Tecnologías de la Información y las Comunicaciones - TIC

Adscrito a la Rectoría, el Departamento de Sistemas administra los bienes y servicios de la plataforma tecnológica en software y hardware, el soporte técnico de los equipos, el desarrollo y mantenimiento de las aplicaciones y la administración de los servidores institucionales para asegurar la confidencialidad, integridad y disponibilidad en los servicios de TI; a su vez, procura el mejoramiento continuo cumpliendo unas políticas que respaldan los procedimientos que se llevan a cabo dentro de éste mismo para cumplir con el proceso de "Tecnologías de la Información TIC" al que conforma, y que se articula con los Procesos Estratégicos del Sistema de Gestión de la Calidad, los cuales están destinados a definir y controlar las metas de la organización, sus políticas y estrategias, incluyen además procesos relativos a la fijación de objetivos, provisión de comunicación y consolidación de la imagen.[1]

Objetivos

- Planear y ejecutar proyectos informáticos que se incluyan en los procesos académicos y administrativos de la Institución para promover el interés por la cultura tecnológica.
- Velar por el correcto funcionamiento de los equipos que conforman la planta tecnológica del Instituto programando mantenimientos correctivos y preventivos oportunamente.
- Controlar el debido aprovechamiento de los recursos informáticos a través de la implementación de políticas y procedimientos respaldados por los procesos de Gestión de la Calidad.
- Contribuir al Plan de Desarrollo Institucional supliendo las necesidades con nuevos desarrollos tecnológicos que permitan dar cumplimiento a los objetivos planteados de una manera eficiente y siempre a la vanguardia de la tecnología.
- Lograr una óptima administración de los recursos tecnológicos.

[1] Manual de Políticas de Operación, pág. 6

- Dar soporte y solución a los inconvenientes presentados por los usuarios en cuanto a los servicios tecnológicos que presta el Departamento.
- Velar por la conservación y seguridad de la información institucional llevando a cabo procesos de respaldo y recuperación de la misma.

Políticas de Operación

Con las políticas de operación, el proceso de Tecnologías de la Información - TIC dispone de unas pautas que ayudan a planificar, organizar, dirigir y controlar su desempeño, siendo aplicables para funcionarios, contratistas, personal de apoyo y terceros no vinculados directamente al ITM, que presten su servicio y utilicen tecnologías de información, equipos propios del ITM o arrendados y a los equipos de personas externas que sean conectados a la red del ITM.

El responsable de las presentes políticas de operación en el ITM, será el Departamento de Sistemas quien a través de sus tres áreas (Sistemas de Información, Soporte, Infraestructura) se encargará de lo siguiente:

SOPORTE

I. Portal de Soluciones – Mesa de Servicios TI

El Portal de Soluciones ITM – Mesa de Servicios TI es una solución que permite gestionar y resolver los requerimientos e incidentes asociados a la infraestructura tecnológica del ITM, ofreciendo una mesa de servicio con un único punto de contacto para generar, administrar, responder y monitorear todos los casos relacionados, la cual se puede acceder con la siguiente URL: https://portaldesoluciones.itm.edu.co/usdkv8/#/login/

La autenticación para el ingreso al Portal de Soluciones es por medio del usuario y contraseña institucional.

I.1 Políticas de funcionamiento del Portal de Soluciones

1. Todos los casos de incidentes y/o requerimientos tecnológicos deben ser registrados en el Portal de Soluciones.

2. Todo usuario al registrar un caso en el Portal de Soluciones debe detallar la información de su solicitud, el especialista de TI solicitará cualquier información complementaria requerida.

3. Los especialistas de TI atenderán los casos de forma remota o presencial según las características de estos.

4. Todo usuario solicitante debe ser notificado a través del Portal Soluciones - Mesa de Servicios TI de cada uno de los avances y actualizaciones sobre sus casos. En caso de ser necesario el especialista podrá pausar el ticket para solicitar información adicional, en esta pausa los tiempos de servicio también se detendrán.

5. Todos los incidentes y/o requerimientos serán atendidos cumpliendo los Acuerdos de Niveles de Servicio (Tiempos de atención según la naturaleza de la solicitud) definidos por el Departamento de Sistemas.

6. Después de la solución de un caso el usuario deberá diligenciar la encuesta de satisfacción del servicio, que llegará a su correo institucional, el cual permitirá medir la satisfacción del usuario y tomar medidas de mejora continua.

II. Préstamo y Uso de espacios y Equipos

7. Los diferentes espacios institucionales deben ser objeto de cuidado por toda la comunidad académica, por lo que el personal que ingrese a un aula de clase debe abstenerse de ingerir alimentos y bebidas, rayar muebles, muros o pisos, desconectar

cables, teclados, mouse y en general alterar de alguna manera las condiciones físicas de las instalaciones.

8. Todo docente, estudiante, empleado o contratista que use alguna de las aulas, debe asegurarse, al terminar sus actividades, de que queden bien cerradas las puertas y ventanas con la seguridad respectiva, además del apagado de los computadores, proyectores y otros equipos tecnológicos.

9. El préstamo de equipos y de aulas con equipos de cómputo, se hará de acuerdo con las directrices estipuladas en las guías “Guía para Reservar Equipos de Cómputo” y “Guía para Reservar Aulas”. La reserva y préstamo de otros espacios, se hará previa solicitud a la Dirección de Sedes al estudio y disponibilidad.

10. La Institución debe utilizar el Sistema de Información Académico SIA para administrar el uso y ocupación de los equipos asignados a las salas de cómputo en las diferentes sedes del ITM.

IV. Adquisición de equipos de cómputo

11. El Departamento de Sistemas es el área responsable de liderar la adquisición y mantenimiento de los equipos de cómputo que usan la infraestructura de TI de la institución.

12. El Departamento de Sistemas define que los equipos de cómputo que se adquieran para la institución, para realizar actividades de docencia, extensión, investigación y administrativa, deben ser de línea corporativa, ya que son equipos diseñados con arquitecturas más robustas y resistentes en todos sus componentes, de tal forma que están adaptados para un trabajo más exigente, brindando más seguridad tanto del equipo como de la información.

13. Así mismo estos equipos deben contar con una garantía de mínimo 3 años en sitio, lo que significa que por este tiempo la reparación y suministros de las partes estarán a cargo de la empresa o fabricante que provee estos activos.

14. Estos equipos deben traer instalado al menos una licencia de Windows OEM, ya que el contrato que se tiene actualmente con Microsoft se puede subir a un licenciamiento mayor, pero en ningún caso se podrán adquirir equipos sin sistema operativo Windows.

15. El Departamento de Sistemas definirá directrices técnicas para la adquisición de bienes y servicios relacionados con informática (equipos de cómputo, portátiles, impresoras, aparatos telefónicos, entre otros).

V. Carnetización y Control de Acceso

16. El acceso a diferentes áreas de la institución, incluyendo aulas de clase, podrá darse a personal de Servicios Varios, Vigilancia y docentes, estos últimos solo en las franjas horarias en las cuales tiene clase programada y 10 minutos antes de esta.

17. Los docentes y personas autorizadas que ingresen a estos espacios deberán asegurarse de ser los primeros y últimos en salir y dejar la puerta cerrada.

18. El Departamento de Sistemas pondrá a disposición de los empleados y estudiantes el enlace procesocarnetizacion.itm.edu.co para acceder al formulario de solicitud de Carnet Institucional, en este encontrará las instrucciones y detalles importantes para su solicitud.

19. Una vez creado el documento, se informará a través de correo electrónico al solicitante que ya puede acercarse a recogerlo. En este correo se especifican los horarios y oficinas donde podrá hacer la diligencia.

20. Los carnets del ITM darán acceso a diferentes áreas de los campus de la institución a sus propietarios, Si le hace falta algún permiso específico, el usuario deberá solicitarlo a través de nuestro Portal de Soluciones o en las oficinas de Soporte técnico del Departamento de Sistemas.

21. El carnet es un documento de identificación de uso personal e intransferible.

22. En caso de hurto o pérdida es obligación de su propietario reportarlo de forma inmediata al Departamento de Sistemas de la institución, en caso de requerirse nuevamente, debe realizar el pago en tesorería o taquilla virtual y diligenciar nuevamente el formulario para la expedición de uno nuevo

VI. Impresión

23. El líder de cada dependencia será el encargado de asegurar el uso responsable y eficiente de los servicios de impresión del ITM.

24. Se recomienda la impresión de documentos a doble cara, con tamaños de letra que permitan el ahorro de consumibles, además se debe procurar el uso de modo de ahorro de tinta.

25. Los funcionarios del ITM solo deberán imprimir en caso de ser estrictamente necesario, además solo está permitido la impresión de documentos institucionales.

26. Evitar la impresión a color si no es necesaria.

27. El ITM podrá realizar campañas de eliminación o centralización de equipos de impresión con el objetivo de lograr eficiencia administrativa y ambiental.

28. Cada área solicitará el papel para las impresoras y estarán al cuidado de su uso responsable.

SISTEMAS DE INFORMACIÓN

I. Software – Derechos de Autor

29. Para asegurarse de no violar los derechos de autor, no está permitido a los colaboradores copiar ningún programa instalado en los activos informáticos de la entidad, en ninguna circunstancia sin la autorización del Departamento de Sistemas. No está permitido instalar ningún programa en los equipos sin la autorización o la clara verificación de que la entidad posee una licencia que cubre dicha instalación.

30. Para instalar software en los activos informáticos de la entidad, se debe realizar una solicitud a través del Portal de Soluciones ITM – Mesa de Servicios TI. El Departamento de Sistemas verificará la disponibilidad de licencias previo a su instalación.

31. No está autorizada la descarga de programas informáticos no autorizados por el Departamento de Sistemas, de ser necesario por cualquier área del ITM se debe solicitar la validación del programa informático por medio del Portal de Soluciones ITM – Mesa de Servicios TI.

32. No está permitido que los colaboradores realicen copias no autorizadas de programas informáticos, cualquier tipo de información institucional, sistemas de información, base de datos, etc.

II. Implementación y mantenimiento de Sistemas de Información y/o aplicativos institucionales.

33. El Departamento de Sistemas es el área responsable de liderar la adquisición, la implementación y mantenimiento de los sistemas de información, aplicativos y otros servicios tecnológicos de la institución.

34. El Departamento de Sistemas es responsable de realizar el análisis de las solicitudes de desarrollo de software institucional, el estudio de viabilidad y definiciones técnicas

de las soluciones a implementar, estableciendo espacios colaborativos con los líderes de las áreas solicitantes

35. En los casos de adquisiciones de software de terceros el Departamento de Sistemas tendrá la potestad de analizar, definir lineamientos o impedir el uso de un software si este trae riesgos de seguridad, jurídicos o logísticos para la institución

36. Los requerimientos de implementación y/o mantenimiento de sistemas de información, aplicativos y otros servicios tecnológicos deben ser solicitados a la jefatura del Departamento de Sistemas para su previo análisis por parte del equipo del área de desarrollo y nuevas tecnologías del departamento, lo anterior deberá hacerse mediante el Portal de Soluciones institucional.

37. El Departamento de Sistemas será el único ente institucional encargado de la adquisición, implementación y/o mantenimiento de los sistemas de información institucionales. En casos particulares el Departamento de Sistemas podrá autorizar la adquisición de software por parte de otra dependencia sin renunciar a la debida vigilancia del mismo.

38. Cualquier sistema de información, aplicativo u otro servicio tecnológico debe ser desarrollado teniendo en cuenta la Guía de Arquitectura de Software del Departamento de Sistemas que incluye entre otras cada una de las etapas del ciclo de vida del software (análisis, diseño, desarrollo, pruebas, puesta en producción y mantenimiento), además debe atenerse a la arquitectura, recursos de infraestructura, IDE de desarrollo, motor de base de datos, políticas de seguridad y otros componentes normativos definidos por el Departamento de Sistemas.

39. Los sistemas de información y/o aplicativos a medida, desarrollados por terceros bajo la figura de prestación de servicios, deben ser cedidos por el contratista a la institución a través del proceso de cesión de los derechos patrimoniales, bajo la supervisión de la Secretaría Jurídica institucional.

40. Todas las soluciones a medida desarrolladas por terceros, deben cumplir con una lista de requisitos de entrega como anexo técnico al contrato, la estructura de la lista de entrega deberá contener los siguientes ítems: Arquitectura, casos de uso, requerimientos, Integración continua, control de versiones, manual de despliegue, manual técnico, manual del usuario final, código fuente, entre otras definidas por el Departamento de Sistemas para casos particulares.

41. La designación de los administradores para cada sistema de información está a cargo de la jefatura del Departamento de Sistemas, y se hará teniendo en cuenta su perfil y manual de funciones.

42. La creación de usuarios se debe solicitar por el jefe de la dependencia en el Portal de Soluciones ITM – Mesa de Servicios TI, indicando los permisos requeridos para cada usuario

INFRAESTRUCTURA

I. Internet

30. El Departamento de Sistemas provee el servicio de internet a todos los usuarios del ITM, con el fin adelantar exclusivamente las funciones asignadas a su cargo utilizándose de forma austera y eficiente. El Departamento de Sistemas aplicará controles con el fin de garantizar el uso adecuado y eficiente del acceso a internet, procurando la seguridad y disponibilidad del servicio

31. Se prohíbe a los usuarios de utilizar aplicaciones que tengan como objetivo evadir los controles implementados por el Departamento de Sistemas.

32. El ITM cuenta con acceso restringido a ciertas páginas Web, si por la naturaleza del cargo se requiere el acceso a alguno de estos sitios, se debe solicitar por medio del

Portal de Soluciones ITM – Mesa de Servicios TI, su acceso deberá ser solicitado por parte del jefe de cada dependencia.

II. Correo electrónico

El correo electrónico institucional es un servicio tecnológico ofrecido por el Instituto Tecnológico Metropolitano – ITM, y su uso debe ser exclusivamente laboral y/o académico. En este sentido se han dispuesto los dominios “itm.edu.co” y “correo.itm.edu.co”. Los lineamientos que se deben tener presentes para su uso son:

II.1 Uso del correo electrónico

33. El buzón de correo electrónico institucional ligado a la identidad digital es de uso personal e intransferible, por lo tanto, es responsabilidad del usuario salvaguardar la clave, cambiarla periódicamente por contraseñas complejas y no revelarla en ninguna circunstancia. Su acceso está definido en las guías “Guía para Ingresar al Correo Vía Web”.

34. El buzón de correo institucional es creado para el uso exclusivo de las funciones propias de su vinculación con el Instituto Tecnológico Metropolitano – ITM, por lo tanto, debe hacer uso de este servicio implementando criterios de racionalidad, respeto, responsabilidad, integridad y seguridad de la información.

II.2 Creación de cuentas de correo

35. Se asigna el primer nombre y el primer apellido, en caso de que ya se encuentre registrado en el directorio activo un usuario con el mismo nombre se adicionará al nombre y al apellido, la primera letra del segundo apellido o del segundo nombre, por ejemplo:

    - Jorge Andrés Gomez Villegas jorgegomez@itm.edu.co
    - Jorge Andrés Gomez Villegas jorgegomezv@itm.edu.co
    - Jorge Andrés Gomez Villegas jorgeagomez@itm.edu.co

II.3 Cuentas de correo genéricas

36. Se debe generar la solicitud por el jefe de la dependencia que lo requiere en el Portal de Soluciones ITM – Mesa de Servicios TI, en la solicitud de creación de cuentas genéricas se da la opción al solicitante de sugerir el nombre de la cuenta, sin embargo, no significa que vaya a ser el nombre definitivo ya que ésta se debe asemejar al siguiente estándar:

    - Departamento de Admisiones - adminsiones@itm.edu.co
    - Dirección de Planeación - planeacion@itm.edu.co

***Nota**: Cualquier variación a los estándares de asignación de nombres en las cuentas de correo, debe ser aprobada por el Departamento de Sistemas.*

II.4 Desactivación de buzones de correo

37. El buzón de correo se desactiva cuando se presenta alguna de las siguientes situaciones:

    - ✓ Existe requerimiento generado en El Portal de Soluciones ITM – Mesa de Servicios TI, por el jefe inmediato del funcionario.
    - ✓ Existe una novedad de desvinculación, previamente enviada por el Departamento de Personal o Secretaría General enviada a través de la Mesa de Servicios TI.
    - ✓ Toda cuenta creada con tiempo de expiración en una fecha especificada al momento de la creación, la cual está vencida y no se ha solicitado su ampliación.
    - ✓ El no cumplimento total o parcial de cualquiera de las indicaciones de esta política

38. El Instituto Tecnológico Metropolitano – ITM, en cualquier momento podrá implementar medidas necesarias en la plataforma del correo institucional, en aras de incrementar los niveles de seguridad y/o de brindar un mejor servicio.

II.5 Prohibiciones

39. Envío de correos con mensajes que contravengan las normas legales, la moral, el orden público, la intimidad o el buen nombre de las personas, que contengan contenido irrespetuoso, difamatorio, racista, vulneración a la libertad de culto, discriminatorio, temerario, de acoso o intimidación; así como imágenes o videos con contenidos ilegales, ofensivo, extorsivo, indecente, con material sexual o publicitario.

40. Propagar correos masivos sin autorización del jefe inmediato (Administrativo o de Programa). Enviar correos de procedencia desconocida, software malicioso, correo basura o no deseado.

41. Compartir contactos o listas de distribución de la institución con personal externo, con el objetivo de propiciar el envío de propagandas, ofertas, negocios personales, avisos publicitarios o información de otro tipo ajena a las labores propias del cargo.

42. Usar el correo electrónico institucional para el envío de propaganda política, ofertas, negocios personales, avisos publicitarios o cualquier información ajena a las labores propias del cargo.

43. Utilizar mecanismos y sistemas que intenten ocultar o suplantar la identidad del emisor de correo.

44. Violar los derechos de cualquier persona o institución, incluso aquellos que se encuentren protegidos por derechos de autor, patentes o cualquier otra forma de propiedad intelectual.

45. Introducir software malicioso en la red o en los servidores (virus, worms, ráfagas de correo electrónico no solicitado, Entre otros).

46. Revelar la clave o permitir su uso a terceros para actividades ajenas a la misión de la institución.

47. Enviar, reenviar o responder a mensajes de correo que contengan datos sensibles sin la autorización del responsable.

48. Enviar correos a nombre del Instituto Tecnológico Metropolitano – ITM, en caso de ser requerido, el interesado debe solicitar autorización ante la Secretaría General o la Dirección de Comunicaciones.

III. Uso de contraseñas

49. Los usuarios del ITM deben proteger sus contraseñas siguiendo las siguientes recomendaciones:

- ✓ No escribir ni reflejar la contraseña en papel o documento donde quede constancia de esta.
- ✓ No enviar nunca la contraseña por correo electrónico, redes sociales o en un mensaje de texto (SMS).
- ✓ No se debe facilitar ni mencionar la contraseña en conversaciones o comunicaciones de cualquier tipo.
- ✓ No utilizar en ningún caso contraseñas que se ofrezcan en los ejemplos explicativos de construcción de contraseñas robustas.
- ✓ No escribir las contraseñas en equipos de cómputo de los que se desconozca su nivel de seguridad y puedan estar monitorizados, o en computadores de uso público (bibliotecas, cibercafés, telecentros, etc.).
- ✓ No compartir su contraseña con terceros, el uso de la contraseña es personal e intransferible.
- ✓ No revelar su contraseña vía telefónica.
- ✓ No utilizar la función "Recordar Contraseña " de programas de aplicación, como navegadores de Internet (Edge, Chrome, FireFox etc.), Correo Electrónico, o cualquier otro programa.
- ✓ Informar cualquier incidente de seguridad que ponga en riesgo su contraseña al Departamento de Sistemas por medio de El Portal de Soluciones ITM – Mesa de Servicios TI.

- ✓ Informar al Departamento de Sistemas por medio de El Portal de Soluciones ITM – Mesa de Servicios TI si alguien dentro o fuera de la entidad le solicita su contraseña.
- ✓ No permitir que le observen al escribir su contraseña.
- ✓ Cambiar las contraseñas por defecto proporcionadas por desarrolladores/fabricantes.
- ✓ No utilizar información personal en la contraseña: nombre del servidor o de sus familiares, ni sus apellidos, ni su fecha de nacimiento, ni cuentas bancarias, ni tarjetas de crédito, etc.
- ✓ Se deben utilizar mínimo 8 caracteres para crear la clave.
- ✓ Las contraseñas deben utilizar la combinación aleatoria de los siguientes tipos de caracteres: Minúsculas, Mayúsculas, Números y Caracteres especiales como (+*! @ # $)
- ✓ Evitar utilizar secuencias básicas de teclado (por ejemplo:" qwerty", "asdf", "1234", "98765").
- ✓ No repetir los mismos caracteres en la misma contraseña. (ej.: "111222").
- ✓ Las contraseñas no deben ser FECHAS.
- ✓ La contraseña no debe basarse en dos palabras separadas por un espacio ( ), guion (-) o guion bajo (_).
- ✓ No utilizar datos relacionados con el usuario que sean fácilmente deducibles, o derivados de estos.
- ✓ No se deben utilizar palabras que se contengan en diccionarios en ningún idioma.
- ✓ Cuando el sistema le solicite cambio de contraseña esta no debe haber sido utilizada en los históricos del sistema.
- ✓ Elegir una contraseña que pueda recordarse fácilmente y es deseable que pueda escribirse rápidamente, preferiblemente, sin que sea necesario mirar el teclado.
- ✓ Realizar cambio de contraseña como mínimo cada 90 días.
- ✓ No utilizar generadores de contraseñas
- ✓ Cambiar la contraseña máximo cada 3 meses
- ✓ No haga uso de equipos públicos para acceder a sistemas de información institucional

50. Cuando un usuario inicie sesión por primera vez o cuando se realice una activación del usuario, el sistema exigirá cambio de contraseña para el directorio activo y para los dominios @itm.edu.co y @correo.itm.edu.co

51. Luego de 5 intentos de ingreso de contraseña fallidos, la cuenta del Directorio Activo será bloqueada. Esta cuenta se desbloqueará automáticamente pasados 60 minutos. Lo anterior afecta el acceso a Directorio Activo, y al dominio @itm.edu.co. Para el dominio @correo.itm.edu.co la cuenta se desbloqueará automáticamente en 1minutos.

IV. Red

Las redes tienen como propósito principal servir en la transformación e intercambio de información dentro del ITM entre los usuarios, dependencias, oficinas y hacia el exterior a través de conexiones con otras redes u otras entidades.

51. El Departamento de Sistemas no es responsable por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.

52. Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del responsable del equipo.

53. No se permite el uso de los servicios de la red cuando no cumplan con las labores propias dentro del ITM.

54. Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad del ITM y se usarán exclusivamente para actividades relacionadas con la labor asignada.

55. Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles, se permite su uso única y exclusivamente durante la vigencia de derechos del usuario.

56. El Departamento de Sistemas es el único que cuenta con permisos para el uso de analizadores de red, los cuales son usados para monitorear la funcionalidad de las redes.

57. No se permitirá el uso de analizadores para monitorear o censar redes ajenas a el ITM y no se deben realizar análisis de la Red desde equipos externos a la entidad sin previa autorización del Departamento de Sistemas.
58. Cuando se detecte un uso no aceptable, se cancelará la cuenta o se desconectará temporal o permanentemente al usuario o red involucrada, dependiendo de las políticas, la reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.

59. Se prohíbe la desconexión de un equipo para conectar un equipo personal u otro equipo de comunicaciones.

60. Se prohíbe configurar dispositivos en la red LAN que permitan conexiones remotas a la red, para esto el departamento de sistemas proveerá el mecanismo de conexión.

61. Se prohíbe la conexión de equipos inalámbricos en cualquier punto de red institucional.

IV.1 Redes Privadas Virtuales (VPN)

62. Los funcionarios del ITM podrán tener acceso a la red interna cuando se encuentren fuera de esta con acceso a Internet público, utilizando las redes privadas VPN habilitadas por el Departamento de Sistemas.

63. El Departamento de Sistemas será el encargado de configurar el software necesario y asignar las claves a los usuarios que lo soliciten.

64. El usuario debe validar el equipo desde el que usa la VPN, que esté en óptimas condiciones; sistemas operativo y aplicaciones actualizado, y contar con un Endpoint de última generación.

65. El usuario que utilice una VPN es responsable del acceso remoto y del uso de este.

66. Para que un funcionario o proveedor del ITM pueda acceder a los equipos, ya sean servidores u otros equipos de la red interna del ITM desde una conexión externa con la tecnología VPN, cumplirá con el siguiente procedimiento:
    - ✓ La solicitud debe ser realizada por medio del Portal de Soluciones - Mesa de Servicios TI la cual debe incluir el formato con la justificación para la solicitud de este acceso e indicará el tiempo requerido para el mismo, la información completa de la conexión y la información del aprobador de la solicitud, esto aplica a todos los colaboradores y proveedores que tiene que realizar tareas fuera de horas laborables o en instalaciones que necesiten este tipo de acceso, participar en proyectos que requieran apoyo remoto, o alguna otra circunstancia especial que así lo amerite.
    - ✓ Si un proveedor requiere acceso por VPN, este se debe gestionar por medio del supervisor del contrato o el jefe de dependencia para la cual presta los servicios.
    - ✓ El Departamento de Sistemas evaluará la solicitud, si aprueba la misma, se procederá a otorgar los permisos y acceso a la VPN. De no ser aprobada, se devuelve al usuario o proveedor solicitante con las razones de la decisión.
    - ✓ Una vez aprobada la solicitud, se notifica al usuario o proveedor y se le dan las instrucciones para conectarse vía VPN, si es necesario, personal técnico asistirá al usuario en el proceso de configuración.

IV.2 Seguridad en Centros de Cómputo y de Cableado

67. Las instalaciones con fines específicos que alberguen equipos de procesamiento, almacenamiento, conectividad, seguridad, considerados críticos, requieren una mayor protección que la proporcionada a las instalaciones comunes, debe considerarse a todas las funciones de TI y al material relacionado como confidencial y protegerlos de

manera acorde, esto se debe coordinar con el área encarda de la seguridad perimetral de los centros de cómputo.

68. El acceso a los centros de cómputo y centros de cableado es restringido y solo el personal de Infraestructura del Departamento de Sistemas puede tener acceso a estos, en caso de requerir el acceso de otra persona deberá contar con los permisos necesarios del jefe de departamento o jefe de administración de red.

69. Solo el personal autorizado por el operador de servicios TIC cuenta con el acceso a los gabinetes (racks) donde se encuentre alojada infraestructura de procesamiento, almacenamiento, networking y seguridad, si alguna área requiere el acceso a estos gabinetes (rack) se debe solicitar al Departamento de Sistemas el respectivo acceso a estos.

70. Garantizar el monitoreo y diligenciamiento de la bitácora para los accesos otorgados a los centros de cómputo, previa autorización del responsable del ITM, al personal de soporte técnico, proveedores, operador de servicios TIC, colaboradores, etc.

71. No está permitida la toma de fotografías o grabación de video, en áreas de procesamiento de información o donde se encuentren activos de información que comprometan la seguridad o la imagen de la entidad, a menos que esté autorizado.

V. Telefonía

V.1 Telefonía Fija

72. El Departamento de Sistemas es el responsable de contar con los recursos de hardware y software para dar solución a las necesidades de telefonía fija institucional.

73. Los usuarios que requieran de este elemento deberán solicitar a través del Por tal de Soluciones los equipos y la extensión necesaria.

74. El uso correcto del servicio deberá ser vigilado por los líderes de cada área.

75. El equipo será cargado al inventario del empleado o del jefe de área.

V.2 Telefonía Celular

76. Sólo le serán asignadas líneas de telefonía móvil y equipos celulares corporativo a los funcionarios autorizados por el rector de la institución, estos equipos y/o líneas celulares son propiedad de ITM y deben ser regresados cuando haya desvinculación laboral de estos empleados.

77. Si por necesidades del servicio se requiere líneas de telefonía móvil para otras dependencias de la Institución, estas serán autorizadas por la Jefatura del Departamento Financiero y Comercial, previamente justificación de la dependencia solicitante.

78. Al funcionario al cual se le asigne el equipo de telefonía móvil será el responsable y debe velar por el buen uso del equipo y la línea telefónica asignados, no se podrá endosar, ni prestar, reasignar equipos y líneas telefónicas que hayan sido asignadas.

79. Antes de emitir el “paz y salvo”, el responsable de Bienes Muebles debe solicitar un concepto para valorar el estado actual del teléfono celular al Departamento de Sistemas.

80. El responsable del grupo Bienes Muebles de la entidad realiza el respectivo reintegro del equipo, teniendo en cuenta el cumplimiento de los aspectos relacionados en el procedimiento de Bienes Muebles.

81. El Departamento de Sistemas será el enlace con el proveedor de telefonía móvil para adquirir, modificar y cancelar los planes de las líneas telefónicas, además de verificar los consumos mensuales.

82. Una vez terminado el uso de la línea telefónica asignada, el grupo Bienes Muebles debe notificar al Departamento de Sistemas para la cancelación o reasignación de dicha línea.

83. En caso de pérdida o hurto, el funcionario/a responsable del teléfono celular corporativo y de la línea telefónica, está obligado a reportar la pérdida del equipo al Departamento de Sistemas y a Bienes Muebles. adjuntando la respectiva denuncia ante la autoridad competente.

VI. Servidor de Archivos

80. Todos los usuarios de la plataforma tecnológica son responsables de la información que en esta se manipula y que el uso de los recursos informáticos debe responder estrictamente a necesidades institucionales, para tal efecto el ITM posee dos repositorios en los cuales los usuarios son responsables de depositar allí la información institucional: el Servidor Hathor y la Biblioteca Documental en SharePoint.

81. Es responsabilidad del funcionario mantener la información en estos repositorios.

82. No se permite el almacenamiento en estos de información personal o no relacionada con la institución, en caso de encontrarse allí información personal o no institucional, el Departamento de Sistemas procederá a eliminarla sin previo aviso al colaborador.

83. El acceso a la información depositada en los servidores de archivos será de acceso restringido al propietario de esta, si por alguna razón es necesario conceder acceso a otro usuario, este se debe solicitar a través El Portal de Soluciones ITM – Mesa de Servicios TI por el propietario de la misma.

84. El Departamento de Sistemas solamente hace copias de respaldo de la información contenida en nuestras Bibliotecas Documentales. En ningún caso hacemos copias de respaldo de la información almacenada en los equipos de cómputo de los usuarios, por esto, los funcionarios son los responsables de sus respaldos. Por lo motivos anteriores, los líderes de las diferentes dependencias son llamados a instar a sus colaboradores a que eviten almacenar localmente su información.

85. Ante el retiro de cualquier empleado, el ITM podrá acceder, recuperar, trasladar y hacer uso de la información que estos hayan dejado en cualquier medio de almacenamiento para asegurar así la correcta continuidad de los procesos.