Normativo de Seguridad, el endurecimiento y delimitación clara de los privilegios de usuarios, grupos, roles y la configuración de servicios.

7.4. Protección contra malware

Gestamp dispone de medidas para detectar, eliminar y proteger los sistemas de información contra los diferentes tipos de software malicioso conocidos. Se realizan, como mínimo, con carácter anual, evaluaciones donde se identifican y evalúan las nuevas amenazas, con el objetivo de verificar que los sistemas están preparados para contenerlas y confirmar qué nuevos sistemas pueden estar expuestos a las mismas. De este modo, todos los sistemas de información de Gestamp cuentan con soluciones actualizadas para la protección contra el malware.

Gestamp dispone de software *End Point Protection* (EPP) en servidores y puestos de trabajo, y realiza actualizaciones de estos de forma automática. Está totalmente prohibido desactivar o alterar los mecanismos EPP o herramientas existentes de este tipo, por parte de usuarios que no estén autorizados y que no tengan una necesidad técnica autorizada por el Área de Ciberseguridad.

7.5. Seguridad de las redes

Gestamp gestiona y controla las redes de manera adecuada, a fin de protegerse de las amenazas y mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluido el control de acceso a la red, protegiendo de este modo toda la información que se transfiera a través de estos elementos y/o entornos.

La información transmitida por redes de comunicaciones, públicas o privadas, es adecuadamente protegida mediante mecanismos de seguridad que garantizan su confidencialidad, disponibilidad e integridad. Se establecen los controles necesarios que impiden la suplantación del emisor, modificación o pérdida de la información transmitida, tanto en las comunicaciones con sistemas situados en las redes internas, como con entidades con las que Gestamp tenga relación.

En cuanto a la conexión remota a las redes de Gestamp, se establece un conjunto de tecnologías y controles de seguridad según el perfil de usuario.

La red inalámbrica para invitados está separada de las demás redes y dispone de medidas de seguridad como autenticación, monitorización, cifrado, etc.

Todas las conexiones a las redes corporativas de Gestamp deberán cumplir con los requerimientos técnicos establecidos por el Grupo, y cualquier excepción deberá ser previamente revisada y autorizada por el Área de Ciberseguridad.

7.6. Seguridad de los dispositivos de usuario final

Gestamp dispone de directrices de uso y manejo de los dispositivos corporativos, que hacen uso de los servicios de información del Grupo.

Los usuarios no pueden ser administradores locales de los dispositivos corporativos puestos a su disposición y queda prohibida la manipulación de los mismos tanto en hardware como en configuraciones, no permitiéndose la instalación de software no aprobado por IT Corporativo de Gestamp.

7.7. Seguridad de los recursos humanos

Las responsabilidades en materia de seguridad son consideradas en el proceso de selección de personal, en la elaboración de los contratos, y son comunicadas una vez iniciada la relación laboral, a fin de reducir los riesgos de manipulación, robo, fraude o uso inadecuado de la información.

En este sentido, las obligaciones contractuales para los empleados reflejan las políticas y normas de seguridad de la información de Gestamp. Los términos y condiciones incluyen aspectos como la confidencialidad, derechos legales, responsabilidades para el cumplimiento del Cuerpo Normativo de Seguridad y para el tratamiento de información de terceros y acciones a tomar si la persona no cumple con los requisitos de seguridad.

Asimismo, Gestamp comunica al personal las responsabilidades de seguridad de la información que le son aplicables desde su incorporación y después de la finalización de la relación laboral.

Todo el personal del Grupo recibe un nivel adecuado de formación y concienciación en materia de seguridad de la información, y es informado correctamente de sus funciones y responsabilidades en esta materia.

7.8. Seguridad física y del entorno

Las instalaciones del Grupo, incluidas oficinas y plantas productivas, donde se lleva a cabo la actividad laboral, así como las instalaciones propias o de terceros donde se ubican los sistemas de información del Grupo, están adecuadamente protegidas mediante controles de acceso perimetrales, sistemas de video vigilancia y medidas preventivas de accidentes, de manera que pueden evitarse incidentes de seguridad y/o ambientales.

Gestamp establece medidas de seguridad para proteger los activos físicos, y establece procedimientos que contemplan el almacenamiento, manipulación, transporte y destrucción de la información sensible soportada tanto en formato papel como en soportes informáticos, con el fin de mitigar el riesgo de acceso no autorizado y hurto.

7.9. Gestión de la información

Gestamp dispone de medidas de seguridad en cada una de las fases del ciclo de vida de la información: creación, distribución, tratamiento, almacenamiento y borrado/ destrucción.

Gestamp dispone de procedimientos y periodos de retención, almacenamiento y destrucción de información, y estos son revisados y actualizados conforme a la normativa aplicable en cada momento.

Gestamp clasifica la información corporativa para facilitar los procesos de control de acceso, custodia y monitorización. Según el nivel de clasificación de la información, se establecen medidas y controles preventivos. Cuanto más confidencial se considere la información más restrictivos son dichos controles.

7.10. Privacidad de los datos

En los sistemas y aplicaciones donde se tratan datos de carácter personal o sensible, Gestamp dispone de requisitos de privacidad especiales para evitar el acceso inadecuado, robo y divulgación de dichos datos.

En la externalización de procesos de Gestamp que conlleven el acceso o tratamiento de datos personales o sensibles, se establecen contratos de encargo de tratamiento de datos y acuerdos de confidencialidad con los proveedores externos para asegurar la privacidad de los datos durante todo su ciclo de vida.

En este sentido, Gestamp dispone de una Política de Protección de Datos que recoge las garantías y principios aplicables en esta materia, contando asimismo con una serie de normas, instrucciones y procedimientos adicionales destinados a la aplicación más detallada de dichas garantías y principios. Gestamp adopta las medidas de índole técnica y organizativas necesarias que garantizan la seguridad de los datos de carácter personal y evitan su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos.

7.11. Seguridad en Cloud

Gestamp solicita a los proveedores de servicios *cloud*, toda la información correspondiente a sus controles y medidas de seguridad, y se comprueba que estos controles estén alineados con los estándares de seguridad *cloud* exigidos por Gestamp.

En este sentido, Gestamp se asegura de que los proveedores de servicios *cloud* disponen de los mecanismos necesarios para reportar los incidentes de seguridad que afecten a la integridad, confidencialidad y disponibilidad de la información, conforme a la legislación aplicable.

Además, se tienen en cuenta, en los planes de gestión de incidentes y de continuidad de negocio, los servicios que están externalizados en proveedores de servicios *cloud*. Del mismo modo, se realizan las auditorías necesarias para garantizar la protección del entorno *cloud.*

La información que reside en un entorno *cloud* privado tiene las mismas medidas de seguridad que la información que reside habitualmente en las infraestructuras propiedad del Grupo.

Por su parte, la información que reside en un entorno *cloud* público es evaluada previamente por el Comité Táctico de Ciberseguridad, quien define las medidas específicas de seguridad a implantar, considerando las técnicas de cifrado, anonimización, ofuscación y tokenización de la información.

7.12. Gestión del riesgo de terceras partes

Gestamp pone especial atención a la evaluación de la criticidad de todos los servicios susceptibles de ser subcontratados de manera que puedan identificarse aquellos que sean relevantes desde el punto de vista de la seguridad de la información, ya sea por su naturaleza, la sensibilidad de los datos que deban tratarse o la dependencia sobre la continuidad del negocio.

Sobre los proveedores de estos servicios, se priorizan los procesos de selección, requerimientos contractuales, la monitorización de los niveles de servicio y las medidas de seguridad implantadas por dichos proveedores, siendo además obligatoria la presentación de evidencias sobre el buen estado del proveedor en materia de cumplimiento con la legislación fiscal y laboral. Estos controles sobre los proveedores de dichos servicios se revisan con carácter anual.

Asimismo, Gestamp dispone de procesos formales para la finalización de la relación con los proveedores, que incluyen cláusulas contractuales específicas para asegurar la privacidad y el retorno de la información una vez finalizado el servicio.

7.13. Vigilancia

Pruebas de penetración y análisis de vulnerabilidades

Gestamp realiza escaneos de vulnerabilidades de acuerdo con la planificación anual realizada, con el objetivo de examinar la seguridad de los sistemas y aplicaciones y de desarrollar planes de remediación. El alcance, la metodología y la cobertura de estas pruebas se ajustan en función de los niveles de riesgo de los sistemas y aplicaciones, así como por la criticidad de los activos.

Las pruebas de penetración se realizan con diferentes compañías proveedoras, con el objetivo de modificar metodologías, pero garantizando un seguimiento comparativo sobre las mejoras. Se realiza un proceso de evaluación del riesgo en la fase de selección de dichas pruebas de penetración.

Análisis de ciberseguridad

Gestamp dispone de procesos que analizan el comportamiento de usuarios con el objetivo de detectar comportamientos anómalos y patrones de ataque. Asimismo, dispone de procesos para detectar actividades fraudulentas potencialmente dañinas. Estos procesos generan alertas al equipo de respuesta a incidentes.

Del mismo modo, se analizan las redes y los sistemas de Gestamp para detectar anomalías en su comportamiento.

Monitorización de eventos de seguridad

Gestamp dispone de un servicio de registro, correlación y monitorización de eventos y tratamiento de alertas. Toda actividad crítica es registrada y monitorizada por los dispositivos de seguridad.

En este sentido, la recolección y correlación de registros se realiza de manera 24x7 y se utiliza para apoyar investigaciones, realizar análisis forenses y dar respuesta a requerimientos regulatorios.

Asimismo, se conserva el historial de registros por parte de los sistemas durante, al menos, dos años para el personal autorizado por el Grupo para acceder a estos registros.

A este respecto, el registro de *logs* es únicamente accesible para aquellos empleados que, por motivos de su trabajo, necesiten tener acceso a estos y, además, se protegen los archivos que almacenan los *logs* para evitar modificaciones no autorizadas y se realizan copias de seguridad de todos los registros.

Monitorización y control de equipos y recursos de tecnologías de información y comunicación

Gestamp es propietaria de los equipos y recursos de tecnologías de información y comunicación que pone a disposición de sus directivos y empleados, así como de la información contenida en los mismos.

Los equipos y recursos de tecnologías de información y comunicación y la información contenida en ellos sólo podrán ser utilizados por los empleados y directivos de Gestamp para el desarrollo de sus funciones y en ningún caso con fines de uso personal, de ocio o ilegal.

Gestamp podrá libremente tratar, almacenar, monitorizar, borrar o destruir definitivamente cualquier dato, información o comunicación contenida, permanente o temporalmente en los equipos y recursos de tecnologías de información y comunicación de su propiedad, respetando siempre los derechos de privacidad, propiedad intelectual o industrial, o cualesquier otro derecho o interés legítimo previsto en el ordenamiento jurídico.

7.14. Resiliencia

Gestión de incidentes

Gestamp dispone de un proceso de respuesta ante incidentes de seguridad de la información para gestionar de forma correcta todas las amenazas materializadas en el Grupo. Este proceso incluye aspectos como la monitorización, seguimiento, clasificación y remediación de dichos incidentes.

Todo incidente que pueda comprometer o haya comprometido la confidencialidad, integridad y/o disponibilidad de la información es registrado y analizado para aplicar las correspondientes medidas correctivas y/o preventivas según lo establecido en el Procedimiento de Gestión de Incidentes Gestamp.

Todos los empleados del Grupo, así como el personal y colaboradores externos tienen la obligación y responsabilidad de notificar a los responsables de seguridad de la entidad, de cualquier sospecha, incidente o delito que pueda comprometer la seguridad de los activos de información del Grupo.

Además, se establece un plan anual de simulaciones que ayudan al entrenamiento y concienciación del personal del Grupo.

Gestión de la continuidad de negocio

Gestamp dispone de un plan de continuidad de negocio para garantizar la continuidad en la prestación de sus servicios vitales y el adecuado manejo de los impactos sobre el negocio ante posibles escenarios de crisis, proporcionando un marco de referencia para actuar en caso de ser necesario.

En el desarrollo de este plan, se considera no solo el plan de contingencia de sistemas de información, sino también las dependencias físicas, las personas que dan soporte a la actividad del negocio y los recursos que estas puedan necesitar para que el Grupo pueda seguir desarrollando su actividad productiva y de atención a sus clientes.

El plan de contingencia se desarrolla e implementa para asegurar que los procesos críticos de negocio pueden restablecerse en el tiempo requerido, incluyendo controles para identificar y reducir los riesgos, limitar las consecuencias de los incidentes que afectan negativamente, y asegurar el tiempo de respuesta de las operaciones esenciales. Dentro de este plan, son partes fundamentales la formación a los componentes del equipo de gestión de crisis, así como el ejercicio de ensayo y verificación regular sobre los planes de respuesta definidos.

Este plan es publicado y, además, revisado con carácter anual o con motivo de cambios importantes tales como la incorporación de nuevos activos inmobiliarios, tecnológicos u organizativos.

Toda la información sensible, confidencial o datos de carácter personal están registrados en copias de respaldo. La gestión de estas copias de seguridad se realiza y conserva de acuerdo con las medidas de seguridad definidas por Gestamp.

8. Cumplimiento

Gestamp debe verificar el cumplimiento de la presente Política con carácter anual.

La dirección de Gestamp velará por promover y apoyar el establecimiento de medidas técnicas, organizativas y de control que garanticen la autenticidad, integridad, disponibilidad, confidencialidad y auditabilidad de la información.

La gestión de esta Política corresponde al Área de Ciberseguridad, que deberá, por tanto, interpretar las dudas que puedan surgir en su aplicación, así como proceder a su revisión cuando sea necesario o requerido, para proponer la actualización de su contenido.

La Dirección de Auditoría Interna del Grupo podrá efectuar cuantos análisis y verificaciones considere convenientes para constatar la correcta aplicación de los aspectos contenidos en esta Política.

La Comisión de Auditoria supervisará el cumplimiento de esta Política con carácter anual, dando cuenta de ello al Consejo de Administración.

Cualquier violación de esta Política puede resultar en la adopción de las medidas disciplinarias correspondientes. Es responsabilidad de todos los empleados del Grupo, así como del personal y colaboradores externos notificar al Área de Ciberseguridad cualquier evento o situación que pudiera suponer el incumplimiento de la presente Política.

9. Excepciones

Toda excepción a la presente Política debe ser notificada al Área de Ciberseguridad la cual deberá autorizarla, en su caso, con carácter previo a su puesta en práctica, así como registrar las excepciones autorizadas.

10. Referencias

La presente Política cumple con los siguientes estándares internacionales y normativa en materia de seguridad de la información:

- ISO/IEC 27001 "Information technology - Security techniques - Information security management systems - Requirements".
- ISO/IEC 27002 "Information technology — Security techniques — Code of practice for information security controls".
- Reglamento General de Protección de Datos (GDPR)
- Cyber Security Framework

11. Aprobación y revisión

Esta Política ha sido aprobada por el Consejo de Administración de la Sociedad y cualquier modificación de la misma, requerirá de la aprobación por dicho órgano, previa propuesta de la Comisión de Auditoría.

Esta Política será objeto de revisión con carácter anual por el Comité Táctico de Ciberseguridad con el apoyo, en su caso, del Área de Ciberseguridad.

Versión	Emisor	Supervisor	Órgano de aprobación	Entidad	Fecha aprobación
1.0	Corporate IT	Comisión de Auditoría	Consejo de Administración	GESTAMP AUTOMOCIÓN, S.A.	27 de febrero de 2023