PROCEDIMIENTO SEGURIDAD INFORMATICA	
FECHA APROBACIÓN FORMATO: Mayo 30 de 2012	**IPSE-TIC-P03**

1. OBJETIVO

Velar por la seguridad de la información e infraestructura tecnológica del *IPSE*.

2. DEFINICIONES

Activo: Cualquier cosa que tiene valor para la organización.

Autenticidad: Es la propiedad de garantizar la identidad de un sujeto o recurso declarado. La autenticidad se aplica a entidades tales como usuarios, procesos, sistemas e información.

Backup: Es la copia total o parcial de información importante del disco duro, *CD´s*, bases de datos u otro medio de almacenamiento, la cual puede recuperarse en caso de pérdida de la copia original.

CSS (Cross Site Scripting): Es un tipo de inseguridad informática de las aplicaciones *Web*, que permite a una tercera parte inyectar código *JavaScript* en páginas *Web* vistas por el usuario, evitando medidas de control como la Política del mismo origen.

Confidencialidad: Es la propiedad de determinar que la información no esté disponible ni sea revelada a individuos, entidades, procesos o procedimientos no autorizados.

Dirección IP (Dirección de protocolo de Internet): Etiqueta numérica que identifica a un equipo que esté conectado a una red que utilice el protocolo *IP* (*Internet Protocol*). La dirección IP consta de cuatro segmentos de números separados por puntos y cada número es menor de 256.

Disponibilidad: Es la propiedad de la información de ser accesible y utilizable por solicitud de una Entidad o funcionarios autorizados.

DNS (Domain Name System): Es una base de datos distribuida, con información que se usa para traducir los nombres de dominio, fáciles de recordar y usar por las personas, en números de protocolo de Internet (*IP*) que es la forma en la que las máquinas se encuentran en Internet.

Firewall: Es un ordenador, software o dispositivo físico que se conecta en una red con salida a Internet con el fin de impedir el acceso no autorizado, incorporando elementos que garantizan la privacidad, autentificación, etc., conforme a las políticas de seguridad de quien los instala.

Forefront: es un producto de seguridad que permite proteger los puestos de trabajo, portátiles y servidores de la empresa de las nuevas amenazas que aparecen, como *spyware* y *rootkits*, así como virus y otras modalidades de ataque más tradicionales.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

GLPI (Gestion Libre de Parc Informatique - Gestión Libre de Parque Informático): Es un script de código abierto instalable en servidores *Apache* con *PHP* y *MySQL* que permite la creación *online* de inventarios informáticos de cualquier empresa, con soporte de asistencias técnicas, orientada a administradores de redes y soporte técnico en el ámbito de sus empresas, entre otros, consultar la base del conocimiento y/o manuales con soluciones a problemas conocidos de instalación/configuración de una Organización.

Hardware (Hw): Son las partes físicas y tangibles de una computadora, sus componentes eléctricos, electrónicos, electromecánicos y mecánicos, sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.

Incidente: Causa potencial que puede producir daño a un sistema u organización.

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: Es la propiedad de salvaguardar la exactitud y estado completo de los activos.

Intranet: Red privada de computadoras que permite compartir recursos entre ellas y se encuentra enlazada para uso exclusivo dentro de una empresa u hogar. Puede o no tener acceso a Internet.

IPSE: Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas no Interconectadas.

ISO (International Organization for Standardization): Deriva del griego *isos*, que significa "igual"; Organización creada el 23 de Febrero de 1947, en Ginebra, Suiza, con el fin de “facilitar la coordinación internacional y unificación de normas industriales". Actualmente son miembros 165 países.

LAN (Local Area Network): Red de Área Local, es una interconexión de computadoras y periféricos que forman una red dentro de una empresa u hogar. Con esta Red, se pueden intercambiar datos y compartir recursos entre las computadoras que la conforman.

ORFEO: El sistema de gestión documental *ORFEO*, se encuentra conectado a un servidor Institucional con capacidad para almacenar toda la información digitalizada de los documentos físicos, internos y externos relacionados con el *IPSE*. Para tener acceso a esta información digitalizada se cuenta con modelos jerárquicos de seguridad (I-II-III-IV-V).

Parche(s): Programa que se encarga de modificar una aplicación para corregirla o alterarla por algún motivo y deben ser aplicados al programa para el cual fueron exclusivamente diseñados, en otras palabras, un parche sirve para solucionar errores (bugs) en una aplicación, para compatibilizarla o actualizarla.

Phishing: Es la obtención de información importante como números de tarjetas de crédito, claves, datos de cuentas bancarias, etc., al ingresar a un sitio que presume ser legal o auténtico.

Principal: Calle 99 No. 9 A - 54 Torre 3
Piso 14 Edificio Street 100
PBX: (57 1) 639 7888
Fax: (57 1) 639 7888 Ext. 127
Bogotá D.C. – Colombia

Red lógica: Hace referencia a la forma en que los medios físicos (Cables –cobre, fibra óptica-, *switches*, computadoras, impresoras y demás dispositivos) establecen una conexión lógica o comunicación mediante direcciones *IP*.

Riesgo: Potencial de que una amenaza determinada aproveche las vulnerabilidades de una activo o grupo de activos y produzca daño a la organización. Se mide en términos de la combinación de la probabilidad de un evento y sus consecuencias.

Riesgo residual: Nivel restante de riesgo después del tratamiento del riesgo.

Router: Determina (basado en diversos parámetros) la mejor ruta para el envío de datos a través de una red interconectada y luego redirige los paquetes hacia el segmento y puerto de salida adecuados.

SAN (Storage Area Network): Es una red concebida para conectar servidores, matrices de discos y librerías de soporte. Permite conectar de manera rápida, segura y fiable los distintos elementos que la conforman, también transportar datos entre servidores y recursos de almacenamiento. La tecnología *SAN* permite conectividad de alta velocidad de servidor a almacenamiento, almacenamiento a almacenamiento, o servidor a servidor.

Seguridad informática: Consiste en preservar la confidencialidad, integridad y disponibilidad de la información; además puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.

SFI (Sistema Financiero Integrado): Software que permite transacciones en línea entre sus módulos, con capacidad de manejar varias estructuras de cuentas, empresas, periodos, lugares geográficos, centros de costos y multiusuario (Super usuario financiero y Super usuario informático).

SIGMA: Herramienta que permite el manejo y administración del Sistema de gestión integrado del *IPSE*, que facilita el acceso a una fuente de datos de un plan de mejoramiento continuo. Cuenta con 3 modelos jerárquicos de seguridad: Básico, directivo y administrativo.

Sniffing: Programa encargado de obtener datos que circulan por una red que detecta problemas de congestión, mediante la búsqueda de cadenas numéricas o de caracteres en los paquetes.

Spoofing: Suplantación de la dirección *IP* de otro sistema.

Software (Sw): Equipamiento lógico de una computadora digital, comprende el conjunto de componentes lógicos como aplicaciones informáticas, sistema operativo, funcionamiento de programas, interacción con los componentes físicos, interfaz del usuario y demás aplicaciones debidamente licenciadas.

Switch: Dispositivo analógico o conmutador que permite la interconexión de redes informáticas, mejorando el rendimiento y seguridad de una *LAN*.

PROCEDIMIENTO SEGURIDAD INFORMATICA	
FECHA APROBACIÓN FORMATO: Mayo 30 de 2012	**IPSE-TIC-P03**

TIC´s (Tecnologías de la Información y las Comunicaciones): Es la entidad que se encarga de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones. Dentro de sus funciones está incrementar y facilitar el acceso de los usuarios de la organización a las Tecnologías de la Información, las Comunicaciones y a sus beneficios.

USB (Universal Serial Bus): Un puerto *USB* funciona como dispositivo que facilita la conexión de periféricos y accesorios a un ordenador, permitiendo el fácil intercambio de datos y ejecución de operaciones.

Virus: Los virus informáticos son programas que pueden replicarse y ejecutarse por sí mismo. En su accionar, suelen reemplazar archivos ejecutables del sistema por otros infectados con el código maligno, bloquear las redes al generar tráfico inútil o destruir los datos almacenados en el disco duro del ordenador.

Vulnerabilidad: Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

Web: Significa “red”, “telaraña” o “malla”. El concepto se utiliza en el ámbito tecnológico para nombrar a una red informática y, en general a Internet.

WSUS (Windows Server Update Services): Permite a los administradores de las tecnologías de la información (*IT*) implementar las últimas actualizaciones de producto de *Microsoft* para equipos que ejecutan el sistema operativo *Windows*. Mediante el uso de *WSUS*, se distribuyen las actualizaciones que se publican a través de *Microsoft Update* a los equipos en la red.

3. DESARROLLO

ADMINISTRACIÓN IDENTIDAD Y CUENTAS DE USUARIO			
No.	**ACTIVIDAD**	**RESPONSABLE**	**REGISTROS**
1	**Crear cuenta Administrador:** en cada equipo se debe crear una cuenta de Administrador con contraseña que solo debe ser manejada por el grupo de Organización y Sistemas.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	
2	**Recibir Formato creación de cuentas:** Cada Jefe o supervisor de contrato debe diligenciar el formato de creación de cuentas suscribirlo y entregarlo al área de Organización y Sistemas con la firma de autorización de la Secretaria General.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Formato de creación cuentas usuario

Principal: Calle 99 No. 9 A - 54 Torre 3
Piso 14 Edificio Street 100
PBX: (57 1) 639 7888
Fax: (57 1) 639 7888 Ext. 127
Bogotá D.C. – Colombia

PROCEDIMIENTO SEGURIDAD INFORMATICA	
FECHA APROBACIÓN FORMATO: Mayo 30 de 2012	**IPSE-TIC-P03**

ADMINISTRACIÓN IDENTIDAD Y CUENTAS DE USUARIO			
No.	**ACTIVIDAD**	**RESPONSABLE**	**REGISTROS**
3	**Crear cuenta de usuario de red:** se debe crear cuenta de red con inicial del primer nombre y primer apellido completo.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Formato de creación cuentas usuario
4	**Crear cuenta de usuario de Orfeo:** se debe crear cuenta de Orfeo con inicial del primer nombre y primer apellido completo.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Formato de creación cuentas usuario
5	**Crear cuenta de usuario de Correo Institucional:** se debe crear cuenta de Correo con primer nombre y primer apellido completo.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Formato de creación cuentas usuario
6	**Crear cuenta de usuario de Mesa de ayuda:** se debe crear cuenta de Mesa de ayuda con inicial del primer nombre y primer apellido completo.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Mesa de Ayuda
7	**Entrega de Cuentas de Usuario:** Personalmente se debe entregar cuentas de Red, Orfeo, Correo y Mesa de ayuda para que cada usuario ingrese sus contraseñas y firme el formato para constancia de entrega.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Formato de creación cuentas usuario
8	**Solicitud de retiro:** cancelar las cuentas de red, Orfeo, correo institucional, SFI y mesa de ayuda, previa solicitud del Coordinador de Talento Humano o Supervisor del contrato vía Mail al área de Organización y Sistemas.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	
9	**Administrar cuentas de usuario:** controlar y administrar las solicitudes, suspensiones, modificaciones, cierres de cuentas y privilegios.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	

PROCEDIMIENTO SEGURIDAD INFORMATICA	
FECHA APROBACIÓN FORMATO: Mayo 30 de 2012	**IPSE-TIC-P03**

ADMINISTRACIÓN IDENTIDAD Y CUENTAS DE USUARIO			
No.	**ACTIVIDAD**	**RESPONSABLE**	**REGISTROS**
10	**Asignar Impresora:** según el área donde se desempeña el funcionario a la cuenta de red se le debe asignar una impresora.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	

POLITICAS DE SEGURIDAD			
No.	**ACTIVIDAD**	**RESPONSABLE**	**REGISTROS**
1	**Implementar Sistema de Gestión de Seguridad:** implementar la política de seguridad informática, resolución interna que está basada en (*ISO 27001 - ISO 27002*) para mantener la integridad, confidencialidad y disponibilidad de la información.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Documento Intranet "Política de seguridad informática" del *IPSE*
2	**Proteger la información de amenazas externas:** se debe proteger la información de amenazas como Sabotaje, vandalismo, robo, intrusión, virus, violación derechos de autor.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Formato acceso Data Center • Formato solicitud acceso a la red equipos externos
3	**Proteger la información de sucesos físicos:** Se debe proteger la información de sucesos de origen físico, como: sismo, polvo, sobrecarga eléctrica, falla de sistema, daño de Hardware y Software.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Memorando backup's
4	**Proteger la información de mal manejo:** El usuario es responsable de su información institucional, se debe proteger la información de sucesos como: la impericia, negligencia, pérdida de datos.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Memorando solicitud de backup's

Principal: Calle 99 No. 9 A - 54 Torre 3
Piso 14 Edificio Street 100
PBX: (57 1) 639 7888
Fax: (57 1) 639 7888 Ext. 127
Bogotá D.C. – Colombia

POLITICAS DE SEGURIDAD			
No.	**ACTIVIDAD**	**RESPONSABLE**	**REGISTROS**
5	**Verificar permisos:** verificar en el servidor de dominio que los permisos activos correspondan al usuario.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	
6	**Realizar retroalimentación de acciones tomadas:** determinar si las acciones para solucionar un problema de seguridad fueron eficientes y eficaces con el fin de entender las vulnerabilidades de la infraestructura de la Institución.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Encuesta diligenciada por funcionarios del IPSE • Oficio ORFEO
7	**Evaluar acciones de seguridad:** Determinar si las acciones tomadas para solucionar un problema de seguridad informática del *IPSE* fueron eficaces y realizar su respectiva retroalimentación con las partes involucradas.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	
8	**Denunciar amenazas ante la Entidad competente:** denunciar cualquier intento o incidente que perjudique la seguridad informática del *IPSE*.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Memorando Orfeo
9	**Adquirir y renovar tecnología de seguridad:** actualizar regularmente *Sw/Hw* encaminados a la protección de la información: de los equipos conectados a la Red lógica del *IPSE* (*SAN*, servidores, equipos de oficina, equipos de acceso inalámbrico, etc.).	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	
10	**Evaluar riegos periódicamente:** Obtener la información oportuna sobre las vulnerabilidades técnicas de la seguridad informática del *IPSE*.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Antivirus

POLITICAS DE SEGURIDAD			
No.	**ACTIVIDAD**	**RESPONSABLE**	**REGISTROS**
11	**Verificar experiencia administradores actualizaciones:** La actualización del *Sw* operativo, las aplicaciones y las librerías de los programas deben ser realizadas por administradores capacitados.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	
12	**Conservar las versiones anteriores del *Software:*** se debe guardar las versiones anteriores de las diferentes aplicaciones de seguridad como medida de contingencia.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Backup's
13	**Reiterar la obligación de los usuarios y/o terceras partes de acceder a los servicios del *IPSE:*** se debe recordar la importancia de las contraseñas, sensibilizar sobre riesgos, recordar uso adecuado de los equipos asignados y recordar políticas de seguridad informática.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Documento Intranet "Políticas de seguridad informática" del *IPSE*
14	**Documentar y clasificar los procedimientos de operación de la seguridad informática del *IPSE:*** facilitar el registro de la base del conocimiento y uso aceptable de la seguridad informática que se ha adquirido y permitir su posterior consulta a quien lo requiera.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Mesa de Ayuda
15	**Identificar el riesgo residual de los equipos informáticos:** dar el aval para retirar los equipos que sean renovados o desechados por el *IPSE* y así procurar su buen tratamiento y/o aporte a la social.		• Memorando Orfeo

Principal: Calle 99 No. 9 A - 54 Torre 3
Piso 14 Edificio Street 100
PBX: (57 1) 639 7888
Fax: (57 1) 639 7888 Ext. 127
Bogotá D.C. – Colombia

PROCEDIMIENTO SEGURIDAD INFORMATICA	
FECHA APROBACIÓN FORMATO: Mayo 30 de 2012	**IPSE-TIC-P03**

BACKUP'S DE INFORMACION			
No.	**ACTIVIDAD**	**RESPONSABLE**	**REGISTROS**
1	**Realizar Backups Servidores:** Cada mes se debe realizar el backup del sistema y las bases de datos instaladas en los servidores.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Copia en medio magnético. • Memorando ORFEO.
2	**Realizar Backups Programas fuentes:** Cada mes se debe realizar copias de seguridad de los códigos fuente de los aplicativos adquiridos por el Instituto. En caso de que estos códigos sean modificados, se debe realizar un Backup antes de dichos cambios.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Copia en medio magnético. • Memorando ORFEO.
3	**Recibir solicitud de backup:** recibir la solicitud de Backup mediante mesa de ayuda cuando el funcionario hace entrega de su cargo, cambie de equipo o se desee archivar información.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Mesa de Ayuda.
4	**Realizar Backup Información:** copiar la información en algún medio magnético en custodia de la Coordinación de Organización y Sistemas.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Copia en medio magnético.
5	**Custodiar la información:** almacenar la información en el lugar que disponga el grupo de Gestión de *TIC´s* por un lapso de 1 año.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Copia en medio magnético.
6	**Realizar Backup de la información en custodia:** copiar la información en custodia para centro de documentación.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Copia en medio magnético.

Principal: Calle 99 No. 9 A - 54 Torre 3
Piso 14 Edificio Street 100
PBX: (57 1) 639 7888
Fax: (57 1) 639 7888 Ext. 127
Bogotá D.C. – Colombia

PROCEDIMIENTO SEGURIDAD INFORMATICA	
FECHA APROBACIÓN FORMATO: Mayo 30 de 2012	**IPSE-TIC-P03**

BACKUP'S DE INFORMACION			
No.	**ACTIVIDAD**	**RESPONSABLE**	**REGISTROS**
7	**Enviar información a centro de documentación:** generar memorando de remisión de envió y enviar cada mes al Centro de documentación copia en medio magnético donde debe ser custodiada por un lapso de 10 años.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Copia en medio magnético. • Memorando Orfeo

PROTECCIÓN DE SOFTWARE			
No.	**ACTIVIDAD**	**RESPONSABLE**	**REGISTROS**
1	**Instalar el agente del antivirus**: en todo computador dentro del dominio ipse.gov se debe instalar el agente del antivirus. Bloquear puertos *USB* que no este autorizado su uso.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Consola Antivirus
2	**Actualizar versión de agente del antivirus:** después de instalar se debe actualizar el agente con las ultimas directivas de seguridad.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Consola Antivirus
3	**Ensayar Parches de Software:** revisar la funcionalidad de los parches, realizar pruebas sobre capacidad de uso, seguridad, efectos en otros sistemas, facilidad para el usuario y verificar si ayudan a eliminar o reducir debilidades de seguridad informática de la institución.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• WSUS
4	**Aprobar Parches:** después de la prueba se deben aprobar parches ejecutables que estén liberados y estables.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	

Principal: Calle 99 No. 9 A - 54 Torre 3
Piso 14 Edificio Street 100
PBX: (57 1) 639 7888
Fax: (57 1) 639 7888 Ext. 127
Bogotá D.C. – Colombia

PROCEDIMIENTO SEGURIDAD INFORMATICA	
FECHA APROBACIÓN FORMATO: Mayo 30 de 2012	**IPSE-TIC-P03**

PROTECCIÓN DE SOFTWARE			
No.	**ACTIVIDAD**	**RESPONSABLE**	**REGISTROS**
5	**Realizar Backups de restauración:** antes de implementar cambios realizar una copia de seguridad como política de restauración al estado anterior del sistema.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Copia en medio magnético.
6	**Archivar información:** se debe archivar el backup siempre y cuando los cambios no afecten el normal funcionamiento del sistema.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Copia en medio magnético.
7	**Restaurar el sistema:** se debe instalar la copia del sistema en la fecha de restauración más próxima.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Copia en medio magnético.
8	**Recibir Solicitud para Recuperar Información:** recibir memorando del área solicitando la información que se quiere recuperar.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Orfeo
9	**Ubicar la información:** ubicar el medio magnético correspondiente o *backup* lógico en el servidor de respaldo (*SAN*) o Data protector donde se puede encontrar la información.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• SAN • Data protector • Copia en medio magnético.
10	**Restaurar Información:** se debe restaurar a la copia de la información con fecha más actualizada.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Copia en medio magnético.

Principal: Calle 99 No. 9 A - 54 Torre 3
Piso 14 Edificio Street 100
PBX: (57 1) 639 7888
Fax: (57 1) 639 7888 Ext. 127
Bogotá D.C. – Colombia

PROTECCIÓN DE SOFTWARE			
No.	**ACTIVIDAD**	**RESPONSABLE**	**REGISTROS**
11	**Informar al Usuario:** responder el memorando al usuario que realizo el requerimiento, se debe informar a través del cuatro de texto del aplicativo Orfeo, la fecha de solución y el estado de la restauración.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Devolución Orfeo
12	**Monitorear Incidentes:** monitorear las alertas o problemas que presenten los usuarios con la ejecución del software del Instituto.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Mesa de ayuda. • Consola Antivirus.
13	**Verificar la presencia de códigos maliciosos:** monitorear el reporte de problemas en todos los archivos en medios ópticos ó electrónicos, archivos adjuntos, descargas del correo electrónico, archivos recibidos, sitios *Web* antes de su uso y/o cuando se ingresa a la red del *IPSE.*	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Consola Antivirus.
14	**Administrar WSUS:** El administrador del *WSUS* debe monitorear que se estén descargando todas las actualizaciones.	Coordinador(a) y Profesional Universitario del área de Organización y Sistemas	• Wsus

4. IDENTIFICACIÓN DE RIESGOS

- Acceso interno y/o externo abusivo al Sistema Informático.
- Obstaculización ilegítima del sistema informático y/o red de telecomunicaciones.
- Interceptación de datos informáticos.
- Daño informático.
- Uso de software malicioso.
- Violación de Datos Personales.
- Publicación e instalación de Sitios *Web* no permitidos en los servidores o *hardware* destinado para tal fin.
- Hurto por Medios Informáticos y Semejantes.
- Transferencia No Consentida de Activos.
- Daños en infraestructura tecnológica (*IT*).
- Información/Datos misionales no confiables.

5. ANEXOS

- Formato de creación cuentas usuario.
- Formato acceso Data Center.
- Formato solicitud acceso a la red equipos externos.
- Formato estándar de firma.
- Encuesta diligenciada por los funcionarios del *IPSE.*

CONTROL DE CAMBIOS

FECHA	MOTIVO DEL CAMBIO
22/05/2013	Se realiza modificación de acuerdo a los cambios en los Sistemas de Información del IPSE.

Revisó	Aprobó
CARGO:	CARGO:
FIRMA:	FIRMA:

Principal: Calle 99 No. 9 A - 54 Torre 3
Piso 14 Edificio Street 100
PBX: (57 1) 639 7888
Fax: (57 1) 639 7888 Ext. 127
Bogotá D.C. – Colombia