Contenido

1. OBJETIVO

Establecer un conjunto de normas, procedimientos y directrices que describan cómo gestiona y protege la organización sus datos sensibles y activos de información.

2. ALCANCE

Los lineamientos de la presente política son de obligatorio cumplimiento para todos los colaboradores de Teleperformance MAR (Colombia, Guyana, Nicaragua, Perú Y Trinidad y Tobago), incluyendo empleados directos e indirectos, contratistas, subcontratistas y proveedores, que brinden soporte a la organización tanto desde las instalaciones físicas como desde teletrabajo.

3. RESPONSABILIDAD

- La **Alta Dirección** es responsable de garantizar los recursos y el apoyo necesarios para el cumplimiento de esta política.
- El Equipo del SGSI es responsable de realizar revisiones anuales del Sistema de Gestión de la Seguridad de la Información (SGSI), incluida toda la información documentada y las actividades relacionadas.
- Los proveedores de servicios, como vendedores, proveedores y contratistas, deben conocer y cumplir las políticas de la organización.
- El equipo de comunicación y relaciones públicas asegurará la comunicación y divulgación de forma física o digital dentro de la organización y accesibilidad de las partes interesadas internas y externas pertinentes.
- Los líderes de las unidades operativas son responsables de tener en cuenta esta política en todos los aspectos de sus funciones y servicios empresariales críticos.

4. AUTORIDAD

- Aprobación: Alta Dirección
- Revisión y actualización: Líder del sistema de gestión de Seguridad de la Información *(ISMS).*

5. DEFINICIÓN DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

El Sistema de Gestión de Seguridad de la Información (SGSI) es un enfoque sistemático para administrar información confidencial con el fin de que permanezca segura. Este Implica establecer políticas, procedimientos y procesos para gestionar los riesgos y garantizar la confidencialidad, integridad y disponibilidad de los activos de la información.

6. CONTENIDO ESPECIFICO DE LA POLÍTICA.

Pilares de la política:

- Confidencialidad: Protección de datos e información sensibles frente a accesos o divulgaciones no autorizadas, tanto internas como externas.
- Integridad: Garantizar que los datos y la información son precisos, completos, fiables, y que no se modifican ni manipulan de ninguna manera.
- Disponibilidad: Garantizar que los datos y la información estén disponibles para los usuarios autorizados cuando los necesiten, y que no estén sujetos a tiempos de inactividad o interrupciones.
- Rendición de cuentas: Garantizar que las personas son responsables y rinden cuentas de sus acciones en relación con la seguridad de la información, y que se toman las medidas adecuadas en caso de incumplimiento.
- Cumplimiento: Garantizar que la organización cumple las leyes, reglamentos y normas aplicables relacionados con la seguridad de la información, como TP Global, SOC 1, SOC 2, GDPR, HIPAA, PCI DSS, ISO 27701 e ISO 27001.
- Gestión de riesgos: Garantizar que la organización identifique, evalúe y gestione los riesgos de seguridad de la información, que se establezcan controles y medidas adecuadas para mitigar estos riesgos.
- Continuidad: Garantizar que la organización pueda seguir funcionando y prestando servicios en caso de que se produzca un incidente disruptivo, como riesgos medioambientales, políticos, pérdida de servicios públicos, cortes relacionados con la tecnología y ciberataques.
- Concienciación: Garantizar que todos los empleados y partes interesadas conozcan las políticas y procedimientos de seguridad de la información de la organización y reciban formación sobre cómo identificar y responder a las amenazas e incidentes de seguridad.

6.1. Políticas de seguridad de la información

6.1.1. Dirección de gestión para la seguridad de la información

6.1.1.1. Seguridad de la Información cuenta con un conjunto de políticas aprobadas por la dirección. Estas serán puestas a la disposición de empleados entes externos.

6.1.1.2. Las políticas de seguridad de la información son revisadas anualmente o cuando se produzcan cambios significativos para garantizar su relevancia y eficacia.

6.2. Organización de la seguridad de la información

6.2.1. Organización interna

6.2.1.1. Se definirán y asignarán todas las responsabilidades en materia de seguridad de la información.

6.2.1.2. Se deben segregar los deberes y responsabilidades en conflicto para reducir las oportunidades de modificación no autorizada, involuntaria y/o el uso indebido de los activos de la organización.

6.2.1.3. Se deben mantener actualizados y documentados los contactos con las autoridades pertinentes y los grupos de interés especial.

6.2.1.4. Se deben mantener contactos con los grupos de interés especial tales como foros de seguridad y otras asociaciones profesionales relacionadas.

6.2.1.5. Se debe incluir a seguridad de la información desde el inicio de cada proyecto.

6.2.2. Dispositivos móviles

6.2.2.1. La organización debe seguir la política local y global y las medidas de seguridad relacionadas con el uso de dispositivos móviles.

6.2.3. Teletrabajo

6.2.3.1. La organización debe seguir las políticas y procedimientos locales y globales relacionadas con el modelo de teletrabajo de la organización.

6.2.3.2. Los empleados son responsables de proteger la información y sistemas de la organización desde teletrabajo.

6.2.3.3. La organización proporcionará a los empleados capacitaciones regulares y campañas de conciencia adecuadas sobre la seguridad de la información en el contexto de teletrabajo.

6.2.3.4. Las violaciones de esta política pueden resultar en medidas disciplinarias, incluyendo la terminación del contrato.

6.2.3.5. El acceso a la información y los sistemas de la organización desde un entorno doméstico estará restringido solo a personas autorizadas.

6.2.3.6. Las redes externas utilizadas para acceder a la información y los sistemas de la organización se protegerán mediante controles técnicos apropiados, como VPN, MFA, firewalls y cifrado.

6.2.3.7. Los dispositivos utilizados para acceder a la información y los sistemas de la organización desde teletrabajo estarán protegidos por EDR y antimalware, serán monitoreados, escaneados por vulnerabilidades y actualizados regularmente con los últimos parches de seguridad.

6.2.3.8. La organización supervisará y probará regularmente sus controles de seguridad de la información en el contexto de teletrabajo para garantizar su efectividad.

6.2.3.9. Seguridad de la Información es responsable de implementar y hacer cumplir esta política, así como de proporcionar los recursos y el apoyo necesarios para mantener la seguridad de la información desde teletrabajo.

6.3. Seguridad de los recursos humanos

6.3.1. Antes del empleo

6.3.1.1. Se debe realizar la verificación de antecedentes de todos los candidatos de conformidad con las leyes y reglamentos pertinentes, los requisitos del negocio y la clasificación de la información a la que el empleado tendría acceso.

6.3.1.2. Los acuerdos contractuales con empleados y terceros deben indicar sus responsabilidades y las de la organización en materia de seguridad de la información.

6.3.2. Durante el empleo

6.3.2.1. Todos los empleados y contratistas deben respetar las políticas y procedimientos establecidas por la organización en cuanto a seguridad de la información.

6.3.2.2. Todos los empleados y terceros deben recibir periódicamente una formación adecuada en relación con las políticas y procedimientos de la organización en cuanto a seguridad de la información.

6.3.2.3. Se debe contar con un proceso disciplinario formal contra los empleados que han cometido una violación de la seguridad de la información.

6.3.3. Terminación y cambio de empleo

6.3.3.1. Las responsabilidades y deberes de seguridad de la información que siguen siendo válidos aún luego de la terminación o el cambio de empleo.

6.4. Manejo de Activos

6.4.1. Responsabilidad por los activos

6.4.1.1. Se deben identificar los activos asociados con la información y el procesamiento de la información.

6.4.1.2. El inventario debe contar con la información del propietario de cada activo.

6.4.1.3. Se deben mantener normas para el uso aceptable de la información y de los activos asociados con la información y las instalaciones de tratamiento de la información.

6.4.1.4. Todos los empleados y terceros deberán devolver los activos de la organización al término de su contrato o convenio.

6.4.2. Clasificación de la información

6.4.2.1. La información se debe clasificar de acuerdo con los requisitos legales, valor, criticidad y sensibilidad a la divulgación no autorizada o modificación.

6.4.2.2. Se debe seguir el procedimiento para el etiquetado de la información.

6.4.2.3. La organización debe cumplir con los procedimientos y políticas documentados relacionados con la clasificación de la información.

6.4.3. Manejo de medios

6.4.3.1. Se aplicarán los procedimientos de clasificación de la información para la manipulación de activos.

6.4.3.2. Se debe eliminar la información de forma segura cuando ya no sea necesaria, utilizando procedimientos documentados por la organización.

6.4.3.3. Se deben proteger los medios contra el mal uso, acceso o modificación no autorizada durante el transporte o almacenamiento.

6.5. Control de acceso

6.5.1. Requisitos empresariales de control de acceso

6.5.1.1. Se cuenta con una política de control de acceso revisada periódicamente, en función de los requisitos de seguridad empresarial y de la información.

6.5.1.2. A los usuarios solo se les aprovisionará acceso a los sistemas que han sido específicamente autorizados a utilizar, con base en el principio de menor privilegio.

6.5.2. Gestión del acceso de usuarios

6.5.2.1. Se cuenta con un proceso formal de aprovisionamiento y des-aprovisionamiento para el registro y la asignación de accesos a los usuarios.

6.5.2.2. Se aplicará el proceso formal de aprovisionamiento y des-aprovisionamiento para asignar o revocar accesos de usuarios para todos los sistemas.

6.5.2.3. Los accesos privilegiados serán restringidos y controlados.

6.5.2.4. Se controla mediante el proceso formal la asignación de autenticación secreta.

6.5.2.5. Los propietarios de los activos deben revisar periódicamente los derechos de acceso de los usuarios.

6.5.2.6. Se deben terminar y/o modificar los accesos a empleados y terceros dentro de las siguientes 24 horas, luego de recibir la notificación formal de terminación de empleo contrato, acuerdo, o cambio de rol.

6.5.3. Responsabilidades del usuario

6.5.3.1. Es responsabilidad de los usuarios cumplir con las políticas y buenas prácticas en relación con la autenticación secreta de usuarios.

6.5.4. Control de acceso a sistemas y aplicaciones

6.5.4.1. Los accesos y funciones a sistemas y aplicaciones deben estar restringidos en cumplimiento con la política de control de acceso.

6.5.4.2. Cuando sea necesario se deberá emplear un procedimiento de inicio seguro de sesión de acuerdo con la política de control de acceso.

6.5.4.3. Se deberá aplicar la política de gestión de contraseña para garantizar contraseñas de calidad.

6.5.4.4. Se debe restringir y controlar el uso de programas capaces de anular los controles del sistema y aplicaciones.

6.5.4.5. Se debe restringir el acceso al código fuente de programas y aplicaciones.

6.6. Criptografía

6.6.1. Controles criptográficos

6.6.1.1. Se cuenta con una política sobre el uso de controles criptográficos para la protección de la información.

6.6.1.2. Se aplicará la política sobre el uso de las claves criptográficas a lo largo de todo su ciclo de vida.

6.7. Seguridad física y ambiental

6.7.1. Áreas seguras

6.7.1.1. Se deben definir los perímetros de seguridad para proteger las zonas que puedan contener información confidencial, crítica, así como las instalaciones de procesamiento.

6.7.1.2. Las zonas seguras deben estar protegidas por controles de acceso adecuados que solo permitan el ingreso al personal autorizado.

6.7.1.3. Se debe aplicar la seguridad física al diseño de las oficinas, salas e instalaciones.

6.7.1.4. Las instalaciones deben contar con protección física contra desastres naturales, ataques maliciosos o accidentes.

6.7.1.5. Se deben aplicar los procedimientos establecidos para trabajar en zonas seguras.

6.7.1.6. Las áreas de entrega, carga y otros puntos de acceso deben estar protegidos contra accesos no autorizados. Cuando sea viable, estas áreas deben estar aisladas de los centros de procesamiento.

6.7.2. Equipamiento

6.7.2.1. Los equipos deben estar ubicados para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para accesos no autorizados.

6.7.2.2. Los equipos deben estar protegidos contra fallos de alimentación y otras interrupciones de energía.

6.7.2.3. Se debe proteger el cableado de alimentación y telecomunicaciones contra la interceptación, interferencia o daño.

6.7.2.4. Los equipos se deben mantener para garantizar su continuidad disponibilidad e integridad.

6.7.2.5. Los equipos solo pueden salir de las instalaciones cuando se cuente con autorización previa.

6.7.2.6. Para los activos de la información se deben tomar en cuenta los riesgos asociados al encontrarse fuera de las instalaciones.

6.7.2.7. Cuando sea necesario se deben validar todos los equipos que contengan medios de almacenamiento. Para asegurar que toda la información confidencial ha sido eliminada de forma correcta.

6.7.2.8. Los usuarios no deben dejar sus equipos desatendidos sin la protección adecuada.

6.7.2.9. Se debe cumplir con la política de escritorios limpios de la organización.

6.8. Seguridad de las operaciones

6.8.1. Procedimientos y responsabilidades operacionales

6.8.1.1. Los procedimientos y responsabilidades de las operaciones deben estar a la disposición de quienes así lo requieran.

6.8.1.2. Se deben controlar y documentar los cambios que pudieran afectar a la seguridad de la información.

6.8.1.3. Se debe monitorear el uso de los recursos y realizar proyecciones que permitan ajustar estos para garantizar el apropiado rendimiento de los sistemas.

6.8.1.4. Los ambientes de desarrollo, pruebas y producción deben estar segregados para mitigar los riesgos de cambios no autorizados, incidentes y fallas.

6.8.2. Protección contra malware

6.8.2.1. Se debe contar con controles y herramientas apropiadas para la detección, prevención y recuperación contra amenazas de tipo malware.

6.8.3. Copia de seguridad

6.8.3.1. Se debe contar con copias regulares de seguridad según la criticidad de la información y realizar pruebas de restauración para asegurar la integridad de estas copias.

6.8.4. Registro y monitoreo

6.8.4.1. La organización debe contar con un registro de eventos en donde se puedan encontrar actividades, excepciones, errores, información del usuario, y eventos de seguridad.

6.8.4.2. Las instalaciones y los registros de eventos deben estar protegidos contra la manipulación y el acceso no autorizado.

6.8.4.3. Se deben mantener, proteger y revisar regularmente los registros sobre las actividades de los usuarios privilegiados.

6.8.4.4. Se debe contar con una configuración de servidor NTP, para asegurar la sincronización a nivel de dominio.

6.8.5. Control de software operativo

6.8.5.1. Cuando sea necesario, se deben aplicar restricciones para controlar la instalación y ejecución de software en los sistemas.

6.8.6. Gestión técnica de vulnerabilidades

6.8.6.1. Se realizarán análisis periódicos de vulnerabilidad. Los resultados deben ser reportados oportunamente a las áreas responsables y estas vulnerabilidades deben ser mitigadas dentro de los plazos establecidos en las políticas de la organización y los marcos normativos aplicables.

6.8.6.2. La organización debe implantar los controles necesarios para restringir la instalación de software no autorizado.

6.8.6.3. Las aprobaciones de instalaciones de software deben documentarse adecuadamente en el sistema de tickets de la organización.

6.8.7. Consideraciones sobre la auditoría de los sistemas de información

6.8.7.1. Las pruebas técnicas que pudieran producir interrupciones en el servicio deben ser planificadas y acordadas para minimizar este riesgo.

6.9. Seguridad de las comunicaciones

6.9.1. Gestión de la seguridad de la red

6.9.1.1. Se debe gestionar y controlar las redes para proteger la información, sistemas y aplicaciones.

6.9.1.2. Se deben identificar e incluir los mecanismos de seguridad, niveles de servicio y demás requisitos en los acuerdos de prestación de servicios de red.

6.9.1.3. Se deben segregar en redes distintas los servicios de información, usuarios y sistemas de la información.

6.9.2. Transferencia de información

6.9.2.1. Se debe proteger la seguridad de la información durante la transferencia, aplicando las prácticas establecidas en el procedimiento formal de transferencia de información.

6.9.2.2. Cuando sea necesario, los acuerdos deben reflejar las condiciones generales para la transferencia segura de información entre la organización y terceros.

6.9.2.3. Solo se utilizarán canales seguros, para la transmisión de información mediante mensajería electrónica.

6.9.2.4. Cuando sea necesario, la organización debe contar con acuerdos de confidencialidad o no divulgación para la protección de la información.

6.10. Adquisición, desarrollo y mantenimiento de sistemas

6.10.1. Requisitos de seguridad de los sistemas de información

6.10.1.1. Se deben incluir los requisitos relacionados con la seguridad de la información en los nuevos sistemas y/o mejoras a los sistemas existentes.

6.10.1.2. Se debe proteger adecuadamente toda la información que se transmita mediante redes públicas contra actividades fraudulentas, disputas contractuales, divulgación y modificación no autorizada.

6.10.1.3. Se debe proteger adecuadamente toda la información para evitar la transmisión incompleta, el enrutamiento incorrecto, alteración, divulgación, duplicación o reproducción.

6.10.2. Seguridad en los procesos de desarrollo y soporte

6.10.2.1. Para desarrollos internos, se debe seguir la política de desarrollo seguro aplicable a programas informáticos y sistemas.

6.10.2.2. Se deben controlar los cambios relacionados con el ciclo de vida del desarrollo.

6.10.2.3. Se debe asegurar completar las pruebas necesarias, que garanticen que no haya efectos adversos ni impacto en las operaciones o la seguridad de la organización.

6.10.2.4. Se debe evitar realizar modificaciones a los paquetes de software y los cambios necesarios deben estar controlados.

6.10.2.5. Se deben aplicar documentar y mantener buenas prácticas y principios de desarrollo seguro en la ingeniería de los sistemas.

6.10.2.6. Se debe establecer y proteger adecuadamente la seguridad en los entornos de desarrollo y la integración de sistemas durante todo su ciclo de vida.

6.10.2.7. Cuando sea necesario, se debe monitorear las actividades de terceros en el desarrollo de sistemas.

6.10.2.8. Se deben realizar pruebas de la funcionalidad y seguridad durante el desarrollo.

6.10.2.9. Se deben emplear los criterios establecidos para la aceptación de pruebas a nuevos sistemas, actualizaciones y nuevas versiones.

6.10.3. Datos de prueba

6.10.3.1. Se debe proteger y controlar los datos de prueba con base en la política y controles relacionados.

6.11. Relaciones con proveedores

6.11.1. Seguridad de la información en las relaciones con los proveedores

6.11.1.1. Se debe acordar y documentar los requisitos de seguridad de la información, para mitigar los riesgos asociados con el acceso de terceros a los activos de la organización.

6.11.1.2. Se debe acordar y documentar los requisitos de seguridad de la información, para que los terceros puedan acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la organización.

6.11.1.3. Se debe incluir en los acuerdos con terceros los riesgos de seguridad de la información asociados con los servicios de tecnología de comunicaciones y cadena de suministro de productos y/o servicios.

6.11.2. Gestión de la prestación de servicios a proveedores

6.11.2.1. Se debe supervisar, revisar y auditar regularmente a los terceros que prestan servicios para la organización.

6.11.2.2. Se deben considerar los cambios en la prestación de servicios por parte de los terceros, incluidos mantener y mejorar las políticas de seguridad de la información existentes y la reevaluación periódica de los riesgos.

6.12. Gestión de incidentes de seguridad de la información

6.12.1. Gestión de incidentes y mejoras de seguridad de la información

6.12.1.1. Se debe seguir el plan de respuesta a incidentes en donde se definen las responsabilidades y procedimientos, para garantizar una óptima respuesta a los incidentes de seguridad.

6.12.1.2. Se debe realizar la notificación oportuna de incidentes, de acuerdo con el plan de respuesta a incidentes y los requerimientos contractuales.

6.12.1.3. Los empleados y terceros tienen la responsabilidad de notificar sobre cualquier información o sospecha de debilidad de seguridad de la información relacionada con sistemas y/o servicios.

6.12.1.4. Se deben revisar todos los eventos de seguridad de la información antes de definir si estos pueden ser clasificados como incidentes de seguridad de la información.

6.12.1.5. Los incidentes de seguridad de la información se deben responder de acuerdo con el plan de respuesta a incidentes y políticas aplicables.

6.12.1.6. Se debe aplicar el principio de mejora continua con base en los incidentes previos, para reducir el impacto y la probabilidad de ocurrencia en incidentes futuros.

6.12.1.7. Se debe asegurar seguir los procesos documentados para la identificación, recopilación, adquisición y conservación de información que pudiera servir como evidencia en relación con los posibles incidentes.

6.13. Aspectos de seguridad de la información de la gestión de la continuidad del negocio

6.13.1. Continuidad de la seguridad de la información

6.13.1.1. Se debe contar con los requisitos necesarios para la continuidad de la seguridad de la información durante eventos potencialmente disruptivos.

6.13.1.2. Se deben establecer, documentar, implementar y mantener procesos, procedimientos y controles que garanticen la continuidad de la seguridad de la información durante eventos potencialmente disruptivos.

6.13.1.3. Se debe validar de forma periódica los controles, procedimientos y políticas establecidas, para garantizar la eficacia de la continuidad de la seguridad de la información durante eventos potencialmente disruptivos.

6.13.2. Redundancias

6.13.2.1. Se debe considerar contar con una adecuada redundancia en las instalaciones de procesamiento de información, para cumplir con los requisitos de disponibilidad.

6.14. Cumplimiento

6.14.1. Cumplimiento de los requisitos legales y contractuales

6.14.1.1. Se debe cumplir con todos los requisitos legislativos, reglamentarios y contractuales aplicables para la organización.

6.14.1.2. Se deben aplicar los procedimientos adecuados para garantizar el cumplimiento con los requisitos legislativos, reglamentarios, contractuales, derechos de propiedad intelectual y de uso de software aplicables para la organización.

6.14.1.3. Se deben proteger adecuadamente los registros contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de cumplimiento con los requisitos legislativos, regulatorios y contractuales.

6.14.1.4. Se debe proteger adecuadamente la privacidad y la protección de la información de identificación personal según los requisitos legislativos, reglamentarios, y contractuales aplicables.

6.14.1.5. Cuando sea necesario, se deben usar controles criptográficos de conformidad con los requisitos legislativos, reglamentarios, y contractuales aplicables.

6.14.2. Revisiones de seguridad de la información

6.14.2.1. Se deben realizar revisiones anuales sobre seguridad de la información y su implementación en la organización, para garantizar el cumplimiento de los controles, políticas, procedimientos y objetivos.

6.14.2.2. Se debe revisar anualmente el cumplimiento con las políticas de seguridad de la información y cualquier otro marco normativo aplicable en la organización.

6.14.2.3. Se deben revisar anualmente los sistemas de información, para comprobar su cumplimiento con las políticas de seguridad de la información y cualquier otro marco normativo aplicable en la organización.

7. CONTROL DE CAMBIOS Y CICLO DE APROBACIÓN:

FECHA	VERSIÓN	DESCRIPCIÓN	CICLO DE APROBACIÓN
08/05/2012	1	Primera versión de la definición de política y objetivos del SGSI	**Elabora:** Ana Gomez **Revisa:** Ivan Fernando Diaz **Aprueba:** Carlos Carrizosa
19/03/2014	2	Revisión de política y objetivos del SGSI 2013/2014	**Elabora:** Ana Gomez **Revisa:** Ivan Fernando Diaz **Aprueba:** Omar Ladino
07/04/2015	3	Revisión y actualización del documento	**Elabora:** Ana Gomez **Revisa:** Ivan Fernando Diaz **Aprueba:** Omar Ladino
09/02/2016	4	Revisión y actualización del documento	**Elabora:** Ana Gomez **Revisa:** Ivan Fernando Diaz **Aprueba:** Omar Ladino
14/08/2017	5	Revisión y actualización del documento	**Elabora:** Ana Gomez **Revisa:** Ivan Fernando Diaz **Aprueba:** Omar Ladino
30/08/2018	6	Revisión y actualización del documento (logo)	**Elabora:** Ana Gomez **Revisa:** Ivan Fernando Diaz **Aprueba:** Omar Ladino
29/04/19	7	Ampliación del alcance de la política e integración con los Sistemas de gestión.	**Elabora:** Gustavo Olaya- Yesenia Brand **Revisa:** Ivan Diaz- Ana Gomez **Aprueba:** Carlos Carrizosa- Omar Ladino
28/10/2020	8	Revisión y correcciones menores al texto	**Elabora:** Luis Gonzalez – William Ricaurte **Revisa:** Alvaro Guerrero **Aprueba:** Carlos Carrizosa
13/09/2021	9	Revisión y correcciones menores al texto	**Elabora:** Luis Gonzalez **Revisa:** Alvaro Guerrero **Aprueba:** Carlos Carrizosa
27/09/2022	10	Ampliación y mejora del contenido la política.	**Elabora:** Jose Montañez **Revisa:** Luis Gonzalez **Aprueba:** Claudio Esteves
01/02/2023	11	Se amplía el alcance en lo relacionado a teletrabajo.	**Elabora:** Jose Montañez **Revisa:** Luis Gonzalez **Aprueba:** Claudio Esteves
24/03/2023	12	Ampliación y mejora del contenido de la política.	**Elabora:** Luis Gonzalez-Liliana Villar **Revisa:** Javier Albiol Fernandez **Aprueba:** Claudio Esteves