## 1. OBJETIVO

La presente política tiene como objetivo minimizar las amenazas y riesgos continuos a los que está expuesta la información de la UPC, con el propósito de asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de inversiones y las oportunidades.

Así también establece los lineamientos para asegurar:

i. La integridad (información sin modificaciones inapropiadas).
ii. La confidencialidad (información protegida de personas no autorizadas).
iii. La disponibilidad (que usuarios autorizados pueden acceder a aplicaciones y sistemas cuando lo requieran para desempeñar sus funciones).

## 2. ALCANCE

La política de Seguridad de la Información aplica a todo colaborador y proveedor que tenga acceso a información de la UPC. La información de la UPC se refiere a la propia, más la que corresponde a las empresas relacionadas y a Laureate International Universities.

## 3. CLASIFICACION DE DATOS.

Los datos se deben de conservar de una forma segura, precisa y confiable y deben de estar rápidamente disponibles para su uso autorizado. De acuerdo con la Política Global de Clasificación de Datos de Laureate, los datos se deben de clasificar en una de las siguientes categorías:

i. Restringidos: datos que están reglamentados legalmente y datos que brindaría acceso a información confidencial o restringida.
ii. Confidenciales: datos que las direcciones de la organización han decidido no publicar o hacer públicos, y datos protegidos por obligaciones contractuales.
iii. Públicos: datos sobre los cuales no se esperan privacidad o confidencialidad.

Los datos confidenciales y los datos restringidos requerirán diversas medidas de seguridad que serán apropiados en función del grado según el cual la pérdida o la corrupción de los datos dañarían el negocio o las funciones de investigación de la organización, produciría una pérdida financiera, o infringiría leyes, políticas o contratos de la organización.

## 4. TRATAMIENTO DE LA INFORMACIÓN

**a) Confidencialidad**. - Las personas que se rigen por la presente política mantendrán absoluta reserva y confidencialidad sobre la información relacionada con las actividades y el funcionamiento de la UPC o de las empresas relacionadas con ella, incluyendo cualquier información sobre los sistemas informáticos. Para cumplir con este objetivo, todas las personas comprendidas bajo esta política deberán adoptar las precauciones necesarias para proteger la seguridad de la información de la UPC o de sus alumnos, lo que comprende:

i. No revelar, reproducir, resumir o suministrar, bajo ninguna modalidad, información de la UPC, excepto para fines propios de la Universidad o de sus alumnos. En los casos que corresponda, deberán contar con la debida autorización de su Director de área. Esta prohibición incluye a los materiales que la UPC entregue al trabajador o a terceros como parte de la documentación necesaria para cumplir sus funciones en el puesto.

ii. Notificar a su jefe inmediato sobre cualquier mal uso de la información de la organización, así como de la difusión no autorizada de información reservada. En caso que el problema se originara en nuestros sistemas de información se deberá de notificar también a la DI2D a través del área designada para tal fin.

**b) Ingreso de datos.-** Sólo será realizado por el personal autorizado. Esta autorización la designa el dueño de cada proceso de la organización.

**c) Mantenimiento de datos. -** La modificación de datos se realizará por las personas autorizadas previamente por el dueño del proceso.

**d) Eliminación de información impresa. -** Toda información restringida y confidencial impresa que desee ser eliminada, debe de ser destruida en su totalidad. Para ello las áreas que así lo requieran deberán contar con trituradores de papel o asegurarse que el documento no sea legible después de ser eliminado**.**

**e) Respaldo de información:**

i. Con relación a la información contenida en los equipos de cómputo asignados al personal, cada Dirección tiene la responsabilidad de definir la información crítica

que se encuentra alojada en su disco duro, por ende, debe de asegurar su disponibilidad en cualquier momento ya que es propiedad de la UPC.

ii. La información contenida en los servidores que están bajo la administración de la DI2D serán respaldados de acuerdo con el procedimiento establecido para tal fin (**"Respaldo y Restauración de Servidores"**). Los respaldos de la información se realizarán de acuerdo con las definiciones hechas en la etapa de diseño de los sistemas, tanto para un nuevo desarrollo como para la modificación de un sistema existente.

## 5. CONTRATACIÓN DE PROVEEDORES

Los proveedores contratados por la UPC deberán mantener la debida confidencialidad sobre la información recibida de la Universidad. Esta obligación incluye a los empleados, empresas y cualquier otro que dicho tercero subcontrate para atender los servicios que proporcionará a la UPC. Esto debe quedar claramente establecido en los contratos respectivos.

El Área o Dirección de la UPC que requiera la contratación de proveedores deberá prever que tengan la capacidad de mantener la confidencialidad de la información de la UPC y su procesamiento, cuando corresponda; así como ofrecer los niveles adecuados de disponibilidad, integridad y trazabilidad, cuyos alcances deberán figurar en el contrato materia del servicio prestado. Adicionalmente, dentro de los contratos, se establecerá la obligación del tercero de informar a la UPC, en forma inmediata, sobre cualquier incidente que ponga en riesgo la seguridad de la información.

## 6. CONTROL DE ACCESO A LA INFORMACIÓN Y A LOS SISTEMAS

Las reglas y mecanismos que se implementen para controlar el acceso a la información y el acceso físico a las instalaciones deben considerar lo siguiente:

a) Los accesos serán establecidos considerando las necesidades funcionales de cada colaborador.

b) Las solicitudes de creación de cuentas, por ingreso o traslado de personal, deberán ser solicitadas por la Dirección de Recursos Humanos a la DI2D, a través del área designada para tal fin bajo las normas establecidas.

c) Las cuentas (accesos) de usuario son de uso personal. Está estrictamente prohibido, bajo responsabilidad del titular, compartir la cuenta de usuario con otra persona.

d) Los accesos a los sistemas de información serán revocados al usuario que deje de trabajar en la UPC desde el momento en que se produzca el cese. Para ello, la Dirección de RRHH. debe informarlo oportunamente al área encargada de la administración de usuarios del sistema.

e) Se deberá efectuar la revisión periódica de los derechos de acceso a la información, para verificar su vigencia.

f) El usuario es responsable de aplicar los mecanismos adicionales de control de acceso a sus equipos de cómputo a los ya establecidos que considere necesarios, con el fin de minimizar el riesgo de sustracción de información de su propiedad. Para ello deberá consultar con la DI2D.

g) El usuario no deberá acceder sin autorización a información restringida o confidencial de la UPC, ni a las bases de datos de personal administrativo de la organización.

h) Está prohibida la copia de información restringida o confidencial a dispositivos personales de los usuarios. De detectarse el caso, el personal que infrinja estará sujeto a amonestación y sanción administrativa.

i) Contraseñas:
   i. Las contraseñas son de carácter privado y personal. El usuario propietario asume la responsabilidad de las acciones ejecutadas con dicha contraseña de acceso.
   ii. La contraseña deberá ser cambiada de manera periódica por el usuario y dentro de un mismo periodo, las veces que éste lo requiera. Asimismo, el usuario debe cumplir con la periodicidad de cambio de contraseña establecida por la DI2D.
   iii. Las contraseñas tendrán características que garanticen su confidencialidad, caducidad periódica, tamaño mínimo, etc., de acuerdo con las facilidades de la plataforma tecnológica. Ningún usuario tendrá la potestad de solicitar la excepción a este punto.
   iv. Las contraseñas de las cuentas de administración de los servidores y administradores de sistemas deberán ser cambiadas de manera periódica de acuerdo con un cronograma establecido o cuando la situación lo amerite.

v. Los detalles de la administración de contraseñas están definidos el procedimiento "**Administración de Ingresos, Promoción, Traslado y Ceses de Cuentas Administrativas**".

j) Acceso Físico

i. Cada Dirección de la UPC podrá establecer restricciones de acceso físico a los ambientes que considere necesario, estableciendo las normas de control correspondientes.

ii. El acceso físico al Centro de Datos (datacenter) está restringido al personal autorizado. El área de TI dispondrá las medidas necesarias para ello.

iii. El jefe de cada área deberá recuperar las llaves o medios de acceso físico otorgados a su personal y que deje de laborar en su área.

## 7. SERVICIOS

### a) Internet

i. El acceso al servicio de Internet rige bajo las disposiciones de la política **Uso del Servicio de Internet Administrativo UPC**.

ii. La DI2D restringirá el acceso a determinadas páginas o sites que se consideren indebidas por su contenido o función, o porque presenten riesgos de seguridad.

iii. Las áreas que requieran establecer restricciones de acceso a Internet, deberán coordinar el bloqueo con la DI2D canalizando la solicitud a través de IT Service.

### b) Sobre redes sociales no institucionales

i. Toda alta o registro en una red social no institucional, deberá ser solo y exclusivo a través de la dirección de correo electrónico personal. En cuanto a nuestras publicaciones, éstas deben estar alineadas a los lineamientos del Código de Conducta y Ética de Laureate, que textualmente indica: "***Solo aquellas personas autorizadas específicamente por Laureate pueden publicar contenido en calidad de representantes de Laureate, y siempre deben identificar su relación con Laureate. Siempre que publiquemos algo, debemos ser honestos, veraces y respetuosos. Si no estamos publicando en nombre de Laureate, debemos aclarar que estamos***

***publicando a título personal y que las opiniones expresadas son nuestras.****"*

ii. Es responsabilidad de los colaboradores de la organización el uso de imágenes, vídeos e información a los cuales hagan referencia en sus publicaciones. La cual deberá estar alineado al Código de Conducta y Ética de Laureate, el cual indica textualmente lo siguiente: "***No podemos publicar información confidencial de Laureate ni información confidencial de nuestros alumnos o socios comerciales. De forma similar, no podemos usar logotipos, marcas registradas, información sujeta a derechos de autor ni otra propiedad intelectual de Laureate sin autorización específica. Asimismo, en ningún caso podemos publicar información identificable de nuestros alumnos en sitios públicos****."*

**c) Uso de Carpetas y Archivos Compartidos**

i. Cada usuario administrativo y académico cuenta con una carpeta de uso personal en la red.

ii. Los usuarios que requieran compartir información (carpetas y archivos) deberán obtener la autorización de su Director correspondiente, quien solicitará dicho servicio a la DI2D a través del área designada para tal fin, indicando la finalidad de la información a compartir y los usuarios que tendrán acceso a ésta, precisando los tipos de permiso para cada uno.

iii. Por ninguna razón una carpeta o archivo deberá ser compartido de manera genérica. Sólo deberá estar compartido para aquellos usuarios que lo necesitan para el ejercicio de sus labores.

iv. En cuanto a los servicios de almacenamiento en la nube ("Cloud") y transferencia de datos, el colaborador debe usar los medios oficiales establecidos por la Institución (carpetas compartidas, OneDrive Institucional y Sharepoint) para el tratamiento de información clasificada como restringida o confidencial (ver sección 3: "Clasificación de datos") los cuales cuentan con los controles de seguridad mínimos. Está estrictamente prohibido el uso de servicios públicos de almacenamiento en la nube tanto para almacenamiento como para transferencia de información restringida o confidencial. Solo información clasificada como "Pública" puede estar sujeta al uso de este tipo de servicios de almacenamiento o transferencia.

De identificarse algún caso de información restringida o confidencial almacenada o compartida sin seguir estos lineamientos, se estará atentando contra la Seguridad de la Información, por lo que el colaborador involucrado estará sujeto a una sanción o amonestación administrativa acorde a la gravedad de la falta.

v. Está prohibido el uso de información restringida o confidencial en equipos de cómputo o dispositivos móviles personales (no asignados por la Institución). De identificarse algún caso de información de este tipo almacenada o compartida sin seguir estos lineamientos, se estará atentando contra la Seguridad de la Información, por lo que el colaborador involucrado estará sujeto a una sanción o amonestación administrativa acorde a la gravedad de la falta.

vi. Es responsabilidad del usuario el almacenamiento de información restringida o confidencial en los medios oficiales brindados por la Institución: OneDrive y SharePoint institucional, no en los discos duros de los equipos de cómputo asignados. De identificarse algún caso de este tipo el colaborador involucrado estará sujeto a una sanción o amonestación administrativa acorde a la gravedad de la falta.

**d) Correo Electrónico**

i. El servicio se debe utilizar sólo para fines laborales.

ii. El usuario de una cuenta es responsable de los correos que sean enviados a través de su cuenta.

iii. La DI2D implementará mecanismos orientados a minimizar el riesgo de daños por virus informático u otros que puedan ingresar a la red interna a través del correo electrónico.

iv. Dado que los mensajes de correo electrónico al exterior se transmiten por redes públicas, no se puede garantizar la confidencialidad de las mismas. En los casos puntuales que así lo ameriten, se utilizarán herramientas de autenticación o encriptación definidas e instaladas por la DI2D.

v. Periódicamente, la DI2D ejecutará procesos de depuración de los mensajes que tengan la antigüedad establecida oportunamente.

vi. Toda comunicación comercial que emita la UPC mediante correo electrónico debe ser canalizada de manera centralizada a través del área designada para tal fin.

vii. UPC no se hace responsable por la pérdida de información del archivo pst contenido en el equipo asignado al colaborador, la bandeja de entrada o carpetas de almacenamiento de mensajes creados por el usuario. Es responsabilidad del usuario la depuración y almacenamiento de los archivos anexos en las carpetas correspondientes.

**e) Transferencia de Archivos bajo modalidad FTP**

i. Será debidamente autorizado por la DI2D a los usuarios que lo necesiten y mediante requerimiento y sustento formal de su Dirección.

ii. No se brindará este servicio de manera masiva.

**f) Red Inalámbrica**

i. Todo personal administrativo de la UPC puede tener acceso a la red inalámbrica de la UPC en las zonas habilitadas para dicho servicio.

ii. El acceso a la red inalámbrica tiene restricciones de seguridad que han sido diseñadas para asegurar la integridad de nuestra red.

**g) Desarrollo, Adquisición, Implementación y Mantenimiento de Sistemas**

i. Solicitudes de desarrollo de Sistemas de Información: Todos los pedidos de desarrollo y mantenimiento de sistemas deben ser solicitados mediante el procedimiento "**Desarrollo de Software Nuevas Soluciones"**, la cual se encuentra publicada en la carpeta pública de normas de la UPC. Dichos pedidos deben precisar los requerimientos operacionales, de gestión, control, trazabilidad y seguridad, acorde con las normas de la UPC y las necesidades identificadas por quien realiza la solicitud.

ii. Seguridad de Aplicaciones: El diseño de las aplicaciones contemplará estándares que incluyan controles relacionados con la exactitud de los datos ingresados en los sistemas, así como de su procesamiento.

iii. Alertas en Aplicaciones: Los problemas que ocurran durante la ejecución de las aplicaciones, generan notificaciones y serán reportadas por quien los

detecta a la DI2D a través del área designada para tal fin, la cual registrará la solicitud y escalará el problema, si es necesario, a las áreas involucradas en la solución.

iv. Contratos de Programación de Aplicaciones con Proveedores: Todas las contrataciones de aplicaciones con terceros, deberán ajustarse al procedimiento **"Atención de Solicitudes de Nuevas Soluciones"** son de uso exclusivo de la DI2D, las cuales serán usadas para todo proyecto desarrollado en UPC.

**h) Certificación de los sistemas:**

i. La certificación de los sistemas se realizará de acuerdo con el procedimiento **"Calidad de Soluciones de TI"**, y se llevará a cabo en un ambiente de prueba representativo del ambiente de producción, según se requiera en cada caso específico.

a. Esta certificación debe ser realizada por un grupo independiente del área de Calidad de TI.

b. La certificación o aseguramiento de calidad de los sistemas de información nuevos o modificados será aprobada de manera formal por el usuario solicitante.

**i) Administración de cambios:**

i. La DI2D dispondrá de una administración de cambios y entrega de los sistemas, con una separación adecuada de los ambientes de desarrollo, de certificación y de producción; minimizando con ello el riesgo de alteraciones no autorizadas y errores. Asimismo, se mantendrá una bitácora de los cambios ejecutados en el ambiente de producción.

## 8. SOPORTE Y OPERACIÓN DE SISTEMAS

**a) Red de Datos:**

i. El acceso de entidades externas debe contar con la autorización correspondiente de la DI2D y deberá estar asegurado, de modo que no existan brechas que posibiliten el acceso no autorizado a información sensible de la organización.

ii. Toda entidad externa que se conecte a la red de la UPC deberá, como prerrequisito, tener sus sistemas y redes asegurados de acuerdo con lo establecido en nuestra política interna. Adicionalmente, la UPC se reserva el derecho de auditar dichas medidas de seguridad.

iii. Ningún usuario está autorizado a manipular el cableado de datos o eléctrico, a excepción del personal de la DI2D y del personal de la Gerencia de TI; en este último caso, con conocimiento previo de la primera.

iv. Las instalaciones de nuevos equipos de comunicación de red (switches de borde o distribución) deberán ser realizadas de manera coordinada con la unidad correspondiente de la DI2D.

## 9. EQUIPAMIENTO

### a) Hardware

i. Todo equipo propiedad de la UPC deberá estar ubicado en instalaciones con condiciones ambientales apropiadas que cumplan con las recomendaciones del fabricante.

ii. Se proporcionará el mantenimiento (preventivo/correctivo) necesario y por personal calificado, debiendo coordinarse adecuadamente para minimizar las interrupciones de los servicios de tecnología de la información.

iii. La DI2D, a través de la unidad que designe, mantendrá un inventario formal actualizado de todos los equipos de cómputo, que permita detectar cualquier pérdida o robo, así como clasificarlos de acuerdo con su uso crítico y efectuar la distribución de los equipos de acuerdo con las necesidades. También contribuirá a evitar cambios o instalaciones no autorizados, así como establecer necesidades y planear compras.

iv. La designación de equipos de cómputo hacia los colaboradores estará dada en base a la política administrada por RRHH y que se rige por el perfil del puesto a implementar.

v. Sobre los dispositivos móviles entregados por la UPC, los colaboradores no tienen permitido instalar aplicaciones no autorizadas por la DI2D, así mismo no deberán cambiar las configuraciones en los mismos, en resguardo de la integridad de los dispositivos y la información contenida en ellos.

vi. Los usuarios de los dispositivos móviles son responsables del manejo de los datos restringidos y confidenciales que se almacenen en ellos.

vii. Los equipos de cómputo serán calificados como obsoletos sólo por el área de Soporte Técnico. Estos equipos serán dados de baja y enviados al área de Almacén de la UPC.

viii. La pérdida de todo equipo de propiedad de la UPC deberá de ser informado de manera inmediata.

b) **Software**.-

Sobre la instalación de software en los computadores individuales.

i. No está permitida la instalación de software no autorizado por la UPC en los equipos asignados al usuario, ya que pone en riesgo el correcto funcionamiento de los equipos y sistemas informáticos de la organización, el estricto cumplimiento de la legalidad del licenciamiento del software utilizado, así como la seguridad de la información de la Universidad. La DI2D realizará periódicamente una revisión del software existente en los equipos y tiene la potestad de proceder a la desinstalación respectiva, así como a comunicarlo al Jefe del área.

ii. En caso sea necesario efectuar alguna instalación de software requerido para su trabajo, deberá hacerse una solicitud formal a la DI2D a través del área designada para tal fin con la sustentación del caso.

iii. La DI2D previene ataques por parte de virus informáticos o código malicioso a través del software antivirus instalado en cada equipo. El usuario debe comprometerse a mantener este software de protección siempre operativo.

iv. El usuario se compromete a vigilar que no se emplee la computadora asignada en actividades de piratería de software propiedad de terceros o propiedad de la UPC. Tampoco en actividades de intrusión sobre servidores o computadoras internas o externas a la UPC, o en otras actividades que sean consideradas ilícitas o que atenten contra la ética o las buenas costumbres.

v. El usuario se responsabiliza por los problemas, que probadamente, pueda ocasionar a terceros o a la misma UPC, el hardware o el software instalado

o residente en la computadora asignada a éste, sin la autorización de la DI2D.

## 10. CUMPLIMIENTO Y EXCEPCIONES:

i. Se debe de verificar en forma periódica el cumplimiento de las políticas de seguridad a través de auditorías y evaluaciones.

ii. El cumplimiento por parte de terceros debe ser evaluado por los gerentes responsables de la relación con dicho tercero.

iii. La DI2D debe de evaluar y autorizar todas las excepciones a esta política.

| **Aprobado por:** | **Fecha:** |
|---|---|
| **Clery Neyra Vera**<br>**Director de Inteligencia e Innovación Digital** | 28/09/2017 |

# ACTA DE CONOCIMIENTO Y ACEPTACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Declaro que he leído la "Política de Seguridad de la Información" y acuerdo cumplir con todos los aspectos de los términos y disposiciones de la misma. También reconozco que esta política puede ser modificada o complementada ocasionalmente, y acuerdo cumplir también con todas sus modificaciones y adiciones.

…….. ……

**Nombre y Apellido del colaborador** **Firma**

**Fecha: …….**