



UNIVERSIDAD
SAN GREGORIO
DE PORTOVIEJO

Departamento de Información Estratégica

Políticas de Seguridad y Gestión de la
Información

UNIVERSIDAD PARTICULAR
SAN GREGORIO DE PORTOVIEJO

Ab. Jorge Cantos Pico
SECRETARIO GENERAL



Marzo-2018

RESOLUCIÓN USGP H.C.U No. 083-03-2018
Marzo 9 de 2018

CONTENIDO:

1.	INTRODUCCIÓN	3
2.	OBJETIVO	4
3.	ALCANCE	4
4.	DEFINICIONES.....	5
5.	POLÍTICA DE CONTROL DE ACCESO LÓGICO.....	9
6.	GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN.....	10
7.	POLÍTICAS DE DESARROLLO SEGURO.....	11
8.	POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS	12
9.	POLÍTICAS DE BACKUPS O COPIAS DE SEGURIDAD	13
10.	POLÍTICA DE GESTIÓN DE LA INFORMACIÓN.....	14
11.	APLICABILIDAD	15



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



UNIVERSIDAD PARTICULAR
SAN GREGORIO DE PORTOVIEJO

Ab. Jorge Cantos Pico
SECRETARIO GENERAL



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 ISO27001 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 ISO27001 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 desempeña.

UNIVERSIDAD PARTICULAR
SAN GREGORIO DE PORTOVIEJO



Ab. Jorge Cantos Pico
SECRETARIO GENERAL



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 en caso de una

UNIVERSIDAD PARTICULAR
SAN GREGORIO DE PORTOVIEJO



Ab. Jorge Cantos Pico
SECRETARIO GENERAL



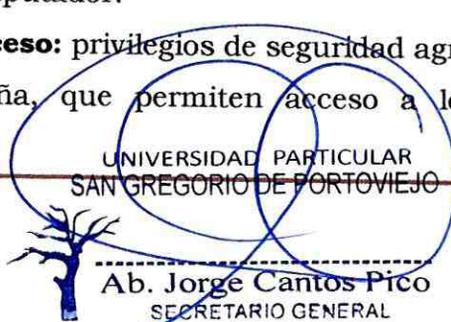
eventual pérdida de datos, para continuar con las actividades rutinarias y evitar pérdida generalizada de datos.

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 auditoría 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

UNIVERSIDAD PARTICULAR
SAN GREGORIO DE PORTOVIEJO



Ab. Jorge Cantos Pico
SECRETARIO GENERAL



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.

UNIVERSIDAD PARTICULAR
SAN GREGORIO DE PORTOVIEJO
Ab. Jorge Cantos Pico
SECRETARIO GENERAL



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.

UNIVERSIDAD PARTICULAR
SAN GREGORIO DE PORTOVIEJO

Ab. Jorge Cantos Pico
SECRETARIO GENERAL



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

UNIVERSIDAD PARTICULAR
SAN GREGORIO DE PORTOVIEJO

Ab. Jorge Cantos Pico
SECRETARIO GENERAL



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.

UNIVERSIDAD PARTICULAR
SAN GREGORIO DE PORTOVIEJO



Ab. Jorge Cantos Pico
SECRETARIO GENERAL



- 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.



UNIVERSIDAD PARTICULAR
SAN GREGORIO DE PORTOVIEJO

Ab. Jorge Cantos Pico
SECRETARIO GENERAL



- 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. APLICABILIDAD

- 11.1. 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.
- 11.2. 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 ecuatorianas vigentes.

Elaborado por:	Ing. Marcos Gallegos Macías, Msc. Jefe del Departamento de Información Estratégica
Fecha:	26 de febrero 2018

UNIVERSIDAD PARTICULAR
SAN GREGORIO DE PORTOVIEJO

Ab. Jorge Cantos Pico
SECRETARIO GENERAL

