

**MANUAL DE POLÍTICAS Y DIRECTRICES DE SEGURIDAD DE LA INFORMACIÓN**

**SIGCMA\_SGSI**

Versión 2

JULIO 2022

**Control de versiones**

|  |  |  |  |
| --- | --- | --- | --- |
| Versión | Fecha | Comentarios | Por |
| 1 | 22-12-2014 | Versión incial de politicas de seguridad de la informacion, teniendo como base los controles propuestos por la ISO/IEC 27002:2013. Aprobación acuerdo PSAA14-10279 de 2014 | CSJ |
| 2 | 28-07-2022 | Actualización de la estructura y politicas de seguridad de la informacion, ciberseguridad y protección de datos personales, teniendo como base la nueva versión de la ISO/IEC 27002:2022 | GPET |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**TABLA DE CONTENIDO**

[**0.** **INTRODUCCIÓN** 5](#_Toc110528068)

[**1.** **ALCANCE** 5](#_Toc110528069)

[**2.** **OBJETIVO GENERAL** 5](#_Toc110528070)

[**3.** **TÉRMINOS Y DEFINICIONES** 5](#_Toc110528071)

[**4.** **LINEAMIENTOS** 5](#_Toc110528072)

[**5.** **CLAUSULAS DE CONTROLES ORGANIZACIONALES** 6](#_Toc110528073)

[5.1. Política de Seguridad de la Información 6](#_Toc110528074)

[5.2. Entidad interna 6](#_Toc110528075)

[5.3. Identificación, clasificación y etiquetado de activos de información 7](#_Toc110528076)

[5.4. Uso aceptable de activos 8](#_Toc110528077)

[5.5. Política de Transferencia de información 9](#_Toc110528078)

[5.6. Política de control de acceso 10](#_Toc110528079)

[5.7. Gestión de acceso de usuarios 10](#_Toc110528080)

[5.8. Información de autenticación 11](#_Toc110528081)

[5.9. Inteligencia de amenazas 11](#_Toc110528082)

[5.10. Acceso a redes, sistemas y aplicaciones 12](#_Toc110528083)

[5.11. Política sobre el uso de servicios en la nube 12](#_Toc110528084)

[5.12. Política de la seguridad de la información en las relaciones con proveedores 13](#_Toc110528085)

[5.13. Planificación y preparación de la gestión de incidentes de seguridad de la información 14](#_Toc110528086)

[5.14. Política de Recolección de Evidencias 14](#_Toc110528087)

[5.15. Preparación de las TIC para la continuidad del negocio 15](#_Toc110528088)

[5.16. Identificación de la legislación aplicable y requisitos contractuales 16](#_Toc110528089)

[5.17. Derechos de propiedad intelectual 16](#_Toc110528090)

[5.18. Revisión independiente de la Seguridad de la Información 16](#_Toc110528091)

[5.19. Privacidad y Protección de la Información de Identificación Personal 17](#_Toc110528092)

[5.20. Procedimientos operativos documentados 17](#_Toc110528093)

[**6.** **CLAUSULAS DE CONTROLES DE PERSONAS** 18](#_Toc110528094)

[6.1. Selección de personal 18](#_Toc110528095)

[6.2. Términos y condiciones de empleo 18](#_Toc110528096)

[6.3. Terminación o cambio de responsabilidades laborales 19](#_Toc110528097)

[6.4. Concientización, educación y capacitación en seguridad de la información 19](#_Toc110528098)

[6.5. Acuerdos de confidencialidad o de no divulgación 20](#_Toc110528099)

[6.6. Política de teletrabajo 20](#_Toc110528100)

[6.7. Reportar debilidades y eventos de seguridad de la información 21](#_Toc110528101)

[**7.** **CLAUSULAS DE CONTROLES FÍSICOS** 22](#_Toc110528102)

[7.1. Perímetro de seguridad física 22](#_Toc110528103)

[7.2. Trabajar en áreas seguras 22](#_Toc110528104)

[7.3. Emplazamiento y protección de equipos 23](#_Toc110528105)

[7.4. Política de escritorio limpio y pantalla limpia 23](#_Toc110528106)

[7.5. Política de Gestión de Medios Extraíbles 24](#_Toc110528107)

[7.6. Utilidades de apoyo 24](#_Toc110528108)

[**8.** **CLAUSULAS DE CONTROLES TECNOLÓGICOS** 25](#_Toc110528109)

[8.1. Dispositivos de punto final de usuario 25](#_Toc110528110)

[8.2. Gestión de derechos de acceso privilegiado 26](#_Toc110528111)

[8.3. Acceso al código fuente 26](#_Toc110528112)

[8.4. Autenticación segura 27](#_Toc110528113)

[8.5. Gestión de la capacidad 27](#_Toc110528114)

[8.6. Protección contra códigos maliciosos 27](#_Toc110528115)

[8.7. Gestión de Vulnerabilidades Técnicas 28](#_Toc110528116)

[8.8. Sincronización de reloj 28](#_Toc110528117)

[8.9. Copias de respaldo 29](#_Toc110528118)

[8.10. Restricciones en la instalación de software 29](#_Toc110528119)

[8.11. Seguridad en redes 29](#_Toc110528120)

[8.12. Filtrado web 30](#_Toc110528121)

[8.13. Política sobre el uso de controles criptográficos 30](#_Toc110528122)

[8.14. Requisitos de seguridad de los sistemas de información 31](#_Toc110528123)

[8.15. Seguridad en los procesos de desarrollo y de soporte 32](#_Toc110528124)

[8.16. Directrices de seguridad para proyectos de desarrollo 32](#_Toc110528125)

[8.17. Directrices de seguridad para la especificación detallada de requerimientos 32](#_Toc110528126)

[8.18. Directrices de seguridad para el diseño de Sistemas 32](#_Toc110528127)

[8.19. Directrices de seguridad para la codificación y pruebas 33](#_Toc110528128)

[8.20. Actividades de seguimiento 35](#_Toc110528129)

# **INTRODUCCIÓN**

Hoy día se encuentra vigente en la Rama Judicial las políticas de seguridad formalizadas mediante el acuerdo PSAA14-10279 de 2014, las cuales no contemplan las amenazas y riesgos emergentes que enfrentamos debido a las nuevas circunstancias y tecnologías en uso a lo largo y ancho de las dependencias de la entidad. En el presente documento se ajustan y crean las políticas de seguridad de la información acordes con los riesgos identificados.

# **ALCANCE**

El presente manual contiene los lineamientos y las políticas de seguridad de la información que tienen como propósito garantizar la confidencialidad, integridad y disponibilidad de los activos de información gestionados por todos los procesos: estratégicos, misionales, de apoyo, y de evaluación de la Rama Judicial, razón por lo cual son de obligatorio cumplimiento por parte de todas las corporaciones, los servidores judiciales, contratistas, proveedores y partes interesadas que generen, accedan o utilicen información de la Entidad.

# **OBJETIVO GENERAL**

Establecer las políticas que regulan la seguridad de la información, ciberseguridad y protección de datos personales en la Rama Judicial y presentar en forma clara y coherente los elementos que deben conocer, acatar y cumplir todos los servidores judiciales, contratistas, proveedores y partes interesadas, con el fin de asegurar la confidencialidad, disponibilidad e integridad de la información de la Rama Judicial.

# **TÉRMINOS Y DEFINICIONES**

El glosario del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales para la Rama Judicial se encuentra unificado en el documento GLOSARIO del Sistema. Por favor consultar dicho documento.

# **LINEAMIENTOS**

Las políticas y directrices contenidas en este manual se encuentran organizadas de acuerdo con las cláusulas de control presentadas en el documento ISO/IEC 27002:2022.

Este Manual de Políticas y Directrices de Seguridad de la Información deberá ser revisado al menos una vez al año, durante las reuniones periódicas del Comité de Seguridad de la Información, donde serán aprobadas por la dirección, publicadas y comunicadas a los servidores judiciales, contratistas, proveedores y partes interesadas de la Rama Judicial.

# **CLAUSULAS DE CONTROLES ORGANIZACIONALES**

## Política de Seguridad de la Información

Directrices:

1. La Rama Judicial gestiona un Sistema de Gestión de Seguridad de la información que le permite minimizar los impactos en la Entidad por la materialización de riesgos de seguridad de la información y ciberseguridad, así como mantener un nivel aceptable de exposición al riesgo, garantizar la confidencialidad, la integridad y disponibilidad a lo largo del ciclo de vida de la información, crear un ambiente de cultura y conciencia de seguridad de la información y mantener un proceso de mejora continua de protección de la información. El Sistema de Gestión de Seguridad de la información de la Rama Judicial, incluye:

* Políticas, directrices y procedimientos en materia de seguridad de la información.
* Controles aplicables.
* Gestión de los riesgos basados en una metodología de análisis, evaluación y tratamiento.
* Un plan de cultura de seguridad de la información en los servidores judiciales, contratistas, proveedores y partes interesadas de la Rama Judicial.
* Reporte periódico de la gestión de eventos e incidentes de seguridad.
* Gestión de la mejora continua del SGSI.

1. Por estas razones la Alta Dirección se compromete a suministrar los recursos necesarios, como: tiempo, equipo humano competente, y recursos económicos para establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información de la Rama Judicial.
2. El incumplimiento de las políticas aquí relacionadas traerá consigo, las consecuencias legales, administrativas, disciplinarias, incluyendo lo establecido en la ley relacionadas con seguridad de la información, ciberseguridad y protección de datos personales, de acuerdo con a lo establecido en el proceso disciplinario de la Rama Judicial.

## Entidad interna

Directrices:

1. La Rama Judicial contará con una estructura para controlar el desarrollo, la implementación y operación del Sistema de Gestión de la Seguridad de la Información, promoviendo iniciativas de seguridad de la información que sean pertinentes a la estructura, tamaño, objeto social y actividades de la Entidad y contando con unas responsabilidades claramente asignadas y comunicadas a todos los niveles de la Entidad. Para lo anterior la Rama Judicial contará con:

* **Comité de Seguridad de la información:** el cual determina las estrategias para el desarrollo del Sistema de Gestión de Seguridad de la Información, garantizando que se cumplan los lineamientos y los objetivos establecidos. Ver: CSJ - Manual del SGSI, numeral 5.2.1 Comité de Seguridad de la Información
* **Oficial de Seguridad de la Información:** responsable de administrar, promover, orientar, mantener, evaluar y tratar proactivamente el Sistema de Gestión de Seguridad de la Información.

1. Se debe mantener y documentar los contactos con autoridades (Policía, bomberos, etc.), con el fin de contactar en caso de que se presente un incidente de seguridad de la información y se requiera de asesoría externa.
2. Se debe mantener contacto con grupos de interés especializados en seguridad y privacidad de la información, con el fin de compartir e intercambiar conocimientos, que permita la mejora continua del Sistema de Gestión de Seguridad de la Información.
3. Los proyectos que se desarrollen en la Rama Judicial deben contemplar la gestión de los riesgos de seguridad de la información asociados, lo cual incluye una identificación de los riesgos y la definición de la forma como serán tratados.
4. En cualquier caso, los proyectos desarrollados por la Rama Judicial deben estar alineados a las políticas de seguridad contenidas en el presente manual.

## Identificación, clasificación y etiquetado de activos de información

Directrices:

1. La Rama Judicial como propietario de los activos de información, mantendrá un inventario actualizado de estos y será responsabilidad de cada líder de proceso los activos de información a su cargo.
2. Los activos de información serán identificados y clasificados teniendo en cuenta los impactos que le pueden causar a la Rama Judicial por la pérdida de confidencialidad, integridad y disponibilidad. Así mismo serán clasificados de acuerdo con las leyes 1581 de 2012 y 1712 de 2014 (Ver Procedimiento identificación clasificación activos).
3. La información estará clasificada en: pública, uso interno, confidencial y sensible, la cual debe ser etiquetada por los responsables de la misma de acuerdo a lo establecido en el documento de clasificación de la información de la Entidad.
4. La Rama Judicial proveerá los recursos necesarios en la aplicación de controles para preservar la confidencialidad, integridad y disponibilidad de la información, de tal manera que permitan su correcto uso por parte de los servidores judiciales, contratistas, proveedores y partes interesadas que se encuentren autorizados y requieran de ella para la ejecución de sus actividades.
5. Todo servidor judicial o líder de proceso será responsable de realizar el etiquetado de la información al momento de la generación del activo o cuando reciba activos sin etiquetar.
6. Todo servidor judicial o líder de proceso será responsable de realizar la valoración de activos y contenedores de información siguiendo la metodología[[1]](#footnote-2) junto con el Oficial de Seguridad de la Información.
7. Todo servidor judicial deberá prevenir los riesgos a los que está expuesta la información, evitando la copia, divulgación o destrucción física o digital de la información sin previa autorización.
8. Todo servidor judicial deberá realizar la entrega formal de todos los activos de información físicos y electrónicos en el proceso de desvinculación.
9. El Oficial de Seguridad de Información coordinará la revisión periódica del inventario de activos de información para validar su clasificación y etiquetado durante el ciclo de vida de los activos de información, por lo menos una vez al año.
10. En caso de requerirse la eliminación de activos de información, los responsables de los activos realizarán una disposición segura del activo de información de acuerdo con cada caso, dejando registro de evidencia y notificando al Oficial de Seguridad de la Información.

## Uso aceptable de activos

Directrices:

Todo servidor judicial, contratista, proveedor y/o parte interesada de la Rama Judicial tendrá a su disposición el uso de activos de información y recursos tecnológicos que los contienen, de acuerdo a las funciones laborales que así lo requieran. Para su uso, acepta y se acoge las Políticas Seguridad de la información y las disposiciones relacionadas a continuación:

1. Toda cuenta de usuario es de uso personal e intransferible. El usuario será responsable de todas las acciones o transacciones efectuadas con su cuenta de usuario.
2. Los recursos se deben usar estrictamente para fines laborales. El servidor judicial no podrá hacer uso de estos recursos para transmitir, almacenar y/o procesar información que atente contra la propiedad intelectual, los derechos de autor o derechos de protección de datos personales.
3. Los servidores judiciales no deben realizar actividades que puedan degradar el desempeño de los recursos tecnológicos y, en consecuencia, generar posibles pérdidas o daños en la información.
4. Los usuarios del correo electrónico tienen prohibido el envío de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para servidores judiciales, contratistas, proveedores y/o partes interesadas.
5. No está permitido el uso de cuentas personales para el intercambio de información propia de la Rama Judicial o de alguno de sus usuarios.
6. Está prohibido acceder a páginas con contenido pornográfico o similares que degraden la condición humana y resulten ofensivas para servidores judiciales, contratistas, proveedores y/o partes interesadas. Así mismo, está prohibido acceder a juegos en línea, uso de redes sociales con fines diferentes a los laborales y queda prohibido el uso de repositorios personales como: Dropbox, Google Drive, One Drive, para almacenar información corporativa a menos que sea autorizado por el jefe directo.
7. Toda la información procesada y almacenada en los recursos de la Rama Judicial, está asociada a la labor que desempeñan los servidores judiciales en desarrollo de sus funciones y cargos, por lo tanto, esta información es de carácter corporativo. En este sentido, los servidores judiciales deben abstenerse de almacenar o procesar información de carácter personal en los recursos provistos por la Rama Judicial.
8. Los usuarios no podrán copiar o distribuir software, cambiar las configuraciones de los recursos tecnológicos y deberán utilizar únicamente los programas y equipos autorizados por la Unidad Informática, única dependencia autorizada para instalar o configurar software y equipos bajo licenciamiento. La descarga, instalación o uso de software ilegal o sin licenciar será considerada como una violación a las políticas de seguridad de la información de la Rama Judicial (Ver procedimiento control de software).
9. Los servidores judiciales o contratistas deben devolver todos los activos de la Rama Judicial que estén en su poder al cambiar o terminar su empleo, contrato o acuerdo. Los activos pueden incluir computadores portátiles, de escritorio, teléfonos inteligentes, dispositivos de almacenamiento, entre otros.

## Política de Transferencia de información

Directrices:

1. Se garantizará la protección de la información confidencial y sensible de la Rama Judicial que sea transmitida o recibida entre servidores judiciales, contratistas, proveedores y partes interesadas, asegurando la conservación de las propiedades de confidencialidad, integridad y disponibilidad.
2. Se deberá implementar las herramientas necesarias para asegurar la transferencia de información al interior y exterior de la Rama Judicial, contra interceptación, copiado, modificación y destrucción (Ver Procedimiento Controles Criptográficos).
3. Cualquier intercambio de información con contratistas, proveedores y partes interesadas debe quedar formalizado en un acuerdo de intercambio de información o cláusula del contrato, determinando las condiciones y controles de seguridad que aseguren dicho intercambio de información. Las condiciones y controles deben ser validadas por el Oficial de Seguridad de Información.
4. En caso de que una autoridad, ente regulador, de control, de vigilancia o judicial requiera la entrega de información, esta se llevará a cabo con la autorización de la alta dirección.
5. La información confidencial transmitida por correo electrónico deberá protegerse mediante archivos Zip con contraseña, y la contraseña se debe comunicar por un canal de comunicación diferente.
6. Los mensajes de correo electrónico deben ir acompañados del siguiente *disclaimer* enseguida de la firma estándar establecida: “*Este mensaje y sus adjuntos se dirigen exclusivamente a su(s) destinatario(s), puede contener información confidencial o sensible que es para el uso exclusivo de la persona o entidad de destino. Si Usted no es el destinatario indicado, queda notificado de que la lectura, utilización, divulgación y/o copia sin autorización expresa de la Rama Judicial está prohibida en virtud de la legislación vigente. Si ha recibido este mensaje por error, le rogamos que nos lo comunique inmediatamente por esta misma vía o al correo* [*protecciondatospersonales@deaj.ramajudicial.gov.co*](mailto:protecciondatospersonales@deaj.ramajudicial.gov.co) *y que proceda a su eliminación inmediata*”.

## Política de control de acceso

Directrices:

1. La unidad de informática debe suministrar y garantizar a los usuarios el cambio de contraseña para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados según su perfil y rol. Las credenciales de acceso son de uso personal e intransferible (Ver Procedimiento Gestión de Usuarios).
2. Las conexiones remotas a los recursos de red y a los recursos de las áreas usuarias, seccionales, altas cortes, entre otras, se debe establecer mediante conexión VPN, la cual debe ser aprobada, registrada y monitoreada por la Unidad Informática de la Rama Judicial y notificada a la Oficina de Seguridad de la Información (Ver Procedimiento Conexión a VPN).
3. La unidad de informática debe asegurar que las redes inalámbricas de la Entidad cuenten con métodos de autenticación que eviten accesos no autorizados.
4. La unidad de informática debe realizar el cambio de contraseña de la red inalámbrica de la Entidad de manera periódica mínimo (3) veces al año.
5. La unidad de informática debe revisar que los equipos personales de los servidores judiciales, contratistas, proveedores o partes interesadas que se conecten a la red de datos de la Rama Judicial cuenten con sistema operativo licenciado y antivirus y únicamente podrán realizar las tareas para las que fueron autorizados.

## Gestión de acceso de usuarios

Directrices:

1. La unidad de informática debe definir un procedimiento que contemple la creación, actualización, activación e inactivación de cuentas de usuario, alineados con lo reportado por parte de la Unidad de Recursos Humanos (Ver Procedimiento Gestión de Usuarios).
2. La unidad de informática suministrará los usuarios y contraseñas temporales, una vez el usuario ingrese deberá hacer cambio de la contraseña.
3. La unidad de informática sólo otorgará a los usuarios, los accesos solicitados y autorizados por el jefe inmediato (Ver Procedimiento control de acceso basado en roles).
4. Los usuarios creados no deben tener permisos de administrador. Sólo se otorgan los privilegios de administración de recursos tecnológicos, servicios de red, sistemas operativos y sistemas de información a aquellos usuarios que cumplan dichas actividades.
5. El usuario y la contraseña asignados para el acceso a los diferentes servicios tecnológicos es personal e intransferible. Cualquier actividad que se realice con el usuario y clave será responsabilidad del servidor judicial, contratista, proveedor o parte interesada.
6. La Unidad Informática debe garantizar que los usuarios, realicen el cambio de contraseña de acceso a los servicios tecnológicos, cada vez que sea requerido.
7. La Unidad Informática debe mantener un listado actualizado de las cuentas de administración de los recursos tecnológicos.
8. La contraseña para la autenticación se debe suministrar a los usuarios de manera segura y el sistema debe solicitar el cambio inmediato de la misma al ingresar.

## Información de autenticación

Directrices:

1. La Unidad Informática debe garantizar que para el ingreso a los servicios tecnológicos de la Entidad las contraseñas no sean visibles en texto claro.
2. La complejidad de la contraseña debe ser mínimo de 10 caracteres, debe combinar mayúsculas, minúsculas, números y caracteres especiales.
3. Las contraseñas no deberán ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal.
4. No se deberán repetir las últimas 3 contraseñas utilizadas en cada sistema o servicio tecnológico.
5. Las contraseñas deben cambiarse obligatoriamente cada 60 días, de lo contrario la contraseña caducará y obligará su cambio. Si el sistema no pide cambio de manera automática el usuario deberá realizarlo como parte de sus obligaciones.
6. Después de tres (3) intentos fallidos de ingreso el usuario se bloquea de manera inmediata y deberá esperar un tiempo de cinco (5) minutos para volver a intentar, o solicitar el desbloqueo a la Unidad Informática.
7. En caso de presentar anomalías en el uso de la cuenta, el servidor judicial debe solicitar el cambio inmediato de su contraseña.
8. Las contraseñas no se deben registrar en papel, correo electrónico o archivos digitales, a menos que se puedan almacenar de forma segura y el método de almacenamiento debe estar aprobado por el Oficial de seguridad de la información.
9. Los administradores de los servicios tecnológicos deben cumplir con los lineamientos de contraseñas seguras indicados.
10. Los administradores de los servicios tecnológicos o sistemas de información deben de entregar de manera adecuada las credenciales de acceso (Ver Procedimiento Gestión de Usuarios).

## Inteligencia de amenazas

Directrices:

1. La Unidad Informática con el apoyo de la Oficina de Seguridad de la Información debe asegurarse de recopilar y analizar la información sobre amenazas existentes o emergentes para facilitar acciones informadas para que reducir el impacto de dichas amenazas.
2. Las actividades de inteligencia de amenazas deben incluir:
   * Establecer objetivos para la producción de inteligencia sobre amenazas.
   * Identificar, examinar y seleccionar fuentes de información internas y externas que sean necesarias y apropiadas para proporcionar la información requerida para la producción de inteligencia de amenazas.
   * Recopilar información de fuentes seleccionadas, que pueden ser internas y externas.
   * Procesar la información recopilada para prepararla para el análisis (por ejemplo, traduciendo, formateando o corroborando la información);
   * Analizar la información para comprender cómo se relaciona y es significativa para la organización.
   * Comunicar y compartirlo con personas relevantes en un formato que pueda ser entendido.

## Acceso a redes, sistemas y aplicaciones

Directrices:

1. Los líderes de los procesos y dueños de los sistemas de información deben aprobar la creación, modificación o desactivación de cuentas de usuario, roles y perfiles en sistemas de información, aplicativos y servicios, acogiéndose al procedimiento establecido para este fin (Ver Procedimiento control de acceso basado en roles).
2. La Unidad Informática junto con la fábrica de software y el área usuaria suministrará y gestionará los accesos a sus ambientes de desarrollo, pruebas o producción y comunicará de los cambios al Grupo de Proyectos Especiales de Tecnología de la Rama Judicial.
3. La Unidad Informática debe velar por que los servicios tecnológicos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico, teniendo en cuenta la matriz de roles y perfiles para cada sistema de información.
4. Mientras el sistema o servicio tecnológico así lo permita, se deberá implementar autenticación por múltiple factor.
5. El administrador del sistema debe revisar los usuarios activos en el sistema, de acuerdo con la matriz de roles y perfiles definida.
6. El repositorio autorizado para el almacenamiento de códigos fuente en la Rama Judicial es GitHub.

## Política sobre el uso de servicios en la nube

Directrices:

1. El Oficial de Seguridad de la Información apoyará a La Rama Judicial, como cliente de los servicios en la nube y los proveedores que actúan como prestadores de los servicios en la nube, para el establecimiento de responsabilidades compartidas para la seguridad de la información debidamente definidas e implementas. Como mínimo se debe definir:
   * Todos los requisitos de seguridad de la información relevantes asociados con el uso de servicios en la nube (Ver Procedimiento tratamiento seguridad en los acuerdos con los proveedores).
   * Criterios de selección y alcance de servicios en la nube.
   * Funciones y responsabilidades relacionadas con el uso y gestión de servicios en la nube y los controles respectivos.
   * Procedimientos de manejo de incidentes que se originen por el uso de servicios en la nube (Ver Procedimiento Gestión de Incidentes).
   * Procesar y almacenar la información confidencial de la organización en ubicaciones aprobadas (país o jurisdicción geográfica particular).
   * Monitoreo de los servicios en la nube.
   * Realización de copias de seguridad de los datos y la información de la configuración de los servicios en la nube.
   * Reglas para el control de los cambios realizados a la infraestructura técnica que puedan afectar la oferta de servicios en la nube (Ver Procedimiento Control de Cambios).

## Política de la seguridad de la información en las relaciones con proveedores

Directrices:

1. La Rama Judicial debe establecer los criterios para la selección de proveedores y terceros, relativos a la experiencia, reputación, capacidad, adecuadas a las necesidades de la Entidad y del bien o servicio a adquirir.
2. La Rama Judicial debe llevar a cabo análisis de riesgos de seguridad de la información al proveedor y/o tercero para establecer los criterios de acceso a los activos de información de la Entidad, a los sistemas de información, aplicativos, redes, etc., así mismo deberá definir los requisitos de seguridad para procesar, almacenar, comunicar o suministrar información y por último deberá definir los planes o acciones de tratamiento para prevenir la materialización de los riesgos identificados.
3. Los acuerdos con los proveedores y terceros deben ser formalizados antes del inicio de las actividades contractuales (Ver Procedimiento tratamiento seguridad en los acuerdos con los proveedores).
4. La Rama Judicial debe definir como mecanismo de control en las relaciones contractuales un acuerdo de confidencialidad sobre la información conocida bien sea por acceso físico o lógico y/o que haya sido entregada directamente por la Rama Judicial en el desarrollo de las actividades, con el fin de prevenir los riesgos de divulgación de información a la que tengan acceso, e incluir cláusulas que indiquen que dichos proveedores o terceros no están autorizados para utilizar los recursos de información, tecnología y conexión de red de la Entidad para propósitos diferentes a los necesarios para el cumplimiento del objeto contractual suscrito.
5. Los proveedores o terceros no están autorizados a ejecutar ningún cambio sobre los recursos tecnológicos o la desactivación de controles de seguridad, sin contar con la autorización formal de la Rama Judicial.
6. Los proveedores o terceros que acceden a la gestión, transformación o transmisión de la información de la Rama Judicial, deben conocer, aceptar y cumplir las políticas de seguridad de la información definidas.
7. la Rama Judicial realizará revisiones periódicas para verificar el cumplimiento de los acuerdos establecidos entre las partes.

## Planificación y preparación de la gestión de incidentes de seguridad de la información

Directrices:

1. La Rama Judicial debe asegurar que los eventos o incidentes de seguridad que se presenten con los activos de información, contenedores y recursos tecnológicos de información sean comunicados y atendidos oportunamente, empleando el procedimiento definido.
2. Todo servidor judicial, contratista, proveedor o parte interesada de la Rama Judicial debe reportar al Oficial de Seguridad de la Información en el menor tiempo posible eventos o incidentes que afecten a la confidencialidad, integridad o disponibilidad de la información, así como la violación a las políticas de seguridad.
3. El Oficial de Seguridad de la Información estará encargado de catalogar los incidentes según el procedimiento definido asegurando una respuesta rápida y eficiente.
4. El Oficial de Seguridad de la Información deberá investigar y proponer la solución más efectiva a los incidentes notificados, implementando las acciones necesarias para prevenir su reincidencia.
5. El Oficial de Seguridad de la Información deberá escalar los incidentes de acuerdo con la criticidad del mismo, manteniendo registro del proceso de investigación y preservando la evidencia que sea recolectada como probatoria en procesos legales.
6. El Oficial de Seguridad de la Información debe contar con una base de datos de los incidentes y eventos presentados que permita identificar los incidentes recurrentes o de alto impacto, al igual que una base de conocimiento con la información de la evaluación y la solución de cada caso que permita tomar acciones para reducir su tiempo de respuesta.
7. El Oficial de Seguridad de la Información documentará las lecciones aprendidas al término del análisis y solución de incidentes de seguridad de la información, estos deben ser socializados a los interesados conservando la respectiva confidencialidad (Ver Procedimiento Gestión de Incidentes).
8. Los servidores judiciales, contratistas, proveedores o partes interesadas que se encuentren responsables del incidente investigado, asumirán las consecuencias legales, administrativas, disciplinarias, incluyendo lo establecido en la ley del país en el que se encuentre, relacionadas con seguridad de la información y protección de datos personales, y de acuerdo con lo establecido en el proceso disciplinario de la Rama Judicial.

## Política de Recolección de Evidencias

Directrices:

1. la Rama Judicial establecerá un procedimiento de recolección de evidencia digital, que aplique una vez se ha identificado un incidente de seguridad de la información con el fin de realizar investigaciones de informática forense que deriven en acciones legales o investigaciones disciplinarias (Ver Procedimiento Gestión de Incidentes).
2. El Oficial de Seguridad de Información será el encargado de coordinar las actividades necesarias para la recolección de evidencia digital y de acuerdo con las circunstancias realizar el contacto con proveedores externos.
3. Deberán mantenerse los contactos apropiados con autoridades pertinentes para atender emergencias y recolectar evidencia de manera técnica, tales como el ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia) o CCP (CAI Virtual de la Policía Nacional).

## Preparación de las TIC para la continuidad del negocio

Directrices:

1. La Oficina de Seguridad de la Información deberá conocer el Plan de Continuidad para la recuperación de los servicios de la Oficina y mantenerlo revisado y actualizado (Ver Plan de Continuidad de la OSI).
2. La Rama Judicial deberá determinar los requisitos para adaptar los controles de seguridad de la información durante una interrupción de la operación.
3. La Rama Judicial deberá contar con un Plan de Continuidad del Negocio que garantice la recuperación de los procesos y sistemas de información más críticos.
4. Estos planes deben incluir las condiciones de seguridad de la información necesarias y suficientes en las etapas de recuperación y retorno a la normalidad.
5. La Rama Judicial deberá implementar y mantener controles de seguridad de la información, sistemas y herramientas de apoyo dentro de los planes de continuidad del negocio y continuidad de las TIC.
6. Los requisitos de continuidad de las TIC son el resultado del análisis de impacto empresarial (BIA) y deberá utilizar criterios de impacto para evaluar los impactos a lo largo del tiempo que resultan de la interrupción de las actividades comerciales que entregan productos y servicios.
7. La magnitud y la duración del impacto resultante deben usarse para identificar actividades y recursos prioritarios a los que se les debe asignar un objetivo de tiempo de recuperación (RTO).
8. El BIA relacionado con los servicios de TIC se puede ampliar para definir los requisitos de rendimiento y capacidad de los sistemas de TIC y los objetivos de punto de recuperación (RPO) de la información necesaria para respaldar las actividades durante la interrupción.
9. Con base en los resultados del BIA y la evaluación de riesgos relacionados con los servicios de TIC, la organización debe identificar y seleccionar estrategias de continuidad de las TIC que consideren opciones para antes, durante y después de la interrupción.
10. Se deberán llevar a cabo pruebas periódicas al Plan de Continuidad del Negocio, y se deberá documentar los resultados de dichas pruebas.
11. La Rama Judicial cuenta con recursos en la nube autorizados, como: Office 365, Azure DevOps, GitHub, etc., los cuales garantizan alta disponibilidad de la información allí almacenada, además se tiene permitido el trabajo para todos los servidores judiciales.

## Identificación de la legislación aplicable y requisitos contractuales

Directrices:

1. La Rama Judicial a través del Oficial de Seguridad de la Información, se asegurará hacer la continua revisión, identificación, documentación y cumplimiento de las disposiciones legales y requisitos aplicables en materia de seguridad de la información aplicables a la Entidad, con el fin de mitigar riesgos ocasionados por incumplimientos legales.
2. Se deberá identificar los requisitos contractuales relacionados con la seguridad de la información establecidos en contratos con clientes, contratos con proveedores y contratos de seguros.
3. Se deberá tener en cuenta el cumplimiento de los acuerdos, leyes y reglamentos pertinentes relacionados con la implementación y uso de la criptografía (Ver Política sobre el uso de controles criptográficos).

## Derechos de propiedad intelectual

Directrices:

1. La Rama Judicial velará porque el software instalado en los recursos tecnológicos cumpla con todos los requerimientos legales y de licenciamiento aplicable referente a derechos de autor y propiedad intelectual, así como propenderá por el cumplimiento por parte de servidores judiciales, contratistas, proveedores y partes interesadas, que hagan uso de los recursos tecnológicos.
2. La Unidad Informática deberá garantizar que todo el software esté protegido por derechos de autor y posea su licencia de uso, o en su defecto sea software de libre distribución y uso, para lo cual contará con un inventario del software permitido en la Entidad e implementará controles para la instalación de software autorizado únicamente (Ver procedimiento control de software).
3. Los servidores de la Rama Judicial deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software y la reproducción no autorizada es una violación a la ley.

## Revisión independiente de la Seguridad de la Información

Directrices:

1. El Comité de Seguridad de la Información verificará el cumplimiento de políticas, procedimientos, objetivos e implementación de controles de seguridad de información definidos para la Rama Judicial, a través de los resultados de las auditorias planificadas, los seguimientos periódicos y los resultados de las métricas establecidas, con la finalidad de abordar iniciativas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de los activos de información.

## Privacidad y Protección de la Información de Identificación Personal

Directrices:

1. La Rama Judicial velará por la protección de los datos personales dando cumplimiento a las disposiciones establecidas en la ley 1581 de 2012 y sus decretos reglamentarios, estableciendo los controles necesarios para asegurar la información que la Entidad conozca y almacene de sus servidores judiciales, contratistas, proveedores y partes interesadas, y velará porque dicha información únicamente sea utilizada para las funciones propias de la Entidad y no sea publicada, revelada o entregada a terceras partes sin autorización.
2. Todo servidor judicial, contratista, proveedor o parte interesada que administre datos personales, deberá conservar estricta confidencialidad de los mismos.
3. La responsabilidad y confidencialidad sobre datos personales, debe quedar explicita y aceptada por los servidores judiciales en un acuerdo de confidencialidad o cláusula del contrato al momento de iniciar alguna relación contractual.
4. Los responsables de los recursos tecnológicos deberán implementar los mecanismos apropiados sobre los sistemas, para el control de los datos personales que permitan conservar su confidencialidad e integridad.
5. Se deberá contar con los procedimientos adecuados para la recolección, almacenamiento, uso, circulación y supresión o disposición final de la información personal incluyendo los requisitos para obtener la autorización de los titulares, la atención de peticiones de titulares para el acceso, actualización y corrección de datos personales, la conservación y eliminación de información personal, así como para dar cumplimiento a las obligaciones frente a la Superintendencia de Industria y Comercio - SIC.

## Procedimientos operativos documentados

Directrices:

1. La Unidad Informática debe documentar y mantener actualizados todos sus procedimientos operativos para garantizar la disponibilidad, integridad y confidencialidad de la información.
2. La Unidad Informática debe establecer un procedimiento que permita asegurar la gestión de cambios a nivel de sistemas de información, aplicativos y servicios tecnológicos para que dichos cambios sean llevados a cabo, teniendo en cuenta los impactos y que defina claramente los responsables y las actividades para retornar el último punto bueno conocido (*rollback*) de los mismos (Ver Procedimiento Control de Cambios).
3. La Unidad Informática y el responsable de seguridad de la información deben evaluar, aprobar o negar la implementación de los cambios requeridos, teniendo en cuenta, los posibles riesgos que se puedan presentar.
4. Los responsables de los sistemas de información y de los servicios tecnológicos deben gestionar la capacidad, llevar a cabo proyecciones de crecimiento y alertar cuando dichas capacidades estén llegando a los límites establecidos (Ver Procedimiento Gestión de Capacidad).
5. El responsable de la unidad informática debe suministrar y gestionar los accesos a sus ambientes de desarrollo, pruebas o producción a la fábrica de software y/o a los proveedores que realizan dichas actividades. Así mismo, la Rama Judicial debe proveer los recursos necesarios para implementar controles que permitan la separación de sus ambientes de desarrollo, pruebas y producción (Ver Procedimiento Separación de Ambientes).

# **CLAUSULAS DE CONTROLES DE PERSONAS**

## Selección de personal

Directrices:

1. La Unidad de Recursos Humanos deberá incluir en el proceso de selección y contratación de servidores judiciales la verificación de antecedentes ante las siguientes entidades: Registraduría Nacional del Estado Civil, Policía Nacional de Colombia, Policía Judicial, Fiscalía General de la Nación, Contraloría General de la República, Procuraduría General de la Nación, RUNT, Boletín De Deudores Morosos del Estado - BDME, Interpol - Entidad Internacional de Policía Criminal, Lista Clinton, Lista OFAC, Entidad de Naciones Unidas – ONU, Ventanilla Única de Movilidad, Demandas Laborales, lo anterior con el fin de confirmar la veracidad de la información suministrada y de esta forma validar la idoneidad y confiabilidad del recurso humano antes de su vinculación.
2. De acuerdo con los requerimientos de las áreas se llevará a cabo el estudio de seguridad del personal a ser contratado.
3. La Unidad de recursos humanos deberá establecer mecanismos o controles necesarios para proteger la confidencialidad y reserva de la información contenida en las historias laborales y expedientes contractuales.
4. Todo servidor judicial debe firmar cláusulas en las que se establezcan un acuerdo de confidencialidad y no divulgación de la información confidencial de la Rama Judicial, lo cual deberá reposar en el expediente contractual del servidor judicial.
5. La Unidad de Recursos Humanos, garantizará que al momento de la vinculación todo servidor judicial acepta el cumplimiento del Manual de Políticas de Seguridad de la Información, así mismo deberá firmar la autorización para el tratamiento de los datos personales según lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios.

## Términos y condiciones de empleo

1. La Unidad de recursos humanos deberá garantizar la capacitación y sensibilización sobre las políticas de seguridad de la información a todo servidor judicial durante el inicio de sus actividades en la Entidad.
2. El Oficial de seguridad de la información debe evaluar que los servidores judiciales hayan entendido las políticas de seguridad de la información socializadas durante el inicio de sus actividades en la Entidad.
3. El servidor judicial deberá declarar en un documento firmado que leyó, entendió y se compromete a aplicar las políticas de seguridad de la información de la Rama Judicial.
4. Es responsabilidad del servidor judicial informar los incidentes de seguridad de la información que observe al responsable de seguridad de la información.
5. La Unidad de Recursos Humanos deberá contar con un proceso disciplinario formalmente establecido, para emprender acciones contra servidores judiciales que hayan cometido una violación a la seguridad de la información, el cual debe ser de conocimiento de los servidores judiciales de la Rama Judicial.
6. En caso de ausencias temporales de servidores judiciales debido a vacaciones o licencias, la Unidad de Recursos Humanos deberá notificar al responsable de la Unidad Informática para que sean desactivados los accesos físicos, tecnológicos y de sistemas de información que tenga autorizados el servidor judicial.
7. En caso de cambios de labor, la Unidad de Recursos Humanos deberá notificar al responsable de la Unidad Informática para que sean actualizados de acuerdo a las nuevas funciones del servidor judicial los accesos físicos, tecnológicos y de sistemas de información a los cuales tenga derecho. Es responsabilidad del jefe inmediato solicitar los accesos requeridos para el desarrollo de las nuevas funciones.

## Terminación o cambio de responsabilidades laborales

1. La Unidad de recursos humanos, deberá informar inmediatamente a la unidad informática sobre la desvinculación de los servidores judiciales de la Rama Judicial para que sean retirados los accesos físicos, tecnológicos y de sistemas de información a los cuales tenga derecho el servidor judicial.
2. Es responsabilidad del servidor judicial realizar la entrega de la información propia de la Rama Judicial a la que tenga acceso y certificar la eliminación de la misma de los dispositivos personales.
3. Se debe solicitar la devolución de los elementos asignados como: carné, equipo de cómputo, etc.

## Concientización, educación y capacitación en seguridad de la información

Directrices:

1. La Unidad de Recursos Humanos destinar los recursos suficientes y a través del responsable de seguridad de la información, Grupo de proyectos especiales - GPET, incluirá en el plan de capacitación de la Entidad campañas de concienciación o sensibilización sobre políticas y procedimientos, para lograr el entendimiento y toma de conciencia en seguridad de información y de esta manera, disminuir vulnerabilidades y amenazas relacionadas con el recurso humano.
2. Los servidores judiciales de la Rama Judicial demostrarán su compromiso con el Sistema de Gestión de Seguridad de la Información, por medio de la asistencia obligatoria a las campañas de concienciación o sensibilización cuando estas tengan lugar.
3. El Oficial de Seguridad de la Información realizará la revisión de los resultados de las evaluaciones de las capacitaciones en seguridad de la información, para identificar oportunidades de mejora.
4. La Unidad de Recursos Humanos destinará los recursos suficientes y a través del Oficial de Seguridad de la Información, se asegurará que se realizan procesos de sensibilización, concientización a contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Rama Judicial según las necesidades identificadas en la evaluación de riesgos.

## Acuerdos de confidencialidad o de no divulgación

Directrices:

1. Es obligación de todo servidor judicial, contratista, proveedor o parte interesada como parte del contrato que se suscribe con la Rama Judicial firmar el acuerdo de confidencialidad y no divulgación, y es su deber entender, aceptar y generar un compromiso con el cumplimiento de las disposiciones contenidas en dicho acuerdo.
2. Todo servidor judicial, contratista, proveedor o parte interesada no debe participar en acciones como comentarios, publicaciones o imágenes en chat, redes sociales, sitios web, correos electrónicos, mensajería instantánea, medios de comunicación u otros, que dañen, difamen o afecten la reserva de la información o la imagen de la Rama Judicial.
3. La responsabilidad y confidencialidad sobre datos personales a las que tenga acceso todo servidor judicial, contratista, proveedor o parte interesada, debe quedar explicita y aceptada en un documento de acuerdo de confidencialidad o cláusula del contrato al momento de iniciar alguna relación contractual.

## Política de teletrabajo

Directrices:

1. El trabajo remoto está permitido en la Rama Judicial para sus servidores judiciales.
2. La Rama Judicial se compromete a entregar un auxilio de Internet para sus servidores judiciales.
3. La Rama Judicial deberá garantizar la doble autenticación en los accesos remotos a los sistemas de información, aplicativos y servicios tecnológicos de la Entidad.
4. El servidor judicial solo puede acceder a los sistemas de información, aplicativos y servicios que le han sido aprobados en teletrabajo y en el horario laboral acordado por la Rama Judicial.
5. Los servidores de la Rama Judicial se conectarán a los ambientes de las seccionales mediante los mecanismos definidos por ellos.
6. Toda información gestionada y que sea accedida remotamente por el servidor judicial debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales.
7. Solo se podrá hacer uso de los repositorios dispuestos por la Rama Judicial. No está permitido el almacenamiento de información en el equipo.
8. Está prohibido instalar programas o software en los equipos suministrados por la Rama Judicial. La Unidad informática es la única autorizada para instalar o configurar software y equipos bajo licenciamiento.
9. El servidor judicial es responsable por el equipo de cómputo asignado y por los daños ocasionados por el mal uso de los mismos.
10. Es responsabilidad del servidor judicial salvaguardar la información contenida en los diferentes recursos de información a los cuales accede, evitando compartir el acceso a dichos recursos con personas ajenas a la Rama Judicial o personas no autorizadas.
11. Está prohibido que el servidor judicial haga uso del equipo de cómputo asignado en sitios públicos o diferentes a los autorizados por la Rama Judicial.
12. El Oficial de seguridad de la información quien designe, verificará periódicamente el cumplimiento de las condiciones técnicas y de seguridad aquí establecidas, para los teletrabajadores que se encuentren activos.

## Reportar debilidades y eventos de seguridad de la información

Directrices:

1. Todos los servidores judiciales y contratistas deben ser conscientes de su responsabilidad de informar los eventos de seguridad de la información lo más rápido posible para prevenir o minimizar el efecto de los incidentes de seguridad de la información.
2. También deben conocer el procedimiento para informar eventos de seguridad de la información y el punto de contacto al que se deben informar los eventos. El mecanismo de presentación de informes debe ser lo más fácil, accesible y disponible posible. Los eventos de seguridad de la información incluyen incidentes, violaciones y vulnerabilidades (Ver Procedimiento Gestión de Incidentes).
3. Las debilidades o eventos que deberán ser reportados incluyen, sin limitarse a estos, los siguientes:

* Controles de seguridad de la información ineficaces;
* Incumplimiento de las expectativas de confidencialidad, integridad o disponibilidad de la información;
* Errores humanos;
* Incumplimiento de la política de seguridad de la información, políticas específicas del tema o normas aplicables;
* Incumplimientos de las medidas de seguridad física;
* Cambios en el sistema que no han pasado por el procedimiento de gestión de cambios;
* Mal funcionamiento u otro comportamiento anómalo del sistema de software o hardware;
* Infracciones de acceso;
* Vulnerabilidades;
* Sospecha de infección por malware.

1. Se debe advertir a los servidores judiciales y contratistas que no intenten probar vulnerabilidades de seguridad de la información sospechosas pues pueden causar daños al sistema o servicio de información.

# **CLAUSULAS DE CONTROLES FÍSICOS**

## Perímetro de seguridad física

Directrices:

1. Las instalaciones de la Rama Judicial cuentan con doble puerta para controlar el acceso físico a las oficinas.
2. El acceso físico a las instalaciones la Rama Judicial, se controla mediante la lectura de huella por medio del biométrico de acceso en las talanqueras y/o el diligenciamiento de una planilla de acceso.
3. Se debe registrar el ingreso y retiro de dispositivos personales como: computadores, cámaras, discos externos. Para el retiro de equipos corporativos se debe contar con la autorización del jefe directo y presentar el formato en la recepción del edificio.
4. Las puertas y ventanas de las áreas deben permanecer cerradas y bloqueadas cuando no haya supervisión o las áreas se encuentren sin la presencia de servidores judiciales.
5. Los visitantes deben estar autorizados por el área responsable de la visita y deben estar acompañados en todo momento por los servidores judiciales del área.
6. Teniendo en cuenta, que son varias sedes y por lo tanto, áreas seguras es importante que se cuente con una persona de la unidad de servicios administrativos o a quien designe para controlar el acceso a las mismas y realizar el cierre de las puertas quedará con llave.
7. La Unidad de Servicios Administrativos es responsable suministrar extintores, la camilla y el botiquín de emergencia.
8. Cabe resaltar que la Rama Judicial cuenta con centros de cómputo propios en: el CAN, las Altas Cortes y las seccionales, mismos que deben ser clasificados y tratados como áreas seguras.
9. La Unidad de Servicios Administrativos debe establecer los controles y planes de emergencia contra amenazas externas y ambientales, como incendio, inundación, sobretensión eléctrica, explosivos y armas.
10. La Unidad de Servicios Administrativos es responsable suministrar y gestionar los sistemas de vigilancia apropiados que permitan monitorear las instalaciones físicas.
11. Los puntos de acceso como las áreas de entrega y carga y otros puntos donde personas no autorizadas pueden ingresar a las instalaciones deben controlarse y, si es posible, aislarse de las oficinas para evitar el acceso no autorizado.

## Trabajar en áreas seguras

Directrices:

1. La Rama Judicial a través del Oficial de Seguridad de la Información y la Unidad de Servicios Administrativos deberá diseñar e implementar medidas de seguridad apropiadas para trabajar en las áreas seguras identificadas.
2. Hacer que el personal sea consciente de la existencia o de las actividades dentro de un área segura solo cuando sea necesario;
3. Evitar el trabajo sin supervisión en áreas seguras tanto por razones de seguridad como para reducir las posibilidades de actividades maliciosas;
4. Cerrar físicamente e inspeccionar periódicamente las áreas seguras vacantes;

## Emplazamiento y protección de equipos

Directrices:

1. La Unidad Informática velará por que los equipos de cómputo, escáneres e impresoras estén situados y protegidos en áreas seguras para reducir el riesgo contra amenazas ambientales y acceso no autorizado.
2. La unidad de servicios administrativos debe propender que los equipos de cómputo portátiles se protejan mediante guayas para prevenir su pérdida.
3. La unidad de servicios administrativos debe propender separar los cables de alimentación de los cables de comunicaciones para evitar interferencias.
4. En las instalaciones se debe etiquetar los cables en cada extremo con suficientes detalles de origen y destino para permitir la identificación física y la inspección del cable.
5. La Unidad de Servicios Administrativos debe definir mecanismos de soporte y mantenimiento para los equipos de cómputo y los equipos red y debe llevar registro de estos.
6. Cuando un equipo sea reasignado o retirado de servicio, la unidad informática debe garantizar la eliminación de toda información mediante mecanismos de borrado seguro, teniendo en cuenta que previo a esta actividad debe realizarse una copia de seguridad.
7. Los servidores judiciales que tengan asignado un equipo portátil propiedad de la Rama Judicial deben asegurarlo con guaya. El equipo deberá ser entregado a la unidad Informática una vez termine su vínculo contractual con la Entidad.
8. La Unidad Informática debe configurar como política general que todos los equipos de cómputo que se encuentren desatendidos se bloqueen automáticamente después de cinco (5) minutos de inactividad. De todas formas, si el control no aplica los servidores judiciales deben bloquear su pantalla cuando se levanten de su puesto de trabajo o se retiren de las oficinas de la Rama Judicial.

## Política de escritorio limpio y pantalla limpia

Directrices:

1. Todos los servidores judiciales de la Rama Judicial deberán mantener protegida la información confidencial o sensible objeto de su labor o propia de la Entidad, que pueda ser accedida, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
2. El puesto de trabajo de los servidores judiciales deberá permanecer organizado y la información clasificada como confidencial o sensible, deberá guardarse bajo llave mientras el servidor judicial responsable de la misma no esté trabajando con ella.
3. Los equipos de cómputo con información de la Rama Judicial deberán conservar la pantalla libre de accesos directos a información clasificada como confidencial o sensible.
4. Los documentos que contengan información clasificada como: confidencial o sensible, se deben retirar inmediatamente de las impresoras, fax, fotocopiadoras y escáneres.
5. Para evitar riesgos de pérdidas o deterioro de la información que reposa en los puestos de trabajo, los servidores judiciales deberán abstenerse de consumir alimentos o bebidas en dichos lugares.
6. No se debe reutilizar o reciclar documentos impresos clasificados como: confidenciales o sensibles, estos deben ser destruidos de forma segura.

## Política de Gestión de Medios Extraíbles

Directrices:

1. Los medios extraíbles y las conexiones a dichos medios en los equipos de cómputo como son memorias USB, unidades de CD/DVD, discos externos, entre otros, serán restringidas por parte de la Unidad Informática y en todos los equipos de la Entidad, excepto para aquellos cargos que en desarrollo de sus funciones, requieran hacer uso de medios extraíbles, para lo cual deberán contar con la evaluación y aprobación del jefe directo y del Oficial de Seguridad de la Información, quienes realizarán la evaluación de riesgos a los que está expuesta la información.
2. La Unidad Informática administrará una lista de aprobación (lista blanca) con los medios removibles autorizados y los respectivos responsables. Esta lista, servirá como soporte en caso de presentarse incidentes, investigaciones y auditorias, entre otros temas relacionados con la seguridad de la información.
3. La Unidad Informática debe asegurarse de almacenar todos los medios de almacenamiento en un entorno seguro y protegido de acuerdo con su clasificación de información y protegerlos contra amenazas ambientales (como calor, humedad, campo electrónico o envejecimiento), de acuerdo con las especificaciones de los fabricantes.
4. La Unidad Informática deberá establecer procedimientos para la reutilización o eliminación segura de los medios de almacenamiento para minimizar el riesgo de fuga de información confidencial a personas no autorizadas. Estas actividades deberán ser supervisadas por el Oficial de Seguridad de la Información.
5. Cuando la información confidencial en los medios de almacenamiento no está encriptada, se debe considerar adicionalmente la protección física de los medios de almacenamiento.

## Utilidades de apoyo

Directrices:

1. Los equipos de cómputo y equipos de comunicaciones deben estar protegidos contra cortes de los servicios públicos de apoyo (por ejemplo, electricidad, telecomunicaciones, suministro de agua, gas, alcantarillado, ventilación y aire acondicionado).
2. La Unidad Informática deberá asegurarse de que el equipo de apoyo a los servicios públicos esté configurado, operado y mantenido de acuerdo con las especificaciones del fabricante correspondiente.
3. La Unidad Informática deberá asegurarse de que el equipo que respalda a los servicios públicos esté en una red separada de las instalaciones de procesamiento de información si está conectado a una red.

# **CLAUSULAS DE CONTROLES TECNOLÓGICOS**

## Dispositivos de punto final de usuario

Directrices:

1. El uso de teléfonos inteligentes está autorizado para todos los servidores judiciales, contratistas, proveedores y partes interesadas de Rama Judicial, siempre y cuando se declare por parte del propietario en documento firmado que dicho dispositivo cuenta con antivirus instalado y se hace responsable de:

* Instalar aplicaciones únicamente desde los repositorios oficiales.
* Dar un manejo confidencial a la información almacenada o accedida desde dichos dispositivos.
* Hacer un uso adecuado del Internet según las políticas de navegación definidas en este manual.

1. La Rama Judicial asignará equipos corporativos a sus servidores judiciales, dichos equipos contarán con sistema operativo y software antivirus licenciados, así mismo, los privilegios de administración sobre el equipo estarán restringidos mediante la configuración de un usuario administrador local.
2. En caso de requerirse el uso de equipos personales por parte de los contratistas, deberá solicitarse la autorización por el jefe inmediato mediante el formato de control de cambios (Ver Procedimiento Control de Cambios), en cuyo caso el contratista deberá declarar en documento firmado que dicho equipo cuenta con sistema operativo licenciado y se hace responsable de:

* Instalar aplicaciones únicamente desde los repositorios oficiales.
* Ejecutar su labor desde los recursos en la nube autorizados, como: Office 365, Azure DevOps, GitHub, etc.
* Dar un manejo confidencial a la información almacenada o accedida desde dicho equipo.
* Hacer un uso adecuado del Internet según las políticas de navegación definidas en este manual.

1. La Rama Judicial instalará el software de antivirus corporativo en los equipos personales autorizados.
2. La Rama Judicial verificará que los equipos autorizados cumplan las políticas establecidas y gestionará un inventario de los mismos.
3. Cuando la labor contractual termine, los servidores judiciales deberán declarar en documento firmado que se llevó a cabo el borrado de toda la información de la Rama Judicial y de sus usuarios (áreas internas o ciudadanos) que pudo haberse almacenado en el equipo personal.
4. El servidor judicial que cuente con asignación de dispositivos móviles de la Rama Judicial es responsable de:

* Cuidar de la seguridad física del dispositivo móvil y de los controles de acceso mediante el uso de las contraseñas.
* No conectarlo en redes públicas o evitar hacer uso en lugares con algún riesgo de seguridad.
* No almacenar información en el dispositivo móvil de la Rama Judicial
* Ante la pérdida de un dispositivo móvil deberá realizar la respectiva denuncia ante la entidad competente y reportar inmediatamente el incidente, con el fin de que se cambien los accesos a las plataformas utilizadas.

## Gestión de derechos de acceso privilegiado

Directrices:

1. La Unidad Informática deberá controlar la asignación de derechos de acceso privilegiado a través de un proceso de autorización de acuerdo con la política de control de acceso.
2. Deberá identificar a los usuarios que necesitan derechos de acceso privilegiado para cada sistema o proceso (por ejemplo, sistemas operativos, sistemas de gestión de bases de datos y aplicaciones).
3. Deberá asignar derechos de acceso privilegiado a los usuarios según sea necesario solo a personas con la competencia necesaria para llevar a cabo actividades que requieren un acceso privilegiado y con base en el requisito mínimo para sus roles funcionales.
4. Deberá otorgar acceso privilegiado temporal solo durante el período de tiempo necesario para implementar cambios o actividades aprobados (por ejemplo, para actividades de mantenimiento o algunos cambios críticos), en lugar de otorgar derechos de acceso privilegiado de forma permanente.
5. Deberá establecer reglas específicas para evitar el uso de identificaciones de usuario de administración genéricas (como “root”), dependiendo de las capacidades de configuración de los sistemas. Administrar y proteger la información de autenticación de dichas identidades.

## Acceso al código fuente

Directrices:

1. El acceso al código fuente y elementos asociados (como diseños, especificaciones, planes de verificación y planes de validación) y herramientas de desarrollo (por ejemplo, compiladores, constructores, herramientas de integración, plataformas y entornos de prueba) debe controlarse estrictamente.
2. Otorgar acceso de lectura y escritura al código fuente en función de las necesidades del negocio y administrado para abordar los riesgos de alteración o uso indebido.
3. no otorgar a los desarrolladores acceso directo al repositorio del código fuente, sino a través de herramientas para desarrolladores que controlan las actividades y autorizaciones en el código fuente.
4. Se deberá mantener un registro de auditoría de todos los accesos y de todos los cambios en el código fuente.

## Autenticación segura

Directrices:

1. Se debe elegir una técnica de autenticación adecuada para corroborar la identidad reclamada de un usuario, software, mensajes y otras entidades.
2. La fuerza de la autenticación debe ser adecuada para la clasificación de la información a la que se accede.
3. Cuando se requiera una fuerte autenticación y verificación de identidad, los métodos de autenticación alternativas a las contraseñas, como certificados digitales, tarjetas inteligentes, tokens o medios biométricos, deben ser usados.
4. La información de autenticación debe ir acompañada de factores de autenticación adicionales para acceder a los sistemas de información crítica (también conocida como autenticación de múltiples factores).

## Gestión de la capacidad

Directrices:

1. La Unidad Informática deberá identificar los requisitos de capacidad para los equipos de cómputo, los recursos humanos, las oficinas y otras instalaciones, teniendo en cuenta la importancia comercial de los sistemas y procesos en cuestión.
2. Se debe aplicar el ajuste y la supervisión de los sistemas para garantizar la disponibilidad y la eficiencia de los sistemas.
3. La Unidad Informática deberá asegurar que las proyecciones de los futuros requisitos de capacidad tengan en cuenta los nuevos requisitos del negocio y del sistema y las tendencias actuales y proyectadas en las capacidades de procesamiento de información de la organización (Ver Procedimiento Gestión de Capacidad).
4. Deben establecerse controles de detección para indicar los problemas a su debido tiempo.

## Protección contra códigos maliciosos

Directrices:

1. La Rama Judicial contará con un antivirus corporativo el cual debe instalarse en todos los equipos corporativos y en aquellos equipos de uso personal autorizados en la Entidad.
2. La Unidad Informática debe garantizar que el software antivirus se mantenga actualizado con las últimas firmas y deberá monitorear las alertas generadas por dicho software en donde se encuentre instalado.
3. La Oficina de seguridad debe definir como soporte al procedimiento de gestión de incidentes los pasos para la detección, prevención y recuperación contra códigos maliciosos (Ver Procedimiento Gestión de Incidentes).
4. El Oficial de Seguridad de la Información deberá generar cultura entre los servidores judiciales, contratistas, proveedores y partes autorizadas para prevenir ataques de software malicioso.
5. Se debe garantizar que la información sea escaneada por el software de antivirus, así mismo, se debe escanear la información contenida y transmitida mediante correo electrónico.
6. La Unidad Informática debe asegurar que no se pueda detener el software antivirus instalado en los equipos corporativos y en aquellos equipos de uso personal autorizados en la Entidad.
7. Los servidores judiciales deben abstenerse de abrir o ejecutar archivos y/o documentos de fuentes desconocidas, especialmente los que se encuentran en medios de almacenamiento externo o que provienen de correos electrónicos desconocidos.
8. Los servidores judiciales, contratistas, proveedores y partes interesadas que sospechen o detecten alguna infección por software malicioso deben notificar de inmediato al Oficial de Seguridad de la Información con el fin de ejercer los controles correspondientes.

## Gestión de Vulnerabilidades Técnicas

Directrices:

1. La Oficina de seguridad de la información, debe realizar mínimo una vez al año una revisión de vulnerabilidades técnicas y pruebas de penetración en los sistemas de información y servicios tecnológicos críticos.
2. La Unidad Informática debe documentar, informar, gestionar y corregir las vulnerabilidades encontradas.

## Sincronización de reloj

Directrices:

1. Los relojes de los sistemas de procesamiento de información utilizados por la organización deben sincronizarse con las fuentes de tiempo aprobadas.
2. La configuración correcta de los relojes de los equipos de cómputo es importante para garantizar la precisión de los registros de eventos, que pueden ser necesarios para investigaciones o como evidencia en casos legales y disciplinarios.
3. Deben utilizarse protocolos como el protocolo de tiempo de red (NTP) o el protocolo de tiempo de precisión (PTP) para mantener todos los sistemas en red sincronizados con un reloj de referencia.

## Copias de respaldo

Directrices:

1. Los servidores judiciales de la Rama Judicial ejecutan su labor desde los recursos en la nube autorizados, como: Office 365, Azure DevOps, GitHub, etc., dichos recursos garantizan alta disponibilidad de la información allí almacenada. Además, los servidores judiciales no deben almacenar información en los equipos de cómputo.
2. Los líderes de procesos en la Rama Judicial deben definir y documentar un procedimiento de copias de respaldo y restauración de la información más crítica almacenada de los recursos en la nube, donde se establezca qué, cómo, quién, con qué periodicidad, tipo de respaldo y nivel de criticidad.
3. La Unidad Informática debe llevar a cabo pruebas de restauración de las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.
4. Los líderes de procesos deben guardar la información en los recursos de la nube autorizados, como: Office 365, Azure DevOps, GitHub, etc. La información que no se aloje en dichos recursos no será respaldada y cualquier pérdida de esta será responsabilidad del usuario.
5. Las copias de respaldo deben ir cifradas siempre y cuando contengan información clasificada o de reserva, así como información de datos personales que sean sensibles.

## Restricciones en la instalación de software

Directrices:

1. La Unidad Informática controlará la instalación de software no autorizado mediante la configuración de un usuario administrador local en los equipos corporativos (Ver procedimiento control de software).
2. La Unidad Informática configurará los equipos corporativos para que instalen actualizaciones de seguridad en los sistemas operativos automáticamente.
3. La Unidad Informática definirá el listado de productos permitidos para estar instalados en los equipos corporativos.
4. La Unidad Informática debe realizar de manera periódica una inspección del software instalado en los equipos corporativos y debe desinstalar el software no autorizado.

## Seguridad en redes

Directrices:

1. La Unidad Informática debe generar registros de navegación de los accesos de los usuarios a Internet, así como establecer e implementar procedimientos de monitoreo sobre la utilización del servicio de Internet.
2. La Unidad Informática debe implementar controles que eviten el ingreso a páginas con código malicioso incorporado o sitios catalogados como peligrosos.
3. La Unidad Informática debe proteger la red mediante el uso de dispositivos perimetrales, como firewalls.
4. La Unidad Informática debe proteger el acceso a la red inalámbrica mediante el uso protocolos fuertes de autenticación como WPA2, así mismo deberá cambiar la contraseña de acceso a la red inalámbrica periódicamente mínimo (3) veces al año.
5. La Unidad Informática debe asegurarse que los proveedores de servicios de red identifiquen e implementen las medidas de seguridad necesarias para servicios particulares, tales como características de seguridad, niveles de servicio y requisitos de servicio (Ver Procedimiento tratamiento seguridad en los acuerdos con los proveedores).
6. Deberá determinar y controlar periódicamente la capacidad del proveedor de servicios de red para gestionar los servicios acordados de forma segura.
7. Deberá asegurar que los grupos de servicios de información, usuarios y sistemas de información estén segregados en las redes de la Rama Judicial.
8. La red de acceso inalámbrico para invitados debe separarse de las del personal si el personal solo usa dispositivos de punto final de usuario controlados que cumplen con las políticas específicas del tema de la organización.

## Filtrado web

Directrices:

1. La Unidad Informática deberá reducir los riesgos de que los servidores judiciales y contratistas accedan a sitios web que contengan información ilegal o que se sepa que contienen virus o material de phishing, mediante la implementación de herramientas de filtrado web.
2. La Unidad Informática deberá identificar los tipos de sitios web a los que el personal debe o no tener acceso. Se debería bloquear el acceso a los siguientes tipos de sitios web:

* Sitios web que tienen una función de carga de información a menos que esté permitido por razones comerciales válidas.
* Sitios web maliciosos conocidos o sospechosos (por ejemplo, aquellos que distribuyen malware o contenido de phishing).
* Servidores de comando y control.itio web malicioso adquirido a partir de inteligencia de amenazas.
* Sitios web que comparten contenido ilegal.

1. El filtrado web puede incluir una variedad de técnicas que incluyen firmas, heurística, lista de sitios web o dominios aceptables, lista de sitios web o dominios prohibidos y configuración personalizada para ayudar a evitar que el software malicioso y otras actividades maliciosas ataquen la red y los sistemas de la organización.

## Política sobre el uso de controles criptográficos

Directrices:

* + 1. Es deber de todo servidor judicial, contratista, tercero y/o parte interesada cifrar los activos de información clasificados como: confidenciales o sensibles que sean transmitidos mediante canales de comunicación públicos. Esto, mediante el uso de archivos Zip con contraseña, y la contraseña se debe comunicar por un canal de comunicación diferente (Ver Procedimiento de Controles Criptográficos).
    2. Se deben generan llaves criptográficas sólidas (TDES, AES-256) con una longitud de 256 bits como mínimo, para garantizar que su distribución es independiente a la distribución de la información cifrada (Ver Procedimiento Gestión de Llaves Criptográficas).
    3. Se deben definir mecanismos seguros para el almacenamiento de las llaves y realizar cambios periódicos de estas.
    4. Al realizar el cifrado de información, se debe mantener copia de las llaves de cifrado en un lugar seguro de forma que la recuperación de la información cifrada sea factible, en caso de ausencia temporal o permanente del custodio de la información cifrada.
    5. Las llaves criptográficas de las que se tenga sospecha de exposición deben ser destruidas.
    6. Se debe definir un tiempo de vida de las llaves.
    7. Se deben sustituir las llaves criptográficas tras la caducidad o compromiso de las mismas.
    8. Toda llave de cifrado utilizada en entornos de pruebas y desarrollo no debe ser instalada en producción.
    9. Está expresamente prohibido revelar las llaves privadas de cifrado de información a personal no autorizado.
    10. Se debe asegurar que los mecanismos de cifrado para las conexiones remotas por VPN site to site utilicen mínimo protocolo IPSec y algoritmo de cifrado AES-256 (Ver Procedimiento Conexión a VPN).
    11. Si se requiere el uso de controles criptográficos en los desarrollos por parte de la Unidad Informática, la fábrica de software y el área usuaria se debe utilizar algoritmos robustos como: AES-256 (simétrico), RSA (asimétrico), SHA2 (funciones hash).
    12. Está expresamente prohibido cifrar información con mecanismos no autorizados por la Rama Judicial.

## Requisitos de seguridad de los sistemas de información

Directrices:

1. La Rama Judicial debe establecer metodologías para el desarrollo de software seguro, que incluyan la definición de requerimientos de seguridad y las buenas prácticas, con el fin de proporcionar a los desarrolladores, sean de la entidad o de terceros, una visión clara de lo que se espera (Ver Procedimiento Adquisición Desarrollo Mto Software).
2. Los líderes de proceso en acompañamiento del Oficial de Seguridad de la Información deben establecer las especificaciones de adquisición o desarrollo de sistemas de información considerando siempre los requerimientos de seguridad de la información.
3. El Oficial de Seguridad de la Información debe garantizar que cada vez que se pretenda implementar un sistema de información ya sea propio o de terceros, este sea sometido a un análisis de vulnerabilidades supervisadas, las cuales deberán ser remediadas antes del despliegue en producción.

## Seguridad en los procesos de desarrollo y de soporte

Los Líderes de la Unidad Informática junto con el Grupo de Proyectos Especiales de Tecnología y la fábrica de software son los responsables de planificar, desarrollar y ejecutar las actividades relacionadas con el desarrollo de productos informáticos o servicios basados en software, el Especialista DevOps es el responsable de las actualizaciones, instalaciones de software y despliegues. El equipo de QA, debe planificar la ejecución de pruebas funcionales y de seguridad de los sistemas nuevos o modificados antes de que el especialista DevOps realice la instalación o despliegue en los servidores de producción (Ver Procedimiento Adquisición Desarrollo Mto Software).

## Directrices de seguridad para proyectos de desarrollo

Como parte de las actividades a realizar en la fase inicial de levantamiento de requerimientos o historias de usuario, con sus respectivos criterios de aceptación y/o durante la etapa de conceptualización de cada proyecto de desarrollo, se deberán describir los requerimientos de seguridad que deben ser cubiertos por el nuevo sistema (Ver Procedimiento Adquisición Desarrollo Mto Software).

## Directrices de seguridad para la especificación detallada de requerimientos

1. En el análisis de factibilidad de los requerimientos, se deberá considerar el nivel de criticidad del sistema, además del nivel de protección de seguridad que requerirán los datos y las aplicaciones que lo compongan.
2. Los requerimientos de seguridad deberán ser compatibles con lo que se establece en las demás políticas de seguridad o políticas relacionadas con la seguridad de la información en la Rama Judicial.

## Directrices de seguridad para el diseño de Sistemas

1. El nivel de confidencialidad de todos los elementos que componga el software deberá ser definido teniendo en cuenta la criticidad de los datos.
2. Si se requiere el uso de cifrado de datos, este deberá ceñirse a los lineamientos descritos en la política del uso de controles criptográficos (Ver Procedimiento de Controles Criptográficos).
3. Si se utiliza un sistema gestor de bases de datos, se deberá emplear las herramientas de seguridad necesarias para garantizar el nivel de protección adecuado.
4. En el diseño de un sistema o proyecto de desarrollo, se debe tener en cuenta el uso de repositorios de código fuente GitHub haciendo uso del modelo GitFlow. Sin embargo, los detalles de la implementación del modelo quedarán descritos en el manual de desarrollo seguro (Ver Procedimiento Adquisición Desarrollo Mto Software).
5. En la etapa de conceptualización, se debe sugerir al área usuaria de manera enfática la inclusión de un módulo que permita manejar registros de auditoría, se sugiere que la funcionalidad incluya al menos la identidad del usuario que lee, borra, escribe, o actualiza, y las consultas a la información o datos críticos, el tipo de evento y la fecha y hora del evento. Estos registros deben ser protegidos contra la manipulación no autorizada.
6. En la etapa de diseño, se deberá proyectar el rendimiento esperado del sistema y los requerimientos de hardware para cumplir con este objetivo, con el propósito de no sobre-dimensionar los recursos necesarios para el funcionamiento del sistema, ni de sub-dimensionarlos (ancho de banda, RAM, procesadores, etc.), no obstante, durante la etapa de conceptualización, se establecerá en conjunto con la Unidad Informática, la fábrica de software y el área usuaria, la forma en la que se hará el escalamiento de recursos o generación de archivos históricos, en caso de las bases de datos o repositorios de archivos.

## Directrices de seguridad para la codificación y pruebas

1. No está permitido modificar programas sin que quede registrado o documentado el cambio, en etapa de desarrollo eso se logra con el uso de los repositorios de código fuente y en sistemas productivos con un control de cambios o evolutivos, teniendo en cuenta lo que se definió con anterioridad, que cualquier cambio de la funcionalidad de un desarrollo requiere de la actualización de la documentación afectada. En caso de requerirse la implementación de un cambio, este deberá ceñirse a los lineamientos descritos en el procedimiento de control de cambios.
2. No está permitido escribir o modificar código auto replicante o cualquier otro tipo de código malicioso, como virus, troyano, gusano, bombas lógicas, o cualquier otro software, módulo o trozo de software que genere riesgos o vulnerabilidades para la Rama Judicial, así como funciones u operaciones no documentadas o no autorizadas en los programas, como puertas traseras o huevos de pascua.
3. En lo posible, las pruebas del sistema y/o pruebas de desempeño, deberán incluir: pruebas de instalación, volumen, carga y stress, almacenamiento, configuración, funcionalidad, seguridad y recuperación ante caídas del sistema.
4. En lo posible, las pruebas deberán ser realizadas en forma automática, almacenando criterios y datos de pruebas en archivos, para permitir la verificación rápida y repetitiva.
5. Se deberán tener las siguientes consideraciones con relación a los datos de entrada y salida de los sistemas de información:

* Realizar las validaciones de datos de entrada y salida en un sistema confiable (por ejemplo: un servidor).
* Construir los aplicativos para que validen los datos de entrada y generen los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.
* Validar la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como tipos de datos, rangos válidos y longitud, entre otros.
* Validar las entradas de datos con una “lista blanca” que contenga un directorio de caracteres aceptados.
* Validar el intento de ingreso de bytes nulos, caracteres de nueva línea o caracteres de alteración de rutas.
* Limpiar las salidas de datos no confiables que se usen como parámetros o parte de consultas (queries), hacia sistemas SQL, XML y LDAP o hacia comandos del sistema operativo.

1. Se deberán establecer los siguientes controles para la autenticación en los sistemas de información:

* Realizar los controles de autenticación en un sistema confiable.
* Si la aplicación administra un almacenamiento de credenciales, asegurar que únicamente se almacena el hash de las contraseñas.
* Validar los datos de autenticación, luego de haber completado todos los datos de entrada.

1. Se deberá realizar una gestión de las sesiones, que tenga en cuenta los siguientes aspectos:

* Realizar la creación de identificadores de sesión en un sistema en cual se confíe
* Garantizar la existencia de opciones de desconexión o cierre de sesión de los aplicativos (logout) que permita terminar completamente con la conexión asociada.
* No exponer los identificadores de sesión en URL, mensajes de error, ni logs, y no transmitirlos como parámetros por URL a no ser que se envíen encriptados.
* Asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros, jamás almacenar contraseñas sin cifrado y solo cuando sea estrictamente necesario.
* Asegurar que la sesión expire después de cierto tiempo, el cual debe ser un parámetro gestionable de la aplicación.
* No permitir la apertura de sesiones simultaneas con el mismo usuario en diferentes equipos (PCs o Servidores).

1. Se deberá señalar al área usuaria las ventajas de implementar soluciones que utilicen doble factor de autenticación para la ejecución de operaciones que se hayan identificado como sensibles durante la etapa de conceptualización. En caso de que el área usuaria no desee implementar dicha funcionalidad, se dejará constancia en la documentación del proyecto.
2. Todas las funciones de criptografía de las aplicaciones desarrolladas deben ser implementadas en sistemas confiables (Ver Procedimiento Gestión de Llaves Criptográficas).
3. Se deben considerar los siguientes aspectos en el manejo de errores:

* Garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios. Los mensajes de error deben ser genéricos, nunca deben presentar información sensible.
* Liberar espacio en memoria cuando ocurra una condición de error.
* Nunca se debe almacenar contraseñas en los logs.

1. Para el manejo de archivos se deberán acatar las siguientes consideraciones:

* Remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.
* Prevenir la revelación de la estructura de directorios o listado de archivos en los sistemas construidos.

1. Para el establecimiento de conexión a las bases de datos se deberán considerar los siguientes aspectos:

* No incluir las cadenas de conexión a las bases de datos en el código de los aplicativos, estas deberán guardarse cifradas en un directorio diferente al de la aplicación publicada para el caso de las aplicaciones web.
* Cerrar la conexión a las bases de datos desde los aplicativos, tan pronto como estas no sean requeridas (se abre la conexión, se usa y se cierra).

1. Se deberá remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.
2. Se deberán desarrollar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y garantizar que dichos archivos solo tengan privilegios de lectura.
3. No se deberá incluir en parámetros, nombres de directorios o rutas de archivos. En su lugar, se deben utilizar índices que internamente se asocien a directorios o rutas predefinidas.
4. Se deberá liberar la memoria previa a la salida de una función y de todos los puntos de finalización de la aplicación.
5. Se deberá garantizar la protección del código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios finales.
6. No se deberá permitir que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo, salvo que sea absolutamente necesario o sea parte de la funcionalidad del sistema, en ese caso debe quedar registrado (el comando, usuario, fecha y hora) como mínimo en el log de auditoría y que se realice con privilegios elevados.
7. Se deberán utilizar funciones de control de integridad (hash) para verificar la integridad del código interpretado, bibliotecas, ejecutables y archivos de configuración previo a su utilización

## Actividades de seguimiento

1. La política general y las políticas específicas de seguridad de la información deben ser revisadas por el Oficial de Seguridad de la Información de manera periódica, como mínimo una vez al año o cuando se presenten cambios significativos que requieran de su actualización.
2. Las redes, los sistemas y las aplicaciones deben monitorearse para detectar comportamientos anómalos y deben tomarse las medidas apropiadas para evaluar posibles incidentes de seguridad de la información.
3. Se deberá velar por la implementación de los controles de seguridad al mismo tiempo que la implementación de los componentes, funciones o módulos a los cuales controla.
4. Se deberá efectuar ajuste (tuning) de los controles establecidos en la fase de diseño.
5. Las aplicaciones deberán contar con un sistema de autenticación de usuario, que mínimo exija nombre de usuario y contraseña. Además, en los casos que la aplicación esté expuesta a internet, debe implementarse la validación de captcha y doble autenticación.
6. Las aplicaciones deberán contar con manejo de diferentes roles con permisos de acceso y operaciones asociados a estos.
7. Se deberá revisar y auditar la existencia de los controles de seguridad definidos en la etapa de diseño.
8. Al menos una vez cada año, se debe realizar un escaneo de las aplicaciones más recientes puestas en producción en busca de vulnerabilidades, manteniendo un registro de los resultados y las acciones correctivas tomadas.

1. Hace referencia a la metodología de identificación y clasificación de activos. [↑](#footnote-ref-2)