Centro Informático Científico de Andalucía
CONSEJERÍA DE ECONOMÍA, CONOCIMIENTO, EMPRESAS Y UNIVERSIDAD

JUNTA DE ANDALUCIA

NORMAS DE SEGURIDAD INFORMÁTICA

CENTRO INFORMÁTICO CIENTÍFICO DE ANDALUCÍA

Fecha: 22 agosto 2019

Índice de contenido

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 22 de agosto de 2019 por el Centro Informático Científico de Andalucía.

Este conjunto de Normas de Seguridad de la Información es efectivo desde dicha fecha y hasta que sea reemplazado por uno nuevo.

2. INTRODUCCIÓN

El Centro Informático Científico de Andalucía (CICA en adelante), para llevar a cabo su cometido, precisa de Políticas de Seguridad de la Información (en adelante PSI) que establezcan las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de las Tecnologías de la Información y las Comunicaciones (en adelante TIC), consistentes en sistemas de información, equipos de cómputo, redes de voz y datos, etc., de las y personas que interactúan haciendo uso de los servicios asociados a dichas TIC.

El CICA depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

Como organismo parte de la Administración de la Junta de Andalucía, el CICA se encuentra dentro de la Política de Seguridad TIC publicada en **DECRETO 1/2011, de 11 de enero**, por el que se establece la **política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía** (http://www.juntadeandalucia.es/boja/2011/11/d2.pdf), modificado por el **Decreto 70/2017, de 6 de junio**, por el que se modifica el Decreto 1/2011 (http://www.juntadeandalucia.es/boja/2017/110/1).

Según el apartado 2 del artículo 1 del citado Decreto, "*cada entidad incluida en el ámbito de aplicación del Decreto desarrollará y aprobará el documento de política de seguridad TIC de la entidad, así como las normas y procedimientos que adecuen, en su caso, las directrices comunes de la Administración de la Junta de Andalucía a sus particularidades.*". Además, el artículo 10 dice: "*Sin perjuicio de las directrices establecidas en el marco regulador de seguridad TIC de la Administración de la Junta de Andalucía, cada Consejería y entidad incluida en el ámbito de aplicación del presente Decreto deberá disponer formalmente de su propio documento de política de seguridad TIC, así como de las disposiciones de desarrollo que adecuen, en su caso, las directrices comunes de la Administración de la Junta de Andalucía a sus particularidades*".

Cumpliendo con dichos artículos, se ha redactado el documento de Política de Seguridad TIC del CICA.

3. OBJETO

El presente documento constituye la relación de normas de seguridad correspondientes a la Política de Seguridad TIC del CICA.

4. ALCANCE

El ámbito de aplicación de las normas contempladas en este documento es el definido en la Política de Seguridad TIC del CICA.

5. NORMAS DE SEGURIDAD

5.1. INFORMACIÓN

5.1.1. ACCESO A LA INFORMACIÓN

5.1.1.1. Gestión y seguridad de acceso (PSI-1.1-01)

Objetivo	Garantizar un adecuado ambiente de control en la definición y mantenimiento de accesos de usuarios a los diferentes servicios del CICA.
Alcance	Esta norma aplica a todo el personal que haga uso de los servicios del CICA.
Responsables	Jefes de área. ATIs. Todos los usuarios.

1) Gestión de contraseñas

a) Para garantizar la seguridad tanto de la información como de los equipos, el Área de Sistemas asignará a cada usuario las claves de acceso estrictamente necesarias para la realización de las labores encomendadas: acceso al computador, acceso a la red interna, acceso al correo electrónico, acceso a las aplicaciones correspondientes.

b) La autorización para la creación, eliminación o modificación de perfiles de acceso es responsabilidad directa del RSIS de cada aplicación.

c) Los usuarios no deben tener acceso a opciones del Sistema de Información que no utilicen.

d) El Área de Sistemas, los administradores de las aplicaciones, responsables de activos tecnológicos y los propietarios de la Información serán los responsables de velar por que los perfiles de acceso existentes sean acordes con las funciones realizadas por cada uno de los usuarios.

e) En todas las aplicaciones se debe contar con un administrador del Sistema de Información, el cual diseña y aprueba e implementa los perfiles de acceso, para esta actividad se debe utilizar el formato establecido por el Área de Sistemas.

f) En el evento que algún usuario deje de tener vínculo laboral con la Organización, el Área Administrativa debe notificarlo por escrito a las Áreas correspondientes, con la finalidad de inactivar todas las cuentas y accesos, equipos y recursos informáticos asignados.

2) Uso de Contraseñas

a) Las contraseñas establecidas, deben cumplir con los parámetros mínimos contemplados para contraseñas fuertes o de alto nivel:

I. Debe tener como mínimo nueve caracteres alfanuméricos de longitud.

II. Debe contener como mínimo cuatro letras, de las cuales al menos una debe ser Mayúscula.

III. Debe contener como mínimo cuatro números.

IV. Debe contener como mínimo un carácter especial de los siguientes (+-*/@#$%&).

V. No debe contener vocales tildadas, ni eñes, ni espacios.

VI. Los sistemas recordarán las últimas 6 claves utilizadas, por lo que no se podrán reutilizar.

b) Las contraseñas deben ser cambiadas de forma obligatoria cada 4 meses. Este cambio será forzado desde la administración de las aplicaciones, o cuando los administradores de los sistemas lo consideren necesario debido a alguna vulnerabilidad en los criterios de seguridad.

3) Recomendaciones respecto de las claves:

I. Las claves deben ser fáciles de recordar.

II. No deben ser basadas en información personal, ni fechas especiales.

III. NO serán escritas ni guardadas en la oficina, en papeles, agendas u otro medio físico.

IV. NO serán proporcionadas ni se hará alusión a su formato, con compañeros de trabajo cuando este en vacaciones.

V. NO serán comentadas ni reveladas delante de otros, en el teléfono, a superiores, familiares. Se pondrá especial cuidado en no permitir que nadie vea cuando teclea la clave en un computador.

VI. NO se enviarán por correo electrónico.

VII. NO se utilizará la característica "recordar contraseña" de ninguna aplicación (ej: Outlook, Internet Explorer, Thunderbird).

VIII. Las claves NUNCA se deben almacenar en un servidor o maquina en red sin utilizar algún tipo de encriptación.

IX. NO serán utilizadas su clave en computadores considerados como no confiables.

4) Incidencias

a) Los usuarios deben informar inmediatamente al Área de Seguridad, toda vulnerabilidad encontrada en los sistemas asignados.

5.1.1.2. Gestión de usuarios (PSI-1.1-02)

Objetivo	Administrar el control de los usuarios de los servicios del CICA para garantizar un adecuado uso de la información y del acceso a los sistemas de información.
Alcance	Esta norma aplica a todo el personal que haga uso de los servicios del CICA.
Responsables	Jefes de área. ATIs. Todos los usuarios.

1) Administradores

a) Aplica a todas aquellas personas cuyo cargo está relacionado con la administración funcional y/o tecnológica de sistemas de información.

b) Debe existir una cuenta de usuario que será utilizada exclusivamente para monitorización por parte del Personal Técnico o quien ejerza sus funciones.

c) Las actividades realizadas por los administradores deben reflejarse en un registro, que debe ser monitorizado periódicamente por el Administrador de Seguridad de los Sistemas (ASS).

2) Usuarios avanzados

a) Aplica a los usuarios que por sus funciones requieran acceso de usuario privilegiado a los sistemas, servicios y aplicaciones asignados, jefes de área y usuarios de perfil medio.

b) Ningún usuario avanzado debe modificar información directamente de las Bases de Datos, sin previa autorización del Responsable del Sistema relacionado.

3) Usuarios finales

a) Aplica a los usuarios finales que por sus funciones requieran acceso de usuario para los sistemas, servicios y aplicaciones asignados por la organización.

4) Directrices generales

a) Se deben asignar usuarios unificados para todos y cada uno de los sistemas, servicios y aplicaciones, garantizando la estandarización por cada usuario. Es decir, cada persona debe tener el mismo nombre de usuario para todos los sistemas y aplicaciones del CICA.

b) La nomenclatura de los nombres de usuario será:

- Primera letra del primer nombre + primer apellido.

  En caso de existir duplicidad:

- Primera letra del primer nombre + Segunda letra del primer nombre + primer apellido)

c) Ningún usuario debe ser eliminado de ningún sistema, servicio o aplicación, debe aplicarse la inactivación del usuario.

d) Las cuentas de usuario son de uso personal e intransferible.

e) Debe existir un procedimiento para el almacenamiento, protección y administración de las contraseñas de los todos los usuarios.

5.2. RECURSOS

5.2.1. ACTIVOS

5.2.1.1. Adquisición de bienes TIC

Objetivo	Garantizar que los activos TIC propiedad del CICA cumplen con los requisitos exigidos

	en cuanto a seguridad, calidad, fiabilidad y proporcionalidad del gasto.
Alcance	Esta norma aplica a todos los bienes adquiridos por el CICA.
Responsables	Jefes de área. ATIs.

Toda adquisición de tecnología informática se efectuará a través del CSTIC, que será quien apruebe en última instancia las adquisiciones. Los ATI, al planear las operaciones relativas a la adquisición de bienes informáticos, establecerán prioridades y en su selección deberá tomar en cuenta los siguientes parámetros:

Calidad

Es uno de los parámetros más importantes a tener en cuenta a la hora de adquirir recursos informáticos. Se tendrán especialmente en cuenta los certificados de calidad de los organismos mundialmente reconocidos.

Experiencia

Deben ser productos de éxito probado en el mercado, con estructura de servicio postventa que asegure su mantenimiento durante su ciclo de vida.

Desarrollo Tecnológico

Se deberá analizar su grado de obsolescencia, su nivel tecnológico con respecto a la oferta existente en el mercado y su permanencia en el mercado.

Estándares

Toda adquisición debe de cumplir los estándares reconocidos nacional e internacionalmente.

Capacidades

Para la adquisición de Productos de Seguridad TIC se tendrán en cuenta las recomendaciones y guías publicadas por el CCN-CERT, así como los Catálogos de Productos de Seguridad de las Tecnologías de la Información y Comunicación, CPSTIC, según el nivel de clasificación de la información a proteger.

Consideraciones

Se deberá analizar si satisface la demanda actual, con un margen suficiente para el crecimiento esperado, para soportar la carga actual y la prevista por parte del CICA. Para la adquisición de Hardware se tendrá en cuenta lo siguiente:

- El equipo que se desee adquirir estará dentro de las listas de ventas vigentes de los fabricantes y/o distribuidores del mismo y dentro de los estándares.
- Los equipos complementarios deberán tener una garantía mínima de un año y deberán contar con el servicio técnico correspondiente.
- La marca de los equipos o componentes deberá contar con presencia y permanencia demostrada en el mercado nacional, así como con asistencia técnica y de repuestos local.
- Los dispositivos de almacenamiento, así como las interfaces de entrada / salida, deberán estar acordes con la tecnología de punta vigente, tanto en velocidad de transferencia de datos, como en procesamiento.

- Las impresoras deberán apegarse a los estándares de Hardware y Software vigentes en el mercado, corroborando que los suministros (cintas, papel, etc.) se consigan fácilmente en el mercado y no estén sujetas a un solo proveedor.
- Los equipos adquiridos deben contar con asistencia técnica durante la instalación de los mismos.
- En lo que se refiere a los servidores, equipos de comunicaciones, concentradores, switches y otros equipos que se justifiquen por ser de operación crítica y/o de alto costo, deben de contar con un programa de mantenimiento preventivo y correctivo que incluya el suministro de repuestos al vencer su período de garantía.
- En lo que se refiere a los computadores personales, al vencer su garantía por adquisición, deberán de contar por lo menos con un programa de servicio de mantenimiento correctivo que incluya el suministro de repuestos.
- Todo proyecto de adquisición de bienes de tecnología, debe sujetarse al análisis, aprobación y autorización del Comité.

5.2.1.2. Gestión de los activos (PSI-2.1-01)

Objetivo	Garantizar un adecuado uso de la Infraestructura (Software y Hardware) del CICA por sus empleados y usuarios.
Alcance	Esta norma aplica para todos los usuarios de componentes de la infraestructura tecnológica del CICA.
Responsables	Jefes de área. ATIs. Todos los usuarios.

1) Responsabilidad Administrativa

a) Se debe garantizar la elaboración y actualización de un inventario de activos al mayor detalle posible, que garantice un fácil nivel de acceso, recuperación, trazabilidad, auditabilidad y responsabilidad de sus activos.

b) Se deben destinar las herramientas necesarias que permitan la oportuna gestión de inventarios de los activos, empleando como mínimo identificación plaquetas o etiquetas de identificación externa, contemplando tecnologías que faciliten la gestión de inventarios y el control de entradas y salidas de activos de las instalaciones de la organización.

2) Responsabilidad del usuario

a) Cada usuario es responsable del cuidado y uso adecuado de los recursos informáticos que se le asignen para el desarrollo normal de sus funciones.

b) Los recursos informáticos asignados a cada usuario, son para uso limitado para el desarrollo de sus funciones, por lo tanto no está permitido el uso de cualquiera de los recursos con propósitos de ocio o lucro.

c) Los usuarios de los activos de información no podrán usar los elementos de cómputo asignados

para realizar actividades personales distintas a las contratadas.

d) Los usuarios de activos de información son responsables de la información y los recursos asignados, por lo cual deben ser responsables de notificar, la definición de controles de acceso y otros controles de seguridad, con el fin de garantizar su responsabilidad por incumplimientos, no conformidades y otros incidentes que se presenten en la organización.

e) La instalación de software no autorizado es responsabilidad del usuario, y cualquier daño en la configuración del equipo que se produzca por el incumplimiento de esta política debe ser asumido por el responsable del activo.

f) El uso de activos de información o recursos corporativos para actividades personales será considerado como un incumplimiento a esta política.

3) Gestión de activos

a) Todo cambio a la configuración de los computadores puede efectuarse únicamente por personal de soporte, y supervisión del Área de Sistemas.

b) Todos los activos de información (computadores, periféricos) deben estar protegidos por reguladores de voltajes y sus instalaciones eléctricas deben haber sido realizadas técnicamente controlando las fases correspondientes.

c) Todos los equipos de cómputo y comunicaciones deben estar protegidos y soportados por equipos ininterrumpidos de electricidad UPS y sus instalaciones eléctricas deben haber sido realizadas técnicamente controlando las fases correspondientes. Cuando se concentren varios equipos en un área se debe hacer un estudio del consumo por equipo para determinar que el circuito no presente sobrecarga.

d) Todo el sistema eléctrico de cableado estructurado, debe estar independiente al sistema de energía de iluminación, y su gestión debe estar centralizada, acogiendo las normas eléctricas correspondientes para tal fin.

e) La gestión de las copias de seguridad, será responsabilidad del Área de Sistemas, quien debe implementar los procesos y procedimientos necesarios, que garanticen el adecuado tratamiento de los medios físicos internos y externos, y los medios digitales locales.

f) La responsabilidad de la gestión de la seguridad de la información, la aplicación de reglas de controles de acceso definidas por el CICA, o por los propietarios de las los activos de información, estará a cargo del Área de Seguridad.

4) Restricciones

a) No está permitida la descarga, instalación, almacenamiento y/o transferencia de juegos, archivos de audio, archivos de video, software y/o programas desde o hacia Internet, que atenten contra las leyes de derechos de autor, salvo los requeridos para el funcionamiento y mantenimiento de la plataforma tecnológica, gestionados por el Área de Sistemas.

b) Los activos de información no deben moverse o reubicarse sin la aprobación previa del Jefe de Área involucrado. El traslado debe realizarlo únicamente el personal de soporte, con la autorización del Área de Sistemas.

c) No está permitido el uso de hardware y/o software personales en las instalaciones de la Organización, sin previa autorización del Área Administrativa y notificación al Área de Sistemas.

d) No está permitido a los usuarios y/o visitantes: comer, fumar o beber en los puestos de trabajo, centros de cómputo o instalaciones con equipos tecnológicos, sin excepciones; al hacerlo estarían exponiendo los equipos a daños eléctricos y a riesgos de contaminación sobre los dispositivos de almacenamiento.

e) Ningún ente interno o externo del CICA estará autorizado para generar copias de la información de la organización, sin previa autorización por parte del Comité.

5.2.2.HARDWARE

5.2.2.1. Gestión de servidores (PSI-2.2-01)

Objetivo	Establecer estándares para la configuración y mantenimiento de los servidores de tal forma que se preserve la seguridad de los mismos, del software y datos en ellos instalados.
Alcance	Las políticas se aplican para el personal responsable de poner en producción los servidores.
Responsables	Jefes de área. ATIs. Todos los usuarios.

1) Configuración

a) El Área de Sistemas debe implementar los protocolos y/o guías de configuración de todos los servidores de la organización, deben ser establecidas y actualizadas por cada tipo de servidor.

b) Se debe tener toda la información de configuración por cada servidor, que garantice como mínimo: función principal, configuración de Hardware, configuración de Software, inventario de aplicaciones, servicios y servidores, ubicación de las copias de respaldo.

c) Debe existir un diagrama de configuración de plataforma y servidores.

d) La configuración de los servidores se debe hacer de acuerdo a los protocolos y/ guías establecidas por el Área de Sistemas.

2) Control de accesos

a) Para la parametrización de los accesos privilegiados al servidor, la clave máster de "administrador" será gestionada únicamente por el responsable del Área de Sistemas, y debe existir una copia de respaldo compartida de la misma en poder de 2 usuarios designados por la dirección.

b) Para la gestión de los servidores por parte de los ATIs del CICA, se debe crear y asignar una clave con privilegios de administración, que será responsabilidad del personal asignado para tal fin.

c) La gestión de servidores se debe realizar únicamente bajo la utilización de canales seguros.

d) El acceso físico a servidores debe ser gestionado, programado y autorizado por el Área de

Sistemas.

3) Gestión

a) La gestión, operación, instalación, desinstalación y mantenimiento de servidores es responsabilidad de los ATIs, y la supervisión y control son responsabilidad del Área de Sistemas.

b) Los ATIs deben ser personal altamente calificado en la gestión de servidores y notificar todas las novedades inherentes a la gestión del mismo.

c) La operación de servidores desde áreas de trabajo diferentes a las designadas para soporte técnico, debe ser autorizada por el Área de Sistemas.

d) Los cambios en la configuración de los servidores debe hacerse siguiendo los procedimientos establecidos para dicha operación.

4) Monitoreo

a) Para todos los eventos críticos de seguridad y los sistemas sensibles es necesario mantener Log's y se deben gestionar acorde a los protocolos establecidos.

b) Todos los servidores deben tener activos los servicios de auditoría de eventos que garanticen la auditabilidad de las transacciones realizadas en ellos.

c) Todos los eventos relacionados con la seguridad, rendimiento, fallas y vulnerabilidades se deben reportar al Área de Seguridad, estos eventos se contemplan en los protocolos establecidos.

d) Debe existir un protocolo de acceso remoto, que garantice el adecuado uso de las herramientas existentes para tal fin.

5) Accesos Remotos

a) Toda herramienta de acceso remoto a servidores y equipos de cómputo, debe ser autorizada por el Área de Seguridad e instalada por el ingeniero de Soporte designado.

b) El acceso remoto a los equipos de cómputo será autorizado por el Área de Seguridad, previa solicitud por parte del responsable de cada Área, garantizando la confidencialidad de la información de cada usuario.

c) Los soportes remotos se realizaran únicamente en caso de no tener acceso directo al equipo que requiera el soporte, por eventos de localización física externa o distante del CICA.

d) Los accesos desde Internet/Intranet para utilizar sistemas de información de la Organización en forma remota y en tiempo real deben ser autorizados por el Área de Sistemas y el Área de Seguridad.

e) Todo acceso remoto debe ser establecido sobre Redes Privadas Virtuales - VPN con encriptación, previa configuración y aprobación por parte del Área de Seguridad.

f) Los accesos remotos para soportes en redes por terceros, proveedores de Servicios, deben ser asignados, aprobados y documentados por el Área de Redes.

g) La asignación de claves a terceros, proveedores de servicio, para la comunicación remota con la red central, debe estar supervisada permanentemente y será de asignación temporal.

6) Mantenimiento

a) Se debe hacer el mantenimiento periódico del servidor, utilizando el protocolo y/o procedimiento diseñado por el Área de Sistemas, y será documentado acorde a los procedimientos establecidos.

b) Los procedimientos de instalación y mantenimiento de los servidores deben ser actualizados con cada cambio de versión de los sistemas y aplicaciones por cada servidor.

c) Los parches más recientes de seguridad se deben probar, aprobar e instalar tanto al sistema operativo del servidor como a las aplicaciones activas, a menos que esta actividad interfiera con la producción.

d) Los servicios, servidores y aplicaciones que no se utilicen, deben ser deshabilitadas y/o desinstaladas.

e) Debe mantenerse un inventario actualizado de software y hardware de cada uno de los servidores del CICA.

f) Se debe generar los procedimientos y protocolos necesarios que garanticen la adecuada generación, custodia y disposición de las copias de seguridad para los servidores del CICA, acordes con la política de copias de respaldo.

5.2.2.2. Gestión de equipos de cómputo (PSI-2.2-02)

Objetivo	Establecer estándares para la configuración y mantenimiento de los Equipos de Cómputo y periféricos de tal forma que se preserve la seguridad de los mismos, del software y datos en ellos instalados.
Alcance	Las políticas se aplican para el personal responsable de poner en producción los equipos de cómputo y periféricos, y a todos los usuarios del CICA que tengan asignados recursos informáticos.
Responsables	Jefes de área. ATIs. Todos los usuarios.

1) Configuración

a) Se debe implementar los protocolos y/o guías de configuración de todos los equipos de cómputo y periféricos del CICA, y deben ser establecidas y actualizadas por cada tipo de dispositivo.

b) Se debe tener toda la información de configuración por cada equipo de cómputo y periférico, que garantice como mínimo: función principal, configuración de Hardware, configuración de Software, inventario de aplicaciones, servicios, responsables.

c) La configuración de los equipos de cómputo y periféricos se debe hacer de acuerdo a los protocolos y/ guías establecidas.

d) Los equipos de cómputo y periféricos deben ser configurados de tal forma que los usuarios no puedan alterar la configuración ni instalar software, salvo autorización expresa.

2) Control de acceso

a) Para la parametrización de los accesos a los equipos y periféricos, la clave máster local de "administrador" será gestionada únicamente por el responsable del Área de Sistemas, y debe ser estándar unificado para todos los equipos del CICA.

b) Para la gestión de los equipos de cómputo y periféricos por parte de los ATIs, se debe crear y asignar una clave con privilegios de administración, que será responsabilidad del personal asignado.

c) La correcta utilización de la cuenta de usuario para administración y su contraseña a nivel de computadores personales esta bajo la responsabilidad del personal de Soporte designado.

3) Gestión

a) La gestión, operación, instalación, desinstalación y mantenimiento de los equipos de cómputo y periféricos es responsabilidad de los ATIs, y la supervisión y control son responsabilidad del Área de Sistemas.

b) El Responsable del Área de Sistemas debe asignar personal calificado en la gestión de equipos y periféricos y notificar todas las novedades inherentes a la gestión del mismo.

c) Toda actividad que implique reasignación y traslado de equipos de cómputo y periféricos entre diferentes áreas de trabajo deben ser realizadas únicamente por el personal de soporte y autorizadas por Área de Sistemas.

d) Los cambios en los equipos de cómputo y periféricos debe hacerse siguiendo los procedimientos establecidos para dicha operación.

4) Monitorización

a) Para todos los eventos críticos de seguridad y los sistemas sensibles es necesario mantener Log's y se deben gestionar acorde a los protocolos establecidos.

b) Todos los eventos relacionados con la seguridad, rendimiento, fallas y vulnerabilidades se deben reportar al Área de Seguridad, estos eventos se contemplan en los protocolos establecidos.

c) Se deben garantizar los mecanismos necesarios que mitiguen el riesgo de extracción no autorizada de la organización, de equipos de cómputo y periféricos.

5) Mantenimiento

a) Se debe hacer el mantenimiento periódico de los equipos de cómputo y periféricos, y deberá ser documentado.

b) Los procedimientos de Instalación y mantenimiento de los equipos de cómputo y periféricos deben ser actualizados con cada cambio de versión de los sistemas y aplicaciones por cada equipos de cómputo o periférico.

c) Los parches más recientes de seguridad se deben probar, aprobar e instalar tanto al sistema operativo de equipos de cómputo y periféricos como a las aplicaciones activas, a menos que esta actividad interfiera con la producción.

d) Los servicios y aplicaciones que no se utilicen, deben ser deshabilitadas y/ desinstaladas.

e) Debe mantenerse un inventario actualizado de software y hardware de cada uno de los equipos de cómputo y periféricos del CICA.

f) El personal de Soporte designado tiene la potestad para remover y notificar, cualquier software que no esté autorizado por el Área de Sistemas.

g) El Área de Sistemas debe generar los procedimientos y protocolos necesarios que garanticen la adecuada generación, custodia y disposición de las copias de seguridad para los Equipos de Cómputo y dispositivos de almacenamiento portátiles de la organización, acordes con la política de copias de seguridad.

6) Restricciones

a) Todos los usuarios de los equipos de cómputo y periféricos deben tener en cuenta los siguientes aspectos:

I. No ingerir bebidas y/o alimentos cerca de los equipos de cómputo y periféricos.

II. No fumar dentro de las instalaciones y/o cerca a los equipos de cómputo y periféricos.

III. No insertar objetos extraños en las ranuras de los equipos de cómputo y periféricos.

IV. No realizar actividades de mantenimiento de hardware.

V. No Instalar Software no autorizado en los equipos de cómputo y periféricos, si se instala software no licenciado, el usuario debe asumir las consecuencias legales y económicas.

VI. Apagar los equipos cuando no estén en uso.

VII. Bloquear la sesión cuando esté ausente.

b) Es responsabilidad del Área de Sistemas garantizar:

I. Conservar los equipos en adecuadas condiciones ambientales.

II. Mantener una adecuada protección contra fluctuaciones de voltaje.

III. Únicamente el personal de Soporte pueda instalar software en los equipos de cómputo y periféricos.

IV. Establecer programas de mantenimiento de equipos de cómputo y periféricos.

5.2.2.3. Gestión de equipos móviles (PSI-2.2-03)

Objetivo	Establecer estándares para la configuración y mantenimiento de los equipos de cómputo y dispositivos de almacenamiento portátiles de tal forma que se preserve la seguridad de los mismos, del software y datos en ellos instalados.
Alcance	Las políticas se aplican para el personal responsable de poner en producción los equipos de cómputo y dispositivos de almacenamiento portátiles, y a todos los usuarios del CICA que tengan asignados recursos informáticos portables.
Responsables	Jefes de área. ATIs. Todos los usuarios.

1) Configuración

a) Se debe implementar los protocolos y/o guías de configuración de todos los Equipos de Cómputo y dispositivos de almacenamiento portátiles del CICA, y deben ser establecidas y actualizadas por cada tipo de dispositivo.

b) Se debe tener toda la información de configuración por cada equipo de cómputo portátil y dispositivos de almacenamiento, que garantice como mínimo: función principal, configuración de Hardware, configuración de Software, inventario de aplicaciones, servicios, responsables.

c) La configuración de los equipos de equipos de cómputo portátiles y dispositivos de almacenamiento se debe hacer de acuerdo a los protocolos y/ guías establecidas.

d) Los equipos de cómputo y dispositivos de almacenamiento portátiles deben ser configurados de tal forma que los usuarios no puedan alterar la configuración ni instalar software.

2) Configuración

a) Para la parametrización de los accesos a los Equipos de Cómputo portátiles y dispositivos de almacenamiento, la clave máster local de "administrador" será gestionada únicamente por el responsable del Área de Sistemas, y debe ser estándar unificado para todos los equipos del CICA.

b) Para la gestión de los equipos de cómputo y dispositivos de almacenamiento portátiles por parte de los ATIs, se debe crear y asignar una clave con privilegios de administración, que será responsabilidad del personal asignado.

c) La correcta utilización de la cuenta de usuario para administración y su contraseña a nivel de computadores personales esta bajo la responsabilidad del personal de Soporte designado.

3) Gestión

a) La gestión, operación, instalación, desinstalación y mantenimiento de los equipos de cómputo y dispositivos de almacenamiento portátiles es responsabilidad de los ATIs, y la supervisión y control son responsabilidad del Área de Sistemas.

b) El Área de Sistemas debe asignar personal calificado en la gestión de equipos de cómputo y dispositivos de almacenamiento portátiles y notificar todas las novedades inherentes a la gestión del mismo.

c) Los cambios en los equipos de cómputo y dispositivos de almacenamiento portátiles debe hacerse siguiendo los procedimientos establecidos para dicha operación.

d) Se debe generar protocolos e implementar controles necesarios de protección de información para todos los equipos de cómputo y dispositivos de almacenamiento portátiles, por su alto nivel de riesgo en información.

4) Monitorización

a) Para todos los eventos críticos de seguridad y los sistemas sensibles es necesario mantener Log's y se deben gestionar acorde a los protocolos establecidos.

b) Todos los eventos relacionados con la seguridad, rendimiento, fallas y vulnerabilidades se deben reportar al Área de Seguridad, estos eventos se contemplan en los protocolos establecidos.

c) Se deben garantizar los mecanismos necesarios que mitiguen el riesgo de extracción no autorizada del CICA, de equipos de cómputo y dispositivos de almacenamiento portátiles.

5) Mantenimiento

a) Se debe hacer el mantenimiento periódico de los equipos de cómputo y dispositivos de almacenamiento portátiles, y deberá ser documentado.

b) Los procedimientos de instalación y mantenimiento de los equipos de cómputo y dispositivos de almacenamiento portátiles deben ser actualizados con cada cambio de versión de los sistemas y aplicaciones por cada equipo de cómputo o dispositivo de almacenamiento portátiles.

c) Los parches más recientes de seguridad se deben probar, aprobar e instalar tanto al sistema operativo del equipos de cómputo y dispositivos de almacenamiento portátiles como a las aplicaciones activas, a menos que esta actividad interfiera con la producción.

d) Los servicios y aplicaciones que no se utilicen, deben ser deshabilitadas y/ desinstaladas.

e) Debe mantenerse un inventario actualizado de software y hardware de cada uno de los equipos de cómputo y dispositivos de almacenamiento portátiles del CICA.

f) El personal de Soporte designado tiene la potestad para remover y notificar, cualquier software que no esté autorizado por el Área de Sistemas.

g) El Área de Sistemas debe generar los procedimientos y protocolos necesarios que garanticen la adecuada generación, custodia y disposición de las copias de seguridad para los equipos de cómputo y dispositivos de almacenamiento portátiles de la organización, acordes con la política de copias de seguridad.

h) Se deben garantizar los mecanismos necesarios que permitan la generación de las Copias de Seguridad de forma remota.

6) Restricciones

a) Todos los usuarios de equipos de cómputo y dispositivos de almacenamiento portátiles, deben registrar la entrada y salida de los mismos en los mecanismos destinados para tal fin.

b) Todos los equipos de uso personal del usuario, deben ser registrados en la entrada y salida de las instalaciones en los mecanismos destinados para tal fin.

c) Por el alto riesgo en la manipulación externa de los equipos de cómputo y dispositivos de almacenamiento portátiles, se deben contemplar las siguientes recomendaciones de seguridad.

   I. No transportar los equipos de cómputo y dispositivos de almacenamiento portátiles, en vehículos a la vista, o en maletines que sugieran el contenido, mitigando el riesgo de robo / hurto.

   II. No prestar o reasignar equipos de cómputo y dispositivos de almacenamiento portátiles a personal externo no autorizado por el CICA.

   III. En caso de pérdida o robo / hurto, se debe notificar el incidente de forma inmediata al Área de Sistemas y al Área Administrativa.

d) Todos los usuarios de los equipos de cómputo y dispositivos de almacenamiento portátiles deben tener en cuenta los siguientes aspectos:

   I. No ingerir bebidas y/o alimentos cerca de los equipos de cómputo y dispositivos de almacenamiento portátiles.

II. No fumar cerca a los equipos de cómputo y dispositivos de almacenamiento portátiles.

III. No insertar objetos extraños en las ranuras de los equipos de cómputo y periféricos.

IV. No realizar actividades de mantenimiento de hardware.

V. No Instalar Software no autorizado en los equipos de cómputo y dispositivos de almacenamiento portátiles, si se instala software no licenciado, el usuario debe asumirá las consecuencias legales y económicas.

VI. Apagar los equipos cuando no estén en uso.

VII. Bloquear la sesión cuando esté ausente.

e) Es responsabilidad del Área de Sistemas garantizar:

I. Mantener una adecuada protección contra fluctuaciones de voltaje, dentro de las instalaciones.

II. Únicamente el personal de Soporte pueda instalar software en los equipos de cómputo y periféricos.

III. Establecer programas de mantenimiento de equipos de cómputo y dispositivos de almacenamiento portátiles.

5.2.3.SOFTWARE

5.2.3.1. Gestión de software corporativo (PSI-2.3-01)

Objetivo	Establecer estándares para la gestión de todo el Software Corporativo.
Alcance	Aplica para el personal responsable de administrar y llevar el control de Software corporativo.
Responsables	Jefes de área. ATIs.

1. Licenciamiento

a) Todo software corporativo, es decir sistemas operativos, sistemas de información y herramientas corporativas de gestión, debe ser dirigido y controlado de forma centralizada, y gestionado operativamente por el personal de Soporte Informático.

b) Todo software no comercial, es decir Freeware, Shareware, Trial, CPL, EPL, GNU, Open Source, debe tener el respectivo soporte de licencia, en el que se garantice el alcance de la licencia, y debe ser autorizado y gestionado por el Área de Seguridad.

c) El personal de Soporte designado será el único autorizado para realizar la instalación, configuración, parametrización, actualización y desinstalación, previo autorización del Área de Sistemas.

d) Debe existir un inventario de las licencias de software del CICA, con el fin de facilitar la administración y control de software no licenciado.

2. Gestión

a) El Área de Sistemas debe garantizar la generación y actualización de inventarios de licencias corporativas que garanticen la legalidad del mismo ante entes de vigilancia externos.

b) La utilización de software corporativo para fines personales, dentro o fuera de la organización será responsabilidad de usuario del activo.

c) La extracción, préstamo, copia, venta y/o renta de software corporativo para fines externos y/o personales, no está autorizado bajo ninguna circunstancia.

5.2.3.2. Gestión de vulnerabilidades técnicas (PSI-2.3-02)

Objetivo	Reglamentar los controles necesarios para prevención, detección y eliminación de virus informáticos en los equipos de cómputo del CICA.
Alcance	Esta política aplica a todos los empleados del CICA.
Responsables	Jefes de área. ATIs. Todos los usuarios.

1) Seguridad

a) Debe tener Software Antivirus que garantice la protección ante amenazas por virus informáticos, que a su vez debe contemplar como mínimo los siguientes componentes:

I. Componente de consola de servidor: encargado de distribuir y actualizar las actualizaciones de antivirus en los equipos de cómputo de la red.

II. Componente de correo externo: encargado filtrar el contenido y tráfico de correos entrantes y salientes.

b) Debe existir uno o varios software que gestionen la salida hacia internet y desde internet, filtrado de contenidos, filtrado de páginas y monitoreo de navegación.

c) A nivel perimetral se debe contar con software de seguridad que permita controlar el acceso de virus, troyanos, malware, spyware, phishing y spam.

d) El software de detección de virus y demás Software de Seguridad seleccionados por el CICA, deben ser instalado en todos los servidores y equipos de computo, incluyendo computadores portátiles del CICA.

e) Para la utilización de medios electrónicos externos, de uso corporativo y/o personal, correos electrónicos y descarga de archivos, se debe realizar previamente un escaneo de seguridad.

f) Los usuarios deben conocer los procedimientos de detección y eliminación de virus informáticos, para lo cual el Área de Seguridad, debe garantizar la difusión necesaria para el uso de las

herramientas de seguridad existentes.

g) Es responsabilidad del Área de Seguridad que todos los equipos asignados estén libres de virus, y responsabilidad de los usuarios que la información gestionada en los activos asignados, y medio de almacenamiento sean filtrados con el Software Antivirus y demás software de seguridad instalados en cada uno de los equipos del CICA.

2) Gestión de herramientas

a) Debe existir un protocolo de gestión de aplicaciones de seguridad informática que contemple las actividades de instalación, configuración, parametrización, administración, mantenimiento y desinstalación.

b) Debe realizarse la evaluación de la relevancia y criticidad o urgencia de los parches a implementar.

c) La instalación, configuración, parametrización, administración, mantenimiento y desinstalación del software antivirus existente, es responsabilidad los ATIs, previa autorización por parte del Área de Seguridad.

d) La actualización del antivirus debe ser gestionada de forma centralizada en el servidor de la aplicación y de forma automática en cada uno de los equipos de cómputo del CICA.

e) Las actualizaciones de nuevas versiones serán gestionadas únicamente por los ATIs previa autorización por el Área de Seguridad.

f) Debe realizarse una evaluación periódica, mínimo cada 2 años, de la gestión y desempeño de las herramientas de seguridad informática existentes, y de ser necesario, cambiar las soluciones por aquellas que generen mayores características y niveles de seguridad.

3) Notificación de incidentes

a) Debe existir un procedimiento de gestión de incidentes que registre todo el seguimiento de los incidentes presentados hasta su solución.

b) Los usuarios de cada uno de los Sistemas de Información son responsables de solicitar soporte informático en caso de encontrar situaciones sospechosas en los sistemas asignados o cualquier virus detectado en equipos de cómputo asignados.

c) Todos los registros de detección de virus y otras vulnerabilidades, serán revisados y analizados por los ATIs del CICA, y notificados al Área de Seguridad.

4) Tratamiento de vulnerabilidades

a) Para todas las configuraciones de los sistemas de seguridad, se debe contemplar una política de cuarentena, que garantice que las vulnerabilidades encontradas no se difundan por las redes a otros equipos, hasta que se realice un análisis y tratamiento por parte del Área de Seguridad.

b) Cuando los virus no puedan ser eliminados a pesar de haber agotado los mecanismos existentes para tal fin, se debe escalar al Comité, encargado de evaluar los aspectos de Seguridad de la Información

5.2.3.3. Gestión de trazabilidad y auditabilidad (PSI-2.3-03)

Objetivo	Reglamentar las pistas de auditoría con las que deben contar los Sistemas de Información del CICA.
Alcance	Esta Política aplica a todos los Sistemas de Información del CICA.
Responsables	Jefes de área. ATIs. Todos los usuarios.

1) Tipo de información

a) Debe realizarse un análisis de riesgos sobre la criticidad de la información gestionada por los Sistemas Operativos, Bases de Datos, Sistemas de Información, que identifique y defina los datos a los que deben aplicar las pistas de auditoría.

b) Debe existir un protocolo de configuración, implementación, gestión, respaldo y recuperación de pistas de auditoría, Log's y/o registros auditables.

c) Todos los Sistemas Operativos, Bases de Datos, Sistemas de Información, debe tener activa y habilitada las funciones de Log's.

d) Las pistas de auditoría deben ser contempladas como un archivo adicional a los de datos, que evidencie todas las actividades realizadas por los usuarios, conteniendo como mínimo: fecha, hora, usuario, tipo de operación realizada (modificación, inclusión y borrado de información), archivo o tabla en la que se realizo la operación, numero del registro o id, para el caso de modificación de información, debe incluir los campos de valor anterior y nuevo valor.

2) Control de accesos

a) El acceso a las pistas de Auditoría debe ser de carácter restringido a los Usuarios.

b) Debe garantizarse la restricción de modificación a las pistas de Auditoría para todos los Sistemas Operativos, Bases de Datos, Sistemas de Información.

3) Control de accesos

a) Todas las pistas de Auditoria deben contar con una Copia de Seguridad periódico, programado y automático.

b) Debe garantizarse la disponibilidad y preservación de las Copias de Seguridad.

5.2.4.SISTEMAS DE INFORMACIÓN

5.2.4.1. Gestión de sistemas operativos (PSI-2.4-01)

Objetivo	Establecer estándares para la Información que debe se gestionada por los sistemas operativos de la organización.
Alcance	Las políticas se aplican para el personal responsable de administrar los sistemas

	operativos del CICA.
Responsables	Jefes de área. ATIs. Todos los usuarios.

1) Gestión

a) Deben existir protocolos de instalación, configuración, parametrización, gestión y soporte, de usuarios, roles y perfiles, para todos los sistemas operativos del CICA.

b) Deben aplicarse políticas de gestión y control propias de los sistemas operativos del Servidor, que den cumplimiento al punto anterior.

c) La instalación, configuración y parametrización de todos los sistemas operativos del CICA, debe ser responsabilidad de los ATIs designados, previa autorización del Área de Sistemas.

d) Debe existir una política centralizada, incluida en los protocolos de configuración de equipos, que estandarice en todos los equipos de cómputo, el particionamiento de discos duros en un mínimo de 3 unidades virtuales: sistema operativo, datos y Copias de Seguridad local.

e) Debe aplicarse una política centralizada de Escritorios limpios que minimicen el riesgo de pérdida y confidencialidad de archivos, teniendo en cuenta que lo contenido en el escritorio es susceptible de perdidas en caso de fallas del sistema operativo.

f) Debe aplicarse un política para equipos desatendidos, que garantice la confidencialidad de la información cuando el usuarios no esté en su puesto de trabajo.

2) Seguridad

a) Debe existir un protocolo de encriptación de Información en los Sistemas Operativos y Redes.

b) Se deben habilitar todas las funcionalidades de los sistemas operativos del Servidor, de tal forma que toda la información viaje por las redes (LAN o WAN) en forma encriptado, con el fin de preservar su confidencialidad.

c) La encriptación de datos se debe realizar mediante Software y/o Hardware.

d) Todo tipo de información transmitida desde y hacia entidades externas, debe ser encriptada.

3) Organización

a) Debe existir un procedimiento de creación y eliminación de cuentas de usuario para redes y sistemas operativos.

b) Se debe asignar una cuenta a todo usuario, que lo identificará y le dará acceso a los recursos informáticos asignados.

c) Es responsabilidad del usuario, el buen uso y las actividades realizadas con la cuenta asignada.

d) La asignación de cuentas y configuración de perfiles debe ser solicitada por el Jefe del Área, y aprobada por el Área de Sistemas.

e) La creación de cuentas y perfiles en los Sistemas de Información, es competencia de los ATIs

desigandos.

f) La estructura de creación de usuarios debe ser estandarizada y unificada para todos los sistemas operativos, bases de datos y sistemas de información, y debe estar contemplada en el procedimiento de administración de usuarios.

g) Las cuentas de usuario de administradores de red y su contraseña, debe ser conocida sólo por estos, en caso de que otro Ingeniero requiera realizar funciones propias del administrador de la Red, por autorización expresa de éste, debe utilizar una cuenta alterna que contenga exclusivamente los permisos para realizar las actividades para la cual está autorizado.

h) Las claves para la administración de red y sistemas de información deben ser cambiadas en forma forzosa por lo menos una vez cada seis meses.

4) Control de accesos

a) No se deben asignar cuentas de usuario genéricas, entendiendo como genérica aquellas que son utilizadas por varios usuarios de la organización.

b) Todas las cuentas serán creadas con los permisos del grupo general, si el usuario necesita permisos adicionales o necesita pertenecer a un grupo especifico para acceso a recursos propios de su trabajo debe hacer una solicitud al Área de Sistemas.

c) Las cuentas de usuario de la red deben ser suspendidas cada vez que un usuario se ausente por largo tiempo por motivo de incapacidad, licencia etc... La cuenta sólo será habilitada durante este período de tiempo bajo solicitud escrita debidamente justificada del Jefe de Área al que pertenece el usuario dirigida al Área de Sistemas.

d) Las características de asignación de claves, debe estar acorde a lo contemplado en el protocolo correspondiente.

5) Recomendaciones

a) NO se debe revelar información de cuentas ni contraseñas a NADIE, por ningún medio (teléfono, correo, o personalmente).

b) NO se deben escribir las claves en medios físicos (papel, agenda, etc.).

c) NO se debe revelar, compartir, prestar o hablar de las claves, o formato de claves a nadie de la organización, incluyendo jefes, ni a miembros de la familia, conocidos o amigos.

d) NO debe suministrar ni delegar las claves en periodos de ausencia o vacaciones.

e) NO debe habilitarse en ningún sistema o aplicación, la característica de “recordar claves”.

f) NO debe guardar claves en ningún tipo de computador sin utilizar un mecanismo de encriptación.

g) NO se deben utilizar las cuentas y claves asignadas en equipos externos a la organización o que considera no confiable.

h) Las claves se deben crear de manera que puedan ser fácilmente recordadas.

i) Cualquier empleado y contratista que se encuentre responsable de violar esta política está sujeto a acciones disciplinarias correspondientes.

5.2.4.2. Gestión de sistemas de información (PSI-2.4-02)

Objetivo	Establecer estándares para la gestión de los sistemas de información del CICA.
Alcance	Las políticas se aplican para el personal responsable de administrar los sistemas de información del CICA.
Responsables	Jefes de área. ATIs. Todos los usuarios.

1) Gestión

a) Deben existir protocolos de instalación, configuración, parametrización, gestión y soporte, de usuarios, roles y perfiles, para todos los sistemas de información existentes en el CICA.

b) Deben aplicarse políticas de gestión y control propias de los sistemas de información existentes.

c) La instalación, configuración y parametrización de todos los sistemas de información de la organización, debe ser responsabilidad de los ATIs designados para tal fin.

d) El Área de Sistemas, debe asignar a cada usuario las cuentas necesarias para la gestión de los sistemas que le sean asignados.

e) Los datos, bases de datos, programas, herramientas y sistemas de información del CICA deben ser modificados únicamente por personal autorizado de acuerdo con los procedimientos establecidos, al igual que el acceso a la información debe restringirse únicamente a personal autorizado por el CICA.

f) Toda la información histórica almacenada y respaldada debe contar con los medios, procesos, programas y sistemas de información que permitan su consulta en el tiempo, teniendo en cuenta la evolución de los componentes tecnológicos y las aplicaciones a través del tiempo.

g) La eliminación de la información en medios físicos debe seguir procedimientos seguros y aprobados por el Área de Sistemas, y acorde a los protocolos establecidos para tal fin.

2) Seguridad

a) Debe existir un protocolo de Encriptación de Información en los Sistemas de información.

b) Debe existir un procedimiento de creación y eliminación de cuentas de usuario para todos los sistemas de información existentes.

c) Se debe asignar una cuenta a todo usuario que requiera acceso a los Sistemas de Información asignados.

d) No se deben asignar cuentas de usuario genéricas para ningún tipo de sistema de información, entendiendo como genérica aquellas que son utilizadas por varios usuarios de la organización.

e) Todas las cuentas serán creadas de acuerdo con el perfil requerido en la solicitud de creación de usuarios, tramitada por cada Jefe de Área y aprobada por el Área de Sistemas.

f) Los ATIs desigandos son los encargados de la creación de cuentas y perfiles de usuarios en los

sistemas de información del CICA.

g) Las cuentas deben ser suspendidas cada vez que un usuario se ausente por largo tiempo por motivo de incapacidad, vacaciones... La cuenta sólo será habilitada durante este período de tiempo bajo solicitud escrita debidamente justificada del Jefe de área al que pertenece el usuario; será suspendida permanentemente cuando termine definitivamente el contrato de un empleado del CICA.

h) La estructura de creación de usuarios debe ser estandarizada y unificada para todos los sistemas de información asignados.

i) La cuenta de usuario de Administrador de cada aplicación es responsabilidad del Área de Sistemas, para el soporte del proveedor del sistema, se debe crear una cuenta con privilegios de administrador.

j) Las características de asignación de claves, debe estar acorde a lo contemplado en el protocolo correspondiente y las claves deben ser cambiados en forma forzosa por lo menos una vez cada seis meses.

k) Los usuarios no deben tener acceso a opciones del Sistema de Información que no utilicen.

3) Responsabilidades

a) La información de los sistemas existentes es de carácter confidencial y reservado, por tanto no podrá ser utilizada para propósitos distintos con los relacionados con el objeto del CICA.

b) Es responsabilidad del usuario, el buen uso y las actividades realizadas con la cuenta asignada.

c) Los usuarios del CICA son responsables de la información que usan y deben seguir las líneas establecidas por el CICA para protegerla, evitar pérdidas, accesos no autorizados y utilización indebida de la misma.

d) Las cuentas de usuario de las aplicaciones asignadas son personales e intransferibles. Bajo ninguna circunstancia este tipo de cuentas deben ser conocidas por una persona diferente a su propietario.

e) Todos los derechos de propiedad intelectual de las herramientas o aplicaciones desarrollados o modificados por los usuarios durante el tiempo de contratación, son de propiedad exclusiva del CICA.

4) Recomendaciones

a) NO se debe revelar información de cuentas ni contraseñas a nadie, por ningún medio (teléfono, correo, o personalmente).

b) NO se deben escriba las claves en medios físicos (papel, agenda libreo, etc.).

c) NO se debe revelar, compartir, prestar o hablar de las claves, o formato de claves a nadie de la organización, incluyendo jefes, ni a miembros de la familia, conocidos o amigos.

d) NO debe suministrar ni delegar las claves en periodos de ausencia ovacaciones.

e) NO debe habilitarse en ningún sistema o aplicación, la característica de “recordar claves”.

f) NO debe guardar claves en ningún tipo de computador sin utilizar un mecanismo de encriptación.

g) NO se deben utilizar las cuentas y claves asignadas en equipos externos a la organización o que

considera no confiable.

h) Las claves se deben crear de manera que puedan ser fácilmente recordadas por cada usuario.

i) Cualquier empleado y contratista que se encuentre responsable de violar esta política está sujeto a acciones disciplinarias correspondientes.

5.3. REDES Y COMUNICACIONES

5.3.1. REDES

5.3.1.1. Gestión de redes (PSI-3.1-01)

Objetivo	Establecer estándares para proteger la integridad de información que es transmitida interna y externamente, contra amenazas y vulnerabilidades.
Alcance	Esta política se aplica para todo el personal responsable de administrar la red interna del CICA y la red RICA.
Responsables	Jefes de área. ATIs. Todos los usuarios.

1) Gestión

a) Se debe contar con un procedimiento para la administración y configuración de todas las redes del CICA.

b) Se debe realizar un monitoreo permanente tanto de la infraestructura de comunicaciones como de los servidores, de manera que se detecten los problemas que pueden llegar a causar fallas en la disponibilidad de los servicios de las redes del CICA.

c) Los centros de cableado, centros de datos, centros de monitoreo/vigilancia y centros eléctricos, están catalogados como zonas restringidas, con control de acceso y restricción a personal no autorizado.

2) Seguridad

a) Deben existir protocolos de parametrización y directrices de seguridad informática para redes y herramientas de seguridad de red como Sistemas de Detección de Intrusos (IDS), Sistemas de Prevención de Intrusos (IPS), gestión de vulnerabilidades, y otras herramientas que sean convenientes.

b) Deben existir protocolos de transmisión de información que garanticen que todos los datos que se transmitan por las redes internas de la organización y entre redes externas, sean encriptados.

c) La configuración de accesos a la información de las estaciones de trabajo desde la red, deben tener acceso restringidos a los directorios no autorizados.

d) Debe existir un protocolo de Hacking Ético (ataques de seguridad éticos), que garantice la generación de ataques de intrusión controlados (interna y externa) a las redes del CICA, con el fin de determinar las debilidades y adoptar nuevos controles a implementar. Estas pruebas deben ser generadas por entes externos que garanticen la independencia y objetividad en los resultados.

e) Debe existir un protocolo de seguridad en todas las redes que permita periódicamente la realización de monitoreo a los ataques en tiempo real, y garantice la seguridad de las redes ante terceros no autorizados e intrusos.

f) Deben existir protocolos de verificación física a las redes del CICA que garanticen la calidad de las instalaciones de cableado de datos.

3) Controles de Acceso

a) Deben existir los protocolos de seguridad que describan los mecanismos de control y accesos a las diferentes redes existentes en el CICA.

b) Deben existir todos los documentos técnicos que describan las configuraciones de red.

c) Deben existir los protocolos que describan controles de seguridad perimetrales de las Redes de Área Local (LAN) y Redes de Área Global (WAN); e internos entre Redes de Área Local (LAN) y Redes de Área Local WiFi (WLAN); y su integración con los controles de seguridad en sistemas operativos y aplicaciones.

d) La gestión de accesos, roles y perfiles de las redes deben estar contempladas y gestionadas a través del LDAP.

4) Restricciones

a) Los usuarios de la red interna del CICA, no pueden realizar o ejecutar acciones en la red que sean exclusivas de los administradores de red.

b) Los usuarios no deben llevar a cabo ningún tipo de instalación de líneas telefónicas, canales de transmisión de datos, módems, etc., ni cambiar su configuración sin haber sido formalmente aprobados por el Área de Redes.

5.3.2.COMUNICACIONES

5.3.2.1. Gestión de Internet (PSI-3.2-01)

Objetivo	Garantizar el uso adecuado de Internet como herramienta fuente de información, investigación y comunicación en la Red Informática Científica de Andalucía.
Alcance	Esta norma se aplica a todos los usuarios de la red RICA.
Responsables	Jefes de área. ATIs. Todos los usuarios.

1) Gestión

a) Debe existir una política de uso de acceso a la red que garantice el buen uso de esta y de las herramientas disponibles para su gestión.

b) El servicio de Internet debe ser utilizado para facilitar el cumplimiento de las funciones asignadas a los empleados del CICA.

c) El servicio de Internet debe ser utilizado por los usuarios de acuerdo a las políticas de uso de red definida por el CICA.

d) Debe existir un proceso y procedimientos que garanticen el monitoreo y revisiones periódicas del uso apropiado de Internet.

2) Seguridad

a) Deben existir los mecanismos de gestión y control apropiados para garantizar el adecuado uso del internet tales como Firewall, Proxy, DNS, Filtro de Contenidos, Anti-virus, anti-spam, anti-spyware, anti-phising, anti-malware y demás software para gestión de vulnerabilidades de redes, aprobados por el Área de Seguridad.

b) Los usuarios con acceso a Internet deben estar seguros de los sitios visitados, identificando las advertencias de acceso a sitios desconocidos.

c) No se debe registrar en los sitios de Internet datos específicos de las máquinas del CICA como la dirección IP, nombre de la máquina, nombres de usuarios, claves, nombre de redes corporativas entre otros, que puedan exponer la confidencialidad de las redes y exponerse a la recepción no deseada de mensajes o información.

3) Responsabilidades

a) El usuario es responsable de respetar y acatar las leyes para derechos de reproducción, patentes, marcas registradas y todo lo relacionado con derechos de autor las cuales aplican en Internet.

b) Se debe hacer uso racional del servicio de Internet, y se considera como uso indebido cuando:

I. Atenta contra la integridad, veracidad y confidencialidad de la información del CICA.

II. Atenta contra la integridad de los sistemas y componentes de la plataforma tecnológica del CICA.

III. Reduce la productividad de los empleados del CICA.

IV. Pone en riesgo la disponibilidad de los recursos informáticos del CICA.

4) Restricciones

a) No está permitida la transmisión o recepción de material protegido por Copyright infringiendo la Ley de Protección Intelectual.

b) No está permitida la transmisión o recepción de ficheros que infrinjan la Ley de Protección de Datos de Carácter Personal.

c) Está prohibido el acceso, transmisión o recepción de toda clase de material pornográfico, mensajes o bromas de una naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.

d) Los empleados deben limitar su acceso a páginas de entretenimiento, distracción o correos en portales públicos. El CICA podrá aplicar restricciones o sanciones en casos que se encuentren

excesos.

e) Se debe auto-regular el uso de herramientas de mensajería instantánea y chat, tales como Skype, Messenger, Facebook, Yahoo Messenger, Gmail Talk, entre otros, en horas laborales, evitando a toda costa que se afecte la productividad.

f) No está permitido instalar y usar juegos en los computadores, debido que estos se deben usar como una herramienta de trabajo y no como forma de distracción.

g) No está permitido descargar música de ningún sitio de Internet, de cualquier otro formato existente, dado que ello constituye una a la violación al derecho de autor sobre ese tipo de obras grabadas o descargada libremente.

h) No está permitido descargar ni instalar software de Internet. El único personal autorizado para instalar cualquier tipo de software será los ATIs, supervisado por el Área de Sistemas y acorde a las políticas existentes.

5.3.2.2. Gestión de Intranet (PSI-3.2-02)

Objetivo	Garantizar el uso adecuado de Internet como herramienta fuente de información, investigación y comunicación del CICA
Alcance	Esta norma se aplica a todos los usuarios del CICA
Responsables	Jefes de área. ATIs. Todos los usuarios.

1) Gestión

a) El servicio de Internet debe ser utilizado para facilitar el cumplimiento de las funciones asignadas a los empleados del CICA.

b) Debe existir un procedimiento de administración de la intranet, en especial el mantenimiento y depuración de la información publicada, que garantice el buen uso de este y de las herramientas disponibles para su gestión.

c) La información de Intranet debe ser únicamente utilizada por el personal autorizado. Los usuarios no deben re-direccionar información que aparezca en Intranet a terceros sin autorización del CICA.

d) La información que se publique en la Intranet del CICA, debe contar con la aprobación del responsable de cada Área.

2) Seguridad

a) Deben existir los mecanismos de gestión y control apropiados para garantizar el adecuado uso de la Intranet, tales como Firewall, Proxy, DNS, Filtro de Contenidos, Anti-virus, antispam, anti-spyware, anti-phising, anti-malware y demás software para gestión de vulnerabilidades de redes, aprobados por el Área de Seguridad y avaladas por el CICA.

b) El material que se publique en la Intranet del CICA debe ser revisado previamente para confirmar la actualidad, oportunidad e importancia de la información y evitar que los programas o archivos incluyan virus. Así mismo, se debe evaluar posibles problemas operativos y de seguridad de acuerdo con las políticas establecidas.

3) Responsabilidades

a) Se debe hacer uso racional del servicio de Internet, y se considera como uso indebido cuando:

I. Atenta contra la integridad, veracidad y confidencialidad de la información del CICA.

II. Atenta contra la integridad de los sistemas y componentes de la plataforma tecnológica del CICA.

III. Reduce la productividad de los empleados del CICA.

IV. Pone en riesgo la disponibilidad de los recursos informáticos del CICA.

4) Restricciones

a) Está prohibida la publicación de material de pornografía y de cualquier otra índole que atente contra la integridad de los usuarios del CICA.
b) No está permitido publicar o usar juegos en redes internas de trabajo.
c) No está permitido publicar, transmitir, almacenar o copiar música desde ni hacia componentes de redes, unidades publicas o unidades internas del CICA.
d) No está permitido publicar, transmitir, almacenar o copiar software corporativo u otros.

5.3.2.3. Gestión de correo electrónico (PSI-3.2-03)

Objetivo	Evitar la propagación de correo basura, o cualquier tipo de virus a través del correo interno, prevenir proyectar una mala imagen pública del CICA, cuando se utilice el correo.
Alcance	Establecer las reglas que debe cumplir cualquier correo electrónico enviado desde una cuenta de correo del CICA.
Responsables	Jefes de área. ATIs. Todos los usuarios.

1) Gestión

a) Debe existir un protocolo de gestión y asignación de correos electrónicos.

b) Todos los empleados del CICA, tendrán correo electrónico personalizado el cual se implementará en la medida en que se disponga de computadores para tal fin.

c) Todas las direcciones de correo electrónico deben ser creadas usando el estándar establecido por el CICA y deben tener una cuota de almacenamiento máximo.

d) El correo del CICA, no se debe usar para la creación o distribución de cualquier mensaje corrupto u ofensivo, incluyendo comentarios ofensivos acerca de raza, genero, color del cabello,

discapacidades, edad, orientación sexual, pornografía, creencias o prácticas religiosas, creencias políticas o nacionalidad. Cualquier usuario que reciba mensajes de correo con este tipo de contenido desde cualquier cuenta del CICA debe reportar este asunto al Área de Seguridad.

e) Se debe eliminar todo el correo basura, cartas, cadenas o similares inmediatamente sin reenviarlo. Los usuarios del CICA no deben contar con ningún tipo de privacidad respecto de cualquier información que guarden, envíen o reciban en el sistema de correo de la Organización.

2) Seguridad

a) Debe existir una herramienta o mecanismo de encriptación establecido como estándar, para los mensajes de correo intercambiados con entes externos.

b) Se bebe realizar un análisis de virus, con la herramienta asignada para tal fin, de todos los archivos adjuntos que son enviados o recibidos por el correo electrónico.

c) Todo incidente de seguridad o desempeño del correo electrónico, debe ser notificado al Área de Sistemas, empleando los canales establecidos para tal fin.

3) Responsabilidades

a) El usuario responsable del buzón debe dar un trámite ágil al correo electrónico recibido (responder, eliminar, archivar mensajes en el disco duro local).

b) El sistema de correo electrónico debe ser utilizado únicamente para la transmisión de información relacionada con asuntos laborales del usuario y/o asuntos de interés común que incidan en la buena marcha y en el mejoramiento de la armonía laboral del CICA.

c) Los buzones de correo configurados son de uso exclusivo del usuario al que fue asignado y serán de su responsabilidad todos aquellos mensajes enviados en su nombre.

d) Es responsabilidad de los usuarios de correo electrónico mantener o archivar los mensajes enviados y/o recibidos para efectos de soportar ante terceros (internos o externos) la ejecución de operaciones o acciones.

e) Es responsabilidad de los usuarios de Correo Electrónico hacer limpieza / depuración a su buzón de correo.

f) Todos los mensajes que se envíen a través del correo electrónico deben estar enmarcados en normas mínimas de respeto.

4) Restricciones

a) Está prohibido Enviar cartas, cadenas o mensajes con bromas desde un correo del CICA, así como enviar alertas o correos masivos a menos que se tenga autorización del Área de Seguridad.

b) El correo electrónico no debe ser utilizado por terceros sin previa autorización.

c) Solo se permite el software cliente establecido como estándar para el servicio de correo en el CICA.

d) No está permitido la parametrización de los mensajes a enviar, que contengan fondos, imágenes o logos no corporativos.

e) Los usuarios de la Organización no deben utilizar versiones escaneadas de firmas hechas a mano para dar la impresión de que un mensaje de correo electrónico o cualquier otro tipo de

comunicación electrónica ha sido firmada por la persona que la envía.

f) No se debe abrir o revisar correo que tenga procedencia de remitentes desconocidos.

g) Como uso inapropiado del correo electrónico se considera:

I. Intentos de acceso y/o accesos no autorizados a otra cuenta de correo.

II. Transmisión de mensajes de correo con información sensible o confidencial a personas u organizaciones externas sin autorización.

III. Cadenas de mensajes que congestionen la red.

IV. Transmisión de mensajes obscenos.

V. Cualquier actividad no ética que afecte al CICA.

VI. Enviar correo a nombre de otra persona.

VII. Prestar el buzón de Correo a personas diferentes a las asignadas por el CICA.

5.4. INSTALACIONES

5.4.1. SEGURIDAD FÍSICA

5.4.1.1. Gestión de áreas seguras (PSI-4.1-01)

Objetivo	Establecer un control de acceso a las zonas restringidas y al Centro de Procesamiento de Datos del CICA.
Alcance	Las políticas se aplican para todas las zonas restringidas y para el CPD del CICA.
Responsables	Jefes de área. ATIs. Todos los usuarios.

1) Áreas seguras

a) Se consideran áreas seguras: las oficinas de la Secretaria, centro de procesamiento de datos del CICA, centro de procesamiento de datos compartido (RedIRIS, CICA, Junta de Andalucía), centros de cableado y centros eléctricos, centros de monitoreo / vigilancia, y demás que determine la Dirección.

b) Las áreas seguras deben ser discretas y ofrecer un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.

c) Se deben revisar y actualizar periódicamente los perfiles de acceso a las áreas protegidas.

d) Los materiales peligrosos o combustibles deben ser almacenados en lugares seguros a una distancia prudencial del área protegida

e) Debe existir un Plan de Evacuación en casos de siniestros de cualquier índole.

f) El ingreso para fines de aseo y mantenimiento de áreas seguras, se debe realizar con acompañamiento del responsable del área o un delegado por el mismo.

2) Control Accesos

a) Debe existir un protocolo de gestión de accesos físicos a las instalaciones y áreas de la organización, debidamente documentado y soportado, que garantice el registro de todo tipo de actividad de acceso hacia y desde las instalaciones.

b) El acceso a las oficinas de visitantes está permitido únicamente bajo acompañamiento de los empleados, con el fin de reducir riesgo de hurto a equipos portátiles, dispositivos periféricos u otros.

c) El acceso de visitantes, o terceros en horarios no laborales a las instalaciones del CICA debe estar supervisado.

d) Se debe registrar la fecha y horario del ingreso y egreso de los visitantes o terceros a las instalaciones del CICA.

e) Se deben registrar las actividades realizadas en las zonas restringidas por personal externo. Se debe anotar el nombre, fecha, hora entrada, hora salida y actividad, el personal que ingrese debe permanecer acompañado por personal del CICA.

f) Se debe registrar todo paquete, dispositivo u otro, con el fin de garantizar la entrada y salida de soportes del CICA.

3) Acceso al CPD

a) Ningún usuario ajeno al Área de Sistemas y Supercomputación o al Área de Redes y Seguridad debe ingresar al CPD, únicamente podrán acceder las personas autorizadas en caso obligatorio para efectos de mantenimiento, previa autorización por parte del Área de Sistemas.

b) El CPD debe permanecer cerrado y con mecanismos de control de acceso apropiados, debe mantener un registro que permita auditar todos los accesos, deben estar físicamente separadas de áreas administradas por terceros.

c) La configuración del CPD debe cumplir con los mínimos requerimientos de seguridad, adoptando estándares internacionales.

d) El equipamiento de sistemas de soporte para la recuperación de información perdida y los medios informáticos de resguardo deben estar situados a un sitio diferente al CPD, para evitar pérdidas y/o daños ocasionados por eventuales desastres en el sitio principal.

5.5. GESTIÓN DE CONTINUIDAD

5.5.1. COPIAS DE SEGURIDAD

5.5.1.1. Gestión de copias de seguridad (PSI-5.2-01)

Objetivo	Garantizar que toda la información almacenada en los componentes de la

	infraestructura tecnológica del CICA, se encuentre debidamente respaldada mitigando el riesgo de pérdida de la información.
Alcance	Esta norma aplica a todos los usuarios del Área de Sistemas del CICA.
Responsables	Jefes de área. ATIs. Todos los usuarios.

1) Gestión

a) Debe existir un procedimiento que determine actividades, periodicidad, responsables y mecanismos de almacenamiento de las copias de respaldo de todos los sistemas de información del CICA.

b) Debe existir una definición formal de las políticas y procedimientos de generación, retención y rotación de copias de respaldo.

c) Debe existir un Plan de Copias de Respaldo, y debe contemplar la generación de copias de respaldo de los sistemas operativos, los sistemas de información, las aplicaciones corporativas, acorde con los procedimientos establecidos en el Plan de contingencia y en los procedimientos diseñados para realizar dicha actividad.

d) Cada vez que se cambien los servidores o el Software, los procedimientos para realizar las Copias de Respaldo y el Plan de Contingencia deben ser actualizados.

e) Con el objetivo de garantizar la continuidad del negocio, se determina como de carácter obligatorio, la ejecución de políticas y procedimientos relacionados con copias de respaldo definidas por el CICA.

2) Generación

a) Debe existir un protocolo de generación de Copias de Respaldo por cada sistema operativo, sistema de información y aplicación corporativa, que contemple la definición de los tipos de copias, tipos y medios de almacenamiento, aplicación de respaldo, frecuencia de copia, plan de prueba, esquemas de seguridad y actividades de restauración.

b) Cada vez que se cambien los servidores o el Software, los procedimientos para realizar el Copias de Respaldo y el Plan de Contingencia deben ser actualizados.

c) Se deben realizar pruebas de los medios utilizados con el fin de asegurar su adecuado funcionamiento o descartarlos.

3) Almacenamiento y custodia

a) Deben usarse medios que permitan almacenar la información apropiadamente, no utilizar CD o DVD ya que dichos medios se degradan y la información se pierde.

b) Los medios deben ser almacenados en un sitio que posea las condiciones ambientales correctas (Temperatura y Humedad), el cual asegure el adecuado funcionamiento de los mismos.

c) Los medios deben contar con un periodo de vida (registro de fecha de inicio del uso de los mismos y una fecha de descarte).

d) Los medios descartados no se deben usar ya que existe el riesgo de pérdida de la información en ellos almacenada.

e) Todos los medios se deben mantener en un área restringida y bajo llave.

f) El acceso a los medios será autorizado únicamente al Área de Sistemas o al personal que sea autorizado por dicha área.

g) Los medios deben estar adecuadamente etiquetados de tal forma que sean fácilmente identificables.

4) Responsabilidades

a) La gestión de las copias de respaldo es responsabilidad del Área de Sistemas y la ejecución operativa del Ingeniero de Soporte designado.

b) La responsabilidad de verificar la realización de copias de respaldo de los servidores y de las estaciones de trabajo es del Área de Sistemas.

c) El almacenamiento de las copias de respaldo es responsabilidad del Área de Sistemas.

d) El Área de Sistemas debe garantizar la realización de las copias de respaldo acorde a la frecuencia y alcance identificados en el Análisis de Riesgos de la información.

5) Seguridad

a) Todas las copias de respaldo deben estar encriptadas.

b) El acceso al registro de ubicación y contenido de los medios debe estar restringido.

c) Se debe contar con un registro, el cual permita identificar la ubicación y el contenido de cada medio (con un número o un código).

5.5.2.CONTINGENCIA Y RECUPERACIÓN DE DESASTRES

5.5.2.1. Gestión de contingencias (PSI-5.3-01)

Objetivo	Regular las actividades a realizar ante situaciones de contingencia.
Alcance	Esta Política cubre todas las situaciones de contingencia que se pueden presentar, tales como: incendios, terremotos, inundaciones, tanto en el centro de procesamiento de datos, como en los diferentes sitios donde se resguardan equipos informáticos en todas las instalaciones del CICA.
Responsables	Jefes de área. ATIs. Todos los usuarios.

1) Gestión

a) Debe existir un BCP-Plan de Continuidad de Negocio, que a su vez involucre un Análisis de Riesgos, Plan de Contingencias, Plan de Recuperación de Desastres y Plan de Disponibilidad, con

el objetivo de garantizar la continuidad en el funcionamiento de los activos tecnológicos del CICA.

b) Debe existir un protocolo de acción y un cronograma de ejecución, pruebas y ajustes, por cada uno de los planes enunciados anteriormente.

c) Se entiende por Plan de Continuidad de Negocio todas las acciones administrativas y/o operacionales que tienden a garantizar la continuidad del negocio ante eventualidades externas o internas que atente contra el normal funcionamiento del CICA.

d) Se entiende por Análisis de Riesgos el estudio que se realiza por un ente interno y/o un ente externo, con el objetivo de identificar los riesgos existentes, la probabilidad de ocurrencia y su impacto, para finalmente determinar los controles que mitiguen los riesgos identificados.

e) Se entiende por Plan de Contingencia todas las acciones administrativas y/o operacionales que tienden a superar fallas, incidentes y eventos en general que interrumpan el normal funcionamiento de los activos tecnológicos del CICA.

f) Se entiende por Plan de Recuperación de Desastres todas las acciones administrativas y/o operacionales que tienden a restaurar todos los componentes afectados una vez se han presentado pérdidas materiales o físicas en eventos o situaciones catastróficas.

g) El plan de Contingencias debe permitir reaccionar ante eventos no esperados sea por efectos de la naturaleza o humanos (robo, sabotaje, terremoto, incendio, inundación, toma de las instalaciones del CICA, entre otros).

h) Se deben de establecer períodos de actualización, mantenimiento y pruebas del Plan de Continuidad del Negocio.

5.6. LICENCIAMIENTO

Todos los productos de Software que se utilicen deberán contar con su factura y licencia de uso respectiva; por lo que se promoverá la regularización o eliminación de los productos que no cuenten con el debido licenciamiento.

Se promoverá y propiciará que la adquisición de software de dominio público provenga de sitios oficiales y seguros.