

	DIRECTIVA DE SEGURIDAD INFORMÁTICA	Código	SIS-OT-03
		Versión	1.1
		Documento de Aprobación	Resolución de Consejo Universitario N° 226-2019-CU-UPSJB
		Fecha de Aprobación	24/07/2019
	DIRECTIVA	N° Página	1 de 13



UNIVERSIDAD PRIVADA SAN JUAN BAUTISTA

Preparando el camino....


DIRECTIVA DE SEGURIDAD INFORMÁTICA

Elaborado por:

CRISTIAN SALDAÑA GOLDSCHMIDT
FRED PAOLO MOYA ESPINOZA
RUBÉN RAYME SERRANO
WALTER RIVERA VALERIO


Aprobado por:

CONSEJO UNIVERSITARIO

	DIRECTIVA DE SEGURIDAD INFORMÁTICA	Código	SIS-OT-03
		Versión	1.1
		Documento de Aprobación	Resolución de Consejo Universitario N° 226-2019-CU-UPSJB
		Fecha de Aprobación	24/07/2019
	DIRECTIVA	N° Página	2 de 13

ÍNDICE

1. OBJETIVO	3
2. ALCANCE	3
3. BASE LEGAL	3
4. RESPONSABILIDADES	3
4.1 DIRECCIÓN DE SISTEMAS DE INFORMACIÓN:	3
4.2 DEPARTAMENTO DE REDES Y COMUNICACIONES	3
4.3 DEPARTAMENTO DE SOPORTE TÉCNICO:	3
5. DISPOSICIONES	4
5.1 USO DE LOS RECURSOS INFORMÁTICOS	4
5.2 DE LAS ESTACIONES DE TRABAJO.....	4
5.3 USO DE SOFTWARE.....	5
5.4 DEL CONTROL DE ACCESOS.....	6
5.5 DE LAS CONTRASEÑAS Y SEGURIDAD	7
5.6 DE LOS CENTROS DE DATOS	8
5.7 DE LOS EQUIPOS DE COMUNICACIÓN	9
5.8 PROTECCIÓN CONTRA ATAQUES INFORMÁTICOS, VIRUS Y MALWARE.....	9
6. VIGENCIA	10
7. APROBACIÓN	10
8. DEFINICIÓN DE TÉRMINOS	11
9. CONTROL DE CAMBIOS	13

	DIRECTIVA DE SEGURIDAD INFORMÁTICA	Código	SIS-OT-03
		Versión	1.1
		Documento de Aprobación	Resolución de Consejo Universitario N° 226-2019-CU-UPSJB
		Fecha de Aprobación	24/07/2019
	DIRECTIVA	N° Página	3 de 13

1. OBJETIVO

El presente documento establece los lineamientos buscando contar con niveles de protección y control de acceso a los recursos informáticos dentro de la Universidad Privada San Juan Bautista (UPSJB).

2. ALCANCE

La presente Directiva es obligatorio cumplimiento y aplicación por parte de toda la comunidad universitaria de la UPSJB.

3. BASE LEGAL

Estatuto de la Universidad
 Norma Técnica Peruana – ISO /IEC 27001: 2014
 Ley N° 29733, Ley de Protección de Datos Personales
 Decreto Legislativo No. 822, Protección Jurídica del Software.

4. RESPONSABILIDADES

4.1 DIRECTOR DE SISTEMAS DE INFORMACIÓN:

Es responsable de velar por el cumplimiento del presente documento con la colaboración de sus representantes en todas las filiales y demás locales, así como de los Coordinadores de Sistemas de Información y el usuario final.

4.2 JEFE DEL DEPARTAMENTO DE REDES Y COMUNICACIONES:

Es responsable de:

- a) La administración de la seguridad informática, así como las acciones que sean necesarias para asegurar la confiabilidad del mismo, en función a los recursos y capacidades disponibles.
- b) La implementación y administración de la plataforma de antivirus, así como de su monitoreo y actualización.
- c) Administrar los Centros de Datos (DATA CENTER) y velar por su integridad física.

4.3 JEFE DEL DEPARTAMENTO DE SOPORTE TÉCNICO:

Es responsable de mantener un registro actualizado de todas las computadoras de la universidad con sus características (configuración de sistema y de red, software instalado, Etc.), es responsable también de mantener las PCs con versiones actualizadas de sistema operativo y antivirus, también es responsable de gestionar la asignación de PCs a los usuarios finales.

4.4 REPRESENTANTE DE LA DIRECCIÓN DE SISTEMAS DE INFORMACIÓN:

Es responsable de velar por la integridad física de los equipos de cómputo asignados en su filial o local.

	DIRECTIVA DE SEGURIDAD INFORMÁTICA	Código	SIS-OT-03
		Versión	1.1
		Documento de Aprobación	Resolución de Consejo Universitario N° 226-2019-CU-UPSJB
		Fecha de Aprobación	24/07/2019
	DIRECTIVA	N° Página	4 de 13

4.5 USUARIO FINAL:

Es responsable de:

- a) Cumplir con las disposiciones señaladas en el presente documento. En caso de incumplimiento por parte de trabajadores de la Universidad, será considerado una falta, y como tal se aplicarán las acciones disciplinarias del caso, conforme lo señalado en el Reglamento Interno de Trabajo. En el caso de estudiantes, se aplicará lo dispuesto en el Reglamento de Disciplina del Estudiantes.
- b) Reportar a Soporte Técnico en Chorrillos y al representante de la Dirección de Sistemas de información en los demás locales cualquier anomalía física y/o lógica en los sistemas y/o equipos informáticos a su cargo, debiendo otorgar las facilidades necesarias, en caso amerite, para que el personal especializado efectúe las acciones correctivas que permitan solucionar los incidentes reportados.

5. DISPOSICIONES


5.1 USO DE LOS RECURSOS INFORMÁTICOS

Los recursos informáticos de la UPSJB están conformados por todo el equipamiento de hardware (computadoras, servidores, impresoras, escáneres, etc.) y software, sean éstos de terceros, herramientas de internet o desarrollados dentro de la universidad, así como los equipos de comunicación (módems, routers, switches, etc.), también lo conforman los medios que permiten la transferencia de datos (cables, antenas, etc.). Al respecto:

- a) La instalación y configuración de los recursos informáticos es responsabilidad del personal de la Dirección de Sistemas de Información; cualquier cambio a la configuración de algún equipo debe ser autorizado y ejecutado por el personal expresamente autorizado.
- b) Ningún usuario debe dañar deliberadamente los recursos informáticos de la UPSJB, tampoco degradar o detener su operatividad (performance), ni privar de acceso a personal autorizado a estos recursos.
- c) Es responsabilidad del usuario final la eficacia de las medidas de control sobre los recursos informáticos, para lo cual deberá seguir las pautas puestas a su disposición en esta Directiva.

5.2 DE LAS ESTACIONES DE TRABAJO

- a) Los equipos de cómputo son de uso exclusivo para las labores que han sido asignadas a cada trabajador. Estos no deben ser usados para fines personales o actividades no relacionadas a la UPSJB. Cada usuario es responsable del buen uso de los equipos asignados.

	DIRECTIVA DE SEGURIDAD INFORMÁTICA	Código	SIS-OT-03
		Versión	1.1
		Documento de Aprobación	Resolución de Consejo Universitario N° 226-2019-CU-UPSJB
		Fecha de Aprobación	24/07/2019
	DIRECTIVA	N° Página	5 de 13

- b) Los usuarios son responsables de bloquear sus respectivos equipos de cómputo (PC) cuando se ausenten momentáneamente de su puesto de trabajo; para ello deben pulsar las teclas “Control”, “Alt” y “Supr” o “Del” en algunos casos y luego seleccionar la opción “Bloquear”. Esto impide tanto el acceso no autorizado al sistema, como a las aplicaciones. **El usuario que no deje bloqueado su computador al ausentarse será responsable por el uso no autorizado del equipo, de la red o de las aplicaciones instaladas.**
- c) Está prohibido guardar en los discos duros de las computadoras de la universidad archivos de música y video, cuando estos no sean utilizados en sus actividades laborales y funciones asignadas; asimismo está prohibido compartir este tipo de archivos a través de la red; esta práctica pone en riesgo el rendimiento de la red institucional. La Dirección de Sistemas de Información a través, del Departamento de Redes y Comunicaciones, está facultada a tomar las medidas preventivas y correctivas necesarias.
- d) La ubicación actual del usuario y de su estación de trabajo dentro de un ambiente determinado es definido sobre un plano de distribución, el cual es aprobado por la Dirección de Infraestructura de la UPSJB y el área usuaria; por lo tanto, la ubicación del usuario y de su estación de trabajo forman parte de la implementación de cableado estructurado de red; por ello, todo cambio de ubicación debe darse en coordinación con la Dirección de Sistemas de Información y el Departamento de Redes y Comunicaciones (encargada de la Administración de la Infraestructura física de red), para la determinación de la factibilidad técnica de los trabajos de acondicionamiento del cableado estructurado de red de datos; solo de esta manera se garantiza la conexión a la red de la estación de trabajo del usuario.
- e) Se debe contar con un control de acceso al Sistema Operativo y así evitar accesos no autorizados a las computadoras. El acceso solo se podrá realizar mediante la autenticación.
- f) Se debe contar con un control para la identificación y autenticación único y exclusivo para uso personal, a fin de manifestarse y auditarse las actividades de cada responsable particular.

5.3 USO DE SOFTWARE

La UPSJB declara que, para todo efecto utiliza software debidamente autorizado, por lo tanto, NO está permitido:

- a) El copiado de software protegido por Copyright ®, en ningún tipo de medio magnético, óptico o de cualquier otra índole.
- b) La copia de software de propiedad de la UPSJB; salvo que la copia del software sea para fines de respaldo y sólo en caso de estar permitido por la licencia del software.

	DIRECTIVA DE SEGURIDAD INFORMÁTICA	Código	SIS-OT-03
		Versión	1.1
		Documento de Aprobación	Resolución de Consejo Universitario N° 226-2019-CU-UPSJB
		Fecha de Aprobación	24/07/2019
	DIRECTIVA	N° Página	6 de 13

- c) La instalación de ningún tipo de software en equipos de la UPSJB que no haya sido autorizado expresamente por la Dirección de Sistemas de Información.

El departamento de Soporte técnico tiene como responsabilidad establecer mecanismos de restricción de acceso por perfiles para:

- La instalación de software no autorizado.
- Acceso al panel de control y otras opciones de configuración de los computadores.

La instalación de software en una PC debe ser solicitado por el jefe o responsable del área a la que pertenece el usuario final, si la UPSJB cuenta con la licencia respectiva disponible, se procederá con la instalación; el software debe ser instalado únicamente por el personal del área de Soporte Técnico.

5.4 DEL CONTROL DE ACCESOS

La gestión de acceso de usuarios debe evitar accesos no autorizados (a los sistemas de información, servicios, así como a las redes). Esto contempla la supervisión de los accesos.

La creación de una cuenta de acceso al dominio interno de la universidad es factible para el personal de la UPSJB al momento de adquirir vínculo laboral con la misma. Y para todos los demás miembros de la comunidad universitaria, desde el inicio de sus actividades académicas.

- a) Todo usuario tiene una cuenta que lo identifica. Cada cuenta es específica y debe cumplir con la siguiente política de conformación y sintaxis:

Primer nombre del usuario + punto(.) + primer apellido

En caso de existir una cuenta de dominio coincidente con la que se pretende crear, se añadirán progresivamente las letras del segundo apellido hasta conseguir evitar la coincidencia con la nueva cuenta de dominio.

Esta política es de obligatorio cumplimiento y cualquier cambio o modificación deberá contar con la autorización expresa del Director de Sistemas de Información.

Para acceder al Sistema Operativo se cuenta con controladores de Dominio que autentican a los equipos cuando éstos inician una sesión e ingresan a la red de la UPSJB, esta información se encuentra registrada en cada Catálogo Global del Directorio Activo la cual permite el control y autenticación.

- b) La conexión será validada sólo si el usuario ha ingresado todos los datos solicitados: usuario y contraseña y se registra en el visor de eventos de los Controladores de Dominio su intento de ingreso sea

	DIRECTIVA DE SEGURIDAD INFORMÁTICA	Código	SIS-OT-03
		Versión	1.1
		Documento de Aprobación	Resolución de Consejo Universitario N° 226-2019-CU-UPSJB
		Fecha de Aprobación	24/07/2019
	DIRECTIVA	N° Página	7 de 13


éste exitoso o no.

- c) La desactivación de las cuentas de los trabajadores administrativos se realizará de manera automática cuando el usuario sea dado de baja en el Sistema de Recursos Humanos.
- d) Las cuentas creadas para los docentes se mantendrán activas durante el periodo de duración del vínculo contractual.
- e) El acceso a los servicios restringidos de la red (streaming, redes sociales, facebook, etc.) deberá ser solicitado por el Gerente, director del área usuaria, al que pertenece el usuario y estará sujeto a la aprobación de la autoridad correspondiente.
- f) No está permitido el uso de carpetas compartidas dentro de la red de la UPSJB, para tal fin (compartir archivos) todos los usuarios de la UPSJB cuentan con acceso al servicio ONEDRIVE.
- g) Se permite el acceso remoto a los servicios de la red vía el sistema VPN (Virtual Private Network), en la cual los datos y la información viajan sobre canales de acceso cifrados. Se autoriza el acceso remoto por VPN (por un tiempo determinado) exclusivamente para labores de administración de sistemas, aplicaciones y servicios críticos de la Universidad, únicamente a usuarios autorizados por el Director de Sistemas de Información.
- h) El uso de certificados digitales del tipo SSL (Secure Socket Layer) en los servidores de aplicación tiene por finalidad garantizar la confidencialidad de la información en las comunicaciones electrónicas.

5.5 DE LAS CONTRASEÑAS Y SEGURIDAD

Las contraseñas representan un factor fundamental de la seguridad de los recursos informáticos, ya que es la primera línea de protección para el usuario y para la red.

- a) Al crearse cada cuenta se establece una contraseña por defecto, la cual debe ser cambiada por el usuario en el primer inicio de sesión.
- b) Para garantizar la confidencialidad de la información en la red de la UPSJB el formato y sintaxis de cada contraseña queda establecido bajo los siguientes lineamientos:
 - No puede tener menos de 9 caracteres (puede ser de 9 o más caracteres).
 - Combinación mínima obligatoria de letras mayúsculas, letras minúsculas y números.
 - Vigencia de 90 días, al término de los cuales el Sistema de Seguridad solicitará automáticamente al usuario el cambio de contraseña, no pudiendo repetir las tres últimas. Esta política solo aplica a usuarios administrativos. Se considera el manejo de excepciones bajo la autorización del Director de Sistemas de Información.
 - Se recomienda cambiar las contraseñas siempre que el usuario sospeche que la seguridad de su contraseña puede estar

	DIRECTIVA DE SEGURIDAD INFORMÁTICA	Código	SIS-OT-03
		Versión	1.1
		Documento de Aprobación	Resolución de Consejo Universitario N° 226-2019-CU-UPSJB
		Fecha de Aprobación	24/07/2019
	DIRECTIVA	N° Página	8 de 13

comprometida o vulnerada e informar a la Dirección de Sistemas de Información a través del Departamento de Redes y Comunicaciones para la evaluación correspondiente.

- Las contraseñas no deben ser palabras comunes o simples variaciones del nombre del trabajador, usuario, nombre de la computadora, servidor o compañía. Por ejemplo, una contraseña fuerte puede ser: uW9jUp2x4.
- c) Las contraseñas no deben ser enviadas en mensajes de correo electrónico, ni en ningún otro medio de comunicación electrónica. Tampoco deben ser reveladas o escritas en notas, documentos u otros medios escritos, incluyendo conversaciones telefónicas.

A partir de la activación de la cuenta y establecimiento de la contraseña, el usuario asume la responsabilidad sobre la inviolabilidad de la misma. El propietario de una cuenta de usuario es el único responsable del uso que se le dé a ésta. Siendo la cuenta de usuario y su contraseña, de carácter personal e intransferible, queda totalmente prohibido compartirlas para ser usados por otras personas. Por lo mismo, está prohibido solicitar el reseteo de la contraseña de una cuenta de dominio para ser utilizada por personal distinto a su titular, sin importar el sustento (enfermedad repentina, ausencia al trabajo, vacaciones, etc.).

Si el usuario detecta que su cuenta ha sido vulnerada deberá de informar inmediatamente a la Dirección de Sistemas de Información a través del Departamento de Redes y Comunicaciones para que se ejecute las acciones correspondientes a este hecho.

Ante situaciones de sustracción o pérdida de información causados por la violación de la cuenta, debido a una definición débil de su contraseña o un mal uso de la misma, el usuario (estudiante, docente o trabajador) será responsable por los daños que pueda causar a los recursos informáticos de la UPSJB, los cuales serán evaluados por la Dirección de Sistemas de Información y luego comunicados a la Gerencia de Recursos Humanos o de la Escuela Profesional correspondiente para su evaluación y sanción que corresponda.

5.6 DE LOS CENTROS DE DATOS

Para su acceso físico y/o lógico se ha establecido lo siguiente:

- a) Las áreas y el entorno donde se encuentran los Centros de Datos, deben ser áreas seguras, protegidas por perímetros de seguridad definidos, con barreras de seguridad, controles de entrada y acceso apropiados para prevenir la exposición a riesgo de sabotaje, robo de información y de los recursos de tratamiento de información y evitar pérdidas, daños o comprometer la actividad y continuidad de los mismos.
- b) Los equipos y servidores de la infraestructura informática de la UPSJB

	DIRECTIVA DE SEGURIDAD INFORMÁTICA	Código	SIS-OT-03
		Versión	1.1
		Documento de Aprobación	Resolución de Consejo Universitario N° 226-2019-CU-UPSJB
		Fecha de Aprobación	24/07/2019
	DIRECTIVA	N° Página	9 de 13

están ubicados en el Centro de Datos del local principal de la universidad (local Chorrillos).

- c) Se debe contar con controles de acceso para el ingreso del personal al Centro de Datos. Para el ingreso del personal al Centro de Datos se cuenta con tres tipos de accesos:

Acceso Directo: Se otorga al personal que por naturaleza de sus funciones tiene acceso permanente a las instalaciones del Centro de Datos y no requiere autorización expresa. Ejemplo: Administradores de servidores.

Acceso Autorizado: Se otorga al personal que requiere ingresar al Centro de Datos eventualmente. Este personal debe figurar en la lista autorizada y debe registrar su ingreso en la Bitácora de Control de Acceso del Centro de Datos.


Acceso Especial: Se otorga excepcionalmente a personal diverso y por lo tanto requiere autorización expresa del responsable del Centro de Datos. A su vez debe registrar su ingreso en la Bitácora de Control de Acceso del Centro de Datos.

5.7 DE LOS EQUIPOS DE COMUNICACIÓN

Se refiere a los equipos de comunicación de la infraestructura de comunicaciones de la UPSJB, que se encuentran instalados en los diferentes locales.

Se deben establecer medidas de seguridad para la administración de los equipos de comunicaciones, tales como clave de acceso, servicio de alimentación ininterrumpida, flujo de alimentación estabilizada, sistema de refrigeración, así como control del ingreso solo a personal autorizado.

- a) El Representante de la Dirección de Sistemas de cada local es responsable por la integridad física de los equipos de su local. Queda prohibido el acceso y la manipulación a dichos equipos por parte de personal que la Dirección de Sistemas de Información no autorice.
- b) Los equipos de comunicación deben estar protegidos dentro de un gabinete cerrado con llave o dentro de un cuarto de comunicaciones.
- c) Estos equipos deben encontrarse protegidos por un sistema de alimentación continua de energía (UPS).
- d) Es responsabilidad de la Dirección de Sistemas de Información, a través del Departamento de Redes y Comunicaciones, llevar un inventario de todos los recursos de comunicación, en donde se registra la ubicación, modelo, fin, detalles propios como: serie, código patrimonial, etc. Todo traslado, manipulación y/o modificación de las configuraciones deben ser autorizados por el departamento indicado a fin garantizar el normal desenvolvimiento de las actividades.

	DIRECTIVA DE SEGURIDAD INFORMÁTICA	Código	SIS-OT-03
		Versión	1.1
		Documento de Aprobación	Resolución de Consejo Universitario N° 226-2019-CU-UPSJB
		Fecha de Aprobación	24/07/2019
	DIRECTIVA	N° Página	10 de 13

5.8 PROTECCIÓN CONTRA ATAQUES INFORMÁTICOS, VIRUS Y MALWARE

La Dirección de Sistemas de Información, a través del Departamento de Redes y Comunicaciones, es responsable de implementar una solución antivirus, que reduzca la probabilidad de una infección directa en las computadoras; esta solución debe contar con repositorios remotos para replicación de las actualizaciones.

- a) Queda terminantemente prohibido a los usuarios finales la descarga de archivos y/o programas (software gratuito) de los tipos: ejecutables (*.exe, *.msi, etc.), de música y video en todos sus formatos (*.mp3, *.wav, etc), pues pueden contener virus, spyware, gusanos, y malware en general; los cuales podrían perjudicar la seguridad de la información de la Universidad. En caso se requiera algún programa del tipo gratuito, deberá ser solicitado a la Dirección de Sistemas de información especificando el motivo de la necesidad y en que computadora(s) será(n) instalada(s). Previa evaluación de riesgos, dicho requerimiento podrá ser atendido.
- b) Se debe contar con una solución de Filtro de Contenido web, para restringir la navegación por páginas web prohibidas y para mitigar la infección por descarga de archivos y software de internet.
- c) Cuando se detecte una infección o ataque en progreso, originado por el uso de medios extraíbles de almacenamiento (USB, CD, etc.), el

usuario será responsable por los daños de software y/o hardware causados por dicha infección, por lo cual los usuarios deberán tener mucho cuidado en que los dispositivos que traigan no hayan sido utilizados en otras computadoras infectadas.

Adicionalmente a la protección antivirus, la universidad puede contar con una solución “antispam” que impida la propagación de mensajes maliciosos que tengan adjuntos archivos potencialmente peligrosos, contenido para adultos, phishing, Etc.


Si en un computador se detecta una infección o malware en progreso o propagación, el personal de la Dirección de Sistemas, a través del Departamento de Redes y Comunicaciones, está facultado a tomar el control físico o remoto del equipo en cuestión, a fin de controlar y mitigar los efectos del agente dañino.

La Dirección de Sistemas de Información, en coordinación con los proveedores del servicio de transmisión de datos de nuestra red, debe garantizar la seguridad en la transmisión de los datos a través de ella.

6. VIGENCIA

Entrará en vigor a partir de su aprobación.

7. APROBACIÓN

	DIRECTIVA DE SEGURIDAD INFORMÁTICA	Código	SIS-OT-03
		Versión	1.1
		Documento de Aprobación	Resolución de Consejo Universitario N° 226-2019-CU-UPSJB
		Fecha de Aprobación	24/07/2019
	DIRECTIVA	N° Página	11 de 13

Será aprobada mediante RESOLUCIÓN DE CONSEJO UNIVERSITARIO.

8. DEFINICIÓN DE TÉRMINOS

Confidencialidad.

Principio fundamental de seguridad que busca garantizar que toda la información de las personas, (trabajadores, estudiantes, docentes, etc.), y sus medios de procesamiento y/o conservación, estén protegidos del uso no autorizado o divulgación accidental, sabotaje, espionaje industrial, violación de la privacidad y otras acciones que pudieran poner en riesgo dicha información.

La información sólo deberá ser conocida por el personal que la requiera para el desarrollo de sus funciones.

Disponibilidad.

Principio fundamental de seguridad busca garantizar que los usuarios autorizados tengan acceso a la información cuando está es requerida por el proceso del negocio. Para ello se debe procurar que la información y la capacidad de procesamiento sean resguardados y puedan ser recuperados en forma rápida y completa ante cualquier hecho contingente que interrumpa la operatividad o dañe las instalaciones, medios de almacenamiento y/o equipamiento de procesamiento.

La información deberá estar disponible para el personal, usuarios y universidades reguladoras de manera oportuna y acorde a sus niveles de autorización.

Estación de Trabajo.

Área destinada para que un usuario de la red pueda acceder a la misma mediante dispositivos de red (Pc's, Lap top, tablet, teléfono, etc.).

Firewall.

Normalmente conocido como barrera cortafuegos. Es un filtro en software o hardware que controla todas las comunicaciones entrantes y salientes de una red a otra red, cuya función principal es denegar o permitir el acceso de dicha comunicación. Así para denegar o autorizar una comunicación, el firewall primero analiza el perfil del usuario si tiene o no acceso a un determinado servicio tales como: acceso a Internet, correo, transferencia FTP, etc.; y luego denegará o dará paso a dicha comunicación.

Integridad.

Principio fundamental de seguridad busca garantizar la precisión, suficiencia y validez de la información, métodos de procesamiento y todas las transacciones de

	DIRECTIVA DE SEGURIDAD INFORMÁTICA	Código	SIS-OT-03
		Versión	1.1
		Documento de Aprobación	Resolución de Consejo Universitario N° 226-2019-CU-UPSJB
		Fecha de Aprobación	24/07/2019
	DIRECTIVA	N° Página	12 de 13

acuerdo con los valores y expectativas de la organización, así como evitar fraudes y/o irregularidades de cualquier índole que haga que la información no corresponda a la realidad.

La información no puede ser alterada ni eliminada por cambios no autorizados o accidentales. La información no puede ser alertada ni eliminada por cambios no autorizados o accidentales.

LAN (Local Área Network).

Red de Área Local, tipo de arreglo para comunicación de datos a alta velocidad (típicamente en el rango de los Mbit/s) en donde todos los segmentos del medio de transmisión (cable de par trenzados, o fibras ópticas) están circunscritos a una región geográficamente reducida.

Malware.

Se define como software malicioso que cubre un amplio rango de software hostil como son los virus, gusanos, caballos de troya, etc., capaces de causar daños o alteraciones del sistema operativo, archivos, u otros componentes de computadoras y redes informáticas.

Memoria USB (Universal Serial Bus).

Dispositivo de almacenamiento que utiliza una memoria flash para guardar información.

Seguridad de la Información.

Conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de la información.

Seguridad Informática.

Conjunto de medidas técnicas destinadas a preservar la confidencialidad, integridad y disponibilidad de la información, pudiendo además abarcar otras propiedades como la autenticidad, la fiabilidad y el no repudio.

Soporte Técnico.

Servicio de soporte en línea que brinda la Dirección de Sistemas a todos usuarios de la universidad. Cuenta con herramientas en hardware y software que le permite colaborar en la resolución de cualquier tipo de problemas.

SPAM.

	DIRECTIVA DE SEGURIDAD INFORMÁTICA	Código	SIS-OT-03
		Versión	1.1
		Documento de Aprobación	Resolución de Consejo Universitario N° 226-2019-CU-UPSJB
		Fecha de Aprobación	24/07/2019
	DIRECTIVA	N° Página	13 de 13

Se define como Correo Electrónico “tipo basura” o también conocido como “correo no solicitado”. Estos mensajes son normalmente enviados a través de listas de correo invisibles o grupos de noticias que bombardean con propaganda de todo tipo de productos o servicios. Muchos de estos mensajes vienen infectados de virus, gusanos y caballos de Troya.

Spyware.

Software parásito que actúa como espía o secuestrador, y se auto instala en un computador sin el permiso del usuario. Así existen varios tipos de spyware, unos que recopilan y sustraen información para luego enviarla a una universidad externa, otros actúan como secuestradores de las herramientas de navegación. Su funcionamiento puede traer serios problemas de estabilidad y rendimiento en la computadora infectada, llegando incluso a inhibir la misma. Normalmente causan serias dificultades a la hora de conectarse a Internet.

VPN (Virtual Private Network).

Red Privada Virtual construida dentro de una red pública mediante protocolos que reservan su uso a un grupo restringido de usuarios.

Virus.

Pequeño programa malicioso, escrito intencionalmente para auto instalarse en la computadora de un usuario sin conocimiento o permiso de éste. Se comporta como un programa parásito porque infecta y ataca a los archivos contenidos en el computador. Para propagarse, se replica a sí mismo ilimitadas veces, llegando a producir serios daños que pueden afectar a los sistemas y archivos en general, pudiendo estos últimos daños borrar, corromper o destruir dichos archivos.

9. CONTROL DE CAMBIOS.

Versión	Fecha	Cambio	Responsable
1.0	20/11/2017	Versión original	Cristian Saldaña Goldschmidt Fred Paolo Moya Espinoza Rubén Rayme Serrano Walter Rivera Valerio
1.1	24/07/2019	<p>Numeral 5.4 Se incluye la excepción que cualquier cambio o modificación deberá contar con la autorización expresa del Director de Sistemas de Información.</p> <p>Numeral 5.5 De las contraseñas y seguridad, indicando las excepciones al aplicar la política.</p>	Cristian Saldaña Goldschmidt Fred Paolo Moya Espinoza Walter Rivera Valerio Juan Laura Quincho

RESOLUCIÓN DE CONSEJO UNIVERSITARIO N° 226 - 2019 - CU - UPSJB

Lima, 24 de Julio de 2019

VISTA:

La propuesta del Rector a fin de aprobar la Directiva de Seguridad Informática de la Universidad Privada San Juan Bautista SAC, Versión 1.1.

CONSIDERANDO:

1. Que, el artículo 8° de la Ley Universitaria N° 30220 establece que la autonomía inherente a las Universidades, se ejerce de conformidad con la Constitución y las leyes de la República e implica el ejercicio de derechos, entre ellos, el de organizar sus sistemas académico, económico y administrativo.
 2. Que, el artículo 122° de la Ley Universitaria N° 30220 establece que las instancias de gobierno de las universidades privadas se sujetan a lo dispuesto por su Estatuto.
 3. Que, la seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los trabajadores y de la organización en general y como principal contribuyente al uso de programas realizados por programadores.
 4. Que, mediante Resolución Rectoral N° 587-2017-R-UPSJB de fecha 28 de diciembre de 2017, se aprobó la Directiva de Seguridad Informática de la Universidad Privada San Juan Bautista SAC, Versión 1.0, la cual ha sido objeto de modificaciones.
 5. Que, el Consejo Universitario de la Universidad Privada San Juan Bautista SAC en su sesión de fecha 24 de julio de 2019 acordó por unanimidad aprobar la Directiva de Seguridad Informática de la Universidad Privada San Juan Bautista SAC, Versión 1.1.
- Que estando a lo considerado y en ejercicio de sus atribuciones.



upsjb.edu.pe

CHORRILLOS
Av. José Antonio Lavalle s/n
(Ex Hacienda Villa)
T: (01) 214-2500

SAN BORJA
Av. San Luis 1923 - 1925
T: (01) 212-6112 / 212-6116

ICA
Carretera Panamericana Sur Ex Km 300
La Angostura, Subtanjalla
T: (056) 256-666 / 257-282

CHINCHA
Calle Albilla s/n Urbanización Las Viñas
(Ex-toche)
T: (056) 260-329 / 260-402

SE RESUELVE:

ARTÍCULO PRIMERO: Dejar sin vigencia la Directiva de Seguridad Informática de la Universidad Privada San Juan Bautista SAC, Versión 1.0, aprobada mediante Resolución Rectoral N° 587-2017-R-UPSJB de fecha 28 de diciembre de 2017.

ARTÍCULO SEGUNDO: Aprobar la Directiva de Seguridad Informática de la Universidad Privada San Juan Bautista SAC, Versión 1.1, documento que constituye parte integrante de la presente Resolución.

ARTÍCULO TERCERO: Derivar la presente Resolución a la Junta General de Accionistas para su ratificación.

ARTÍCULO CUARTO: Hacer de conocimiento de las áreas pertinentes de la Universidad Privada San Juan Bautista SAC la presente Resolución, para los fines consiguientes.

Regístrese, comuníquese, cúmplase y archívese



Dr. RAFAEL URRELO GUERRA
Presidente del Consejo Universitario de la
Universidad Privada San Juan Bautista SAC



Abg. CRISTIAN JESUS SOSA CANALES
Secretario General de la
Universidad Privada San Juan Bautista SAC