POLÍTICA DE SEGURIDAD Y GESTION DE LA INFORMACIÓN UNIVERSIDAD AUTÓNOMA DEL CARIBE

1. INTRODUCCIÓN

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen necesarios para lograr los objetivos de la organización y asegurar el cumplimiento de objetivos misionales.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el "hacking" o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

El Consejo Directivo de la Universidad Autónoma del Caribe mediante Acuerdo No. 806-01 de diciembre 04 de 2009 aprobó el *Reglamento para uso adecuado de las tecnologías de la información y comunicaciones* el cual estableció políticas para el uso apropiado, mantenimiento y conservación de la infraestructura tecnológica en la Institución, sin embargo, La Universidad para satisfacer su creciente demanda educativa, ha aumentado su inventario tecnológico tanto en infraestructura de hardware, software e información, por lo que se hace necesario crear una la Política de Gestión y Seguridad de la Información que esté basada y sirva como referencia a la futura implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) según la norma IS027001 con el objetivo de garantizar la integridad, confidencialidad y disponibilidad de este importante activo, teniendo como eje el cumplimiento de los objetivos misionales.

En el contexto del presente documento se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma

en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

2. OBJETIVO

- Establecer los lineamientos necesarias para proteger, preservar y administrar correctamente la información de la Universidad Autónoma del Caribe junto con las tecnologías utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

- Crear una la Política de Seguridad de la Información que esté basada y sirva como marco de referencia a la futura implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) según la norma IS027001 para la Universidad Autónoma del Caribe.

3. ALCANCE

Esta política aplica a todas las áreas que componen la institución, a sus recursos, a la totalidad de los procesos internos o externos vinculados a la universidad a través de contratos o acuerdos con terceros y a todo el personal de la Universidad Autónoma del Caribe, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

4. DEFINICIONES

Para efectos de la aplicación de las políticas se adoptan las siguientes definiciones:

4.1. **Activos de Información:** cualquier componente (humano, tecnológico, software, manuales, documentación, entre otros) que tiene valor para la organización y signifique riesgo si llega a manos de personas no autorizadas.

4.2. **Información:** todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

4.3. **Reportes básicos académicos (RBA):** son aquellos informes generados por el sistema de información institucional que soportan o sirven de base para la toma de decisiones en la gestión académica y el reporte a los organismos de inspección, control y vigilancia, tanto en el ámbito interno como externo.

4.4. **Activos de Información críticos:** activo de información cuya afectación o alteración puede generar un impacto negativo de carácter económico, legal o al buen nombre de la institución.

4.5. **Archivo:** colección de datos e información del mismo tipo, almacenada en forma organizada como una unidad, que puede emplearse y tratarse como soporte material de la información contenida en éstos.

4.6. **Aplicación:** programa informático diseñado para permitir a los usuarios la realización de tareas específicas en computadores, servidores y similares.

4.7. **Base de Datos:** conjunto de datos almacenados y organizados con el fin de facilitar su acceso y recuperación.

4.8. **Backups o Copias de respaldo:** copia que se realiza a la información institucional definida como sensible o vulnerable, con el fin de utilizarla posteriormente para restablecer el original ante una eventual pérdida de datos, para continuar con las actividades rutinarias y evitar pérdida generalizada de datos.

4.9. **Clasificación de seguridad del documento:** clasificación estratégica adoptada por el Sistema de Gestión de la Calidad, con el fin de llevar a cabo la gestión interna referente al mantenimiento de la seguridad de la información de acuerdo a su importancia para la organización, esta clasificación se define como:

- Público: información de dominio público, sean físicos o electrónicos, que la universidad puede dar a conocer a terceras partes como estudiantes, proveedores, docentes y demás estamentos que tengan alguna relación directa o indirecta. Dicha información puede estar publicada en cartelas de la entidad o en las páginas web de la Universidad.

- Controlado: documentos de gestión físicos o electrónicos de las diversas unidades de la institución, que contienen los métodos de trabajo usados para su operación y/o para formación del personal. El acceso a esta información está restringido a los miembros de cada área o disponibles para los ejercicios de auditoria interna o externa de la institución.

- Reservado: documentos estratégicos, o con información descriptiva de claves o datos técnicos de funcionamiento de las diversas unidades de la institución, que pueden ser físicos o electrónicos. Esta información solamente será accedida por personal autorizado para su uso y/o para atender solicitudes derivadas de los procesos de auditorías internas o externas y/o para atender requerimientos de orden legal o jurídico.

4.10. **Código fuente:** conjunto de instrucciones escritas en algún lenguaje de programación de computadoras, hechas para ser leídas y transformadas por alguna herramienta de software (compilador, intérprete, ensamblador) en lenguaje de máquina o instrucciones ejecutables en el computador.

4.11. **Credenciales de acceso:** privilegios de seguridad agrupados bajo un nombre y contraseña, que permiten acceso a los sistemas de información.

4.12. **Custodio:** es el encargado de gestionar y administrar la adecuada operación del activo y la información relacionada con éste. En ocasiones el responsable y el custodio son la misma persona.

4.13. **Datacenter, centro de datos o sala de servidores:** área dispuesta para el alojamiento seguro de los equipos de cómputo necesarios para el procesamiento y almacenamiento de la información de una organización (Servidores, SAN, equipos de comunicación, etc.).

4.14. **Dispositivo biométrico:** dispositivo de seguridad utilizado en sistemas computarizados que sirve para identificar atributos físicos como rasgos faciales, patrones oculares, huellas digitales, la voz y la escritura.

4.15. **Dispositivo móvil:** aparato electrónico con capacidades de cómputo y conexión a redes inalámbricas cuyo tamaño y diseño permite ser fácilmente transportado para utilizarse en diversas ubicaciones con facilidad (portátiles, tablets, celulares inteligentes y demás dispositivos con características similares).

4.16. **Información sensible o vulnerable:** también llamado activo sensible, es el nombre que recibe la información personal o institucional (datos personales, información financiera, contraseñas de correo electrónico, datos personales, datos de investigaciones), la cual puede ser alterada, descompuesta, mal utilizada, divulgada y/o eliminada, causando graves daños a la organización propietaria.

4.17. **Niveles de backup:** se refiere a la cantidad de copias o respaldos que se tiene de datos determinados. Si se cuenta con una sola copia, se está hablando de un backup de 1er. Nivel; si se tienen dos copias, de un backup de 2do. Nivel. Cuanto mayor sea el número de niveles de backup, menor será el riesgo de perder los datos.

4.18. **Propietario:** en la estructura administrativa de la institución, se le otorga la propiedad del activo a cada una de las unidades estratégicas, divisiones organizacionales, gerencias, rectorías o vicerrectorías.

4.19. **Responsable:** el Jefe de área o gerente de cada una de dichas áreas, será el responsable ante la Institución, de los activos de información registrados como de su propiedad.

4.20. **SAN (Storage Area Network) O Red de Área de Almacenamiento:** recurso compartido, empleado como repositorio de información institucional tanto de funcionarios, docentes y/o contratistas como de grupos y unidades funcionales, donde se definen permisos de acceso de acuerdo a los roles al interior de la organización.

4.21. **Seguridad de la Información:** son todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información.

4.22. **Servidor:** equipo de computación físico o virtual, en el cual funciona un software, cuyo propósito es proveer servicios a otros dispositivos dentro de la red.

4.23. **Servidor de Almacenamiento:** equipo servidor dotado con varios discos duros destinados a respaldar y compartir datos.

4.24. **Sistema Operativo (SO) u Operating System (OS):** programa o conjunto de programas que en un sistema informático gestiona los recursos de hardware y provee servicios a los programas de aplicación, ejecutándose en modo privilegiado respecto de los restantes.

5. POLÍTICA PARA DISPOSITIVOS MÓVILES

5.1. Se permite el uso de dispositivos móviles de conexión inalámbrica al interior de las instalaciones de la Universidad Autónoma del Caribe, únicamente para desarrollar y cumplir con los objetivos laborares y/o contractuales del personal, procurando que no se almacene en estos dispositivos información institucional y siempre en cumplimento del *Reglamento para el uso de las TICS* de la Institución.

5.2. Los dispositivos móviles asignados a administrativos, contratistas y/o docentes, son de propiedad de la entidad, y los responsables de dichos equipos deberán velar por su adecuado uso, cuidado, mantenimiento y protección.

5.3. Los medios de almacenamiento de estos dispositivos pueden ser protegidos tecnológicamente con medios de cifrado de datos o mediante cualquier otro mecanismo definido por la Centro de Sistemas, con el fin de evitar la interceptación y/o uso indebido de la información que en ellos se almacene.

5.4. El funcionario asumirá los riesgos y costos asociados a la perdida, fuga o uso indebido de la información que se encontraba en los dispositivos extraviados, además del cumplimiento de

las políticas y regulaciones vigentes por parte de la Vicerrectoría Administrativa y/o Financiera, concernientes a los costos del activo físico.

5.5. La solicitud de conexión de dichos dispositivos a la red inalámbrica de la institución se realizará por intermedio de la mesa de ayuda de tecnología o por los funcionarios debidamente autorizados por el Centro de Sistemas.

5.6. La autorización de retiro de las instalaciones de los dispositivos móviles se deberá regir por las regulaciones emitidas por la Oficina de Infraestructura Física de la Vicerrectoría Administrativa en lo concerniente a autorización de salida de elementos.

5.7. Se prohíbe conectar a los perfiles de red institucionales dispositivos móviles de uso personal, salvo que exista autorización explícita emitida por el Centro de Sistemas.

5.8. Se prohíbe el ingreso de teléfono celulares y otros dispositivos móviles a los centros de datos y centros de cableado de la institución, salvo que exista una autorización explícita emitida por el Centro de Sistemas.

5.9. La alta dirección de la institución podrá exigir para determinadas reuniones la ausencia de dispositivos móviles, dispositivos de grabación y cualquier otro equipo electrónico que se especifique por razones confidencialidad o de evitar la interceptación y/o uso indebido de la información que en ellos se almacene.

5.10. Para los visitantes y personal de apoyo que ingrese a la institución y que requiera para sus funciones o servicios a prestar, el uso de alguno de estos dispositivos móviles, deben aplicarse las mismas restricciones de uso; adicionalmente, deberá estar siempre acompañado del responsable por parte de la Universidad para esta visita, con el fin de evitar usos indebidos de las tecnologías.

6. POLÍTICA DE CONTROL DE ACCESO LÓGICO

6.1. Es responsabilidad de la Oficina de Talento Humano, informar a el Centro de Sistemas sobre los nuevos administrativos, contratistas y/o docentes que ingresan a la institución, con el fin de poder asignar desde el Centro de Sistemas, los respectivos permisos para el acceso a los recursos tecnológicos de la institución.

6.2. El Centro de sistemas es el área encargada de definir y suministrar los mecanismos de acceso lógico para la asignación de permisos y privilegios a los usuarios de acuerdo a sus funciones, términos contractuales y/o roles definidos al interior de la entidad, así como la modificación los permisos y privilegios de los usuarios en los mecanismos y/o sistemas de autenticación definidos.

6.3. La Oficina de Talento Humano es la encargada de notificar y dar los lineamientos para la creación, modificación y supresión de permisos y privilegios de usuarios.

6.4. Se prohíbe el uso de las cuentas de usuario administrador local en la institución, salvo en aquellos casos que estén debidamente justificados y autorizados.

6.5. Los propietarios, responsables y/o custodios de los activos de información de la institución deben revisar periódicamente los derechos de acceso de los usuarios.

6.6. Los propietarios y/o responsables de los activos deben informar inmediatamente sobre las novedades de los derechos de acceso lógico de los usuarios.

6.7. Para la creación y administración de las credenciales de acceso institucionales, estudiantes y egresados, se deben adoptar los lineamientos establecidos por el Centro de Sistemas.

6.8. Los usuarios son los únicos responsables por la seguridad de sus credenciales de acceso (usuario y contraseña), las cuales son de uso exclusivo, único e intransferible.

7. POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS

7.1. La Universidad a través del Centro de Sistemas establecerá la implementación de los sistemas y técnicas criptográficas para la protección de la información, con base en los análisis de riesgos efectuados y con el fin de mantener la confidencialidad, integridad y autenticidad de la información.

7.2. Cada unidad de la Universidad debe velar por tener una óptima administración de la información y debe implementar sistemas y técnicas criptográficas a la información catalogada como reservada o controlada, acorde a los lineamientos institucionales, con el fin de prevenir riesgos relacionados con la fuga de información durante su transmisión o almacenamiento.

7.3. Se deben definir custodios o responsables de la información de carácter reservado en cada dependencia de la Universidad.

7.4. El Centro de sistemas debe brindar el apoyo necesario a administrativos, contratistas y docentes, en el uso de las herramientas tecnológicas para protección de la información sensible, que debe ser cifrada.

7.5. El Centro de sistemas, debe definir las herramientas necesarias para el cifrado de datos, de tal forma que preserve la confidencialidad, la integridad y el no-repudio en la transmisión de información sensible entre la comunidad Universitaria.

7.6. El Centro de sistemas, debe definir un procedimiento de gestión de claves, donde incluirán los métodos para la generación, longitud, eliminación y recuperación de claves en caso de pérdida, divulgación o daño.

7.7. El procedimiento de gestión de claves debe tener en cuenta la fecha de finalización de contratos o de retiro de cada responsable del activo de información; de esta manera podrán desactivar, bloquear o eliminar los accesos no autorizados durante el periodo no laboral para que la información no corra ningún riesgo que afecte la continuidad de los procesos de la universidad.

7.8. Es responsabilidad de la Oficina de Talento Humano informar al Centro de Sistemas sobre las novedades de retiro, con el fin de poder realizar las acciones de desactivación, bloqueo o eliminación de los respectivos accesos.

8. POLÍTICA DE TRANSFERENCIA E INTERCAMBIO DE INFORMACIÓN

8.1. El Centro de sistemas debe realizar acciones de mejoramiento respecto a la seguridad de la información, especialmente respecto al uso de protocolos para realizar transferencia de información digital y/o física entre unidades, usuarios y terceras partes de la institución.

8.2. Los mensajes enviados a través de cualquier medio electrónico que contengan información pública, controlada o reservada, deben ir cifrados y se debe propender porque sólo sean conocidos por el emisor y por el receptor(es), del mensaje.

8.3. Cada unidad y/o supervisor de los contratos firmados con terceros, está en la obligación de verificar la firma de los acuerdos de confidencialidad previo a la transferencia de información entre la Universidad y sus proveedores y/o contratistas.

8.4. Las terceras partes involucradas se verán obligadas a firmar los formatos de confidencialidad aplicables. Estos formatos están disponibles en la página del Componente de Seguridad de la Información, según corresponda para Proveedores y/o Terceros, o administrativos, contratistas y docentes.

8.5. Toda la información que se reciba o envié a través de impresoras, máquinas de fax u otros medios de reprografía y transmisión de datos, debe ser monitoreada por el funcionario que los esté utilizando y debe permanecer siempre sin ningún tipo de documentos o información clasificada como controlada o reservada.

8.6. Toda la información verbal que sea intercambiada por conversaciones formales, atención de llamadas telefónicas y demás procesos que no dejen soportes físicos, debe cumplir con el protocolo de manejo y escalamiento de comunicaciones vigente para la institución.

8.7. El Centro de sistemas debe realizar capacitaciones y/o difundir los lineamientos institucionales para evitar que se traten temas de la Universidad Autónoma del Caribe en sitios públicos o escenarios no autorizados formalmente para la divulgación de información.

8.8. Salvo casos de estricta necesidad y bajo previa autorización y/o recomendación del Centro de Sistemas, no se suscribirán o diligenciarán formularios electrónicos para uso personal o para medíos de investigación a través de internet, así mismo se debe evitar el diligenciamiento de los datos de ubicación física, teléfonos móviles, teléfonos fijos, estructura organizacional, divulgación de cargos o información sensible de la Universidad Autónoma del Caribe, cuando el personal se suscriba o diligencie formularios electrónicos para uso personal o para medíos de investigación a través de internet.

8.9. La Universidad a través de la unidad de planeación establecerá los propietarios, responsables y/o custodios de los reportes oficiales que serán utilizados para la certificación de totales, valores o listados, especialmente al reportar a entidades externas.

8.10. La descarga de reportes a herramientas ofimáticas tipo hoja de cálculo será permitida, pero el archivo de salida será plenamente identificable como un reporte diferente a los que el sistema genere en salidas de solo lectura.

8.11. Los reportes extraídos directamente de los sistemas de información Institucionales contaran con las siguientes características mínimas:

- Deberán ser generados, almacenados y codificados según una fecha de corte claramente estipulada.
- Tienen asignado un propietario, responsable o custodio y un validador de la información contenida.
- El propietario es el único autorizado para su generación, difusión al interior de la institución y el subsecuente archivo o salvaguarda.

8.12. Los reportes oficiales utilizados para la certificación de totales, valores o listados, especialmente los dirigidos a entidades externas, organismos de inspección, control y/o vigilancia, deberán ser validados y firmados física o digitalmente por el responsable de la información, para esto la Institución establecerá en sus procesos y procedimientos los propietarios, responsables y/o custodios para cada caso.

8.13. Cada líder de unidad será el responsable de definir los permisos de acceso a los dispositivos de almacenamiento central o SAN, como repositorio de información institucional.

8.14. El Centro de sistemas será el encargado de definir los mecanismos y lineamientos de uso de la unidad de almacenamiento SAN.

8.15. La recepción de correspondencia rotulada como "Información Confidencial" únicamente podrá ser revisada y visualizada por el destinatario de los documentos.

8.16. El envío de correspondencia rotulada como "Información Confidencial" solo podrá salir de la Universidad en medio impreso o digital con la expresa autorización del emisor.

8.17. Cada unidad está encargada de solicitar a la Oficina de Infraestructura física, que la correspondencia rotulada como "No Confidencial" no sea abierta por parte del grupo de correspondencia.

8.18. Toda información clasificada como sensible o vulnerable que sea enviada por medios electrónicos, debe usar algoritmos de cifrado según los lineamientos del Centro de sistemas.

8.19. El custodio de la información de cada unidad, es el responsable de velar por el cumplimiento de la clasificación, foliación y rotulación de los documentos, de conformidad con los términos ordenados por la oficina Jurídica y/o la Secretaria General de la Institución.

9. POLÍTICAS DE DESARROLLO SEGURO

9.1. Las solicitudes de desarrollos nuevos o modificación de las aplicaciones actualmente instaladas que se encuentran en producción, deben ser tramitadas conforme a los procedimientos de calidad vigentes y estipulados para tal fin. De acuerdo al procedimiento, las solicitudes realizadas en el tiempo estipulado, serán sometidas a un proceso de verificación y posterior aprobación o rechazo de la solicitud. La sola radicación no implica aceptación y estará sujeta a un cronograma de desarrollo con prioridades según los objetivos misionales de la Universidad.

9.2. El Centro de sistemas es la única unidad encargada de la realización de desarrollos dentro de la Universidad y dará cumplimiento a los lineamientos de construcción de aplicaciones seguras adoptados por la Universidad a través de esta gerencia.

9.3. Todo desarrollado será puesto en producción según las presentes políticas, los términos y condiciones de privacidad y el reglamento para el uso adecuado de las TICs.

9.4. La Universidad apoyará la debida aplicación de los lineamientos de desarrollo mediante la facilitación de elementos y ambientes de trabajo adecuados para el equipo de desarrollo de la Universidad.

9.5. Queda prohibido el acceso y/o uso de los recursos físicos y/o tecnológicos a personal no autorizado y en general, a los recursos asignados al grupo de desarrollo del Centro de Sistemas. El intento de uso total o parcial del código fuente de las aplicaciones administradas y/o adquiridas por el Centro de Sistemas por parte de personal no autorizado queda expresamente prohibido.

9.6. Con el fin de garantizar la seguridad, estabilidad y usabilidad de las soluciones, todos los desarrollos nuevos o modificaciones a desarrollos existentes, se deben realizar de conformidad con el Procedimiento de desarrollo de sistemas de información aprobado y vigente para tal fin.

9.7. Las áreas solicitantes de desarrollos nuevos o modificaciones a desarrollos ya existentes, deben asignar a funcionarios idóneos para colaborar en la realización y aprobación de los resultados de las pruebas.

9.8. Las solicitudes de desarrollo o modificación de aplicaciones que no pueden ser atendidas por el Centro de Sistemas, se regirán por el procedimiento de "Contratación de bienes y servicios" vigente en la Universidad.

10. POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS

10.1. El escritorio de trabajo de todos los administrativos, contratistas, docentes o proveedores de la institución, debe permanecer completamente despejado y libre de documentos controlados y/o reservados a la vista del público.

10.2. Todos los documentos controlados y/o reservados y en general, toda la documentación clasificada como "Información confidencial" debe permanecer guardados en un lugar seguro (archivadores con llaves o cajas fuertes), ya sea en un espacio físico o virtual, siempre que mantenga las debidas condiciones de almacenamiento y claves de acceso.

10.3. El escritorio o la pantalla de inicio del computador, tableta, escritorio virtual o cualquier dispositivo que permita el acceso a información institucional, debe permanecer libre de documentos, carpetas e íconos de acceso directo a archivos y/o carpetas que contengan documentos. En lo posible, sólo deben permanecer en la pantalla los íconos por defecto del sistema operativo instalado en el equipo.

10.4. Todos los administrativos, contratistas, docentes y/o proveedor son responsables de velar por la adecuada protección de la información física y lógica al ausentarse de su puesto de trabajo.

11. POLÍTICA DE GESTIÓN DE CAMBIOS

11.1. Los recursos que se encuentran administrados por el Centro de sistemas que son cobijados por el procedimiento de Gestión de Cambios y Despliegue del Servicio y Despliegue del Servicio son: las Aplicaciones de Software que han sido desarrolladas internamente o desarrolladas externamente y entregadas formalmente para su administración, los equipos de cómputo misionales (Servidores), las redes de telecomunicaciones locales, extendidas y externas, los manejadores de bases de datos institucionales y la información documentada de los servicios gestionados por esta gerencia.

11.2. Cualquier modificación a las condiciones actuales de funcionamiento de los recursos administrados por el Centro de sistemas y serán cobijados por el Procedimiento de desarrollo de sistemas de información aprobado y vigente para tal fin, serán considerados como Cambios Tecnológicos y por tanto, deben cumplir con los procedimientos y protocolos emitidos por el área de tecnología Institucional.

11.3. El Centro de sistemas determinará las fechas y responsables de efectuar la validación de condiciones y la correspondiente ejecución controlada del cambio.

11.4. En casos de emergencia manifiesta, que estén afectando directamente la normal prestación de los servicios de la Universidad Autónoma del Caribe en cualquiera de sus unidades, se podrán realizar cambios en la configuración de recursos y servicios de infraestructura tecnológica; sin que estos cambios sean susceptibles de revisión posterior por parte del área de Tecnológica. La emergencia manifiesta será estipulada por el Centro de Sistemas o la rectoría.

11.5. La Universidad Autónoma del Caribe propenderá porque los servicios tecnológicos que se encuentran tercerizados, cuenten con procedimientos y/o protocolos definidos para la Gestión de Cambios y Despliegue del Servicio sobre los servicios contratados.

12. POLÍTICAS DE BACKUPS O COPIAS DE SEGURIDAD

12.1. La responsabilidad de la gestión de las copias de respaldo y la administración de los equipos de respaldo masivo de datos estará a cargo de la persona designada por el Gerente/Director del Centro de Sistemas. El ingeniero de plataforma tecnológica es el encargado de la administración de equipos de respaldo masivo de datos.

12.2. El encargado de la administración de equipos de respaldo masivo de datos, velará por los backups y por el resguardo de los datos contenidos en ellos; así como por su integridad, disponibilidad y confidencialidad.

12.3. Los medios de respaldo empleados para efectuar las copias de seguridad en la Universidad Autónoma del Caribe serán los definidos por el gerente/director del Centro de Sistemas o el Ing. Administrador de plataforma tecnológica en el procedimiento de Copias de Respaldo o aquel que lo supla.

12.4. El responsable de la administración de equipos de respaldo masivo de datos, velará por los respectivos medios de respaldo (y los datos contenidos en éstos) y serán quienes tengan acceso a ellos.

12.5. Se hará Respaldo a los archivos, aplicaciones, bases de datos y configuración de los sistemas operativos de los servidores calificados como críticos para la Universidad Autónoma del Caribe, contemplados en el Inventario de Servidores Críticos asociado al Procedimiento Copias de Respaldo.

12.6. Se incluye como información a respaldar, las configuraciones completas de los servidores.

12.7. El Centro de sistemas será la responsable de definir los mecanismos adecuados para la ejecución de los respaldos de información, así como la periodicidad, etiquetado, lugar de archivo y el tiempo de retención de las copias.

12.8. Para todos los casos de criticidad definidos en el Inventario de Servidores Críticos, será obligatorio contar con mínimo dos niveles de respaldo.

12.9. La ejecución de las copias de seguridad debe llevarse a cabo en horas de poca o ninguna actividad laboral; por lo tanto el Centro de sistemas será la responsable de definir el horario de ejecución de éstas.

12.10. En los casos en que el backup no finalice exitosamente dentro de los tiempos establecidos, éste se relanzará después de evidenciado el fallo, en los tiempos establecidos en el procedimiento de Copias de Respaldo.

12.11. Cuando sea necesario un respaldo por demanda de los servidores críticos, se debe solicitar formalmente a través de la mesa de ayuda o mediante correo electrónico por parte del personal autorizado, para informar mínimo con 24 horas de antelación sobre posibles interrupciones en el servicio a las personas afectadas.

12.12. Todos los respaldos se revisarán con la periodicidad definida en el Procedimiento de Copias de respaldo y se evidenciarán en la bitácora de backups.

12.13. La Comprobación periódica del estado de las copias se llevará a cabo con el fin de garantizar la disponibilidad e integridad de los datos almacenados. Los responsables de la administración de equipos de respaldo masivo de datos evidenciarán la comprobación periódica del estado de las copias de seguridad en el formato para pruebas periódicas de restauración de backups.

12.14. Los equipos para el respaldo de información de la Universidad Autónoma del Caribe deben estar ubicados en centros de datos (Datacenters) con las medidas de seguridad pertinentes, y tener contratos de soporte y mantenimiento regular vigentes.

12.15. Los medios de almacenamiento de datos deben tener un manejo adecuado para mitigar la ocurrencia de daños físicos y por consiguiente la pérdida de la información.

13. POLÍTICA DE GESTIÓN, ADMINISTRACIÓN Y CONSERVACIÓN DOCUMENTAL

13.1. La Universidad Autónoma del Caribe está obligada a la creación, organización, preservación y control de los archivos, teniendo en cuenta los principios de procedencia, orden original, el ciclo vital de los documentos y la normatividad archivística.

13.2. La Universidad Autónoma del Caribe deberá garantizar los espacios y las instalaciones necesarias para la conservación de sus archivos. En los casos de construcción de edificios públicos, adecuación de espacios, adquisición o arrendamiento, deberán tenerse en cuenta las especificaciones técnicas existentes sobre áreas de archivos, como lo establece el Archivo General de la Nación.

13.3. La documentación institucional es producto y propiedad de la Universidad Autónoma del Caribe, y ésta ejercerá el pleno control de sus recursos informativos. Los archivos públicos, por ser un bien de uso público, no son susceptibles de enajenación.

13.4. La Universidad podrá contratar con personas naturales o jurídicas, los servicios de custodia, organización, reprografía y conservación de documentos de archivo, esto teniendo en cuenta lo establecido por el Archivo General de la Nación.

13.5. Los funcionarios, contratistas y docentes de la Universidad, al desvincularse de las funciones titulares, entregarán los documentos y archivos a su cargo debidamente organizados e inventariados, conforme a las normas y procedimientos que establezca la Universidad, sin que ello implique exoneración de la responsabilidad a que haya lugar en caso de irregularidades.

13.6. La Secretaría General, tendrá la obligación de velar por la integridad, autenticidad, veracidad y fidelidad de la información de los documentos de archivo, liderando mediante su Sistema de Gestión Documental la planeación, control, dirección, organización, capacitación, inspección o vigilancia, promoción y otras actividades involucradas en la gestión del ciclo de vida de la información, incluyendo la creación, mantenimiento (uso, almacenamiento, recuperación), y disposición, independientemente de los medios o soportes., así como la prestación de los servicios archivísticos en el Archivo Central e Histórico.

13.7. Los funcionarios de archivo trabajarán sujetos a los más rigurosos principios de la ética profesional, a lo dispuesto en la Constitución Política de Colombia.

13.8. La Universidad podrá incorporar tecnologías de avanzada en la administración, gestión, seguimiento, control y conservación de sus archivos, empleando cualquier medio técnico, electrónico, informático, óptico o telemático, siempre y cuando cumpla con los siguientes requisitos mínimos:

13.8.1. Organización archivística de los documentos;

13.8.2. Realización de estudios técnicos para la adecuada toma de decisiones, teniendo en cuenta aspectos como la conservación física, las condiciones ambientales y operacionales, la seguridad, perdurabilidad y reproducción de la información contenida en estos soportes, así como el funcionamiento razonable del sistema a impactar en toda la Universidad Autónoma del Caribe.

13.9. La Gestión Documental dentro del concepto de archivo total, comprende procesos tales como la producción o recepción, distribución, consulta, organización, recuperación y disposición final de los documentos.

13.10. Será obligatorio para la Universidad elaborar y adoptar las respectivas tablas de retención documental y valoración documental.

13.11. Es obligación de la Universidad elaborar inventarios de los documentos que produzcan en ejercicio de sus funciones, de manera que se asegure el control de los documentos en sus diferentes fases.

13.12. Todas las personas tienen derecho a consultar los documentos de archivos públicos y a que se les expida copia de los mismos, siempre que dichos documentos no tengan carácter reservado conforme a la Constitución o a la ley.

13.13. La Universidad garantizará el derecho a la intimidad personal y familiar, honra y buen nombre de las personas y demás derechos consagrados en la Constitución y las Leyes.

13.14. Sólo por motivos legales, la Universidad podrá autorizar la salida temporal de los documentos de archivo, previa autorización de la Secretaría General, de la oficina Jurídica la Rectoría.

13.15. El Archivo de carácter histórico, podrá autorizar de manera excepcional, la salida temporal de los documentos que se conservan con fines investigativos, culturales, científicos, legales e históricos y en tal evento la Secretaría General, deberá tomar todas las medidas que garanticen la integridad, la seguridad, la conservación o el reintegro de los mismos.

13.16. La Universidad contará con instrumentos de planeación, y control para la ejecución de las actividades del Sistema de Gestión Documental a nivel nacional, mediante la elaboración de un Plan Institucional de Archivos, Programa de Gestión Documental Físico y/o Electrónico, Sistema Integrado de Conservación y demás instrumentos informacionales o de control.

13.17. La Universidad a través de un Sistema Integrado de Conservación liderado y estructurado por la Secretaria General, establecerá los diferentes mecanismos, instrucciones o pasos a seguir en temas relacionados con la preservación y conservación a largo plazo de los archivos tanto físicos como electrónicos en cualquier soporte material.

14. APLICABILIDAD

14.1. El contenido de este documento aplica a todos los procesos y procedimientos que conforman el Sistema Integrado de Gestión de la calidad de la Universidad, así como a todas las actuaciones administrativas que desarrollen las distintas unidades, por intermedio de sus administrativos, contratistas y/o docentes.

14.2. Se sancionará disciplinaria, administrativa, civil y/o penalmente a toda persona que viole las disposiciones del presente documento de conformidad con lo establecido en las leyes colombianas vigentes.