CORPORACIÓN EDUCATIVA DEL LITORAL
Resolución No. 002-256 del 20 de septiembre de 2021

Personería Jurídica Resolución No.713 de junio de 1972, de la Gobernación del Atlántico y reconocida por el Ministerio de Educación Nacional
Nit 890104481-6

"Por la cual se establece la Política de Seguridad de la Información de la Corporación Educativa del Litoral."

La Sala General de la Corporación Educativa del Litoral-LA LITORAL –en uso de sus facultades constitucionales y legales.

CONSIDERANDO

Que La Corporación Educativa Del Litoral, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los usuarios, enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

El objetivo de la Política de Seguridad Informática de la Corporación Educativa del Litoral consiste en establecer los criterios, directrices, estrategias y responsabilidades que le permitan a la Institución proteger su información a todos los niveles. Así como la tecnología para el procesamiento y administración de la misma.

La Política de Seguridad Informática proporciona la base para la aplicación de controles de seguridad que reduzcan los riesgos y las vulnerabilidades de los sistemas de información de la Institución, garantizando que los riesgos para la Seguridad Informática sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, eficiente y adaptada a los cambios que se produzcan en el entorno y en las tecnologías de la Corporación Educativa del Litoral para el funcionamiento de los programas académicos y los procesos definidos para tal fin.

Este documento formaliza el compromiso de la Alta Dirección frente a la gestión de la seguridad informática y presenta de forma escrita a los usuarios de los sistemas de información el compendio normas institucionales para proteger de posibles riesgos de daño, pérdida y uso indebido de la información, los equipos y demás recursos informáticos, los cuales están en constante cambio y evolución de acuerdo con el avance de la tecnología y los requerimientos del momento histórico y de las áreas.

Es aplicable al área de TICS, el cual es el responsable designado por la Rectoría para la administración y control de los sistemas de información, así como a todos los colaboradores (Administrativos,

Docentes, practicantes) y estudiantes que deberán comprometerse en el cumplimiento de los requisitos de la Política de Seguridad Informática y de los documentos asociados a la misma.

Esta Política aplica para todos los sistemas (Hardware y Software), entendiéndose como los computadores, redes, aplicaciones y sistemas operativos que son propiedad o son operados por la Corporación Educativa del Litoral.

Con estas disposiciones la Corporación asegura y mantiene las infraestructuras de equipo, hardware, software y TIC relevantes para la gestión del conocimiento organizativo. El conocimiento existente en la Organización debe ser protegido y salvaguardado, aplicando reglas de confidencialidad y de propiedad intelectual, siempre que sea adecuado.

A continuación, se establecen 11 principios de seguridad que soportan el Sistema de Gestión de Seguridad de la Información - SGSI de LA CORPORACIÓN EDUCATIVA DEL LITORAL:

1) Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
2) Protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se generan de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
3) Protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
4) Protegerá su información de amenazas como corrupción de datos, robo de información valiosa, confidencial, e instalación de malware originadas por parte del personal que labora en la institución, usuarios con acceso legítimo a los activos de la empresa.
5) Protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
6) Controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
7) Implementará control de acceso a la información, sistemas y recursos de red.
8) Garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
9) Garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
10) Garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
11) Garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

2.- GLOSARIO

SSL	Certificado de seguridad en la página corporativa para utilizar el protocolo de navegación seguro: https
Derechos de Acceso	Controles de acceso y otras medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información manejada por computadores y sistemas de información de la Litoral.
Derechos de Vigilancia	Restringir o revocar los privilegios de cualquier usuario. Inspeccionar, copiar, remover cualquier dato.
TICS	Área responsable de la plataforma tecnológica institucional: servidores, equipos, conectividad y demás componentes tecnológicos.
Firewall-cortafuegos	Genera el bloqueo al acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Los cortafuegos pueden ser implementados en hardware o software.
Usuario	Persona que tiene un vínculo con la Corporación desde diferentes roles en el sistema de información: Empleado administrativo, docente, estudiantes o público en general.

3.- PROTECCIÓN DE LA INFORMACIÓN GENERAL

La Corporación Educativa del Litoral con la política de seguridad implementada, garantiza la protección de los datos desde diferentes entornos, utilizando la información en la red institucional o en la Internet, por medio de diferentes medios siendo estos los protocolos de seguridad de navegación, protocolos de acceso a la información con usuarios identificados y permitidos, seguridad perimetral de la red, copia de la información con la norma técnica definida y aplicando los principios en todos los entornos específicos.

3.1 REGISTRO Y AUDITORÍA

La responsabilidad del registro y auditoría es del área de TICS.

4.- CONTENIDO

4.1 ROLES Y RESPONSABILIDADES DE LA POLÍTICA DE SEGURIDAD INFORMÁTICA.

Al aclarar las responsabilidades de los usuarios y las medidas que deben adoptar para proteger la información y los sistemas informáticos, la Corporación Educativa del Litoral evita pérdidas graves

o divulgación no autorizada. Por otra parte, el buen nombre de la Organización se debe en parte a la forma cómo protege su información y sus sistemas informáticos en todos los niveles (Directivos, Administrativos, Docentes, practicantes y terceros que tengan acceso a los sistemas informáticos institucionales), estas responsabilidades son:

4.1.1 De los Colaboradores.

- Tomar conciencia de la importancia del establecimiento de la Política de Seguridad Informática, los procedimientos y la normatividad aplicable.
- Ser responsables de la información Institucional, que demuestre la conformidad de sus obligaciones y trazabilidad de los procesos, estableciendo los medios que soporten la toma de decisiones (mantener, conservar, dar disposición final) con base en la información que se encuentre a su cargo.
- Ser responsables de la información, serán también los encargados de administrarla. En consonancia con lo anterior serán responsables todos aquellos que manejen información en los computadores asignados para llevar a cabo sus actividades o que tengan acceso a cualquier aplicación o sistema que sirva de apoyo a sus tareas.
- Ser responsables del correo Electrónico Institucional asignado y mantener la confidencialidad de su contraseña y la información de la cuenta, así como de todas las actividades que ocurran durante la utilización del correo. Notificar de manera inmediata si detecta el uso indebido o no autorizado de su cuenta por terceras personas.
- Son responsables por todas las actividades relacionadas con su identificación. La identificación no puede ser usada por otro individuo diferente a quien esta le fue otorgada.
- Los usuarios no deben permitir que otra persona realice labores bajo su identidad. De forma similar, los colaboradores y usuarios no deben realizar actividades bajo la identidad de alguien más. La utilización de los recursos informáticos por parte de terceras personas con conocimiento o consentimiento del usuario, o por su descuido o negligencia, lo hace responsable de los posibles daños que estas personas ocasionen a los equipos o a la propiedad de la Corporación Educativa del Litoral.
- Los colaboradores responsables de la información deben almacenarla, implementar los controles de acceso (para prevenir la divulgación no autorizada) y periódicamente elaborar copias de respaldo y así evitar la pérdida de información crítica utilizando los medios determinados por la Institución para tal fin.
- Los colaboradores con acceso a Internet, al acceder al servicio están aceptando que: 1. Serán sujetos de monitoreo de las actividades que realizan en Internet. 2. Existe la prohibición de acceso a páginas no autorizadas. 3. Se prohíbe la descarga de software sin la autorización del Departamento de TICS. 4. La utilización de Internet es para el desempeño de su función y no para propósitos personales.
- Cumplir con las responsabilidades del buen uso de correo electrónico.

4.1.2 De los Estudiantes

Los estudiantes

- El uso indebido de los sistemas de información de la Corporación está prohibido.
- Intentar modificar, reubicar o sustraer equipos de cómputo, software, información o periféricos sin la debida autorización.

- Transgredir o burlar las verificaciones de identidad u otros sistemas de seguridad.
- No se debe ingresar alimentos a las salas de sistemas.
- Utilizar los sistemas de información para propósitos ilegales o no autorizados.
- Descargar o publicar material ilegal, con derechos de propiedad o material nocivo usando un computador de la Institución.

El Estudiante debe dar un buen uso a los dispositivos, por lo tanto no debe:

- Propinarle golpes, rayones, etc.
- Derramar líquidos.
- Instalar software diferente al asignado.
- Instalar o configurar dispositivos de hardware diferentes a los asignados.
- Dejarlo sin seguridad en un lugar no vigilado.
- Entre otros que deterioran la integridad del dispositivo.

4.1.3 De la Coordinación de TICS

La Coordinación de TICS asegurará la integridad de la plataforma tecnológica de la Institución:

- El acceso a Internet será monitoreado por la Coordinación de TICS para asegurar el uso apropiado y el cumplimiento de las Políticas de Seguridad; las restricciones de accesibilidad a internet o contenidos específicos serán ejecutadas por solicitud al Coordinador del área o por directriz institucional. De necesitar el acceso a una página bloqueada deberá ser autorizado por el Coordinador de TICS.
- Si fuera necesario leer el correo de alguien más (mientras un empleado se encuentre fuera o de vacaciones) el jefe de la respectiva área determinará a qué buzón deben ser redireccionados sus correos en su ausencia o por su parte solicitar las credenciales para la recuperación de información para los fines definidos en los procesos al área de TICS.
- La información de los computadores debe ser periódicamente respaldada en dispositivos destinados para tal fin, para lo cual el Colaborador o Usuario que requiera según criticidad de la información realizar respaldos con apoyo del área de TICS deberá solicitarlo, para que este sea resguardado en los Servidores de la institución o medios magnéticos según se requiera.

- El Departamento de TICS es el responsable de respaldar la información contenida en los servidores de la Institución.
- El Departamento de TICS brindará apoyo y asistencia técnica para la instalación de software o hardware.

4.2 DECLARACIÓN DE RESERVA DE DERECHOS

4.2.1 DERECHOS DE ACCESO

La Corporación Educativa del Litoral usa controles de acceso y otras medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información manejada por computadores y sistemas de información. Para mantener estos objetivos la Corporación se reserva el derecho y la autoridad de:

1. Restringir o revocar los privilegios de cualquier usuario;

2. Inspeccionar, copiar, remover cualquier dato, programa u otro recurso que vaya en contra de los objetivos antes planteados;
3. Tomar cualquier medida necesaria para manejar y proteger los sistemas de información.

4.2.2 DERECHOS DE VIGILANCIA

La Coordinación de TICS, previa autorización de la Rectoría, Vicerrectoría General, se reservará el derecho de supervisar, monitorear e inspeccionar en cualquier momento los sistemas de información utilizados por los Colaboradores, cuando se detecte posibles irregularidades en el manejo de la información o se requiera la realización de respaldos de la misma. Las inspecciones pueden llevarse a cabo con o sin el consentimiento y presencia del empleado involucrado.

Los Sistemas de Información sujetos a dicha inspección incluyen los registros de la actividad de los empleados: archivos y correos electrónicos institucionales y soportes físicos de la información auditada pueden ser sujetos de la misma inspección en cualquier momento. Lo anterior, sin perjuicio del respeto a la intimidad personal y a la inviolabilidad de la correspondencia y demás formas de comunicación privada en los términos del mandato constitucional.
La Corporación Educativa del Litoral se reserva el derecho de retirar cualquier material o recurso que sea considerado lesivo para los intereses de la Institución o que contenga información ilegal.

4.2.3 Declaración de Propiedad Exclusiva

La Corporación Educativa del Litoral tiene propiedad y derechos exclusivos sobre las patentes, derechos de autor, invenciones, programas o cualquier otra propiedad intelectual desarrollada por sus empleados.

4.3 PROTOCOLOS DE SEGURIDAD INFORMÁTICA

4.3.1 CORREO ELECTRÓNICO

El servicio se otorgará mediante la asignación de una dirección de correo electrónico institucional la cual se podrá acceder mediante un nombre de usuario y una contraseña asociada. Este servicio tiene como función ofrecer una herramienta de comunicación digital para la transferencia de información y documentos entre los miembros de la Comunidad Estudiantil; y con el entorno, en función a las actividades que realiza en la Institución, dentro de los lineamientos se destaca:

4.3.1.1 Administración y operación

- Se podrán otorgar cuentas de correo individuales o genéricas, según las necesidades del área.
- Para correos electrónicos de colaboradores (Administrativos, Docentes, practicantes), el área de Talento Humano será el encargado de solicitar al Departamento de Sistemas, tras la contratación de la persona, la creación y/o acceso al correo institucional correspondiente.
- Las cuentas de correo asignadas a los miembros de la corporación deberán ser eliminadas en caso de que la misma no haya sido utilizada en un lapso de 6 meses o más sin ningún tipo de

notificación; o por requerimiento de su supervisor inmediato siguiendo los procedimientos establecidos para tal fin.

- Para los correos electrónicos de estudiantes nuevos, el área de admisiones envía listado al área de TICS quien se encarga de la creación de usuarios y respectivas contraseñas. El estudiante visualizará a través del primer ingreso los pasos básicos de ingreso al correo.
- Para las dificultades de accesibilidad en correos electrónicos por parte del estudiante se reportan a través del correo electrónico de TICS o a través del servicio telefónico, donde el área de TICS, da solución a los requerimientos del estudiante frente al uso correos.
- El área de TIS deberá notificar a los usuarios de la suspensión del servicio por razones de mantenimiento o por fallas ocurridas en la operatividad de este.

4.3.1.2 Del Usuario

- El usuario del correo electrónico será responsable de mantener la confidencialidad de su contraseña y la información de la cuenta, así como de todas las actividades que ocurran durante la utilización del correo.
- La cuenta de correo electrónico y la clave asociada asignada es personal, intransferible y por razones de seguridad deberá ser cambiada periódicamente, se recomienda una periodicidad de 3 meses.
- Responsabilidades del Usuario: el uso del correo electrónico por parte de los usuarios deberá estar orientado a la transferencia de información de tipo Institucional, evitando:

a) Difundir información confidencial de la Institución; b) Retransmitir o leer correos, donde se desconozca la procedencia del mismo; c) Transmitir información pornográfica o de carácter sexista; d) Enviar información referida a cualquier forma discriminatoria por razones de sexo, raza, filiación política o religiosa, minusvalía física o condición social; E) Mantener la confidencialidad de su contraseña y la información de la cuenta; f) Notificar de manera inmediata si detecta el uso indebido o no autorizado de su cuenta por terceras personas; g) Revisar y depurar su buzón de correo periódicamente, a fin de evitar que el mismo se sature.

4.3.1.3 Requisitos para optar al Servicio:

El usuario solicitante (docente, administrativo,) que no esté adscrito a la nómina de la Corporación, deberá presentar anexo a la solicitud, su constancia de trabajo o cualquier otro documento que acredite su vinculación, avalado por su superior inmediato o autoridad competente, de lo contrario no será procesada la solicitud. Para procesar solicitudes de cuentas genéricas, será necesario que el oficio de solicitud venga acompañado de una exposición de motivos que justifique la utilización de la misma. El usuario deberá aceptar los acuerdos y/o compromisos asociados al servicio.

4.3.2 OTORGAMIENTO DE AVAL TÉCNICO.

Este servicio contempla la evaluación técnica para las adquisiciones de equipos tales como: computadores de escritorio, servidores, laptops, impresoras, scanners, video beams, entre otros; así como software y servicios TIC.

4.3.2.1 Administración y Operación.

- El Departamento TICS deberá realizar la evaluación técnica para las adquisiciones de Equipos y Servicios de TIC de la institución.
- La Coordinación de TICS deberá evaluar y llevar el control de las solicitudes de acuerdo con los estándares vigentes establecidos por la Institución, a través de los organismos competentes; y seguirá las normativas del procedimiento asociado al servicio.
- El responsable de la administración del servicio deberá definir los acuerdos de servicio, divulgarlos a su comunidad y respetarlos para dar cumplimiento a la prestación de dicho servicio de forma oportuna y correcta.

4.3.2.2 Del Usuario

- Deberá tramitar toda solicitud del aval técnico para la adquisición de equipos y servicios de TIC
- Deberá tramitar el aval técnico emitido por el Departamento de TICS, independientemente del tipo de financiamiento que se maneje.

4.3.3. ANTIVIRUS CORPORATIVO

Este servicio ofrece una moderna tecnología con los más altos niveles de seguridad informática de última generación, que integra controles avanzados de red, protección de usuarios, aplicaciones, tráfico interno, accesos. Mejor rendimiento, seguridad y control en las estaciones de trabajo conectadas a la red de la Institución.

4.3.3.1. Administración y Operación

- Implementará mecanismos de alerta ante la presencia de virus o riesgos de seguridad y centralizará en el Departamento TICS la generación de informes dentro de cada dependencia.
- Determina comportamientos sospechosos, lo que permite la detección de malware especialmente diseñado para esquivar las soluciones tradicionales.
- Prefiltra todo el tráfico HTTP y hace un seguimiento del tráfico sospechoso, así como de la ruta del archivo del proceso que está enviando tráfico malicioso.
- El administrador tiene la facultad de aplicar sus políticas de datos, dispositivo, aplicación y web con facilidad, gracias a la perfecta integración en el agente para estaciones y en la consola de administración.
- Elimina virus, troyanos, rootkits, programas espía y otro tipo de malware
- Bloquear programas maliciosos e infecciones al identificar e impedir el puñado de técnicas y comportamientos utilizados en casi todas las vulnerabilidades.
- La comunicación instantánea y automática entre la estación de trabajo y la red advierte al sistema de lo que está detectando el firewall exactamente, lo que permite que el agente de protección de la estación utilice esa información inmediatamente para descubrir el proceso detrás de la amenaza.

- Mantendrá a los usuarios informados mediante correos informativos periódicos donde se alerta sobre nuevos virus y se emitirán recomendaciones para ser aplicadas en los computadores.

4.3.3.2 Del Usuario

- Estará alerta y no abrirá archivos o ejecutará programas de procedencia dudosa, tanto en anexos de correo, mensajería instantánea o Internet (ya sean vía Web o FTP). En caso de que lo descarguen, éstos no deberán ejecutarse, a menos que hayan sido analizados previamente por un software antivirus.
- Estará alerta de los correos electrónicos que reciba y desconfiará de aquellos correos de procedencia desconocida, o de un conocido con un 'Asunto' poco habitual en él, se debe comprobar su procedencia real antes de abrirlo.
- No contestará mensajes spam (publicidad no deseada), ya que al hacerlo reconfirmará su dirección de correo. De igual modo, no distribuirá cartas en cadena, ya que esto puede causar diversos efectos como la sobrecarga de la red, del servidor de correo y además la molestia de los usuarios al inundarle su buzón con muchos correos no deseados.
- En caso de presentar dudas sobre un servicio, aplicación o archivo, entre otros, se recomendará contactar al Departamento de TICS para que tome las acciones debidas.

4.3.3.3 Requisitos para optar al servicio:

- El usuario deberá aceptar los acuerdos y/o compromisos asociados al servicio.
- Dispondrá de una consola de Antivirus Corporativo que sea la principal de la institución.

4.3.4. TELEFONÍA

Este servicio tendrá como función ofrecer a los miembros de la comunidad Litoralista la posibilidad de comunicarse interna o externamente mediante el sistema de telefonía de la Corporación Educativa del Litoral que es basado bajo la plataforma ISSABEL (open source) el cual incluye:
1. La asignación / configuración de extensiones telefónicas IP o Softphone.
2. La asignación, traslado o mudanza de aparatos telefónicos,
3. La eliminación de extensiones telefónicas análogas.
Este servicio se ofrecerá de acuerdo a perfiles predefinidos que permiten realizar llamadas:
1. Internas
2. Locales
3. Nacionales

La asignación de aparato telefónico dependerá de la disponibilidad de estos equipos que tenga la Dirección de Tecnología de Información y Comunicaciones (Dirección de Sistemas de Información) al momento de la solicitud. En caso contrario, si el Dpto. de Sistemas no dispone de este recurso, el solicitante (Administrativo, Docente o Portería), debe remitirle a su jefe de Área para dicho procedimiento, siempre y cuando esté dentro del presupuesto asignado.
Los aparatos telefónicos serán un recurso que la Institución pone a disposición de los usuarios para facilitar el desarrollo de sus funciones. En este sentido como se indica en las Políticas Generales descritas en este documento, los recursos son propiedad de la institución y no de la persona a quién fue asignada para su uso.

4.3.4.1 Administración y Operación

- Velará por el uso racional del servicio telefónico.
- Divulgará y velará por el cumplimiento de las presentes normativas.
- Proveerá y mantendrá la infraestructura necesaria para la disponibilidad del servicio.
- Administrará y gestionará el uso de las extensiones telefónicas y las configuraciones asociadas para planificar el crecimiento futuro, así como para atender oportunamente las averías y/o cambio de perfil de usuario.
- Brindará soporte técnico a los usuarios del servicio telefónico.
- Mantendrá un inventario de los aparatos telefónicos para la administración, reposición, detección de necesidades y resguardo de los bienes de la Institución.

4.3.4.2 Del Usuario

- El usuario será responsable del uso que se le dé a la extensión telefónica que le fue asignada, independientemente de que terceras personas hagan uso indebido de su extensión.
- El usuario será responsable del equipamiento telefónico que le ha sido asignado.
- Notificará a la Dirección de Sistemas de Información cualquier anomalía en el servicio telefónico.
- Notificará a la Dirección de Sistemas de Información la desincorporación o cambio de personal en sus funciones a fin de actualizar la Base de Datos de usuarios del servicio telefónico y poder eliminar el servicio o modificar el perfil.

4.3.4.3 Requisitos para optar al Servicio:

- El usuario solicitante (Docente, Administrativo, o Portería) que no esté adscrito a la nómina de la Corporación Educativa del Litoral y avalado por su supervisor inmediato o autoridad competente, no será procesada la solicitud.
- En el caso de una instalación o modificación, la solicitud deberá incluir el perfil que será asignado al usuario/extensión y deberá contar con la aprobación de la autoridad o en quién éste delegado para estas funciones.
- El Usuario para obtener este servicio debe tener un puesto de trabajo con conexión a la red de la Institución, ya que esta nueva tecnología funciona con configuración IP.

4.3.5 SOPORTE TÉCNICO

Este servicio tiene como objetivo la prevención y/o solución de problemas técnicos de:

- Hardware: Impresoras, teléfonos, portátiles, computadores, video beam, entre otros.
- Software: Aplicaciones institucionales, sistemas operativos, software ofimáticos, entre otros.
- Redes: cableado estructurado e interconectividad de redes.
-

4.3.5.1 Administración y Operación

- El Departamento de TICS a través del personal de soporte técnico atenderá cada solicitud de servicio a su comunidad de usuarios finales. Cada soporte que se realice, se registrará como evidencia en un formato o documento con la finalidad de registrar, documentar y gestionar cada uno de los casos que requieran atención, lo cual contribuirá a controlar y mejorar la prestación de este tipo de servicios.

- Se deberá trabajar con la Planilla de Atención a Usuarios donde se documentará brevemente el caso y las acciones que se realizaron para atenderlo, y la misma deberá ser firmada como señal de conformidad en relación al soporte técnico prestado.

- El Departamento de TICS prestará soporte técnico a nivel de aplicaciones que sean consideradas como herramientas estrictamente institucionales o que se requieran para el desarrollo de sus funciones, debidamente justificadas por el supervisor inmediato. Es bueno acotar que el soporte técnico de estas aplicaciones estará sujeto a la experticia que posea el personal del Departamento de TICS.

4.3.5.2 Del Usuario

- El usuario deberá formalizar su solicitud de servicio a través de correo electrónico, vía telefónica o dirigirse personalmente al Departamento de TICS.
- Cualquier solicitud de traslado de equipo o préstamo del mismo a otro lugar que no sea la institución, deberá ser diligenciado y firmado por el usuario (Docente, Administrativo) por medio de un acta de entrega diligenciada por el Departamento de TICS donde evidencie que este equipo le pertenece a la Institución.

4.3.5.3 Requisitos para optar al Servicio:

- El usuario solicitante podrá ser cualquier miembro de la Comunidad Estudiantil, ya sea personal docente, administrativo, que tenga asignado un equipo, para realizar sus actividades de carácter estrictamente institucional.

VIGENCIA

La Política Seguridad de la Información rige a partir de la fecha de su promulgación y deroga todas las normas que le sean contrarias.

COMUNÍQUESE Y CÚMPLASE

Dado en Barranquilla, a los veinte (20) días del mes de septiembre de 2021

En constancia firman

ALBA LUCÍA CORREDOR GÓMEZ
Presidente Sala General

CECILIA CORREA DE MOLINA
Rectora

Karolays Dayana Muñoz Caro
Coordinadora Secretaría General