RESOLUCIÓN No.562
(29 de noviembre de 2017)

Por la cual se actualiza la Resolución No.0118 del 22 de abril de 2015, en donde se aprobó las Políticas de Seguridad de la Información Versión 2.0 de la Universidad Francisco de Paula Santander Ocaña.

EL DIRECTOR DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA, EN USO DE SUS FACULTADES CONSTITUCIONALES, LEGALES Y REGLAMENTARIAS,

CONSIDERANDO:

Que, el artículo 69 de la Constitución Política de Colombia establece la autonomía universitaria.

Que, el artículo 61 de la Constitución Política define propiedad intelectual, en concordancia con el artículo 2 numeral 8 del Convenio que establece la Organización Mundial de la Propiedad Intelectual, es omnicomprensivo de diferentes categorías de propiedad sobre creaciones del intelecto, que incluye dos grandes especies o ramas: la propiedad industrial y el derecho de autor, que aunque comparten su naturaleza especial o *sui generis*, se ocupan de materias distintas. Mientras que la primera trata principalmente de la protección de las invenciones, las marcas, los dibujos o modelos industriales, y la represión de la competencia desleal, el derecho de autor recae sobre obras literarias, artísticas, musicales, emisiones de radiodifusión, programas para computadores, etc.

Que, la Ley 30 de 1992, en su artículo 29 literal D, confiere a las instituciones de Educación Superior la facultad de definir y organizar sus labores formativas, académicas, docentes, científicas, culturales y de extensión.

Que, el Congreso de la República mediante la Ley 1273 del 5 de enero de 2009, modifica el Código Penal, creando un nuevo bien jurídico tutelado denominado "De la protección de la información y de los datos".

Que, el Congreso de la República de Colombia, estableció la ley 1273 del 5 de enero de 2009, por medio de la cual se modifica el Código Penal, creando un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Que, la División de Sistemas de la Universidad Francisco de Paula Santander Ocaña, se acoge a los controles y sanciones establecidas en la Ley 1273 del 5 de enero de 2009, dando aplicabilidad al artículo 269H.

Que, el Comité Administrativo según consta en el Acta No. 0002 del 11 de marzo de 2015, aprobó las Políticas de Seguridad de la Información.

Que, el Magíster Antón García Barreto, Jefe de la División de Sistemas, mediante oficio O-TT-DSS-0058 del 26 de Marzo de 2015, solicitó al Comité de Apoyo Académico la aprobación de las políticas de seguridad.

Que, el Comité de Apoyo Académico mediante Acta No. 0011 del 21 de abril de 2015, también aprobó las políticas de Seguridad de la Información Versión 2.0 para la Universidad Francisco de Paula Santander Ocaña.

Que, mediante Resolución No. 0118 del 22 de abril de 2015, se aprobaron las Políticas de Seguridad de la Información Versión 2.0.

Que, teniendo en cuenta el Artículo sexto de la Resolución No.0118 del 22 de abril de 2015, se hace necesario mantener la Política de Seguridad de la Información actualizada, vigente, y operativa para asegurar su permanencia y nivel de eficacia.

Que, de conformidad con lo anteriormente expuesto, el Director de la Universidad Francisco de Paula Santander Ocaña,

RESUELVE

ARTÍCULO 1. Actualizar las Políticas de Seguridad de la Información bajo la Versión 2.1 de la Universidad Francisco de Paula Santander Ocaña.

TÍTULO I
PRESENTACIÓN

ARTÍCULO 2. La seguridad de la información se entiende como la preservación, aseguramiento y cumplimiento de las siguientes características de la información:

a. Confidencialidad: los activos de información solo pueden ser accedidos y custodiados por usuarios que tengan permisos para ello.

b. Integridad: el contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.

c. Disponibilidad: los activos de información sólo pueden ser obtenidos a corto plazo por los usuarios que tengan los permisos adecuados.

Para ello es necesario considerar aspectos tales como:

- Autenticidad: los activos de información los crean, editan y custodian usuarios reconocidos quienes validan su contenido.
- Posibilidad de Auditoría: se mantienen evidencias de todas las actividades y acciones que afectan a los activos de información.
- Protección a la duplicación: los activos de información son objeto de clasificación, y se llevan registros de las copias generadas de aquellos catalogados como confidenciales.
- No repudio: los autores, propietarios y custodios de los activos de información se pueden identificar plenamente.
- Legalidad: los activos de información cumplen los parámetros legales, normativos y estatutarios de la institución.
- Confiabilidad de la Información: es fiable el contenido de los activos de información que conserven la confidencialidad, integridad, disponibilidad, autenticidad y legalidad.

En la actualidad la información de la Universidad Francisco de Paula Santander Ocaña se ha reconocido como un activo valioso y a medida que los sistemas de información apoyan cada vez más los procesos de misión crítica se requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de los datos.

Así mismo, el 5 de enero de 2009, el Congreso de la República de Colombia, establece la ley 1273 por medio de la cual se modifica el Código Penal, creando un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. La División de Sistemas de la Universidad Francisco de Paula Santander Ocaña, reconociendo la legitimidad a nivel nacional de la ley 1273 de 2009, se acoge a los controles y sanciones establecidas por la misma.

TÍTULO II
DISPOSICIONES GENERALES

ARTÍCULO 3. *Generalidades.-* La información es uno de los recursos de mayor valor para la institución y por consiguiente debe ser debidamente protegida. Frente a las innumerables amenazas a las que se encuentra expuesta dicha información se han planteado una serie de políticas de seguridad, cuya aplicación contribuye en gran medida a la protección de la misma, a minimizar y mitigar los posibles riesgos asociados de daño.

ARTÍCULO 4. *Ámbito de aplicación.-* Las políticas de seguridad de la información serán de obligatoria aplicación en todas y cada una de las dependencias de la institución, involucrando así los recursos con que cuenta, los procesos internos o externos vinculados a la Institución y a todo el personal de las diferentes área de la Universidad Francisco de Paula Santander Ocaña, independientemente del tipo de contratación que posea y de las funciones y/o actividades que desempeñe.

ARTÍCULO 5. *Objeto de las políticas.-* Son Objetivos de las Políticas de seguridad de la información:

a. Brindar a la Universidad Francisco de Paula Santander Ocaña, un conjunto de lineamientos e instrucciones que permiten garantizar la seguridad en el ambiente informático, la información y demás recursos tecnológicos.

b. Resguardar y disponer objetivamente la información de la Universidad Francisco de Paula Santander Ocaña, asegurando el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

c. Mantener la Política de Seguridad de la Información actualizada, vigente, y operativa para asegurar su permanencia y nivel de eficacia.

ARTÍCULO 6. *Revisión de la política.-* El proceso de Sistemas de Información, Telecomunicaciones y Tecnología SITT de la Universidad Francisco de Paula Santander Ocaña deberá revisar anualmente esta política (o en el momento que se produzcan cambios significativos) para garantizar que es adecuada, eficaz y suficiente.

Además deberá efectuar toda modificación que sea necesaria en función a posibles cambios que puedan afectar su definición, como ser, cambios tecnológicos, variación de los controles, incidentes de seguridad, etc.

ARTÍCULO 7. *Tiempo de respuesta.-* El tiempo estipulado para atender las solicitudes por parte del proceso SITT es de tres días hábiles, dependiendo del problema y de la rapidez del equipo. Dicha solicitud debe registrarse en la aplicación dispuesta para tal fin siguiendo el enlace del portal Web Divisis http://divisis.ufpso.edu.co/registro.html.

TÍTULO III
DE LA SEGURIDAD

Capítulo I
De la Seguridad de los Usuarios

ARTÍCULO 8. *Usuario nuevo*.- La persona que ingrese como usuario nuevo a la Universidad Francisco de Paula Santander Ocaña y que para el desarrollo de sus actividades laborales necesite del uso de equipos de cómputo y de servicios informáticos debe aceptar las condiciones de confidencialidad establecidas dentro del contrato laboral, el uso adecuado de los bienes informáticos y de la información a su cargo, así como cumplir y respetar al pie de la letra las directrices impartidas en las Políticas de Seguridad de la Información.

Todo el personal nuevo de la Institución, deberá ser notificado por parte del proceso de Gestión Humana a la División de Sistemas, para creación y asignación de las respectivas cuentas de usuario (en el caso que lo necesitare) y de correo institucional, o en caso de retiro del funcionario, anular y cancelar los derechos otorgados como usuario.

ARTÍCULO 9. *Obligaciones de los usuarios*.- Es obligación y responsabilidad del personal de la Universidad Francisco de Paula Santander Ocaña que haga uso de sus bienes y servicios informáticos cumplir con las Políticas de Seguridad de la Información para lo cual se aplicarán las disposiciones mencionadas en el artículo 11º.

ARTÍCULO 10. *Capacitación en seguridad informática*.- Al momento del ingreso de nuevo personal a la Universidad Francisco de Paula Santander Ocaña debe brindársele en el proceso de inducción la capacitación sobre las Políticas de Seguridad de la Información por parte de la División de Sistemas, con el propósito de que conozca las obligaciones que tiene frente a la seguridad de la información y de las posibles sanciones a las cuales estará expuesto en caso de incumplir alguna de ellas.

ARTÍCULO 11. *Sanciones.-* El incumplimiento de las disposiciones establecidas por las Políticas de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y característica del aspecto no cumplido.

Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial de la Institución, o de que se le declare culpable de un delito informático.

Se aplicarán las sanciones establecidas en la Ley 1273 de 2009 denominado "de la protección de la información y de los datos" y la Ley 1581 de 2012 correspondiente a la protección de datos personales.

Capítulo II
De la Seguridad Física y del Medio Ambiente

ARTÍCULO 12. *Responsabilidad de la información y de los bienes informáticos.-* La protección de la información y de los bienes informáticos es responsabilidad del usuario

o funcionario, quien debe evitar en todo momento la fuga y/o pérdida de información de la entidad que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

ARTÍCULO 13. ***Protección de la información y de los bienes informáticos.-*** Se adoptarán las siguientes medidas para garantizar la seguridad.

a. En los centros de cómputo o áreas que la entidad considere criticas deberán existir elementos de control de incendio y alarmas.

b. En lo referente a la ubicación de computadores y hardware en general, se debe tener especial cuidado contra fallas del sistema de control del medio ambiente, y otras amenazas que puedan afectar la normal operación del sistema.

c. En todos los centros de procesamiento, sin excepción, deberán existir detectores de calor y humo, instalados en forma adecuada y en número suficiente como para detectar el más mínimo indicio de incendio. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses.

d. Se deben tener extintores de incendios debidamente probados, y con capacidad de detener fuego generado por equipo eléctrico, papel o químicos especiales.

e. El cableado de la red debe ser protegido de interferencias usando canaletas que lo protejan.

f. Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.

ARTÍCULO 14. ***Seguridad en áreas de trabajo.-*** Se adoptarán las siguientes medidas para garantizar la seguridad en áreas de trabajo:

a. Los centros de cómputo o áreas que la entidad considere criticas deberán estar demarcados con zonas de circulación y zonas restringidas.

b. Las centrales de conexión o centros de cableado deben ser catalogados como zonas de alto riesgo, con limitación y control de acceso.

c. Los centros de cómputo o áreas que la universidad considere críticas, deben ser lugares de acceso restringido y cualquier persona que ingrese a ellos deberá registrar el motivo del ingreso y estar acompañada permanentemente por el personal que labora cotidianamente en estos lugares.

ARTÍCULO 15. ***Protección y ubicación de los equipos.-*** Para preservar la protección de los equipos se disponen las siguientes medidas:

a. Está prohibido mover o reubicar, instalar o desinstalar dispositivos y abrir o destapar los equipos de cómputo o de comunicaciones y periféricos por su propia cuenta a excepción del personal autorizado por la División de Sistemas para realizar dicha labor, para tal caso deberá solicitar a la División de Sistemas el movimiento de dicho equipo a través del portal web Divisis siguiendo el enlace http://divisis.ufpso.edu.co.

b. El equipo de cómputo asignado a cada funcionario deberá ser para uso exclusivo de las actividades de la UFPS Ocaña.

c. Es responsabilidad de los usuarios almacenar su información en la partición del disco duro destinada para documentos, generalmente esta partición esta denotada por la letra D:\.

d. Las áreas en donde se tenga equipos de procesamiento de información, no se permitirá fumar, tomar ningún tipo de bebidas o consumir alimentos.
e. Se debe evitar colocar objetos encima del equipo de cómputo o tapar las salidas de ventilación del monitor o de la CPU.

f. Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que utiliza para el desempeño de sus funciones al proceso responsable de la operación de dicha herramienta, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

g. El equipo informático debe permanecer en un lugar limpio y sin humedad.

h. El cableado de la red debe ser protegido de interferencias usando canaletas que lo protejan.

i. Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.

ARTÍCULO 16. ***Mantenimiento de equipos.-*** Únicamente el personal autorizado por la División de Sistemas podrá llevar a cabo los servicios y reparaciones al equipo informático de la Institución siguiendo las pautas contempladas dentro del Plan de mantenimiento preventivo y correctivo de equipos tecnológicos, cabe resaltar que no es función de la División de Sistemas brindar mantenimiento preventivo o correctivo a equipos tecnológicos de propiedad de los funcionarios de la UFPS Ocaña.

ARTÍCULO 17. ***Traslado de activos.-*** Las diferentes áreas de la Universidad Francisco de Paula Santander Ocaña serán encargadas de proporcionar a la División de Sistemas mediante solicitud a través del Portal Web Divisis siguiendo el enlace http://divisis.ufpso.edu.co, la relación de bienes y equipos que se consideren aptos para ser dados de baja, según corresponda, pero será el área de mantenimiento perteneciente al proceso SITT quien realizará la evaluación técnica del equipo y definirá la reasignación o baja definitiva del bien y será el proceso de Almacén el encargado del proceso de disposición final de los mismos.

ARTÍCULO 18. ***Pérdida de equipos.-*** El servidor o funcionario que tengan bajo su responsabilidad o asignado algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

Los equipos de comunicación y/o computación que sean propiedad de la UFPS Ocaña no deben salir de la Universidad sin la debida autorización y supervisión del Jefe de la División de Sistemas.

ARTÍCULO 19. ***Seguridad física en el área de servidores.-*** Para garantizar la seguridad física en el área de servidores se disponen las siguientes medidas.

a. ***Control de acceso físico.*** El acceso físico a la sala de servidores de la UFPS Ocaña se hace mediante llave. Las personas autorizadas para posesión de una copia de dicha llave son específicamente el jefe de la división de sistemas, el administrador de dicha sala y las personas que ellos bajo previa solicitud autoricen. En ningún caso se permite a personas diferentes a las mencionadas obtener copia de dicha llave de forma abusiva y sin consentimiento. En todo caso, el funcionario debe permanecer bajo supervisión de uno o ambos funcionarios mencionados anteriormente.

b. **Autorización de acciones a ejecutar**. Las acciones que se ejecuten en la sala de servidores, pueden variar de acuerdo a la solicitud que solventen, siendo posible que se requiera apoyo técnico de terceros donde las acciones a realizar serán específicamente autorizadas, vigiladas y controladas por el jefe de la división de sistemas y el administrador de dicha sala.

c. ***Mantenimiento de equipos servidores***. Sólo personal autorizado por el Jefe de la División de Sistemas es el responsable de la ejecución del mantenimiento preventivo y/o correctivo a los equipos servidores. Para evitar traumatismos en los usuarios ante cualquier interrupción del servicio por motivo de mantenimiento en los equipos servidores, se debe dar aviso oportuno y anticipado a la comunidad universitaria sobre dichas actividades a realizar.

d. ***Registro del acceso de terceros a las sala de servidores***. El personal autorizado para la administración de servidores debe registrar el acceso a la sala de servidores en el FORMATO DE REGISTRO DE ACCESO A SALA DE SERVIDORES F-TT-DSS-0042 del proceso SITT, de personas ajenas a las autorizadas, discriminando el nombre del funcionario que realiza la operación, fecha, hora de entrada, de salida, acción a ejecutar y nombre del funcionario que autoriza el acceso.

   En todo caso, las personas que permanezcan en la sala y operen con los servidores, deben actuar con prudencia procurando la protección de los mismos, evitando producir cortes de energía, reinicio o apagado de servidores o daño en los mismos.

ARTÍCULO 20. *Video vigilancia.-* Con el fin de implementar estrategias tecnológicas que apoyen las estrategias de seguridad en la institución, se hace uso de cámaras de seguridad en distintos puntos geográficos del campus universitario. La División de Sistemas, acorde a las características técnicas de los equipos, tendrá como periodo de almacenamiento de la información obtenida a través de dichos dispositivos 30 días calendario. Los respaldos de esta información se alojarán en servidores destinados para este uso específico, su administración se realizará con la supervisión del jefe de la dependencia División de Sistemas y solo tendrá acceso a la información el personal asignado y autorizado por el mismo. Bajo ningún caso se entregará información sin previa solicitud.

ARTÍCULO 21. *Sanciones.-* Las cámaras de seguridad como todos los dispositivos tecnológicos están siendo monitoreados y salvaguardados de acciones que conlleven a su deterioro o alteren su buen funcionamiento. Para este caso, cualquier acción que entorpezca la seguridad que pretende ofrecer las cámaras será sancionada con la normativa contenida en el Artículo 269B de la ley 1273 de 2009.

Capítulo III
De la administración de operaciones en los centros de cómputo

ARTÍCULO 22. *Acceso a la información*.- Para la administración de operaciones en los centros de cómputo se disponen las siguientes medidas:

a. Los usuarios que soliciten o requieran acceso a información relacionada, almacenada, generada o procesada por la División de Sistemas de la UFPS Ocaña, deben tener definido un rol o tipo de vinculación con la institución. Éstos usuarios pueden considerarse visitantes, siendo un visitante aquella persona cuya vinculación formal con la universidad es nula pero que solicita información o accede presencialmente a las instalaciones físicas en cualquiera de sus sedes, o solicita información o accede virtualmente a sitios o servicios web, sistemas de información, sistemas de telecomunicaciones o infraestructura relacionada de la UFPS Ocaña.

b. Se consideran estudiantes, aquellas personas que poseen un registro de matrícula activo en cualquier programa académico, ya sea técnico, de pregrado, posgrado a distancia o en cualquier modalidad ofertada por la UFPS Ocaña o que esté realizando actividades bajo convenio de prácticas o pasantías, trabajo de grado dirigido o proyecto de grado (Acuerdo 065 del 26 de agosto de 1996).

c. Se consideran empleados aquellas personas que cumplen funciones con vinculación por posesión, por contrato a término fijo o prestación de servicios y se reconocen dos tipos de docentes: de tiempo completo y docentes catedráticos. Ante la solicitud de información o acceso a la misma (sistemas de información, módulos de software, reportes, entre otros) los usuarios que pertenecen a cualquier estamento: estudiantil, administrativo y docente de la Universidad Francisco de Paula Santander Ocaña o que se consideren visitantes, el suministro de información o de acceso por parte de funcionarios de la División de Sistemas se limita a lo necesario y coherente para el desarrollo de las actividades del solicitante o que responda la solicitud realizada, sin alterar la privacidad y confidencialidad propia de la información y su tratamiento.

d. El personal con cualquier tipo de vinculación al que se ha concedido acceso a los sistemas de información y sus módulos, servicios Web, espacio en servidores, acceso a las bases de datos, dispositivos de telecomunicación y redes, no debe extralimitarse en sus funciones y permisos, por el contrario debe propender por la integridad de la información, confidencialidad y el manejo prudente y reservado de la misma, limitando su accionar a lo contemplado en sus funciones.

e. En el caso de personal ajeno que suministre soporte técnico a la institución, que requieran acceder a las instalaciones físicas o equipo de telecomunicaciones, computadores, servidores y demás elementos relacionados con el área de la división de sistemas, así como proveedores de servicios e infraestructura, el responsable de autorizar su ingreso y generar información requerida por dicho personal, debe permitir solo acceso indispensable de acuerdo con el trabajo a ejecutar, dejando justificación escrita, de su ingreso, hora fecha de entrada y salida, especificando las funciones y actividades que debe realizar. Debe contar con las condiciones de acceso favorables para el desempeño de sus funciones solo y durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas; esto aplica para personal que labora en la institución (personal de servicios generales, de soporte técnico, electricistas entre otros) y que temporal u ocasionalmente suministre algún tipo de servicio.

ARTÍCULO 23. *Sanciones*.- Aplica las sanciones establecidas por los Artículos 269A y 269C ley 1273 de 2009.

ARTÍCULO 24. A*dministración de cambios.-* Para la administración de cambios en los centros de cómputo se disponen las siguientes medidas.

a. Todo cambio (creación, modificación o eliminación de datos, campos, tablas, fechas, formularios, reportes, modificación de registros, usuarios, contraseñas, accesos, entre otros) que involucre o afecte los recursos informáticos, debe ser anunciado y registrado de forma explícita por los usuarios de la información y aprobado formalmente por el responsable de la administración de la misma, al nivel de jefe inmediato o a quienes estos formalmente deleguen. El responsable de la administración de los accesos tendrá la facultad de aceptar o rechazar la solicitud, siempre y cuando se ajuste a las normas de privacidad y confidencialidad establecidas por la universidad y a los requerimientos realizados por el solicitante.

b. Toda la información generada, relacionada y procesada por la división de sistemas debe gozar de veracidad, certeza e integridad y por lo tanto la exposición a cambios o modificaciones debe documentarse de forma detallada. Cualquier manipulación que se realice a la información, módulos, sistemas de información, archivos fuente, registros y demás, debe quedar formalmente registrada en los formatos aprobados correspondientes a cada proceso y actividad determinando fechas y responsables, describiendo el tipo de acción realizada desde su solicitud hasta su implementación, estableciendo si no ha generado u aprobado un formato para el registro de actualización o modificación de cambios, debe establecerse mecanismos que permitan el seguimiento y control. (Documentos soporte: Formato bitácora manejo de errores.)

c. Todo cambio, actualización o modificación realizada a un recurso informático relacionado con modificación de accesos y/o permisos, mantenimiento de software o hardware, equipos de telecomunicación, servidores, modificación de parámetros entre otros, debe realizarse de tal forma que no vulnere, exponga o disminuya el nivel de seguridad existente y la robustez actual de dicha infraestructura, así mismo debe documentarse en los formatos establecidos y/o determinar mecanismos que permitan controlar y dar seguimiento a éstas acciones. (Documentos soporte: Formatos de fichas técnicas y de mantenimientos de los recursos tecnológicos.)

ARTÍCULO 25. *Tratamiento de la Información*.- Los funcionarios de la Universidad Francisco de Paula Santander Ocaña, se consideran responsables de la información a la que tienen acceso y/o manipulan; al hacer parte de la institución asumen el compromiso de dar uso reservado, prudente y adecuado de la información que conocen, por lo tanto deberán cumplir los lineamientos generales y especiales establecidos por la Universidad Francisco de Paula Santander Ocaña y por la ley colombiana, para protegerla, evitar pérdidas, daños, accesos no autorizados, exposición y utilización indebida de la misma. El suministro de información a entes externos debe realizarse bajo las respectivas autorizaciones de quien tiene a cargo la administración de la información.

Se disponen las siguientes medidas para el tratamiento de la información:

a. ***Confidencialidad.-*** El proceso de Gestión Humana debe contar dentro de cada uno de los contratos con una cláusula de cumplimiento donde el funcionario de la Universidad exprese su responsabilidad de contribuir con la seguridad de la información, la confidencialidad y el buen manejo de la información y deba firmarse y renovarse semestralmente o anualmente (según contratación), dicha cláusula debe manifestar lo siguiente:

"CONFIDENCIALIDAD. EL TRABAJADOR tiene y asume la obligación de guardar reserva y confidencialidad respecto de cualquier tipo de información que se le suministre o a la cual llegare a tener acceso o conocimiento por la actividad que desempeñe en ejercicio de sus funciones, durante la vigencia del presente contrato y aún con dos años de posterioridad a su terminación, comprometiéndose en especial a no difundirla, reproducirla, transmitirla, publicarla, divulgarla o revelarla por cualquier medio conocido o por conocer a personas en interés propio o de terceros, independientemente de la finalidad perseguida sin que medie autorización previa y expresa del titular de los derechos y/o de LA UNIVERSIDAD. Además de tomar las previsiones necesarias para que sus funcionarios, técnicos, consultores o contratistas, que tengan acceso a la información suministrada actúen en la misma forma. El incumplimiento a esta cláusula será considerado como falla grave para efectos laborales. Así mismo, EL TRABAJADOR será responsable de todos los daños y perjuicios que para LA UNIVERSIDAD se deriven como consecuencia del incumplimiento de dicha obligación.

PARÁGRAFO. Se excluye de esta obligación la información que claramente resulte del dominio público o que sea del conocimiento previo del receptor, sin constituir reserva o documento de protección de datos y cuya revelación no cause agravio o perjuicio alguno a su titular, de conformidad con lo señalado en la Ley 1581 de 2012 y Decreto Reglamentario 1377 de 2013."

b. Si el trabajador deja de prestar sus servicios a la Institución, se compromete a entregar toda la información y documentación respectiva de su trabajo realizado, contraseñas y usuarios tanto para el acceso a módulos, sistemas de información, correos electrónicos y equipos de cómputo o telecomunicaciones asignados y a no divulgarla directamente o a través de terceros bajo ninguna circunstancia. Este compromiso aplica para contratistas, proveedores, auxiliares, personal de apoyo o asesoría técnica temporal. (Documentos soporte: Formato entrega del puesto de trabajo.

c. Para funcionarios directos de la división de sistemas, pasantes, practicantes, de cualquier plan de estudios, jurados, directores de proyectos de grado y en general toda persona que requiera y obtenga relación directa con los sistemas informáticos, debe someterse a las políticas de sanción internas, de la ley colombiana e internacional que rigen la seguridad en los sistemas de información y equipos de comunicación, así como de propiedad intelectual, si intentan, contribuyen o ejercen complicidad en la ejecución material o concepción intelectual para vulnerar, atacar, disminuir, arriesgar, dañar alterar o poner de cualquier manera en riesgo la información, su integridad y veracidad, los equipos de hardware (incluidos los sistemas de comunicaciones, cableado, redes inalámbricas, documentación), el acceso o tráfico de los sistemas de información y comunicaciones.

d. Todo funcionario de la Universidad que utilice los recursos de los Sistemas, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje.

e. Tanto personal externo como funcionarios de cualquier estamento y con cualquier tipo de contratación así como estudiantes de la Universidad no deben intentar sobrepasar los controles de los sistemas, examinar los computadores y redes en busca de archivos de otros sin su autorización o introducir intencionalmente software diseñado para causar daño o impedir el normal funcionamiento de los sistemas.

ARTÍCULO 26. *Sanciones*.- Aplica las sanciones establecidas por el Artículo 269D ley 1273 de 2009, la Ley Estatutaria 1266 de 2008, la Ley 1581 de 2012, los Artículos 269E y 269F ley 1273 de 2009.

ARTÍCULO 27. *Actualización de Hardware*.- Cualquier cambio que se requiera realizar en los equipos de cómputo de esta institución (cambios de procesador, adición de memoria, tarjetas, reparación técnica de los equipos de cómputo y telecomunicaciones entre otros) debe tener previamente una evaluación técnica y autorización del área responsable y únicamente puede ser realizada por el personal facultado por el Jefe del Área de Sistemas. (Control registrado en los formatos estipulados para tal fin como fichas técnicas de los recursos tecnológicos). Así como los equipos de cómputo (PC, servidores, equipos de telecomunicación, cableado LAN y wireless entre otros) no deben moverse o reubicarse sin la aprobación previa del jefe del área involucrada.

ARTÍCULO 28. Uso del correo electrónico.- Los mensajes de E-mail y archivos adjuntos que se manejen a través del correo electrónico institucional deben ser tratados como información de propiedad de la Universidad Francisco de Paula Santander Ocaña y deben ser manejados como una comunicación privada y directa entre emisor y receptor.

ARTÍCULO 29. *Seguridad del correo electrónico*.- Está prohibido falsificar, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico, así como interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

ARTÍCULO 30. *Contingencia ante desastre*.- Para superar cualquier eventualidad de accidentes que pueda llegar a presentarse ocasionando pérdidas importantes de información, se debe contar con la existencia de un plan de contingencia de TI y con disponibilidad de copias de respaldo para restablecer las operaciones en las áreas de misión crítica definidas.

ARTÍCULO 31. Uso de la red interna e Internet.- Los usuarios de la Universidad Francisco de Paula Santander Ocaña deben cumplir las siguientes medidas en aspectos del uso de la red interna e internet:

- Respetar la privacidad de los usuarios.
- No está permitido suplantar las identidades de otra persona para intentar acceder a conexiones y/o sistemas privados o para enviar información a nombre de la misma sin previa autorización del titular de la cuenta, así como también está prohibido obtener intencionalmente algún tipo de información ajena.
- Respetar la protección legal otorgada a programas, textos, artículos y bases de datos según legislación internacional sobre propiedad intelectual y las normas pertinentes de nuestro país.
- No está permitido acceder a Internet con fines diferentes a los propios de las actividades académicas, o administrativas en la Universidad Francisco de Paula Santander Ocaña.
- La creación de nuevas redes o reconfiguración de las existentes, solo podrá ser adelantada por personal autorizado por la División de sistemas.

- Los usuarios de Internet de la Universidad Francisco de Paula Santander que evidencien incidentes de seguridad que afecten contra la integridad de la información deben reportarlo a la División de Sistemas inmediatamente.

ARTÍCULO 32. *Sanciones.-* Aplica las sanciones establecidas en los artículos 269C, 269D,269G ley 1273 de 2009.

ARTÍCULO 33. *Control de conexión a las redes.-* La creación de nuevas redes o reconfiguración de las existentes, solo podrá ser adelantada por personal autorizado por la División de sistemas y sólo se permite la configuración a las redes de la UFPS Ocaña de equipos pertenecientes a la misma.

ARTÍCULO 34. *Seguridad en comunicaciones*.- Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Universidad Francisco de Paula Santander Ocaña, deberán ser consideradas y tratadas como información confidencial. Aplica el inciso Seguridad de la información.

Capítulo IV
Del acceso lógico

ARTÍCULO 35. *Uso de contraseñas.*- Se disponen las siguientes medidas de acceso lógico:

- Para el desarrollo de las actividades de algunos funcionarios de la Universidad Francisco de Paula Santander Ocaña es indispensable acceder a la red interna de información e infraestructura tecnológica, para lo cual les es asignado por parte de la División de Sistemas previa solicitud del proceso responsable, datos de login como su "usuario" y "contraseña" necesarios para acceder a dichos recursos; cada funcionario es entonces responsable de mantenerlos de forma confidencial.

- Los usuarios y funcionarios son responsables de todas las actividades realizadas con su identificador de usuario (ID). Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, al igual que tiene prohibido utilizar el ID de otros usuarios.

- Todo el personal nuevo de la Institución, deberá ser notificado a la División de Sistemas, para creación y asignación de las respectivas cuentas de usuario (en el caso que lo necesitare) y de correo institucional, o en caso de retiro del funcionario, anular y cancelar los derechos otorgados como usuario.

- La persona que ingrese como usuario nuevo a la Universidad Francisco de Paula Santander Ocaña y que para el desarrollo de sus actividades laborales necesite del uso de equipos de cómputo y de servicios informáticos debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información a su cargo, así como cumplir y respetar al pie de la letra las directrices impartidas en el Manual de Políticas de Seguridad de la Información.

- Los funcionarios de la UFPS Ocaña deben proteger su equipo de cómputo con controles de acceso como contraseñas cuando no se encuentre en su lugar de trabajo, evitando de esta manera la manipulación de su información por terceras personas.

- Los equipos de cómputo deben ser apagados terminada la jornada laboral, contribuyendo al compromiso ambiental.

- El jefe de la División de Sistemas y administrador de la base de datos, velarán por la seguridad en el uso de las contraseñas para acceder a los aplicativos institucionales. Para ello se contempla un período semestral, sincronizando el calendario académico y los períodos de contratación para funcionarios administrativos, estableciendo la respectiva actualización de contraseñas. Se aclara que la división de sistemas requiere el apoyo necesario de la división de personal, para bloquear contraseñas a funcionarios que han culminado contratación o han sido removidos o rotados de su cargo. Bajo conocimiento de estas circunstancias, en todo caso, se aplica la restricción de contraseñas a personal sin vinculación laboral.

- El usuario deberá solicitar a la División de Sistemas la restauración de la contraseña en caso de olvido y/o bloqueo de la misma, para que se le proporcione una nueva.

- Está prohibido fijar las contraseñas en cualquier medio y/o lugar visible y accesible a terceras personas.

- Las contraseña son personales por lo tanto no debe compartirlas ni revelarlas, ya que en caso de acciones fraudulentas que afecten la integridad de la información se responsabilizará al usuario al cual pertenece dicha contraseña.

- Las contraseñas de usuario deben cambiarse de manera periódica.

- Es responsabilidad de los usuarios tener máximo secreto de su contraseña; sobre todo la mantendrá secreta, usará clave que no sean triviales o simples de averiguar. Si requiere el cambio de la clave de ingreso a red o a sistemas de información debe notificar de manera personal para el cambio de contraseña siempre que crea o sospeche que su confidencialidad pueda ser vulnerada.

ARTÍCULO 36. *Sanciones.-* Aplica las sanciones establecidas por el Artículo 269D ley 1273 de 2009.

ARTÍCULO 37. *Escritorios limpios.-* Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento como CD's, USB, con el fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

Capítulo V
De la seguridad para los servicios informáticos

ARTÍCULO 38. *Seguridad para los servicios informáticos.-* A todos los usuarios de los servicios web e intranet, bases de datos, módulos y sistemas de información, tecnología informática e infraestructura de telecomunicaciones de la Universidad Francisco de Paula Santander Ocaña, les está prohibido:

- Suplantar la identidad personal de otros usuarios para realizar en los sistemas de información (SIA, SIF. SIB, SID, Uvirtual. correo electrónico) y en la red cualquier tipo de acción u operaciones asignadas.

- Para los casos específicos de correo electrónico institucional y Uvirtual, está prohibido utilizar la información de otros usuarios relacionada para el acceso a la(s) cuenta(s) de usuario de la plataforma Uvirtual, con el fin de realizar, modificar o anular actividades propuestas por el tutor(a), así como enviar mensajes, participar en foros, agregar eventos, esto se mencionará como suplantación de identidad y acceso abusivo a la información personal (administrador, docente o estudiante). Así mismo, la cuenta de correo electrónico es personal, hacer uso de información de otros usuarios y contraseñas para acceder a la misma, emitir correos electrónicos con cualquier tipo de contenido también se tipifica como suplantación de identidad, ratificando que su asignación y uso es personal.

- Efectuar acciones para obtención de contraseñas, datos u obtención de información de un usuario o proceso.

- Exceder la protección sugerida a los datos, usuarios, sistemas y equipos, así como la seguridad informática establecida para la Universidad Francisco de Paula Santander Ocaña.

- Efectuar actividades que violen la reserva de datos, la producción de contenido intelectual (labores efectuadas por medio de correo electrónico y Uvirtual) y la labor o historial de otros usuarios.

- Usar los servicios o medios de difusión electrónica de la información, el correo electrónico, la publicación web, para la propagación de contenidos que degraden la imagen institucional, contenidos de tipo amenazante, mensajes con tinte de calumnia e injuria o que atenten contra la dignidad y el buen nombre de las personas o de la Universidad Francisco de Paula Santander Ocaña.

- Usar la cuenta de correo electrónico de la Universidad Francisco de Paula Santander Ocaña para fines personales que deformen el sentido académico con que la cuenta de correo electrónico se suministra a sus usuarios.

- Las cuentas de usuarios en los sistemas informáticos de la Universidad Francisco de Paula Santander Ocaña son personales e intransferibles y de uso en el ámbito estrictamente académico, de investigación o de la gestión administrativa.

ARTÍCULO 39. *Gestión para la utilización de la plataforma uvirtual.*- Son funciones del rol Administrador de la plataforma Uvirtual: Gestionar los servicios pertinentes a la administración de cuentas de usuarios, cursos virtuales, creación y actualización de contraseñas y datos de usuario de usuario a estudiantes y docentes de la universidad Francisco de Paula Santander Ocaña, suministrar estadísticas, resultados de acciones llevadas a cabo en cursos, capacitar a estudiantes y docentes que lo requieran. Verificar y procurar el funcionamiento óptimo y permanente vía Web de la plataforma Uvirtual y la integridad y almacenamiento periódico de datos acumulados de usuarios y cursos.

Se definen términos técnicos para dar marcos de legitimidad de acuerdo a su contexto y dentro de las funciones que adquiere el súper-administrador de Moodle se tiene:

a. Pleno conocimiento de los requerimientos de adquisición adecuada del hardware sobre el que se soporta la plataforma.

b. Instalación del Sistema Operativo, Gestor de Base de Datos, Servidor Web y otras aplicaciones de software de base requeridos por Moodle o compatibles con esta plataforma y necesarios para la ejecución de formatos OCW, Hot Potatos y demás aplicaciones de entorno académico.

c. Creación y configuración de la Base de Datos, Servidor Web y estructura de seguridad y comunicaciones.

d. Instalación y configuración inicial de Moodle sobre la infraestructura anterior.

e. Activación y configuración avanzada de las extensiones (plugins) opcionales que acompañan a Moodle.

f. Creación de la Estructura de Cursos del sitio.

g. Creación de las políticas de usuario (sistemas de matriculación de alumnos y profesores).

h. Creación de los respaldos de seguridad y almacenamiento confiable.

i. Tareas de mantenimiento y actualización de versiones.

j. La Administración de la plataforma Uvirtual comprende manipulación de datos, usuarios, herramientas y servicios de la plataforma Moodle. Los usuarios, docentes catedráticos o de tiempo completo vinculados a la universidad Francisco de Paula Santander Ocaña con carga académica asignada y estudiantes matriculados en el presente semestre, estudiantes matriculados, asesores y pares académicos de programas. Las cuentas de usuarios: se definen como registros a los que se asocia un nombre de usuario de identificación única, una contraseña para la validación de la identidad, un correo electrónico para crear un contacto con el usuario y los datos personales como nombre, apellido y ciudad de origen.

k. El rol denominado Docente, será concebido como un usuario que al tener un vínculo legal con la institución, accederá a los permisos técnicos que la plataforma por defecto asigna para la manipulación del curso virtual. Los docentes, se comprometen a dar un buen uso de la información, a mantener el curso actualizado y a informar los inconvenientes técnicos que registren al(os) administrador(es) de la plataforma.

l. El rol denominado docente no Editor, es un tipo de usuario con privilegios similares al docente pero con restricciones similares al rol estudiante. La utilización de este rol dentro del curso, será definida por el docente y los permisos se asignarán por el rol administrador.

m. El estudiante, tendrá como acciones asignadas: subir archivos correspondientes a actividades, ingresar a foros, presentar acciones de tipo evaluativo, de acuerdo a los parámetros académicos y pedagógicos que el docente indique en su programa curricular.

n. Bajo ninguna circunstancia se acepta o se permite el intercambio de contraseñas, la asignación de roles de forma fraudulenta o su modificación, sin previo consentimiento

del docente tutor del curso, el administrador de la plataforma y el jefe de la dependencia.

ARTÍCULO 40. *Sanciones.-* Aplica las sanciones establecidas por los Artículos 269F y 269G ley 1273 de 2009.

Capítulo VI
De los derechos de propiedad intelectual

ARTÍCULO 41. *Derechos de propiedad intelectual.-* Todos los sistemas de información desarrollados en las diferentes dependencias tecnológicas de la Universidad Francisco de Paula Santander Ocaña son propiedad de la misma.

Capítulo VII
De las violaciones de seguridad informática

ARTÍCULO 42. *Violaciones de seguridad informática.-* Se disponen las siguientes medidas para evitar violaciones de seguridad informática:

- Está prohibido sustraer información alojada en las diferentes bases de datos para fines ajenos a sus funciones laborales.
- No está permitido realizar prácticas para probar fallas de la Seguridad Informática, a menos que estas pruebas sean controladas y aprobadas por la División de Sistemas.
- Está prohibido realizar prácticas que atenten contra la integridad de la información como propagar, ejecutar o intentar introducir cualquier tipo de código malicioso conocidos como virus, gusanos o caballos de Troya, entre otras prácticas informáticas destinadas a violentar la información.

Capítulo VIII
De los equipos en el área administrativa

ARTÍCULO 43. *Equipos en el área administrativa.-* No está permitido instalar software no autorizado o que no cuente con licencia y es responsabilidad del usuario a quien esté asignado el equipo de escritorio o portátil, la información contenida en el mismo.

ARTÍCULO 44. *Sanciones.-* Aplica las sanciones establecidas en los artículos 269C, 269D y 269G de la ley 1273 de 2009.

Capítulo IX
De la adquisición y actualización de software y hardware

ARTÍCULO 45. *Actualización de Software.-* El software académico instalado en las salas de cómputo será administrado por la División de Sistemas, dicha administración incluye: instalación de aplicaciones, sugerencia de proveedores, renovación de licencias y soporte.

ARTÍCULO 46. *Adquisición de recursos de TI.-* La División de Sistemas se encargará de determinar la conveniencia y viabilidad para la renovación y actualización del software utilizado en la Institución, de acuerdo con la función que cumpla, las necesidades del servicio y las actividades misionales de la Universidad; así mismo será el área asesora para la compra de servidores, estaciones de trabajo, PC, equipos portátiles, monitores

entre otros. Toda compra de estos equipos será canalizada a través del Comité de TI y Comité de Compras de la Universidad.

Parágrafo. El requerimiento de hardware y software se debe realizar a través del portal Web Divisis siguiendo el enlace http://divisis.ufpso.edu.co/registro.html; dicha solicitud será analizada y atendida teniendo en cuenta el plan anual de adquisición tecnológica.

ARTÍCULO 47. ***Mantenimiento y actualización de los SI.-*** Efectuar el mantenimiento y la actualización de los sistemas de información teniendo en cuenta el manual de mantenimiento preventivo de sistemas de información y analizar los requerimientos de los usuarios dados en el portal Web Divisis http://divisis.ufpso.edu.co para garantizar su correcta operación y sincronización.

ARTÍCULO 48. ***Plan de mantenimiento preventivo y correctivo.-*** Dar cumplimiento al plan de mantenimiento preventivo y correctivo de equipos tecnológicos respetando las frecuencias definidas en el mismo.

ARTÍCULO 49. ***Mantenimiento a los equipos de cómputo.-*** La periodicidad que se recomienda para darles mantenimiento a los equipos de cómputo de la UFPS Ocaña es una vez por semestre, esto quiere decir que como mínimo debe realizarse dos veces al año, pero eso dependerá de cada usuario, de la ubicación y del uso, así como de los cuidados adicionales que se les dan a los equipos tecnológicos. El registro de dicho mantenimiento debe realizarse en el Formato Mantenimiento preventivo de equipos de cómputo (F-TT-DSS-031) y la actividad debe ser ejecutada por personal autorizado por la División de Sistemas.

ARTÍCULO 50. ***Mantenimiento a los equipos servidores.-*** Cada tres (3) meses es necesario realizar mantenimiento preventivo a los equipos servidores por parte de personal autorizado por la División de Sistemas, para mantener el funcionamiento de los mismos lo más óptimo posibles y evitar errores o situaciones que puedan mermar el funcionamiento de la red.

ARTÍCULO 51. ***Mantenimiento a la red de voz y datos.-*** La constante actualización de los equipos activos de la red de voz y datos proporciona continuidad, optimización y seguridad. Realizar las actualizaciones de manera adecuada asegura la no pérdida de la configuración necesaria para el funcionamiento de la red. La periodicidad de esta tarea de mantenimiento preventivo a la red de voz y datos es cada seis (6) meses.

ARTÍCULO 52. ***Mantenimiento correctivo.-*** El mantenimiento correctivo de un equipo cliente o servidor se realiza eventualmente o cuando una falla técnica lo requiera para solucionar problemas operativos de software o hardware; cambio o instalación de nuevos componentes de hardware y cuando la presencia de un virus afecta el desempeño de la computadora, entre otros.

Capítulo X
De las copias de respaldo de la información

ARTÍCULO 53. *Custodia de los respaldos de la información*.- La Universidad definirá la custodia de los respaldos de la información que se realizará externamente con una compañía especializada en este tema. La responsabilidad operativa en el cumplimiento de esta labor está a cargo de la División de Sistemas, quienes procesarán y vigilarán las copias de seguridad y respaldo de la información de cada aplicación Web.

ARTÍCULO 54. ***Almacenamiento de las copias de seguridad.-*** El almacenamiento de copias de seguridad de la información se realizará interna y externamente a la Universidad y las personas responsables de este procedimiento serán definidas por el jefe de la dependencia (División de Sistemas), quien conocerá los estados finales de dichos respaldos y su ubicación definitiva.

ARTÍCULO 55. ***Responsabilidad del funcionario.-*** Cada funcionario es responsable directo de la generación de los backups o copias de respaldo de la información a su cargo. También puede solicitar a la División de Sistemas el servicio de backup mediante asignación de un espacio dentro de los servidores y ser manejado como una unidad dentro del disco de su equipo al cual debe acceder a través de usuario y contraseña.

Capítulo XI
De la realización de backup, replicación y copy backup de máquinas virtuales

ARTÍCULO 56. ***Backups de las máquinas virtuales.-*** La División de Sistemas realiza mediante el software licenciado Veeam Backup & Replication, Backups de las máquinas virtuales, realizando 1 full Backup file y 13 incremental Backup file de la máquina virtual (un Backup completo de la máquina y luego 13 copias incrementales, sólo de los cambios que se realizan desde el full Backup), al llegar al día 15 se borra el Backup más antiguo.

ARTÍCULO 57. ***Replicación de las máquinas virtuales.-*** Se realiza la replicación física de la máquina que se aloja en el UCS Prod (sistema de cómputo unificado) de la división de sistemas, del último Backup realizado en la tarea de Backup y se envía en el UCS DR (actualmente en Divisis y luego en Bellas Artes). Dicha máquina queda apagada para ser activada en caso de que falle la máquina en producción.

ARTÍCULO 58. ***Copias de respaldo.-*** Cada domingo del mes, se realiza una (1) copia de respaldo de cada una de las máquinas, y cada mes se realiza una (1) copia de respaldo de cada una de las máquinas.

Capítulo XII
De los dispositivos móviles

ARTÍCULO 59. ***Propiedad de los dispositivos móviles.-*** Los dispositivos móviles (tablets, portátiles, etc.) asignados por la UFPS Ocaña a administrativos, contratistas y/o docentes, son de propiedad de la Institución y los responsables de dichos equipos deberán velar por su uso adecuado.

ARTÍCULO 60. ***Responsabilidad sobre los dispositivos móviles.-*** El funcionario a cargo del dispositivo móvil que le fue asignado, como responsable del mismo, asumirá los riesgos y costos asociados a la pérdida, fuga o uso indebido de la información que se encontrare en los dispositivos en caso de extravío.

ARTÍCULO 61. ***Uso de conexión inalámbrica.-*** El responsable del dispositivo móvil, en caso de necesitar conexión del dispositivo a la red inalámbrica de la UFPS Ocaña de acceso restringido, deberá tramitar dicho requerimiento al proceso SITT a través del portal web Divisis.

ARTÍCULO 62. ***Uso de dispositivos móviles por personal externo.-*** Para el caso en que se presentare préstamo de algún dispositivo móvil a personal externo a la institución como contratistas para el ejercicio de sus funciones o servicios, se aplicarán las mismas condiciones de uso, así mismo deberá permanecer acompañado por el responsable de

dicho activo, con el fin de evitar el uso indebido de la información contenida en los mismos.

ARTÍCULO 63. ***Seguridad.-*** Los dispositivos móviles institucionales, y los personales que hagan uso de los servicios dispuestos por la Universidad, deberán contar con un sistema de antivirus, a modo de evitar posibles ataques a la red Institucional por la cual navegan; el proceso SITT debe garantizar la correcta instalación de software de antivirus en los dispositivos móviles institucionales. Del mismo modo los responsables de los dispositivos móviles deben evitar conectarlos por puerto USB a cualquier computador público que no sea de propiedad de la Universidad.

ARTÍCULO 64. ***Uso de dispositivos móviles fuera de la institución.-*** Para evitar pérdida o robo de los dispositivos móviles, los usuarios deben evitar usarlos en lugares que no ofrezcan las garantías de seguridad física mínimas. Asimismo deben evitar hacer uso de redes inalámbricas de uso público externas a la Institución.

ARTÍCULO 65. ***Uso de la información.-*** A fin de evitar manipulación inadecuada de la información contenida en los dispositivos móviles en caso de presentarse pérdida o robo del mismo, los usuarios no deben almacenar videos, fotografías o información personal en ellos.

Capítulo XIII
De la seguridad del archivo físico

ARTÍCULO 66. Período de almacenamiento.- El periodo de Almacenamiento de la información física de la UFPS Ocaña, está contemplada en la Tabla de Retención Documental (TRD) y debidamente aprobado por el Comité Interno de Archivo.

ARTÍCULO 67. Destrucción de archivos físicos.- El Comité Interno de Archivo debe utilizar los medios óptimos y necesarios para eliminar la documentación física, siempre y cuando ésta haya cumplido su período establecido en la Tabla de Retención Documental (TRD).

ARTÍCULO 68. ***Uso de impresoras, escáner, fotocopiadoras, fax.-*** Los usuarios que hagan uso de herramientas como impresoras, escáneres, fotocopiadoras y fax, deben asegurarse de recoger los documentos confidenciales inmediatamente después de su uso, impidiendo así la divulgación no autorizada de dicha información.

Capítulo XIV
De la seguridad de la información Cloud Computing y carpeta de red

ARTÍCULO 69. ***Almacenamiento OwnCloud.-*** La UFPS Ocaña suministra un servicio de almacenamiento de la información en un servidor de archivos (OwnCloud) mediante el cual los usuarios pueden guardar información importante, es de aclarar que el usuario final deberá copiar la información necesaria en la carpeta destinada para este fin la cual tiene un acceso directo en el escritorio del PC. El proceso SITT debe garantizar la disponibilidad de dicha información en caso de presentarse daño en el equipo asignado; los funcionarios de la UFPS Ocaña que requieran hacer uso de este servicio de almacenamiento en la nube, deben solicitarlo a través del portal web Divisis; se recomienda evitar el almacenamiento de información Institucional en aplicaciones ajenas a esta.

ARTÍCULO 70. *Copias de seguridad.-* Es responsabilidad del proceso SITT, mantener copias de respaldo de la información almacenada en las unidades de red.

ARTÍCULO 71. *Divulgación de la información.-* Es responsabilidad del usuario mantener la confidencialidad de la información a su cargo, por lo tanto debe tener sumo cuidado en el momento de divulgar la información en la nube con otros usuarios. Asimismo se prohíbe extraer, divulgar o publicar información institucional de cualquiera de las unidades de red o estaciones de trabajo, sin expresa autorización de su jefe inmediato.

ARTÍCULO 72. *Tipo de información a almacenar.-* Las unidades de red están destinadas para almacenamiento de información institucional, por lo que se prohíbe almacenar archivos con contenido que atente contra la moral y las buenas costumbres de la entidad o las personas, como pornografía, entre otros, o cualquier software ilegal o malicioso, ya sea en medios de almacenamiento de estaciones de trabajo, computadores de escritorio o portátiles, tablets, celulares inteligentes, etc. de propiedad de la institución, o en las unidades de red.

Capítulo XV
Del acceso remoto

ARTÍCULO 73. Acceso remoto.- El acceso remoto a servicios de red ofrecidos por la Universidad debe estar sujeto a medidas de control definidas por el proceso SITT.

Capítulo XVI
Del uso de periféricos y medios de almacenamiento

ARTÍCULO 74- *Uso de dispositivos de almacenamiento externo.-* El uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD, memorias USB, agendas electrónicas, celulares, etc.) pueden ocasionalmente generar riesgos para la institución al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada. Es responsabilidad de cada usuario garantizar la disponibilidad, confidencialidad e integridad de la información a su cargo. Se aplicarán las sanciones respectivas estipuladas en la presente política en caso de atentar contra la confidencialidad de la información de la que es responsable.

ARTÍCULO 75. *Almacenamiento de la información.-* Los usuarios son los responsables de la información que administran en los medios de almacenamiento de uso personal, por lo que debe abstenerse de almacenar en ellos información institucional de carácter confidencial.

Capítulo XVII
De la Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

ARTÍCULO 76. Confiabilidad en la a*dquisición y/o desarrollo de software.-* La UFPS Ocaña asegurará que el software desarrollado al interior de la misma, y el adquirido con terceras partes, necesarios para la operatividad de la misma, cumplirán con los requisitos de seguridad y calidad establecidos por el proceso SITT.

ARTÍCULO 77. *Desarrollo de software.-* El proceso SITT y el Departamento de Sistemas debe establecer metodologías de desarrollo de software basadas en la implementación de buenas prácticas y lineamientos de desarrollo seguro de software. Asimismo deberá garantizar la aplicabilidad de dichas metodologías por parte de los funcionarios a su cargo destinados para tal fin.

ARTÍCULO 78. Documentación del software.- Los funcionarios encargados del desarrollo de software, deben documentar dicho proceso en los formatos dispuestos para tal fin.

ARTÍCULO 79. *Soporte a nivel de software.-* Tras la puesta en marcha del software desarrollado, se debe proporcionar soporte técnico por parte del personal dispuesto para tal fin, respetando los tiempos de respuesta establecidos por el proceso responsable del software.

Capítulo XVIII
De la Continuidad, Contingencia y Recuperación de la Información

ARTÍCULO 80. Plan de contingencia.- El proceso SITT debe elaborar un plan de contingencia, que permita la pronta recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados por la Institución en caso de una eventualidad de desastre y/o incidente.

Capítulo XIX
De la Política de Privacidad y Protección de Datos Personales

ARTÍCULO 81. *Protección de datos personales.-* Como cumplimiento a la Ley 1581 de 2012 de la protección de datos personales, la UFPS Ocaña a través del proceso SITT, dispondrá de un manual de políticas de tratamiento de datos personales de los titulares de la UFPS Ocaña.

ARTÍCULO 82. *Socialización de las políticas.-* La UFPS Ocaña garantizará la actualización y divulgación de las políticas de tratamiento de datos personales a toda la comunidad universitaria.

ARTÍCULO 83. *Autorización.-* El manual de políticas de datos personales de los titulares de la UFPS Ocaña deberá enunciar los mecanismos mediante el cual se obtendrá la autorización por parte de la comunidad universitaria para el tratamiento de sus datos.

ARTÍCULO 84. *Seguridad de los datos.-* El proceso SITT debe implementar controles necesarios para salvaguardar la información personal de los titulares de la UFPS Ocaña, que se encuentra almacenada en las bases de datos o cualquier otro repositorio institucional, evitando su divulgación, alteración o eliminación sin la respectiva autorización del responsable del dato.

ARTÍCULO 85. *Confidencialidad.-* Los funcionarios que como ejercicio de sus funciones, hagan uso o manejo de información de la Institución o de sus estudiantes, administrativos, docentes, proveedores, entre otros, deben guardar total discreción o reserva absoluta de la misma, cumpliendo de esta manera con la política de confidencialidad contenida en el presente documento.

ARTÍCULO 86. ***Entrega de información.-*** Los funcionarios de la UFPS Ocaña, deben verificar la identidad de todas aquellas personas, que soliciten información por los diferentes medios de comunicación (teléfono, fax, correo electrónico, entre otros), con el objetivo de suministrar información personal solamente al titular de la información.

ARTÍCULO 87. Esta Resolución rige a partir de la fecha y deroga la Resolución No.0118 del 22 de abril de 2015

COMUNÍQUESE Y CÚMPLASE

EDGAR ANTONIO SANCHEZ ORTIZ
Director

DIRECTOR SECCIONAL OCAÑA

Revisó: BLANCA MERY VELASCO BURGOS
Secretaria General

Proyectó: ANTÓN GARCÍA BARRETO
Coordinador División de Sistemas

Transcriptor: Norma Noguera Amaya