Política de Almacenamiento ITM-Microsoft

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[1], propendiendo que la seguridad y protección de la información institucional sea gestionada correctamente a través de un proceso sistémico conocido por toda la institución.

Objetivo

Informar a todos los usuarios que realizan actividades relacionadas con los servicios que brinda la plataforma tecnológica, las políticas asociadas al acceso, manejo y responsabilidades que les compete frente al adecuado respaldo de la información.

Políticas de Respaldo y Almacenamiento de la Información

La biblioteca oficial de la institución es Microsoft SharePoint, es allí en donde debe hacerse el almacenamiento de la información institucional, los respaldos de históricos institucionales se dispondrán en Hathor. Lo anterior debe ser realizado por cada una de las dependencias como encargados de la información que manejan en su interior.

Los límites de almacenamiento, tamaño de buzón, envío de correos, peso máximo de adjuntos, espacio en OneDrive y SharePoint serán definidos por el Departamento de Sistemas, de acuerdo con las licencias vigentes y la capacidad asignada por Microsoft, estos se aplicarán a @itm.edu.co y @correo.itm.edu.co de forma independiente.

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

Esta política aplica a todos los docentes, estudiantes administrativos, contratistas y cualquier persona que tenga una cuenta institucional de Microsoft (@itm.edu.co o @correo.itm.edu.co).

Responsabilidades por parte de los jefes de dependencias:

- Tramitar ante el Departamento de Sistemas la creación de los sitios necesarios en SharePoint y/o Hathor para su dependencia.
- Tramitar ante el Departamento de Sistemas la creación de cuentas de Microsoft para los usuarios que lo requieren, informando las fechas de inicio y vencimiento de estas.
- Informar al Departamento de Sistemas sobre la necesidad de renovar las fechas de vencimiento de las cuentas de Microsoft de su dependencia.
- Asegurar que la información institucional de los miembros de sus equipos esté siendo almacenada de forma periódica en los repositorios institucionales (SharePoint y Hathor)
- Asegurar que todos los miembros de sus equipos de trabajo dejen con el jefe de la dependencia los archivos de correo electrónico local (PST) de Outlook en el momento de su desvinculación o terminación de contrato con el ITM.
- El jefe de cada área se encarga de establecer los roles y permisos para cada una de las personas que acceden a estos recursos.
- El jefe de cada área debe velar por dar a conocer y garantizar el cumplimiento de esta política en su equipo de trabajo.
- Cada dependencia deberá clasificar la información según su nivel de sensibilidad y aplicar las medidas de seguridad y respaldo que correspondan.
- Cada jefe deberá respaldar en el SharePoint de la dependencia los PST y los archivos de OneDrive de los usuarios que se desvinculen dentro de los 3 meses siguientes a su retiro, transcurrido dicho plazo, toda la información será eliminada de forma definitiva y no podrá ser recuperada.
- Las solicitudes al Departamento de Sistemas deberán hacerse a través de la mesa de ayuda institucional.

Responsabilidades por parte de los usuarios:

- El uso de herramientas como OneDrive se podrá dar a discreción de cada jefe de dependencia, lo anterior teniendo en cuenta que la información que estas cuentas contengan será eliminada una vez sea retirada la persona de la institución.
- Todo empleado, docente, contratista deberá guardar la información institucional generada por cada usuario, en la biblioteca documental (SharePoint) o en Hathor.
- En esta biblioteca solo se deberá guardar información institucional. Cada usuario será el responsable de guardar allí la información, la cual es solo de carácter institucional.
- Hathor deberá ser usado como respaldo de la información histórica del ITM, lo anterior no deberá almacenarse en nube.
- Si el usuario necesita recuperar información de un Backup, debe ingresar el requerimiento a la mesa de ayuda institucional para que allí sea atendido el requerimiento y enviado a la persona encargada en el Departamento de Sistemas.
- El usuario deberá reportar de forma inmediata al departamento de sistemas cuando detecte que existan riesgos reales o potenciales en sus equipos de cómputo que puedan comprometer la integridad de la información.
- Las copias locales de respaldo de correos electrónicos (PST), son responsabilidad del usuario, este deberá, según la criticidad e importancia, adoptar diferentes estrategias para almacenarla.
- La información almacenada de forma local en los discos duros son responsabilidad del usuario y no se realiza copias de respaldo de esta.
- Los videos de reuniones en Teams guardadas, o los archivos adjuntos de las mismas, deben ser descargadas por los usuarios interesados en un plazo máximo de 8 días. Lo anterior ya que SharePoint eliminará los mismos de forma automática.

Responsabilidades por parte del Departamento de Sistemas:

- Crear cuentas de Microsoft a los usuarios que soliciten las diferentes dependencias, lo anterior con las licencias y las capacidades de almacenamiento dispuestas por el Departamento de Sistemas

- Se hará responsable de conservar la información almacenada en la biblioteca documental. La información por fuera de estos medios, incluyendo Outlook será responsabilidad del usuario.
- Será el responsable de la creación de las Bibliotecas Documentales, acorde con las solicitudes de los jefes o coordinadores de estas.
- Será el responsable de garantizar que los accesos suministrados a las bibliotecas documentales sean los informados por los jefes de dependencia.
- Será el encargado de monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Será el responsable de evaluar y aprobar metodologías y procesos específicos relativos a la seguridad de la información dispuesta en las Bibliotecas Documentales.
- Será el responsable de respaldar la infraestructura de servidores y bases de datos corporativa en un Backup incremental de lunes a viernes después de las 6:00pm, y según las políticas de retención definidas en el DRP para cada activo de información.
- Implementar mecanismos de replicación de los Backup a data center alternos.
- Los Backup de la infraestructura de servidores y bases de datos de ambientes productivos, sebe ser a equipos inmutables.
- El Departamento de Sistemas eliminará las cuentas de los usuarios que no tienen vinculo con el ITM 3 meses después de su retiro.
- En caso de realizar un procedimiento invasivo que pueda poner en riesgo la integridad del activo, este deberá ser clonado, una vez se valide el cambio positivamente, se procederá a borrar el clon del activo de información.
- Toda la solución de Backup, debe contar con renovaciones anuales, y contratos de soporte y mantenimiento de esta.
- Deberán realizar pruebas de recuperación aleatorias de servidores para validar la efectividad de los Backup, y definir un formato para su registro.
- Revisar y analizar los reportes diarios de la plataforma de Backup para detectar anomalías y corregirlas en caso de que haya lugar, para garantizar un Backup en óptimas condiciones.

- Las configuraciones de equipos de red y sistemas de seguridad perimetral deberán contar con Backup en la biblioteca documental del departamento de sistemas, con una frecuencia mensual, o cuando existan cambios importantes en la configuración.
- El Departamento de Sistemas realizará auditorías periódicas sobre los repositorios institucionales para verificar el cumplimiento de la política y la integridad de la información.
- El Departamento de Sistemas Podrá dar acceso a la información de cualquier cuenta con dominio institucional a Rectoría, Secretaría General o al Departamento de Personal según la naturaleza del contrato de la persona vinculada a la cuenta mediante solicitud oficial al jefe del Departamento de Sistemas.
- Dar a conocer periódicamente la presente política a los usuarios de cuentas Microsoft de la institución.

Matriz de Respaldo y Almacenamiento

¿Dónde Guardar?	Tipo de Información	Propósito y Nivel de Riesgo	¿Tiene Respaldo Institucional?	Responsable de la Información
Microsoft SharePoint (Sitio oficial del área/dependencia)	Documentos de Trabajo Activos (Informes, minutas, proyectos en curso, etc.)	Repositorio oficial y colaboración. BAJO RIESGO.	Sí (Automático, gestionado por Sistemas)	Usuario / Jefe de Dependencia
Hathor (Repositorio de Históricos / Archivo Institucional)	Archivos Históricos y Cierre (Documentos finalizados, expedientes cerrados, etc.)	Conservación a largo plazo y archivo. BAJO RIESGO.	Sí (Automático, gestionado por Sistemas)	Jefe de Dependencia
Microsoft Outlook 365 (Capacidad limitada)	Correos electrónicos Activos	Correo Electrónico en la nube. BAJO RIESGO.	Sí (Automático, gestionado por Sistemas)	Usuario
Archivos en Disco C:\ y respaldar en un medio externo	Correo Electrónico Local (PST)	En riesgo de pérdida si no se respalda en medios externos	No	Usuario / Jefe de Dependencia
Microsoft OneDrive	Borradores y Archivos Personales (Uso temporal, de un solo usuario, no institucionales)	Almacenamiento personal en la nube. RIESGO MEDIO (Sujeto a eliminación tras desvinculación del usuario).	Sí	Usuario (Pérdida es responsabilidad del usuario)
Archivos en Disco C:\	Archivos que no son necesarios ni importantes	En riesgo de pérdida si no se respalda en medios externos	No	Usuario (Pérdida es responsabilidad del usuario y jefe de dependencia)