SISTEMAS DE GESTIÓN Y CONTROL INTEGRADOS

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Versión 4

Código: MAGT04.04.14.12.PI.01

Macroproceso: Gestión Tecnológica y de la Información
Proceso: Administración de Tecnologías de Información y las Comunicaciones
Septiembre 2018

CONTENIDO

1. INTRODUCCIÓN

En la actualidad, el gobierno Colombiano reconoce la información como un activo valioso y a medida que los sistemas de información apoyan cada vez más los procesos de misión, se requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de los datos.

Por esto, el Ministerio de Tecnologías de la Información y las Telecomunicaciones por medio del Decreto 1078 de 2015, da la directriz para que, entre otros ejes, se implemente el eje de seguridad y privacidad de la información basada en la norma técnica colombiana 27001 "Tecnología de la Información Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información".

Considerando también, el Modelo integrado de Planificación y gestión MIPG y su actualización mediante el decreto 1499 de 2017, en su articulado 2.2.22.1.5 Articulación y complementariedad con otros sistemas de gestión. Establece que: "El Sistema de Gestión se complementa y articula, entre otros, con los sistemas nacional de servicio al ciudadano, de gestión de la seguridad y salud en el trabajo, de gestión ambiental y de Seguridad de la Información".

En ese orden de ideas, la Administración Central del Municipio de Santiago de Cali, implementa la norma técnica colombiana NTC ISO/IEC 27001 dentro del Sistema de Gestión y Control Integrados y reconoce que los sistemas, los activos de información y la red de información enfrentan amenazas de seguridad que incluyen, entre muchas otras: el fraude por computadora, espionaje, sabotaje, vandalismo, desastres naturales.

Las posibilidades de daño y pérdida de información por causa de código malicioso, mal uso de la información, poca protección de la información, la no definición de procedimientos o ataques informáticos, son cada vez más comunes y ponen cada vez más en riesgo los activos de información. Por esta razón se deben definir las políticas que permitan proteger los Sistemas de Información y establecer un sistema de gestión de seguridad de la información.

2. OBJETIVO

Establecer lineamientos que permitan el control efectivo de la información en la Administración Central del Municipio de Santiago de Cali, como una herramienta de gestión que logre identificar y minimizar los riesgos a los cuales se expone la información, ayudar a la reducción de costos operativos y financieros, establecer una cultura de seguridad y garantizar el cumplimiento de los requerimientos legales, contractuales y regulatorios vigentes, buscando preservar la información institucional.

3. ALCANCE

La Política de Seguridad de la Información aplica para todos los usuarios internos en todos los niveles jerárquicos, usuarios externos, proveedores y terceros; que produzcan, administren, custodien o que tengan acceso a la información de la Administración Central del Municipio de Santiago de Cali.

4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Administración Central del Municipio de Santiago de Cali, se compromete a adoptar las medidas técnicas, jurídicas y administrativas necesarias a través de la administración de riesgos, dando un tratamiento transparente y correcto a la información pública del Municipio, fomentando una cultura de mejora de la seguridad de la información, preservando los activos de información y tecnológicos del Municipio, para asegurar la confidencialidad, integridad y disponibilidad de la información; con el fin de apoyar el cumplimiento de la gestión de la entidad y promover la confianza en la ciudadanía.

5. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

- Controlar las vulnerabilidades y amenazas que enfrentan los activos de información y tecnológicos mediante la elaboración de los mapas de riesgos, para asegurar la confidencialidad, integridad y disponibilidad de la información de todos los Organismos de la Alcaldía de Santiago de Cali.

- Fortalecer la cultura de seguridad de la información mediante difusión, sensibilización y capacitación de funcionarios, con el fin de dar tratamiento transparente y correcto de la información de todos los organismos y procesos de la Administración Central del Municipio de Santiago de Cali.
- Gestionar el inventario de los activos informáticos y de información que garantice la Identificación, clasificación y el mantenimiento de la información, para lograr su uso apropiado durante todo su ciclo de vida en todos los organismos de la Administración Central del Municipio de Santiago de Cali.

6. POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

6.1. Seguridad física de los Centros de Procesamiento de Datos - CPD

- Los usuarios visitantes a los Centros de Procesamiento de Datos de la Administración central del municipio de Santiago de Cali deben solicitar autorización previa para visitar el CPD y deben ser acompañados durante todo el tiempo por un funcionario del organismo administrador del CPD.
- Todas las visitas realizadas a los CPD de la administración central del municipio de Santiago de Cali debe ser registrado en el libro de bitácoras registrando mínimo los siguientes datos: Nombre, apellido, fecha de ingreso, hora de entrada, hora de salida, funcionario administrador del CPD que lo acompaña, asunto del ingreso y firmas.
- Los visitantes al DATIC de la Administración Central del Municipio de Santiago de Cali, deben ser acompañados durante todo el tiempo de su visita por un funcionario de este departamento y por ningún motivo debe estar solo el visitante para garantizar la seguridad física del departamento.
- Todos los administradores de los CPD de la administración central deben garantizar la vigilancia de los CPD por medio de circuito cerrado de televisión para verificar y registrar en medio digital los acontecimientos rutinarios y de excepción.

- Todos los administradores de los CPD de la administración central deben garantizar el acceso a los CPD solo a personal autorizado con un sistema de control de acceso que debe considerar al menos un factor de autenticación para mantener el nivel adecuado de control de acceso
- Todos los administradores de los CPD de la administración central, deben evitar intrusiones a personal no autorizado a los CPD con sistemas de detección de movimientos en los puntos susceptibles de intrusión desde el exterior de las áreas al centro de cómputo.
- Todos los administradores de los CPD de la administración central deben garantizar la protección de los CPD ante desastres naturales con elementos de control de incendios, inundación y alarmas para evitar la materialización de riesgos como incendios e inundaciones.
- Los administradores de los CPD de la administración central deben garantizar la confidencialidad del CPD evitando el ingreso de equipos fotográficos, de video, audio u otro equipo de equipamiento que registre información a los CPD de la administración central para evitar comprometer información confidencialidad.
- Los administradores de CPD de la administración central deben revisar y actualizar los derechos de acceso a los CPD cada seis meses en el sistema que administra el control de acceso para garantizar que solo accede a los CPD los usuarios que estén autorizados en sus funciones para el acceso al CPD
- Los administradores de los centros de cableado deben catalogar los centros de cableado como zona de alto riesgo, con limitación y control de acceso considerando las directrices de la oficina de bienes inmuebles para evitar riesgos físicos en los centros de cableado
- Los administradores de los centros de cableado deben garantizar el acceso solo a personal autorizado a los centros de cableado manteniendo siempre el acceso con cerraduras y registrando el acceso en libro de bitácora para evitar accesos no autorizados y daños provocados por personas a los elementos del centro de cableado.

- Los administradores de centros de cableado deben garantizar siempre el acceso a los administradores de CPD en cualquier horario entregando copias de las llaves de las cerraduras de los centros de cableado para garantizar soporte de alto nivel por parte de DATIC en cualquier horario.
- Los administradores de los CPD y centros de cableado deben mantener los gabinetes que hospedan los elementos de TI siempre cerrados con llaves para evitar acceso o daño a elementos de TI ahí hospedados.
- Los administradores de los CPD y centro de cableado deben evitar el consumo de bebidas y alimentos dentro del CPD y lo centros de cableado respectivamente, para evitar daños en los equipos de TI alojados en ellos.
- Los administradores de los CPD deben monitorear constantemente las condiciones de temperatura y humedad registrando eventos y excepciones para evitar que se afecten los equipos dentro del centro de cómputo por cambios de temperatura.
- Los administradores de los CPD y centro de cableado deben garantizar la seguridad física ante siniestros evitando que las paredes, pisos y techos contengan material inflamable para evitar incendios u obstaculizar el paso de funcionarios en caso de emergencia.
- Los administradores de los CPD y centros de cableado deben garantizar el debido aseo y limpieza de los CPD y centros de cableado planificando jornadas de limpieza y organización para evitar el daño de recursos TI por causa de exceso de polvo y suciedad en el área
- El administrador del CPD debe controlar el ingreso y salida de recursos TI de los CPD registrando los elementos TI en un formato para evitar pérdidas de elementos TI propiedad de DATIC.
- El encargado de equipos de cómputo entregados por la administración central debe garantizar la seguridad de los equipos a su cargo cuando los retire de la administración central manteniendo las buenas prácticas de seguridad para evitar riesgos de seguridad informáticos que afecten la información en el equipo

6.2. Políticas para le gestión de comunicaciones y operaciones

6.2.1. Seguridad en la Red de Datos

- Los administradores de la red de la administración central deben proteger la información de las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Administración Central del Municipio de Santiago de Cali y la REMI (Red Municipal Integrada) considerando y tratando dicha información como confidencial para evitar que se exponga información que facilite accesos no autorizados por tercero.

- Los administradores de la red de la administración central deben garantizar que la conectividad a servicios de la administración central deben llevarse a cabo con al menos un método de autenticación que incluya usuario y contraseña para identificar y controlar los usuarios que acceden a los servicios

- Los administradores de la red de la administración central deben garantizar que las conexiones externas a los servicios internos deben filtrarse a través de los dispositivos de seguridad mediante implementación de VPN (Virtual Private Network – Red Privada Virtual) para mantener la confidencialidad y la integridad de la información de conexiones desde redes externas

- Los administradores de la red de la administración central deben garantizar que todo intercambio electrónico de información o interacción entre sistemas de información con entidades externas tienen que estar soportado con un acuerdo o documento de formalización y confidencialidad y la conexión se debe realizar por un canal seguro. Para mantener la confidencialidad y la integridad de la información de conexiones entre las redes

- Los administradores de la red de la administración central deben garantizar que la información que se transmite a redes externas deben estar cifradas implementando controles criptográficos para mantener la confidencialidad y la integridad de la información de conexiones entre las redes

- Los administradores de la red de la administración central deben separar las redes por organismo y/o funciones segmentar la red por cada organismo o grupo de trabajo de los organismos para mantener el control de los acceso a recursos que no sean de la subred

- Los administradores de la red de la administración central deben hacer la segmentación para diferenciar servicios de acceso global y servicios de acceso local con el fin de proteger que los usuarios no accedan a recursos que no sean de su ámbito laboral.

- Los administradores de la plataforma de red de la administración central deben monitorear los nodos de red y registrar todos los eventos presentados en los nodos de la red con una herramienta automática para mantener evidencia de los eventos ocurridos en la red

- Los administradores de la red de la administración central deben garantizar que el acceso a los recursos informáticos de la red por medio de al menos un sistema de control de acceso de un solo factor como es usuarios y contraseña para mantener el control de acceso a los recursos

- Los administradores de recursos informáticos deben identificar los puertos que por funcionamiento deben estar abiertos en el segmento de su red para así garantizar la disponibilidad de los servicios mediante la configuración de firewall en la plataforma de seguridad.

6.2.2. Seguridad en las operaciones

- Los administradores de recursos informáticos deben garantizar la detección de códigos maliciosos que todos los equipos deben contar con programas antivirus instalados y estar en operación para que permitan eliminar cualquier virus de este y/o de otros medios.

- Los administradores de recursos informáticos deben garantizar que los software que tengan instalados los equipos deben ser actualizados cada que el fabricante de software libere una actualización automática o accediendo al fabricante de software para evitar vulnerabilidades técnicas en las aplicaciones de host

- Los administradores de recursos informáticos deben instalar un firewall de software en los equipos de cómputo de manera manual o automática para monitorear, proteger y controlar los puertos lógicos del equipo de cómputo.

- Los administradores de recursos informáticos deben garantizar que los diferentes medios extraíbles que los usuarios conecten a los equipos deberán se explorados por la herramienta de antivirus instalada para proteger contra códigos maliciosos

- El delegado del Comité Tecnológico Operativo de cada organismo es la persona autorizada para la instalación de software para evitar que se instalen software sin licenciamiento o que atente con la integridad de la red de la Administración Central del Municipio Santiago de Cali.

- Los administradores de recursos informáticos deben garantizar que se bloquee la pantalla del equipo de cómputo automáticamente luego de un período de inactividad de 10 minutos para evitar accesos no autorizados a los equipos de cómputo

- Los usuarios de equipos de cómputo deben bloquear la pantalla cuando se levanten del puesto por largo tiempo para evitar accesos no autorizados a los equipos de cómputo.

- Los usuarios de los equipos de cómputo son responsables de apagar los equipos de cómputo que utilizando para sus labores diarias cada que termine su jornada laboral para evitar que estos equipos sean utilizados para otro fin.

- Los administradores de recursos informáticos deben garantizar que los equipos de cómputo estén sincronizados configurando de forma automática la hora con el servidor NTP (Network time protocol- Protocolo de tiempo de red) para garantizar que los registros realizados para cualquier eventualidad tengan ese nivel de coincidencia.

- El administrador del sistema de antivirus debe garantizar que el antivirus cuente con soporte técnico, resolución urgente de nuevos virus y servicios de alerta. Administrando y monitoreando la consola de antivirus para mantener controlado los riesgos de código malicioso en la red de la administración central.

- Los usuarios y funcionarios de la administración central que cuenten con correo institucional, debe preservar la seguridad de su correo institucional manteniendo la privacidad, confidencialidad de la información de acceso y la información contenida en el para evitar suplantación y fuga de información.

- El DATIC debe mantener un responsable de la supervisión del proceso de copias de seguridad a los sistemas de información hospedados en los CPD administrados por DATIC, que verifique su realización, almacenamiento y pruebas de integridad para mantener punto y tiempos objetivos de recuperación adecuados.

- El responsable de los backup de los sistemas de información en DATIC, debe probar los backup realizados con regularidad para asegurarse de que se puede realizar una restauración completa.

- El responsable de los backup de los sistemas de información en DATIC debe documentar las copias de respaldo manteniendo como mínimo la información de Consecutivo de backup, Contenido acorde al procedimiento copias de respaldo.

- Los usuarios de equipos de cómputo de la administración central deben realizar las copias de respaldo de la información producida por ellos utilizando los medios que proporciona la administración central para garantizar la realización de copias de respaldo de información que los funcionarios consideren importantes.

- Los encargados de soporte técnico de cada organismo deben asegurar que las copias de seguridad se realicen de forma automática por medio de un programa de copia, y se debe configurar según la solicitud realizada en el procedimiento para garantizar la realización de copias de respaldo.

- El responsable del respaldo de información de cada organismo debe registrar la eliminación de backup por medio de un acta firmada por el jefe de unidad o quien haga sus veces en cada organismo, con el fin de mantener trazabilidad para auditorías.
- El responsable del respaldo de información de cada organismo debe documentar las copias de respaldo manteniendo una identificación fácil acorde al procedimiento copias de respaldo.

6.2.3. Política para el control de acceso

- Los administradores de recursos informáticos deben asignar un usuario único y exclusivo a los funcionarios y contratistas que ejercen funciones públicas cuyos privilegios de acceso a los recursos informáticos estarán determinados por el tiempo de vinculación con el organismo y así de esta manera poder mantener el control de acceso a dichos recursos.

- El responsable del área administrativa de cada Organismo deben solicitar al delegado del Comité Técnico Operativo de su organismo la creación, activación y desactivación de las claves de acceso a los recursos de red para los funcionarios y contratistas que ejercen funciones públicas de acuerdo al procedimiento de control de acceso para mantener control de acceso a los recursos informáticos y controlar la creación de usuarios.

- Los funcionarios y contratistas deben realizar el cambio de las claves de acceso a los recursos de red al ser entregada por primera vez por medio de la aplicación a la cual va a acceder y pertenece el usuario con el fin de mantener la privacidad de la información.

- Los funcionarios y contratistas deben asegurarse que los usuarios y contraseñas no deben ser compartidos con el fin de mantener la privacidad de la información.

- Los funcionarios y contratistas que ejercen funciones públicas que tomen su período de vacaciones o se ausenten por más de tres (3) días, deben informar al El delegado del Comité Tecnológico Operativo sobre su ausencia, acorde al procedimiento de control de acceso, para que le sea bloqueado su usuario por el período de tiempo establecido.

- Los funcionarios y contratistas que ejercen funciones públicas deben cambiar la contraseña de su(s) cuenta(s) en el sistema de información cada 60 días y ésta no puede coincidir con las cinco (5) anteriores.

6.3. Políticas para la adquisición, desarrollo y mantenimiento de sistemas de información

El responsable de la adquisición de sistemas de información es el DATIC, ya sea por contratación directa, contratando un tercero o implementado un sistema de información de código libre, en cualquiera de los anteriores casos el sistema de información debe cumplir con las políticas de este dominio:

- Los responsables de desarrollo de sistemas de información deben asegurar la autenticación y control de acceso de los usuarios a través de la parametrización e integración del sistema de información con el Directorio Activo para mantener las políticas mínimas de control de acceso que cuenta la administración central.

- Los responsables de desarrollo de sistemas de información deben asegurar que después de 3 intentos fallidos el sistema de información bloquea el usuario a través de la parametrización e integración del sistema de información con el directorio activo para mantener las políticas mínimas de control de acceso que cuenta la administración central.

- Los responsables de desarrollo de sistemas de información debe asegurar que para todos los desarrollos debe ser auditada en cuanto a capacidad y seguridad utilizando las mejores metodologías para mantener características mínimas de seguridad alineadas a estándares de seguridad.

- Los responsables de desarrollo de sistemas de información deben entregar al DATIC, los resultados de la auditoría realizada al sistema de información de acuerdo a la metodología utilizada para mantener registro y control de los resultados.
- Los responsables de desarrollo de sistemas de información deben asegurar que las transacciones hechas en el sistema de información queden guardadas para efectos de auditoria de acuerdo a la norma 27002 para el registro de logs para mantener registros de las transacciones realizadas por cualquier usuario.
- Los responsables de desarrollo de sistemas de información debe asegurar la definición de roles, permisos y control de acceso a la aplicación y las carpetas del sistema de información
- Los responsables de desarrollo de sistemas de información deben mantener buenas prácticas de seguridad desde el comienzo del proyecto y durante el desarrollo del mismo de acuerdo a la buenas prácticas y metodologías que se informara a DATIC para mantener una de acuerdo nivel de seguridad desde el desarrollo hasta la operación del sistema de información
- Los responsables de desarrollo de sistemas de información deben definir, documentar e informar al DATIC los permisos exactos de los usuarios del sistema operativo de acuerdo a la estricta necesidad de operación del sistema de información desarrollado para mantener el debido control de acceso al sistema
- Los responsables de desarrollo deben definir y documentar los permisos que requiere la aplicación sobre los archivos y directorios del servidor de acuerdo a la estricta necesidad de operación del sistema de información desarrollado para mantener el debido control de acceso al backend del sistema
- Los responsables de desarrollo deben asegurar que la carga de archivos y la parametrización del sistema de información deben realizarse únicamente desde direcciones IP aprobadas por DATIC para disminuir el riesgo de intrusión desde redes externas

- Los responsables de desarrollo deben asegurar que el sistema de información está en capas manteniendo siempre el front end, back end y capa de base de datos para separar ambientes operativos del sistema de información
- Los responsables de desarrollo deben desarrollar e implementar el sistema de información de acuerdo al procedimiento de implementación de sistemas de información que tiene la administración central

6.4. Políticas para la gestión de incidentes.

- Los usuarios con incidentes de seguridad deben seguir el procedimiento de administración de la operación, código: MAGT04.04.02.18.P07 disponible en el MOP, para reportar el incidente en la mesa de servicio en el link https://200.29.103.76:8500/fiori

6.5. Políticas para la continuidad del negocio

- La Subdirección de Tecnología Digital, como garante de la operación de los servicios TI, debe ejecutar el plan de continuidad de negocio aprobado por DATIC, en caso de materialización de un riesgo que afecte la disponibilidad del servicio.
- La Subdirección de Tecnología Digital, como garante de la operación de los servicios TI, debe realizar pruebas del plan de continuidad de negocio cada 6 meses para garantizar la vigencia del mismo.

7. RESPONSABILIDADES

- El Consejo Superior de Desarrollo Administrativo es responsable por articular los esfuerzos institucionales, recursos, metodologías y estrategias para asegurar la implementación de esta política del Sistema de Gestión de Seguridad de la Información, la cual hace parte de las políticas del Modelo Integrado de Planeación y Gestión MIPG y la Política de Gobierno Digital (antes Estrategia de Gobierno en Línea)

- El Director del Departamento Administrativo de Tecnologías de la Información y las Comunicaciones es el representante de la alta dirección de la Administración Central Municipal, para la coordinación, seguimiento y verificación de la implementación y desarrollo de la Estrategia de Gobierno en Línea en el Municipio de Santiago de Cali (Decreto No 4112.010.20.0329 de 2017).
- El Comité Coordinador de Control Interno es el responsable de la aprobación de la Política de Seguridad de la Información en la Administración Central del Municipio de Santiago de Cali.
- El Departamento Administrativo de Desarrollo e Innovación Institucional orientará la metodología utilizada para la integración de los sistemas de gestión, la Administración de riesgos y la revisión por la dirección.
- El Departamento Administrativo de Tecnologías de la Información y las Comunicaciones orientará la metodología utilizada para el control de los riesgos de la seguridad informática.
- Los líderes de los procesos aprobados por la entidad, elaborarán y gestionarán los mapas de riesgos de seguridad de la información, bajo la supervisión del Departamento Administrativo de Desarrollo e Innovación Institucional y el Departamento Administrativo de las Tecnologías de la Información y las Comunicaciones, según lo estipulado en el referente NTC ISO/IEC 27001:2015 Numeral 6.1.3 tratamiento de riesgos de la seguridad de la información.
- Los líderes de los procesos aprobados por la entidad implementarán controles que permitan el cumplimiento de las políticas generales de seguridad de la información que hace referencia el numeral 5 del presente documento.
- La Oficina de Comunicaciones se encargará de la difusión de la Política de Seguridad de la Información.
- El Departamento Administrativo de Desarrollo e Innovación Institucional y el Departamento Administrativo de las Tecnologías de la Información y las

Comunicaciones deberán promover el uso y apropiación de la política de seguridad de la información.

- El Comité de Coordinación del Sistema de Control Interno y Gestión de Calidad será el encargado de la aprobación de las modificaciones de la Política de Seguridad de la Información vigente. (Decreto 01149 de 9 marzo 2017)

Se identifican los siguientes actores:

1) Consejo Superior de Desarrollo Administrativo
2) Comité de Coordinación del Sistema de Control Interno y Gestión de Calidad
3) El Departamento Administrativo de Desarrollo e Innovación Institucional
4) Departamento Administrativo de Tecnologías de la Información y las Comunicaciones
5) Los líderes de los procesos aprobados por la entidad
6) Oficina de Comunicaciones

8. SEGUIMIENTO Y MONITOREO

El Departamento Administrativo de Tecnologías de la Información y las Comunicaciones y el Departamento Administrativo de Desarrollo e Innovación Institucional mediante el procedimiento de Revisión por la Dirección realizarán el monitoreo de la Política de Seguridad de la Información por lo menos una vez al año.

Los Líderes de los procesos harán la revisión de los controles establecidos según la periodicidad definida en la política de administración de riesgos definido por la entidad.

El Departamento Administrativo de Control Interno realizará la evaluación independiente según los lineamientos establecidos en el procedimiento de auditorías aprobado por la entidad.

Se identifican los siguientes actores:

1) Departamento Administrativo de Tecnologías de la Información y las Comunicaciones
2) Departamento Administrativo de Desarrollo e Innovación Institucional
3) Líderes de los procesos
4) Departamento Administrativo de Control Interno

9. RECURSOS

El Consejo Superior de Desarrollo Administrativo es responsable por asegurar los recursos para la implementación de esta política del Sistema de Gestión de Seguridad de la Información, la cual hace parte de las políticas del Modelo Integrado de Planeación y Gestión - MIPG y la política de Gobierno Digital.

Elaborado: Jorge Andrés Cultid Mejía Judith Domínguez Vargas	Cargo: No aplica	Fecha: 12/Sep/2018	Firma:
Revisado por: Roger González Pérez, Daniel Jair Chacón Balcázar	Cargo: Subdirector de Tecnología Digital Cargo: Subdirector de Gestión Organizacional	Fecha: 12/Sep/2018	Firma:
Aprobado por: Óscar Eduardo Escobar García	Cargo: Director de Departamento Administrativo de Tecnologías de la Información y las Comunicaciones	Fecha: 12/Sep/2018	Firma: