



Gestión Administrativa  
Gestión de Recursos Tecnológicos  
Seguridad de los Sistemas y Redes de Información

Código: PA-GA-5.3.PR-20

Versión: 2

Fecha actualización: 30-11-2016

Página 1 de 7

<b>1. PROCESO/SUBPROCESO RELACIONADO:</b>	Gestión Administrativa / Gestión de Recursos Tecnológicos
<b>2. RESPONSABLE(S):</b>	Jefe de la División de Tecnologías de la Información y las Comunicaciones
<b>3. OBJETIVO:</b>	Mitigar los riesgos de seguridad en los Sistemas y Redes de la Universidad del Cauca para garantizar la seguridad de la información electrónica.
<b>4. ALCANCE:</b>	Inicia con la identificación de vulnerabilidades, amenazas y riesgos y termina con la evaluación y mejora continua de la seguridad en los Sistemas y Redes de Información.
<b>5. MARCO NORMATIVO:</b>	N.A.

**6. CONTENIDO:**

No.	Actividad / Descripción	Cargo Responsable	Punto de Control
1	Identifica las vulnerabilidades, amenazas y riesgos de seguridad en los Sistemas y las Redes de Información.	Funcionarios encargados en cada Área	Jefe de la DivTIC y Coordinadores de Área verifican la Matriz de Riesgos del Subproceso
2	Gestiona el riesgo en los Sistemas y Redes de Información y define los respectivos controles de seguridad.	Jefe de la DivTIC y funcionarios encargados en cada Área.	Jefe de la DivTIC y Coordinadores de Área verifican la Matriz de Riesgos del Subproceso
3	Implementa mecanismos para: <ul style="list-style-type: none"><li>• La seguridad local mediante procesos de Hardening y configuración segura de servicio específico</li><li>• La seguridad perimetral y de Core en la red (Configuración de Firewall, IDS/IPS y control de aplicación)</li><li>• El transporte seguro de la información en las redes, cuando sea necesario. (Configuración de accesos VPN, SSL y certificados digitales.)</li><li>• El control de acceso al servicio (Configuración de perfiles, usuarios, sistema de autenticación local o remota.)</li></ul>	Funcionarios del Área de SSI	Coordinador del Área de SSI verifica las bitácoras



Gestión Administrativa  
Gestión de Recursos Tecnológicos  
Seguridad de los Sistemas y Redes de Información

Código: PA-GA-5.3.PR-20

Versión: 2

Fecha actualización: 30-11-2016

Página 2 de 7

	<b>NOTA 2:</b> Solamente la información confidencial y/o sensible será transmitida por canales seguros. Por ende, no siempre se va a requerir la implementación de mecanismos de seguridad para el transporte seguro de la información.		
4	Implementa mecanismos de seguridad en las Bases de Datos de los Sistemas de Información.	Funcionarios del Área de DBA	Coordinador del Área de DBA verifica las bitácoras y logs
5	Realiza las respectivas copias de respaldo de manera periódica. <b>NOTA 1:</b> esta actividad se ejecuta siguiendo el procedimiento: <i>PA-GA-5.3-PR-28 Creación y Verificación de Copias de Seguridad.</i>	Funcionarios encargados en cada Área.	Coordinadores de Área verifican que las copias de respaldo se hayan creado
6	Implementa mecanismos de seguridad en los dispositivos de interconexión de redes (VLANs, apagado de puertos, control de tormentas, control de segmento, listas de control de acceso y políticas de ruta)	Funcionarios del Área de Infraestructura.	Coordinador del Área de Infraestructura verifica los registros de configuración
7	Realiza las actualizaciones y parches de seguridad en los Sistemas y Redes de Información, según sean necesarios.	Funcionarios encargados en cada Área.	Coordinadores de Área verifican las bitácoras
8	Atiende y soluciona los incidentes y fallos de seguridad en los Sistemas y Redes de Información.	Funcionarios encargados en cada Área.	Coordinadores de Área verifican el documento de incidentes
9	Realiza la evaluación y mejora continua de la seguridad en los Sistemas y Redes de Información.	Funcionarios encargados en cada Área.	Coordinadores de Área verifican la Matriz de Riesgos del Subproceso

**7. FORMATOS:**

**N.A.**

**8. ABREVIATURAS Y**

**DEFINICIONES:**

**Core:** término usado para referirse al núcleo o centro de algo.  
**DBA:** Administrador de Bases de Datos

**DivTIC:** División de Tecnologías de la Información y las Comunicaciones.



Gestión Administrativa  
Gestión de Recursos Tecnológicos  
Seguridad de los Sistemas y Redes de Información

Código: PA-GA-5.3.PR-20

Versión: 2

Fecha actualización: 30-11-2016

Página 3 de 7

**IDS:** Sistema de Detección de Intrusos. (o IDS de sus siglas en inglés Intrusion Detection System) es un programa de detección de accesos no autorizados a un computador o a una red.

**IPS:** Un sistema de prevención de intrusos (o por sus siglas en inglés IPS) es un software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

**Firewall:** un cortafuegos (firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo, exclusivamente, las comunicaciones autorizadas.

**Funcionario:** Este término se utiliza para referirse a: profesionales especializados, profesionales universitarios, técnicos operativos, técnicos administrativos, contratistas y, en general, a cualquier tipo de personal que desempeñe labores para la DivTIC.

**Hardening:** (palabra en inglés que significa endurecimiento) en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades.

**Log:** Un log es un registro de actividad de un sistema, que generalmente se guarda en un fichero de texto

**SSI:** Servidores y Servicios de Internet

**SSL:** Secure Sockets Layer, Protocolo seguro de conexión para mantener la confidencialidad de la información.

**VLAN:** acrónimo de Virtual LAN (Red de área local virtual). es un método para crear redes lógicas independientes dentro de una misma red física.

**VPN:** Red Privada Virtual para la conexión segura de equipos o redes remotas.



Gestión Administrativa  
Gestión de Recursos Tecnológicos  
Seguridad de los Sistemas y Redes de Información

Código: PA-GA-5.3.PR-20

Versión: 2

Fecha actualización: 30-11-2016

Página 4 de 7

### 9. REGISTRO DE MODIFICACIONES:

FECHA	VERSIÓN: No	CÓDIGO	MODIFICACIONES
04-09-2015	0	PA-GA-5.3.PR-20	Construcción del Procedimiento
29-01-2016	1	PA-GA-5.3.PR-20	Se actualiza el nombre del subproceso en el encabezado del procedimiento
30-11-2016	2	PA-GA-5.3.PR-20	Se actualiza el nombre y se agregan actividades al procedimiento para abordar no solamente la seguridad de las redes sino también de los sistemas de información.

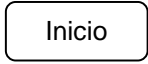
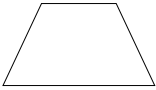


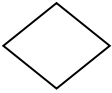
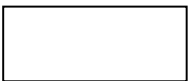
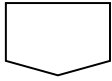
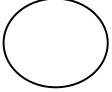
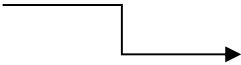

### 10. ANEXOS:

**Anexo A.** Convenciones de procedimientos

**Anexo B.** Diagrama de flujo del procedimiento

ELABORACIÓN	REVISIÓN
Nombre:	Nombre:
Responsable Subproceso	Responsable Proceso
Cargo: Jefe División de TIC	Cargo: Vicerrector(a) Administrativa
Fecha:	Fecha:
REVISION	APROBACION
Nombre:	
Responsable de Gestión de la Calidad	
Cargo: Director	Rector
Fecha:	Fecha: 30-11-2016

**Anexo A.** Convenciones de procedimientos

SÍMBOLO	SIGNIFICADO
	Identifica el inicio del proceso.
	Representa la preparación de un artefacto
	Representa la preparación de un documento en original.
	Representa la preparación de un documento que se elabora en original y varias copias.
	Representa la toma de decisiones.
	Representa una operación.
	Conector de páginas.
	Conector interno. Permite conectar actividades o formatos con otras actividades dentro del Flujograma.
	Indica el sentido de la información. Las flechas se utilizan para conectar los diferentes símbolos y con ello se representa el recorrido de la información entre las diferentes actividades o dependencias.
	Representa el final del procedimiento/proceso.



**Anexo B. Diagrama de flujo**

