UNIVERSIDAD SAN GREGORIO DE PORTOVIEJO

Departamento de Información Estratégica

Políticas de Seguridad y Gestión de la Información

Resolución USGP H.C.U. N° 083-03-2018 <<Versión 1.0>>

Resolución USGP C.R. N° 015-2019 <<Versión 2.0>>

Marzo-2018

Versión 2.0

CONTENIDO:

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 institución y asegurar el cumplimiento de objetivos misionales.

Las instituciones 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 institución 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. Por tanto, estos tres términos constituyen los pilares fundamentales que sostienen un sistema de gestión y 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.

La Universidad San Gregorio de Portoviejo ha aumentado su inventario tecnológico tanto en infraestructura de hardware y software, con el propósito de satisfacer su creciente demanda estudiantil y responder eficientemente a las exigencias del entorno educativo y a los órganos reguladores de calidad del país; en este sentido la generación de información es abundante y se hace necesario crear Políticas de

Gestión y Seguridad de la Información que estén basadas 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 institución o de fuentes externas) o de la fecha de elaboración.

2. OBJETIVO

- ☑ Establecer los lineamientos necesarios para proteger, preservar y administrar correctamente la información de la Universidad San Gregorio de Portoviejo 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 San Gregorio de Portoviejo.
- ☑ Establecer lineamientos de gestión de la información, para maximizar el valor y los beneficios derivados del uso de la información.

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 San Gregorio de Portoviejo, 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 institución, 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, interprete, ensamblador) en lenguaje de máquina o instrucciones ejecutadas 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 (a), Coordinador (a), Director (a) de cada una de las áreas, será el responsable ante la Institución, de los activos de información registrados como de su propiedad.

4.20. SAN (Storage Área 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.

4.25. Departamento de Información Estratégica USGP: es el área encargada de la generación de información útil para la mejor toma de decisiones considerando como eje los objetivos institucionales de la universidad. Así mismo el mencionado departamento tiene a su cargo el desarrollo, mantenimiento y administración de software de la Universidad San Gregorio de Portoviejo.

4.26. Departamento de Redes y Conectividad USGP: es el área encargada de la instalación y mantenimiento de las redes de datos en el campus universitario, así mismo del mantenimiento preventivo y correctivo de los equipos de cómputo de la Universidad San Gregorio de Portoviejo.

5. POLÍTICA DE CONTROL DE ACCESO LÓGICO

5.1. Es responsabilidad del Departamento de Talento Humano, informar al Departamento de Información Estratégica sobre los nuevos administrativos, contratistas y/o docentes que ingresan a la institución, con el fin de poder asignar desde el Departamento de Información Estratégica, los respectivos permisos para el acceso a los recursos tecnológicos de la institución.

5.2. El Departamento de Información Estratégica 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.

5.3. El Departamento de Talento Humano es el encargado de notificar y dar los lineamientos para la creación, modificación y supresión de permisos y privilegios de usuarios.

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

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

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

5.7. Para la creación y administración de las credenciales de acceso institucionales, estudiantes y egresados, se deben adoptar los lineamientos establecidos por el Departamento de Información Estratégica.

5.8. 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.

6. GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN

6.1 Los Coordinadores de Carrera o Jefes Departamentales como propietarios de los activos de información deben reportar al Departamento de Información Estratégica los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.

6.2 El Departamento de Información Estratégica debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.

6.3 El Departamento de Información Estratégica debe evaluar todos los incidentes de seguridad de acuerdo a sus circunstancias particulares y escalar aquellos en los que se considere pertinente.

6.4 El Departamento de Información Estratégica debe designar personal calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su ocurrencia nuevamente.

6.5 El Departamento de Información Estratégica debe crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.

6.6 Los profesores, administrativos, estudiantes y terceros deben reportar cualquier evento o incidente relacionado con la seguridad de la información y los recursos tecnológicos con la mayor prontitud posible.

6.7 Los profesores, administrativos, estudiantes y terceros deben informar, en caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno o confidencial, al Departamento de Información Estratégica, para que se registre y se le dé el trámite necesario.

7. POLÍTICAS DE DESARROLLO SEGURO

7.1. 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.

7.2. El Departamento de Información Estratégica es la única unidad encargada de la realización de desarrollos de software dentro de la Universidad y dará cumplimiento a los lineamientos de construcción de aplicaciones seguras adoptados por la Universidad a través de esta jefatura.

7.3. Todo software desarrollado será puesto en producción según las presentes políticas, los términos y condiciones de privacidad.

7.4. 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 software de la Universidad.

7.5. 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 de software. El intento de uso total o parcial del código fuente de las aplicaciones administradas y/o adquiridas por el Departamento de Información Estratégica por parte de personal no autorizado queda expresamente prohibido.

7.6. 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.

7.7. 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.

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

8. POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS

8.1. 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.

8.2. 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.

8.3. 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.

8.4. 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.

9. POLÍTICAS DE BACKUPS O COPIAS DE SEGURIDAD

9.1. 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 Director (a) Desarrollo Institucional.

9.2. 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.

9.3. Los medios de respaldo empleados para efectuar las copias de seguridad en la Universidad San Gregorio de Portoviejo serán los definidos por el Jefe del Departamento de Información Estratégica en el procedimiento de Copias de Respaldo o aquel que lo supla.

9.4. 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.

9.5. 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 San Gregorio de Portoviejo, contemplados en el Inventario de Servidores Críticos asociado al Procedimiento Copias de Respaldo.

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

9.7. El Departamento de Información Estratégica 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.

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

9.9. La ejecución de las copias de seguridad debe llevarse a cabo en horas de poca o ninguna actividad laboral; por lo tanto, el Departamento de Información Estratégica será la responsable de definir el horario de ejecución de éstas.

9.10. 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.

9.11. 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.

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

9.13. 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.

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

9.15. 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.

10. POLÍTICA DE GESTIÓN DE LA INFORMACIÓN

10.1. La Universidad San Gregorio de Portoviejo garantizará los recursos tecnológicos para recolectar, almacenar, procesar y recuperar la información.

10.2. La Universidad San Gregorio de Portoviejo asegurará que la información producto de las tareas y procesos institucionales tengan condiciones de calidad, aplicando criterios de eficiencia, organización y optimización de recursos.

10.3. La Universidad San Gregorio de Portoviejo promoverá la generación de información útil para la toma de decisiones académicas y administrativas.

10.4. La Universidad San Gregorio de Portoviejo velará por la actualización de la información y la preservación de datos históricos relacionados con los procesos académicos y administrativos.

10.5. La Universidad San Gregorio de Portoviejo velará por la privacidad de la información proporcionada por la comunidad universitaria y de los procesos institucionales, para que sea utilizada exclusivamente para temas de mejoramiento continuo y aseguramiento de la calidad.

11. POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS

11.1. La Universidad a través del Departamento de Información Estratégica 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.

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

11.3. El Departamento de Información Estratégica 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.

11.4. La Universidad San Gregorio garantizará los recursos de hardware y software considerados necesarios y acorde a las exigencias tecnológicas actuales, para la aplicación de controles criptográficos.

11.5. El Departamento de Información Estratégica, 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.

11.6. El Departamento de Información Estratégica, 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.

11.7. 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.

11.8. Es responsabilidad del Departamento de Talento Humano informar al Departamento de Información Estratégica sobre las novedades de retiro, con el fin de poder realizar las acciones de desactivación, bloqueo o eliminación de los respectivos accesos.

12. ACCESO A REDES Y A SERVICIOS EN RED

El Departamento de Redes y Conectividad como responsable de las redes de datos y los recursos de red de la institución, debe velar porque dichas redes sean debidamente protegidas contra accesos no autorizados por medio de mecanismos de control de acceso lógico.

12.1. El Departamento de Redes y Conectividad debe establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de la institución.

12.2. El Departamento de Redes y Conectividad debe asegurar que las redes inalámbricas cuenten con mecanismos de autenticación que evite los accesos no autorizados.

12.3. El Departamento de Redes y Conectividad debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes a las redes o recursos de red de la Universidad, así como velar por la aceptación de las responsabilidades de dichos terceros en cuanto a las Políticas de Seguridad de la Información.

12.4. El Departamento de Redes y Conectividad debe suministrar una herramienta para realizar conexiones remotas a la red de área local de la Universidad de manera segura para los profesores y administrativos que por su labor así lo requiera, la cual debe ser aprobada, registrada y auditada.

12.5. El Departamento de Redes y Conectividad debe contar con un procedimiento de creación de cuentas, donde estén definidas las

condiciones de autorización y acuerdos de confidencialidad respectivos.

12.6. Los profesores y administrativos deben contar con el Acuerdo de Seguridad firmado, otorgado por recursos humanos y la autorización de creación de cuentas otorgado por el jefe inmediato, para tener acceso lógico a los sistemas de información de la institución, según sea el caso.

12.7. Los profesores, administrativos y terceros que deseen que los equipos de cómputo personales accedan a la red de datos de la institución deben cumplir con todos los requisitos o controles para autenticarse en ésta y únicamente podrán realizar las tareas para las que fueron autorizados.

13. SEGURIDAD FÍSICA Y AMBIENTAL

13.1. ÁREAS SEGURAS

13.1.1. La Universidad proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones. Así mismo, controlará de amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

13.1.2. Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.

13.2. PROTECCIÓN POR AMENAZAS EXTERNAS O AMBIENTALES

13.2.1. Los profesores, administrativos, estudiantes o terceros, que requieran ingresar al Data Center, deben realizar las solicitudes de acceso al Departamento de Redes y Conectividad. Además, se deberá realizar un registro del ingreso de los visitantes en una bitácora ubicada en la entrada de estos lugares de forma visible.

13.2.2. Los profesores, administrativos, estudiantes y terceros que deseen ingresar al Centro de Computo y/o Bunker deben realizar el ingreso acompañados de un funcionario de la dependencia responsable de los mismos.

13.2.3. Los profesores, administrativos, estudiantes y terceros deben cumplir completamente con los controles físicos implantados por la institución, ya que los ingresos y salidas a las instalaciones de la Universidad deben ser registrados.

13.2.4. Los profesores, administrativos, estudiantes y terceros no deben intentar ingresar a áreas a las cuales no tengan autorización.

13.2.5. El Departamento de redes y Conectividad deben velar por las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma (infraestructura) tecnológica ubicados en estos sitios. Para cumplir con esto deben existir:

- Sistemas de control ambiental de temperatura y humedad
- Sistemas de extinción de incendios
- Sistemas de vigilancia y monitoreo
- Alarmas en caso de detectarse condiciones ambientales inapropiadas.

13.2.6. El Departamento de redes y Conectividad, deben velar porque los recursos de la plataforma (infraestructura) tecnológica, ubicados en el Data Center y Cuarto de Comunicaciones, se encuentren protegidos contra fallas o interrupciones eléctricas.

13.2.7. El Departamento de Redes y Conectividad, deben certificar que el Data Center y Cuarto de Comunicaciones se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

13.2.8. El Departamento de redes y Conectividad, deben asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y previamente autorizado e identificado.

13.2.9. El Departamento de redes y Conectividad, deben llevar un control de la programación de los mantenimientos preventivos a los Data Center y Cuarto de Comunicaciones, teniendo en cuenta los

niveles de servicio acordados con los responsables de los servicios particulares y acorde a la operación de la institución.

13.2.10. El Departamento de Redes y Conectividad, deben certificar que el Data Center y Cuarto de Comunicaciones tengan los niveles de temperatura y humedad relativa en estos sitios, y que estén dentro de los límites requeridos por la infraestructura allí instalada, para lo cual se deben usar sistemas de aire acondicionado según sea el caso.

13.2.11. El Departamento de Redes y Conectividad, deben solicitar mantenimientos preventivos y pruebas de funcionalidad del sistema de UPS y plantas eléctricas, de los sistemas de detección de incendios y del sistema de aire acondicionado.

13.2.12. La Universidad debe designar y aplicar protección física para desastres como: fuego, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.

13.2.13. El departamento de redes y Conectividad deben velar por el ambiente adecuado para los activos informáticos que reposan en los Data Center y Cuarto de Comunicaciones, como ventilación, iluminación, regulación de corriente, etc.

13.3. TRABAJO EN ÁREAS SEGURAS

13.3.1. La Universidad debe mantener áreas seguras para la gestión, almacenamiento y procesamiento de información en la institución. Las áreas deben contar con:

- Protecciones físicas y ambientales, acordes con el valor y la necesidad de aseguramiento de los activos que se protegen.
- Definición de perímetros de seguridad.
- Controles de acceso físicos.
- Seguridad para protección de los equipos.
- Seguridad en el suministro eléctrico y cableado.
- Condiciones ambientales adecuadas de operación.
- Sistemas de contención, detección y extinción de incendios.

13.4. SEGURIDAD DEL CABLEADO

13.4.1. El Departamento de Redes y Conectividad debe mantener los cables de red del Data Center y Cuarto de Comunicaciones claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.

13.4.2. El Departamento de Redes y Conectividad deben contar con los planos que describan las conexiones del cableado.

13.4.3. El Departamento de Redes y Conectividad debe mantener el acceso a los centros de cableado solo para el personal autorizado.

13.5. MANTENIMIENTO DE EQUIPOS

13.5.1. El Departamento de Redes y Conectividad es el responsable de llevar a cabo los servicios de mantenimiento y reparaciones al equipo informático, por medio de personal idóneo para la labor.

13.5.2. El Departamento de Redes y Conectividad es el único autorizado para realizar la labor descrita en el punto anterior.

13.5.3. Los profesores, administrativos y estudiantes deben respaldar con copias de seguridad toda la información personal o confidencial que se encuentre en el equipo de cómputo asignado, previniendo así la pérdida involuntaria de la misma, derivada del proceso de reparación.

13.5.4. El Departamento de Redes y Conectividad debe realizar procedimientos de borrado seguro en los equipos que se dan de baja y los equipos que son asignados a usuarios diferentes por temas de rotación.

14. POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS

14.1. La Universidad a través del Departamento de Información Estratégica 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.

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

14.3. El Departamento de Información Estratégica 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.

14.4. La Universidad San Gregorio garantizará los recursos de hardware y software considerados necesarios y acorde a las exigencias tecnológicas actuales, para la aplicación de controles criptográficos.

14.5. El Departamento de Información Estratégica, 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.

14.6. El Departamento de Información Estratégica, 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.

14.7. 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.

14.8. Es responsabilidad del Departamento de Talento Humano informar al Departamento de Información Estratégica sobre las novedades de retiro, con el fin de poder realizar las acciones de desactivación, bloqueo o eliminación de los respectivos accesos.

15. ACCESO A REDES Y A SERVICIOS EN RED

El Departamento de Redes y Conectividad como responsable de las redes de datos y los recursos de red de la institución, debe velar porque dichas redes sean debidamente protegidas contra accesos no autorizados por medio de mecanismos de control de acceso lógico.

15.1. El Departamento de Redes y Conectividad debe establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de la institución.

15.2. El Departamento de Redes y Conectividad debe asegurar que las redes inalámbricas cuenten con mecanismos de autenticación que evite los accesos no autorizados.

15.3. El Departamento de Redes y Conectividad debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes a las redes o recursos de red de la Universidad, así como velar por la aceptación de las responsabilidades de dichos terceros en cuanto a las Políticas de Seguridad de la Información.

15.4. El Departamento de Redes y Conectividad debe suministrar una herramienta para realizar conexiones remotas a la red de área local de la Universidad de manera segura para los profesores y administrativos que por su labor así lo requiera, la cual debe ser aprobada, registrada y auditada.

15.5. El Departamento de Redes y Conectividad debe contar con un procedimiento de creación de cuentas, donde estén definidas las condiciones de autorización y acuerdos de confidencialidad respectivos.

15.6. Los profesores y administrativos deben contar con el Acuerdo de Seguridad firmado, otorgado por recursos humanos y la autorización de creación de cuentas otorgado por el jefe inmediato, para tener acceso lógico a los sistemas de información de la institución, según sea el caso.

15.7. Los profesores, administrativos y terceros que deseen que los equipos de cómputo personales accedan a la red de datos de la institución deben cumplir con todos los requisitos o controles para autenticarse en ésta y únicamente podrán realizar las tareas para las que fueron autorizados.

16. SEGURIDAD FÍSICA Y AMBIENTAL

16.1. ÁREAS SEGURAS

16.1.1. La Universidad proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones. Así mismo, controlará de amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

16.1.2. Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.

16.2. PROTECCIÓN POR AMENAZAS EXTERNAS O AMBIENTALES

16.2.1. Los profesores, administrativos, estudiantes o terceros, que requieran ingresar al Data Center, deben realizar las solicitudes de acceso al Departamento de Redes y Conectividad. Además, se deberá realizar un registro del ingreso de los visitantes en una bitácora ubicada en la entrada de estos lugares de forma visible.

16.2.2. Los profesores, administrativos, estudiantes y terceros que deseen ingresar al Centro de Cómputo y/o Bunker deben realizar el ingreso acompañados de un funcionario de la dependencia responsable de los mismos.

16.2.3. Los profesores, administrativos, estudiantes y terceros deben cumplir completamente con los controles físicos implantados por la institución, ya que los ingresos y salidas a las instalaciones de la Universidad deben ser registrados.

16.2.4. Los profesores, administrativos, estudiantes y terceros no deben intentar ingresar a áreas a las cuales no tengan autorización.

16.2.5. El Departamento de redes y Conectividad deben velar por las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma

(infraestructura) tecnológica ubicados en estos sitios. Para cumplir con esto deben existir:

- Sistemas de control ambiental de temperatura y humedad
- Sistemas de extinción de incendios
- Sistemas de vigilancia y monitoreo
- Alarmas en caso de detectarse condiciones ambientales inapropiadas.

16.2.6. El Departamento de redes y Conectividad, deben velar porque los recursos de la plataforma (infraestructura) tecnológica, ubicados en el Data Center y Cuarto de Comunicaciones, se encuentren protegidos contra fallas o interrupciones eléctricas.

16.2.7. El Departamento de Redes y Conectividad, deben certificar que el Data Center y Cuarto de Comunicaciones se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

16.2.8. El Departamento de redes y Conectividad, deben asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y previamente autorizado e identificado.

16.2.9. El Departamento de redes y Conectividad, deben llevar un control de la programación de los mantenimientos preventivos a los Data Center y Cuarto de Comunicaciones, teniendo en cuenta los niveles de servicio acordados con los responsables de los servicios particulares y acorde a la operación de la institución.

16.2.10. El Departamento de Redes y Conectividad, deben certificar que el Data Center y Cuarto de Comunicaciones tengan los niveles de temperatura y humedad relativa en estos sitios, y que estén dentro de los límites requeridos por la infraestructura allí instalada, para lo cual se deben usar sistemas de aire acondicionado según sea el caso.

16.2.11. El Departamento de Redes y Conectividad, deben solicitar mantenimientos preventivos y pruebas de funcionalidad del sistema de UPS y plantas eléctricas, de los sistemas de detección de incendios y del sistema de aire acondicionado.

16.2.12. La Universidad debe designar y aplicar protección física para desastres como: fuego, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.

16.2.13. El departamento de redes y Conectividad deben velar por el ambiente adecuado para los activos informáticos que reposan en los Data Center y Cuarto de Comunicaciones, como ventilación, iluminación, regulación de corriente, etc.

16.3. TRABAJO EN ÁREAS SEGURAS

16.3.1. La Universidad debe mantener áreas seguras para la gestión, almacenamiento y procesamiento de información en la institución. Las áreas deben contar con:

- Protecciones físicas y ambientales, acordes con el valor y la necesidad de aseguramiento de los activos que se protegen.
- Definición de perímetros de seguridad.
- Controles de acceso físicos.
- Seguridad para protección de los equipos.
- Seguridad en el suministro eléctrico y cableado.
- Condiciones ambientales adecuadas de operación.
- Sistemas de contención, detección y extinción de incendios.

16.4. SEGURIDAD DEL CABLEADO

16.4.1. El Departamento de Redes y Conectividad debe mantener los cables de red del Data Center y Cuarto de Comunicaciones claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.

16.4.2. El Departamento de Redes y Conectividad deben contar con los planos que describan las conexiones del cableado.

16.4.3. El Departamento de Redes y Conectividad debe mantener el acceso a los centros de cableado solo para el personal autorizado.

16.5. MANTENIMIENTO DE EQUIPOS

16.5.1. El Departamento de Redes y Conectividad es el responsable de llevar a cabo los servicios de mantenimiento y reparaciones al equipo informático, por medio de personal idóneo para la labor.

16.5.2. El Departamento de Redes y Conectividad es el único autorizado para realizar la labor descrita en el punto anterior.

16.5.3. Los profesores, administrativos y estudiantes deben respaldar con copias de seguridad toda la información personal o confidencial que se encuentre en el equipo de cómputo asignado, previniendo así la pérdida involuntaria de la misma, derivada del proceso de reparación.

16.5.4. El Departamento de Redes y Conectividad debe realizar procedimientos de borrado seguro en los equipos que se dan de baja y los equipos que son asignados a usuarios diferentes por temas de rotación.

17. APLICABILIDAD

17.1. 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.

17.1.1. 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 ecuatorianas vigentes.

UNIVERSIDAD
SAN GREGORIO
DE PORTOVIEJO

RESOLUCIÓN USGP H.C.U No. 083-03-2018
HONORABLE CONSEJO UNIVERSITARIO DE LA UNIVERSIDAD SAN GREGORIO DE PORTOVIEJO

CONSIDERANDO

Que, el Art. 350 de la Constitución del Ecuador señala: "El sistema de educación superior tiene como finalidad la formación académica y profesional con visión científica y humanista; la investigación científica y tecnológica; la innovación, promoción, desarrollo y difusión de los saberes y las culturas; la construcción de soluciones para los problemas del país, en relación con los objetivos del régimen de desarrollo".

Que el artículo 355 de la Constitución del Ecuador, entre otros principios, establece que el Estado reconocerá a las universidades y escuelas politécnicas autonomía académica administrativa, financiera y orgánica, acorde con los objetivos del régimen de desarrollo y los principios establecidos en la Constitución. Se reconoce a las universidades y escuelas politécnicas el derecho a la autonomía, ejercida y comprendida de manera solidaria y responsables. Dicha autonomía garantiza el ejercicio de la libertad académica y el derecho a la búsqueda de la verdad, sin restricciones; el gobierno y gestión de sí mismas, en consonancia con los principios de alternancia, transparencia y los derechos políticos; y la producción de ciencia, tecnología, cultura y arte. La autonomía no exime a las instituciones del sistema de ser fiscalizadas, de la responsabilidad social, rendición de cuentas y participación en la planificación nacional.

Que, el artículo 17 de la Ley Orgánica de Educación Superior determina que: *"Reconocimiento de la autonomía responsable: El Estado reconoce a las universidades y escuelas politécnicas autonomía académica. administrativa. financiera y orgánica, acorde con los principios establecidos en la Constitución de la República. En el ejercicio de autonomía responsable, las universidades y escuelas politécnicas mantendrán relaciones de reciprocidad y cooperación entre ellas y de estas con el Estado y la sociedad; además observarán los principios de justicia, equidad, solidaridad, participación ciudadana, responsabilidad social y rendición de cuentas".*

Que, el artículo 45 de la LOES dice: *"Principio del Cogobierno. El cogobierno es parte consustancial de la autonomía universitaria responsable. Consiste en la dirección compartida de las universidades y escuelas politécnicas por parte de los diferentes sectores de la comunidad de esas instituciones: profesores, estudiantes, empleados y trabajadores, acorde con los principios de calidad, igualdad de oportunidades. alternabilidad y equidad de género. Las universidades y escuelas politécnicas incluirán este principio en sus respectivos estatutos".*

Que, el Art. 18 del Estatuto de la Universidad San Gregorio de Portoviejo, expresa que: "Ejercicio de la autonomía responsable- La autonomía responsable que ejercen las universidades y escuelas

politécnicas consiste en: a) La independencia para que los profesores e investigadores de las universidades y escuelas politécnicas ejerzan la libertad de cátedra e investigación";

Que, mediante a través del oficio No. IE-Of- No. 006-2018 del 26 de febrero de 2018, el ingeniero Marcos Gallegos Macías, hace conocer al Rector de la USGP, que la información de La institución se ha convertido en un activo intangible, ya que se constituye un recurso clave y requisito previo para el suministro eficaz y la gestión de los servicios. El mejor acceso a la información se reconoce como un ingrediente de suma utilidad para los servicios educativos y para la planificación, diagnóstico, funcionamiento y supervisión de planes y programas; además, contribuye a la evaluación de las actividades y de los resultados de la intervención académica y de gestión, por ello y en virtud de que la USGP posee una creciente Plataforma Informática Académica, por ello es necesario implementar la Políticas de Seguridad y Gestión d la Información, las que actuarán como directrices para asegurar la integridad, confiabilidad y disponibilidad de la información.

Que, el oficio suscrito en el considerando anterior, fue apostillado por el rector, para conocimiento y resolución del H. Consejo Universitario.

En ejercicio de las facultades conferidas en el artículo 45 letra e) del Estatuto de la Universidad San Gregorio de Portoviejo, el H. Consejo Universitario de esta institución de Educación Superior:

RESUELVE:

PRIMERO: Aprobar las Políticas de Seguridad y Gestión de la Información de la Universidad San Gregorio de Portoviejo.

SEGUNDO: Disponer al Jefe del Departamento de Información Estratégica, realice las acciones pertinentes para el aseguramiento de la integridad, confiabilidad y disponibilidad de la información de esta institución de educación superior.

DISPOSICIONES GENERALES

PRIMERA: Notificar el contenido de la presente resolución al Rector, Vicerrector Académico; y, Jefe del Departamento de Información Estratégica de la USGP, para el cumplimiento de los resuelto en este acto.

Dada en la ciudad de Portoviejo, en la sesión ordinaria del H. Consejo Universitario de la Universidad San Gregorio de Portoviejo, llevada a cabo el nueve (09) del mes de marzo de 2018.

Dr. Marcelo Iván Farfán Intriago
RECTOR
UNIVERSIDAD SAN GREGORIO DE PORTOVIEJO
cc. Vicerrector Académico, Jefe del Departamento de Información Estratégica

UNIVERSIDAD
SAN GREGORIO
DE PORTOVIEJO

RESOLUCIÓN USGP H.C.U No. 083-03-2018
HONORABLE CONSEJO UNIVERSITARIO DE LA UNIVERSIDAD SAN GREGORIO DE PORTOVIEJO

CONSIDERANDO

Que, el Art. 350 de la Constitución del Ecuador señala: "El sistema de educación superior tiene como finalidad la formación académica y profesional con visión científica y humanista; la investigación científica y tecnológica; la innovación, promoción, desarrollo y difusión de los saberes y las culturas; la construcción de soluciones para los problemas del país, en relación con los objetivos del régimen de desarrollo".

Que el artículo 355 de la Constitución del Ecuador, entre otros principios, establece que el Estado reconocerá a las universidades y escuelas politécnicas autonomía académica administrativa, financiera y orgánica, acorde con los objetivos del régimen de desarrollo y los principios establecidos en la Constitución. Se reconoce a las universidades y escuelas politécnicas el derecho a la autonomía, ejercida y comprendida de manera solidaria y responsables. Dicha autonomía garantiza el ejercicio de la libertad académica y el derecho a la búsqueda de la verdad, sin restricciones; el gobierno y gestión de sí mismas, en consonancia con los principios de alternancia, transparencia y los derechos políticos; y la producción de ciencia, tecnología, cultura y arte. La autonomía no exime a las instituciones del sistema de ser fiscalizadas, de la responsabilidad social, rendición de cuentas y participación en la planificación nacional.

Que, el artículo 17 de la Ley Orgánica de Educación Superior determina que: *"Reconocimiento de la autonomía responsable: El Estado reconoce a las universidades y escuelas politécnicas autonomía académica. administrativa. financiera y orgánica, acorde con los principios establecidos en la Constitución de la República. En el ejercicio de autonomía responsable, las universidades y escuelas politécnicas mantendrán relaciones de reciprocidad y cooperación entre ellas y de estas con el Estado y la sociedad; además observarán los principios de justicia, equidad, solidaridad, participación ciudadana, responsabilidad social y rendición de cuentas".*

Que, el artículo 45 de la LOES dice: *"Principio del Cogobierno. El cogobierno es parte consustancial de la autonomía universitaria responsable. Consiste en la dirección compartida de las universidades y escuelas politécnicas por parte de los diferentes sectores de la comunidad de esas instituciones: profesores, estudiantes, empleados y trabajadores, acorde con los principios de calidad, igualdad de oportunidades. alternabilidad y equidad de género. Las universidades y escuelas politécnicas incluirán este principio en sus respectivos estatutos".*

Que, el Art. 18 del Estatuto de la Universidad San Gregorio de Portoviejo, expresa que: "Ejercicio de la autonomía responsable- La autonomía responsable que ejercen las universidades y escuelas

Dirección General de Desarrollo Institucional
RECIBIDO
23 AGO 2019
15h55

UNIVERSIDAD
SAN GREGORIO
DE PORTOVIEJO

RESOLUCIÓN USGP - C.R. No. 015-2019
CONSEJO DE REGENTES
UNIVERSIDAD SAN GREGORIO DE PORTOVIEJO

CONSIDERANDO

Que, el artículo 343 de la Constitución del Ecuador determina que el sistema nacional de educación tendrá como finalidad el desarrollo de capacidades y potencialidades individuales y colectivas de la población, que posibiliten el aprendizaje, y la generación y utilización de conocimientos técnicas, saberes, artes y cultura.

Que, el Art. 350 de la Constitución del Ecuador señala: "El sistema de educación superior tiene como finalidad la formación académica y profesional con visión científica y humanista; la investigación científica y tecnológica; la innovación, promoción, desarrollo y difusión de los saberes y las culturas; la construcción de soluciones para los problemas del país, en relación con los objetivos del régimen de desarrollo".

Que el artículo 355 de la Constitución del Ecuador, entre otros principios, establece que el Estado reconocerá a las universidades y escuelas politécnicas autonomía académica administrativa, financiera y orgánica, acorde con los objetivos del régimen de desarrollo y los principios establecidos en la Constitución.

Que, el artículo 17 de la Ley Orgánica de Educación Superior manifiesta: "*Reconocimiento de la autonomía responsable. El Estado reconoce a las universidades y escuelas politécnicas autonomía académica, administrativa, financiera y orgánica, acorde con los principios establecidos en la Constitución de la República...*".

Que, Art. 47.1 de la Ley Reformatoria a la Ley Orgánica de Educación Superior dice: "*Consejo de Regentes. Las instituciones de educación superior particulares podrán constituir un Consejo de Regentes que tendrá como principal función la de velar por el cumplimiento de la misión, la visión y los principios fundacionales de estas instituciones. Este Consejo estará integrado por un mínimo de cinco y máximo de siete miembros. Podrán formar parte del Consejo los promotores o fundadores de la institución, siempre que su representación no supere el número de dos integrantes...*".

Que, el 47.2 de la Ley Reformatoria a la Ley Orgánica de Educación Superior expresa que son: "*Atribuciones del Consejo de Regentes. Serán deberes y atribuciones del Consejo de Regentes: a) Rendir cuentas e informar al Órgano Colegiado Superior de las actividades relativas al cumplimiento de sus funciones, según lo establecido en los estatutos de las instituciones de educación superior a la cual pertenecen, o cuando éste lo requiera. b) Aprobar la planificación estratégica institucional en el marco de las disposiciones de la Constitución y la ley, promoviendo la articulación con el desarrollo nacional. c) Proponer o elegir, de ser el caso, y conforme los mecanismos previstos en esta Ley, el Rector o Rectora, Vicerrector o Vicerrectora, respetando el principio de alternabilidad. d) Solicitar la remoción del Rector o Rectora, Vicerrector o Vicerrectora, respetando el debido proceso y conforme a las causales y al procedimiento*

determinado en esta Ley y su reglamento. e) Las demás que establezca el estatuto de la institución de educación superior, conforme a la Constitución y las normas vigentes".

Que, el artículo 45 de la LOES dice: *"Principio del Cogobierno. El cogobierno es parte consustancial de la autonomía universitaria responsable. Consiste en la dirección compartida de las universidades y escuelas politécnicas por parte de los diferentes sectores de la comunidad de esas instituciones: profesores, estudiantes, empleados y trabajadores, acorde con los principios de calidad, igualdad de oportunidades, alternabilidad y equidad de género. Las universidades y escuelas politécnicas incluirán este principio en sus respectivos estatutos".*

Que, el Art. 10 del Estatuto de la Universidad San Gregorio de Portoviejo expresa: *Art. 10.- La planificación institucional en la Universidad San Gregorio de Portoviejo, constituye uno de los aspectos relevantes del proceso educativo, toda vez que tiene por finalidad orientar el desarrollo organizacional, previendo las herramientas necesarias para la dirección, la evaluación y coordinación de la prospectiva institucional".*

Que, el Art. 127.- del Estatuto de la Universidad San Gregorio de Portoviejo expresa que el Departamento de Información Estratégica *"Es el Departamento encargado de diseñar e implementar gestores de información automatizados que apoyen al mejoramiento de la gestión de la calidad de procesos académicos – administrativos, y generar indicadores claves de gestión, que apoyen la toma de decisiones en los diferentes niveles de la dirección. Por tanto, centrará su atención en mejorar la producción de información útil a partir de la base de datos institucional".*

Que, el artículo 40 del Estatuto de la USGP, manifiesta que: *"Para el ejercicio de la autonomía universitaria, la Universidad San Gregorio de Portoviejo está estructurada por los siguientes niveles: ... Estos departamentos serán dependientes de la Dirección General Administrativa Financiera... Departamento de Redes de Datos y Conectividad".*

Que, a través de la comunicación de fecha 8 de julio de 2019, el Ing. Marcos Gallegos Macías, Jefe del Departamento de Información Estratégica de la USGP, hace conocer al Arq. Jaime Alarcón Zambrano, Director de Desarrollo Institucional, que con el ánimo de contar con las directrices que respondan a las tendencias actuales, respecto a la gestión y seguridad de la información , en razón de ello solicita la actualización de las Políticas de Gestión y Seguridad de la Información, aprobadas por el Consejo Universitario de la USGP mediante resolución USGP-H.C.U. No. 083-03-2018, que consiste en agregar, políticas sobre el uso de controles criptográficos; acceso a redes y a servicios en red; seguridad física y ambiental; áreas seguras; protección por amenazas externas o ambientales; trabajaos en áreas seguras; seguridad de cableado; mantenimiento de equipos, con el objeto de organizar el rol de la redes de datos y conectividad en la institución.

Que, mediante oficio USGP-DDI-034-2019 del 17 de julio de 2019, suscrito por el Arq. Jaime Alarcón Zambrano, Director de Desarrollo Institucional, hace conocer al Ab. Marcelo Farfán Intriago, Canciller de la USGP, el documento que contiene las Políticas sobre el uso de controles criptográficos, acceso a redes, servicios de red y seguridad física y ambiental, para que sean agregadas a las Políticas de Gestión y Seguridad de la Información de la institución.

UNIVERSIDAD
SAN GREGORIO
DE PORTOVIEJO

En ejercicio de las facultades conferidas por la Ley Orgánica de Educación Superior; y, el Estatuto de la Universidad San Gregorio de Portoviejo, los miembros del Consejo de Regentes:

RESUELVEN

PRIMERO: Aprobar la inclusión de tres acciones denominadas: Políticas sobre el Uso de Controles Criptográficos; Acceso a Redes y Servicios en Red; y, Seguridad Física y Ambiental, dentro de las Políticas de Gestión y Seguridad de la Información de la Universidad San Gregorio de Portoviejo, presentadas por el Departamento de Información Estratégica y la Dirección de Desarrollo Institucional.

SEGUNDO: Disponer al Jefe del Departamento de Información Estratégica, realice las acciones necesarias para que se incluya en las Políticas de Gestión y Seguridad de la Información de la USGP, las Políticas sobre el Uso de Controles Criptográficos; Acceso a Redes y Servicios en Red; y, Seguridad Física y Ambiental.

TERCERO: Disponer al Director de Desarrollo Institucional de la USGP, disponga la socialización y difusión de las nuevas políticas que se agregan a las Políticas de Gestión y Seguridad de la Información.

DISPOSICIONES GENERALES

PRIMERO: Notificar el contenido de la presente resolución a los miembros del Consejo de Regentes, Rectora, Director de Desarrollo Institucional, Jefe del Departamento de Información Estratégica, para el cumplimiento de lo resuelto.

SEGUNDO: Disponer que el presente acto sea publicado en la página web de la USGP.

Dada en la ciudad de Portoviejo, en la sesión del Consejo de Regentes de la Universidad San Gregorio de Portoviejo, llevada a cabo el diecinueve de julio del año dos mil diecinueve.

CONSEJO DE REGENTES USGP
CANCILLER

Dr. Marcelo Iván Farfán Intriago
CANCILLER
CONSEJO DE REGENTES
UNIVERSIDAD SAN GREGORIO DE PORTOVIEJO
cc. Miembros del Consejo de Regentes, Rectora, Director de Desarrollo Institucional, Jefe del Departamento de Información Estratégica