

GUÍA

TRANSFORMACIÓN  
DIGITAL

# GENERACIÓN DE POLÍTICAS DE LA TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN



**GUÍA PARA LA GENERACIÓN DE POLÍTICAS DE SEGURIDAD DE LA TECNOLOGÍA DE  
LA INFORMACIÓN Y COMUNICACIÓN**

GRUPO ESPECIALIZADO DE TRABAJO TRANSFORMACIÓN DIGITAL

Presidencia Pro tempore 2023-2024,  
Poder Judicial de la República Dominicana  
Junio 2024

<https://consejjudicialcc.org/>

# Contenido

<b>1. OBJETIVO.....</b>	<b>4</b>
<b>2. ALCANCE.....</b>	<b>4</b>
<b>3. INTRODUCCIÓN .....</b>	<b>4</b>
<b>4. DEFINICIONES .....</b>	<b>5</b>
<b>5. SEGURIDAD DE INFORMACIÓN .....</b>	<b>8</b>
<b>6. GUÍA PARA LA GENERACIÓN DE POLÍTICAS DE SEGURIDAD DE INFORMACIÓN ..</b>	<b>9</b>
Uso aceptable de los Activos de Información .....	13
Políticas de Pantalla y Escritorio Limpio .....	13
Políticas de Uso de Internet.....	14
Políticas de Uso del Correo Electrónico.....	14
Dispositivos Móviles.....	15
Teletrabajo.....	15
Trae tu propio Dispositivo (BYOD).....	16
Registro de las Actividades y Eventos de Seguridad.....	16
Eliminación y Destrucción de Datos y Equipos.....	16
Seguridad de los Equipos Tecnológicos.....	16
Comunicación de la Política .....	17

## **1. OBJETIVO**

Establecer una plantilla guía para la transformación digital en el desarrollo de políticas de seguridad de información en los Poderes Judiciales de Iberoamérica

## **2. ALCANCE**

Este documento no es una norma o especificación técnica, es sólo una orientación para facilitar el diseño de arquitectura de servicios de computación en la nube y establecer pautas mínimas a considerar durante el proceso de implementación de estas tecnologías en los Poderes Judiciales de Iberoamérica.

## **3. INTRODUCCIÓN**

La estrategia tecnológica se ha erigido como un factor crucial para el éxito de todas las organizaciones, impulsando la digitalización de los procesos a niveles sin precedentes en la historia humana. Este fenómeno se atribuye principalmente al liderazgo organizacional y a la adopción de tecnologías de vanguardia, como la computación en la nube, inteligencia artificial y robotización, entre otras.

La transición de medios analógicos a digitales ha desencadenado una explosión en la utilización de información y tecnología en todos los ámbitos de la sociedad. No obstante, esta digitalización conlleva riesgos, ya sea por ataques malintencionados o por el inadecuado manejo de las tecnologías, lo que podría resultar en la pérdida de información sensible.

La creciente amenaza de los ciberataques ha motivado a los poderes judiciales de Latinoamérica a incrementar sus inversiones en seguridad de la información. En los últimos años, se han registrado numerosos ataques que han tenido un impacto significativo en la administración de justicia. En este escenario, resulta imperativo que los poderes judiciales establezcan políticas de seguridad de información sólidas y efectivas, alineadas con las mejores prácticas internacionales, y que estas políticas sean implementadas y mantenidas de manera continua.

El propósito fundamental de estas políticas es salvaguardar la información sensible y crítica manejada por el poder judicial, previniendo su pérdida, robo, alteración o divulgación no autorizada. Para ello, deben abordar aspectos clave como la gestión de riesgos, identificando y evaluando las posibles amenazas a las que está expuesto el poder judicial; la protección de activos, mediante la implementación de medidas de seguridad

para resguardar la información, la infraestructura tecnológica, y los recursos humanos; y la respuesta a incidentes, estableciendo procedimientos para abordar eventualidades en la seguridad de la información.

La implementación de políticas de seguridad de información efectivas es esencial para proteger la administración de justicia y garantizar la continuidad de los servicios judiciales.

## 4. DEFINICIONES

<b>Acceso:</b>	Capacidad y medios para comunicarse o interactuar con un sistema, utilizar recursos de este para manejar y adquirir conocimiento de la información contenida en el sistema o controlar componentes y funciones de este.
<b>Aplicación:</b>	Es un programa de computadora que se utiliza como herramienta para una operación o tarea específica.
<b>Amenaza:</b>	Circunstancia desfavorable que puede ocurrir y que, de suceder, tendría consecuencias negativas sobre la Seguridad Cibernética y de la Información. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad.
<b>Área sensible:</b>	Son áreas donde se preservan activos de información clasificados como Confidencial y/o Restringido.
<b>Área operativa:</b>	Es el equipo de servidores judiciales que realizan tareas locales o remotas para la continuidad de la justicia a nivel nacional.
<b>BOYD / Bring your own device:</b>	Conocido en español como "trae tu propio dispositivo". Es una política empresarial consistente en que los colaboradores lleven sus propios dispositivos personales (ej. portátiles, tabletas, móviles) a su lugar de trabajo para tener acceso a recursos de la empresa tales como correos electrónicos, bases de datos y archivos en servidores, así como datos y aplicaciones personales.
<b>Clave o contraseña:</b>	Codificación secreta que puede incluir letras, números y caracteres que se utiliza para controlar el acceso hacia algún recurso.

<b>Cifrado:</b>	Es el proceso mediante el cual cierta información o texto sin formato es cifrado de forma que el resultado sea ilegible a menos que se conozcan los datos necesarios para su interpretación.
<b>Cortafuegos:</b>	Aplicación o equipo tecnológico cuyo propósito es bloquear el acceso no autorizado dentro de un sistema o red de información.
<b>Denegación de servicios (DoS/DDoS):</b>	Es un ataque a un sistema o red de información que causa la indisponibilidad de un servicio o recurso.
<b>Dirección IP:</b>	Es un conjunto de números que identifica de manera lógica una interfaz en la red de un dispositivo informático que utilice el protocolo de internet basado en el modelo TCP/IP.
<b>Dispositivo móvil:</b>	Cualquier equipo cuyas características permitan su movilidad o portabilidad y cuente con capacidades de memoria, procesamiento, almacenamiento y conexión a una red.
<b>Entorno en la nube:</b>	Servicios de computación a través de una red que usualmente es internet.
<b>Hardware:</b>	Partes físicas, tangibles, de un sistema informático y sus componentes.
<b>Hotspot (Punto caliente):</b>	Es un lugar que ofrece acceso a Internet a través de una red inalámbrica y un enrutador conectado a un proveedor de servicios de Internet.
<b>Incidente cibernético:</b>	Cualquier evento que ponga en riesgo la confidencialidad, integridad y disponibilidad de los sistemas de información institucional.
<b>Información Sensible:</b>	Es el nombre que recibe la información personal privada de un individuo.
<b>Información clasificada:</b>	Es un tipo de información sensible cuyo acceso está regulado por alguna ley, política o normativa.
<b>Información Confidencial:</b>	Es información que puede comprometer los intereses institucionales. El acceso a esta información solo debe estar permitido a personal autorizado por la máxima autoridad.
<b>Información Restringida:</b>	Esta información podría producir “efectos indeseados” a la institución si estuviera públicamente disponible, por lo que solo deberá estar al alcance de personas autorizadas.
<b>Información de Uso Interno:</b>	Información institucional cuyo acceso está disponible para los servidores judiciales.

<b>Información Pública:</b>	Es información que no está categorizada como confidencial, en consecuencia, puede divulgarse sin riesgos de comprometer a la institución.
<b>Phishing:</b>	Conjunto de técnicas cuyo propósito es engañar una víctima haciéndose pasar por una persona, empresa o servicio de confianza, logrando finalmente que realice acciones que no debería.
<b>Pruebas de seguridad:</b>	son un ejercicio de seguridad en el que un experto en ciberseguridad intenta encontrar y explotar vulnerabilidades en un sistema informático. El propósito de este ataque simulado es identificar puntos débiles en las defensas de un sistema que los atacantes podrían aprovechar
<b>Respaldo:</b>	Copia de los datos de información en un medio magnético alternativo, de tal modo que permita al sistema poder ser restaurado y recuperada la información.
<b>Evaluación de riesgos:</b>	Se entiende por “evaluación de riesgos” a la evaluación de las amenazas, impactos y vulnerabilidad relativos a la información, a las instalaciones de procesamiento de esta y a la probabilidad de que ocurran.
<b>Seguridad de la información:</b>	Se entiende por “seguridad de la información” a la preservación de la confidencialidad, integridad y disponibilidad de la información.
<b>Confidencialidad:</b>	Garantía que la información es accedida sólo por aquellas personas autorizadas a hacerlo.
<b>Integridad:</b>	Mantenimiento de la exactitud y totalidad de la información y los métodos de procesamiento.
<b>Disponibilidad:</b>	Garantía de que los usuarios autorizados tienen acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
<b>Software:</b>	Es un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora.
<b>Usuario:</b>	Persona que utiliza una computadora personal, tableta o portátil para realizar múltiples operaciones con aplicaciones, sistemas o plataformas.
<b>VPN (Virtual Private Network):</b>	Tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada como Internet.

Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.

## 5. SEGURIDAD DE INFORMACIÓN

La ISO 27001 define la seguridad de la información como la preservación de la confidencialidad, integridad y disponibilidad de la información. A continuación, se detallan los principales componentes de la seguridad de la información según la norma ISO 27001:

**Confidencialidad:** Garantiza que la información sea accesible únicamente para aquellos autorizados a tener acceso. Esto implica la implementación de controles que protejan la información contra accesos no autorizados.

**Integridad:** Asegura que la información sea precisa, completa y protegida contra modificaciones no autorizadas. Los controles de integridad buscan prevenir la alteración no deseada de la información.

**Disponibilidad:** Asegura que la información esté disponible y sea utilizable cuando sea necesario por aquellos que están autorizados a acceder a ella. Esto incluye la implementación de medidas para prevenir o minimizar el impacto de interrupciones en el acceso a la información.

**Autenticidad:** Verifica la autenticidad de la información y de los usuarios que acceden a ella. Los controles de autenticación se utilizan para garantizar que solo personas autorizadas tengan acceso a la información.

**No repudio:** Impide que una entidad niegue la autoría de una acción o la emisión de información. Los controles de no repudio buscan proporcionar evidencia que respalde la autenticidad de las transacciones y comunicaciones.

**Responsabilidad:** Define claramente las responsabilidades y expectativas con respecto a la seguridad de la información. Esto incluye la asignación de roles y la implementación de controles para garantizar que las personas cumplan con sus responsabilidades.

**Resiliencia:** La capacidad de resistir y recuperarse de eventos o incidentes de seguridad. Incluye la implementación de medidas para la gestión de riesgos y la continuidad del negocio.

<b>Seguridad física:</b>	Protege los activos de información contra amenazas físicas, como el acceso no autorizado, daños o robo. Involucra la implementación de medidas de seguridad en las instalaciones físicas que albergan los sistemas de información.
<b>Gestión de riesgos:</b>	Evalúa y gestiona los riesgos de seguridad de la información para garantizar que se aborden de manera adecuada y se reduzcan a niveles aceptables.
<b>Cifrado:</b>	La encriptación de la información para protegerla contra accesos no autorizados durante el almacenamiento, procesamiento o transmisión.

Estos componentes son fundamentales para establecer un sistema de gestión de seguridad de la información efectivo, y la ISO 27001 proporciona un marco estructurado para implementar, mantener y mejorar continuamente la seguridad de la información en una organización.

## 6. GUÍA PARA LA GENERACIÓN DE POLÍTICAS DE SEGURIDAD DE INFORMACIÓN

A continuación, los lineamientos generales a considerar en la generación de una política de seguridad de información:

- 1. Gobernanza:** Se debe indicar la estructura orgánica del área responsable de la seguridad de información. Ejemplo:
- 2. Áreas involucradas y responsables:** Se debe indicar el nivel de jerarquía y responsabilidad del área responsable y la relación con las áreas relacionadas.
- 3. Lineamientos o políticas:**
  - a) Gestión de la Seguridad de la Información:**
    - » *Establecer que el Poder Judicial contará con una unidad funcional dedicada a la Seguridad de la Información y Monitoreo, la cual incluirá áreas especializadas.*
    - » *Establecer la conformación de un comité de seguridad de información como parte de su estructura y funciones de control en materia de seguridad de la información, este comité reportará a la máxima autoridad en el Poder judicial.*

**b) Responsabilidades:**

- » *Establecer que la unidad funcional dedicada a la Seguridad de la Información y Monitoreo será responsable de garantizar que esta política sea implementada y mantenida.*
- » *La unidad de Seguridad de la Información y Monitoreo remitirá informes con los indicadores de gestión referentes al equipo de Gobernanza del Poder Judicial, con periodicidad trimestral.*
- » *La máxima autoridad administrativa del Poder Judicial será el responsable de garantizar que los recursos necesarios estén disponibles para la implementación y mantenimiento de la política de manera gradual y conforme a la disponibilidad presupuestaria.*
- » *La unidad de Seguridad de la Información y Monitoreo recomendará los contenidos de charlas y entrenamientos que considere necesarios para la implementación y mantenimiento de esta política.*
- » *La unidad de Seguridad de la Información y Monitoreo realizará pruebas de penetración para asegurar la fiabilidad de las soluciones de seguridad implementadas.*

**c) Gestión de Riesgos:**

- » *Establecer la necesidad de implementar una metodología de gestión de riesgos tecnológicos y de seguridad de la información que permita la mitigación de riesgos a través de la aplicación de controles, considerando:*
  - *El impacto potencial de una falla de seguridad, pérdida de servicio, integridad y/o exposición de datos en la institución.*
  - *La probabilidad de ocurrencia de dicha falla basados en las amenazas y las vulnerabilidades identificadas.*
  - *Los resultados de la evaluación de riesgos permitirán definir las prioridades y tomar decisiones importantes sobre el tratamiento de los riesgos asociados con la seguridad de la información.*

**d) Continuidad del negocio:**

- » *La unidad de Seguridad de la Información y Monitoreo implementará políticas y procesos para la gestión de la continuidad de seguridad de la información a fin de reducir una posible interrupción de los servicios ante desastres o fallas de seguridad a un nivel aceptable.*

- » *La unidad de Seguridad de la Información y Monitoreo construirá planes y procedimientos de respuesta y recuperación ante un evento disruptivo y mantendrá la seguridad de la información en un nivel predeterminado.*
- » *Los controles establecidos deberán ser verificados con periodicidad anual para asegurarse que son válidos y eficaces durante situaciones adversas, realizando cualquier actualización que sea necesaria.*

**e) Respuesta a incidentes Cibernéticos:**

- » *Los sistemas de información deben ser monitoreados para detectar incidentes relativos a la seguridad e iniciar los procedimientos de respuesta pertinentes.*
- » *La unidad de Seguridad de la Información y Monitoreo deberá:*
  - *Establecer un proceso de respuesta a incidentes de ciberseguridad que establezca las acciones que serán ejecutadas ante un incidente de este tipo.*
  - *Establecer un procedimiento formal de comunicación de los incidentes de seguridad de la información, donde se defina qué tipo de información relacionada con la seguridad de la información será comunicada, a qué partes interesadas internas, por quién y cuándo.*
  - *Implementar mecanismos que permitan cuantificar y monitorear los tipos de incidentes de seguridad y su impacto financiero. Esta información debe utilizarse para identificar las anomalías recurrentes o de alto impacto, permitiendo aplicar los controles necesarios para reducir la ocurrencia.*
  - *Definir procedimientos para el tratamiento de evidencias ante incidentes de seguridad de la información.*

**f) Clasificación de la Información:**

- » *La información deberá ser clasificada como Confidencial, Restringida, de Uso Interno o Pública al momento de su creación, modificación o al ser copiada desde otro origen de datos.*
- » *La unidad de Seguridad de la Información y Monitoreo deberá implementar el esquema de clasificación y los procedimientos y tecnologías necesarios para etiquetar la información institucional.*

**g) Gestión de Activos:**

- » *Los activos de información y los recursos asociados con su tratamiento deberán estar claramente identificados e inventariados.*

- » *Todo activo de información deberá tener designado a un gestor en el Inventario de activos. Dicho propietario, así como todo el que tenga acceso a este activo será el responsable de la confidencialidad, integridad y disponibilidad de la información del activo en cuestión.*

#### **h) Control de Acceso**

- » *Los accesos a los sistemas de información deberán otorgarse basados en el principio del menor privilegio.*
- » *Deberán segregarse las funciones y responsabilidades de los usuarios.*
- » *Todo acceso a los sistemas, redes, servicios e información deberá realizarse de acuerdo con el perfil de usuario establecido.*
- » *Las cuentas de usuario del personal que esté de vacaciones o licencia deberán ser deshabilitadas, previa notificación de la Dirección de Gestión Humana y habilitadas automáticamente cumplido el tiempo establecido. En caso de ser requerido, dichas cuentas podrán ser habilitadas previa autorización del supervisor inmediato.*
- » *Los dispositivos de almacenamiento externo para todos los usuarios deberán estar deshabilitados, y solo serán permitidos para el personal técnico especializado cuyas funciones demanden de su uso y para el personal directivo cuyos casos particulares han sido evaluados a través de un proceso de solicitud y aprobación.*
- » *Deberán estar deshabilitados los accesos a recursos externos como OneDrive, Drive, entre otros y solo estarán permitidos para el personal técnico especializado cuyas funciones demanden de su uso y para el personal directivo cuyos casos particulares han sido evaluados a través de un proceso de solicitud y aprobación).*
- » *Se debe definir una política de contraseñas que permita proteger la identidad digital de los usuarios.*
- » *Siempre que un usuario ingrese una clave incorrecta seis (6) veces consecutivas, el sistema deberá bloquear la cuenta de usuario en cuestión.*
- » *Ningún usuario deberá permitir que otra persona utilice sus credenciales de acceso, tampoco utilizará el nombre de usuario y/o clave de otra persona.*
- » *Todas las claves se deberán cambiar cada 30 días, excepto en el caso de los usuarios utilizados para la ejecución de servicios en las aplicaciones tecnológicas.*

- » *Deberá habilitarse la autenticación de múltiples factores siempre que esta opción esté disponible, reduciendo en consecuencia el riesgo de que las credenciales de acceso sean comprometidas.*

## **Uso aceptable de los Activos de Información**

En todo equipo tecnológico, según aplique, propiedad de la institución, deberán instalarse las herramientas institucionales de protección de puntos finales como antivirus y otras soluciones definidas por la unidad de Seguridad de la Información y Monitoreo para salvaguardar la información contenida.

Los usuarios no deberán participar en actividades que puedan ser utilizadas para evadir controles de seguridad de los Sistemas de Información.

La organización podrá utilizar herramientas especializadas para identificar y bloquear cualquier tecnología que ponga en riesgo la información del Poder Judicial/Rama Judicial.

Cada colaborador, proveedor o tercero que esté en contacto con activos de información institucionales deberá reportar de manera oportuna a la Mesa de Servicios de TI toda debilidad o incidente de seguridad.

A todo equipo de usuario final se le deberán instalar las actualizaciones que estén categorizadas como críticas y de seguridad tan pronto sean probadas en un ambiente controlado. Otras actualizaciones deberán ser instaladas no más de dos semanas después de ser liberadas y probadas.

A las soluciones tecnológicas que soportan los servicios administrativos y operativos del Poder Judicial se le deberán instalar las actualizaciones que estén categorizadas como críticas y de seguridad inmediatamente sean probadas en un ambiente controlado. Otras actualizaciones deberán ser instaladas cada 3 meses a través del proceso de gestión de cambios.

A la infraestructura tecnológica se le deberá realizar con periodicidad anual una evaluación externa de la seguridad que incluya un análisis de vulnerabilidades y pruebas de penetración por parte de expertos certificados e independientes contratados para esto.

A todo sistema de información se le deberá realizar un análisis de vulnerabilidades y pruebas de penetración previo a su puesta en operación.

## **Políticas de Pantalla y Escritorio Limpio**

Cuando la persona autorizada no se encuentre en su puesto de trabajo, todos los documentos impresos, así como los soportes de almacenamiento de datos, etiquetados

como confidencial o restringidos, deberán ser retirados del escritorio o de otros lugares para evitar el acceso no autorizado a los mismos. Este tipo de documentos y soportes deberán ser archivados de forma segura.

Todo usuario autorizado que se traslade de su puesto de trabajo deberá bloquear la pantalla o cerrar la sesión en el sistema. En caso de que el usuario olvide bloquear la pantalla o se ausente por un período superior a los 5 minutos (Deberían ser 10-15 minutos), se aplicará la “Política de Pantalla Limpia (La política se llama Política de escritorio limpio”, en la que se bloqueará la pantalla con protección por contraseña.

Todo documento deberá ser retirado inmediatamente de las impresoras y fotocopiadoras por la persona responsable de cada documento.

## **Políticas de Uso de Internet**

La unidad de Seguridad de la Información y Monitoreo podrá bloquear el acceso a determinadas páginas de Internet si estas representan una amenaza para la seguridad de los activos de información. Si el acceso a algunas páginas web está bloqueado, el usuario podrá generar una petición vía la Mesa de Servicios de TI solicitando autorización para acceder a dichas páginas a través del formulario o medio electrónico que sea definido. El usuario no deberá intentar eludir por su cuenta esa restricción.

El usuario será responsable de todas las posibles consecuencias que surjan por el uso no autorizado o inadecuado de servicios o contenidos de Internet.

El perfil de acceso a internet de los colaboradores deberá estar documentado en su perfil de usuario, el alcance de este contemplará las páginas, servicios y/o aplicaciones web a las que podrá acceder y dependerá de las necesidades de cara a sus funciones y será previamente validado con el responsable del área.

Los equipos de las áreas operativas solo tendrán acceso a los servicios de internet necesarios para la ejecución de sus funciones.

## **Políticas de Uso del Correo Electrónico**

Los usuarios solo deberán enviar mensajes que contengan información relativa a la institución y/o sus funciones. Se prohíbe el envío de correo masivo que pudiera ser considerado como no deseado.

Todo correo electrónico enviado desde la institución deberá incluir una exención de responsabilidad avisando sobre su confidencialidad,

Está prohibido utilizar cuentas personales de correo electrónico para tratar asuntos laborales, crear o guardar cualquier información de la institución y enviar o recibir correos en nombre de la institución. Dichas comunicaciones e informaciones deben realizarse a través de los canales institucionales.

## **Dispositivos Móviles**

El acceso a la información institucional o a los sistemas de información del Poder Judicial desde dispositivos móviles, solo será otorgado luego de que el usuario haya firmado una declaración de conocimiento y aceptación de responsabilidades sobre las Políticas de Seguridad e la Información.

Los dispositivos móviles institucionales deberán contar con protección ante software malicioso.

Si un dispositivo móvil es utilizado en lugares públicos, el propietario deberá tener la precaución de que los datos no puedan ser leídos por personas no autorizadas.

El área de Administración de Servicios TIC deberá implementar un procedimiento seguro para gestionar el ciclo de vida de los dispositivos móviles.

Los dispositivos móviles deben estar cifrados para evitar la revelación de la información almacenada y procesada en estos.

Se deberá concienciar de manera periódica a los usuarios sobre los riesgos asociados al uso de dispositivos móviles.

## **Teletrabajo**

El Poder Judicial / Rama Judicial establece el Teletrabajo o trabajo a distancia como un acuerdo institucional que permite a los usuarios trabajar fuera de las instalaciones físicas de la institución haciendo uso de las tecnologías de la información y comunicación. Puede recurrirse a este modelo de trabajo previo acuerdo entre el empleado y el supervisor y posteriormente el supervisor con el Director de Tecnologías de la Información y Comunicación para fines del uso de los recursos institucionales.

## **Trae tu propio Dispositivo (BYOD)**

Todos los datos de la institución que se almacenen transfieran o se procesen en equipos BYOD seguirán perteneciendo a la institución, y la misma mantendrá el derecho a controlar esos datos, aunque no sea propietaria del dispositivo.

Se deberá definir una política para la gestión de estos dispositivos

## **Registro de las Actividades y Eventos de Seguridad**

Se deben registrar de manera centralizada, proteger y revisar periódicamente los registros de actividades de los usuarios asociadas con la seguridad de la información.

Los sistemas de información deben conservar los registros de actividades que de manera suficientemente detallada indiquen quién ejecutó cada acción dentro de los mismos. Deberán incluir como mínimo: el identificador de usuario, la dirección IP, el identificar del equipo, fecha y hora de inicio y cierre de sesión, aplicaciones utilizadas, cambios a los archivos clasificados o propios de los sistemas de información, adiciones y cambios en los privilegios de los usuarios.

## **Eliminación y Destrucción de Datos y Equipos**

Todos los datos almacenados en equipos tecnológicos y/o dispositivos de almacenamiento externo deberán ser eliminados, o se deberá destruir el soporte, antes de ser eliminados o reutilizados.

La Gerencia de Administración de Servicios TIC deberá incluir dentro de sus procesos la verificación y borrado seguro de los datos de los equipos, de acuerdo con la clasificación de la información contenida.

Los datos deberán ser eliminados de manera definitiva, no recuperables, mediante el uso de herramientas de borrado especializado o de sobre escritura para estos fines; pero si teniendo en cuenta la clasificación de los datos, si el proceso no es suficientemente seguro, los soportes de almacenaje deberán ser destruidos.

## **Seguridad de los Equipos Tecnológicos**

La Dirección de Tecnologías de la Información y Comunicación es responsable de lo siguiente:

- Los equipos deben ubicarse y protegerse de manera que reduzcan los riesgos y oportunidades de que se produzcan accesos no autorizados.
- Los equipos tecnológicos deben recibir un mantenimiento correcto y oportuno que garantice su disponibilidad y la seguridad de la información contenida.
- Los equipos tecnológicos, así como el software o la información contenida no deben sacarse de la institución sin autorización previa por parte de la Dirección de Tecnologías de la Información y Comunicación a través de la Mesa de Servicios de TIC.
- Los equipos tecnológicos que estén localizados fuera de las instalaciones del Poder Judicial deberán contar con controles de seguridad que les permitan mitigar los riesgos a los que están expuestos.
- Política de Respaldo
- Deberán realizarse respaldos de todos los datos identificados como críticos para el Poder Judicial, su frecuencia deberá estar documentada en el plan de respaldos.
- Los medios de almacenamiento utilizados para alojar las copias de seguridad deberán estar cifrados.
- Se deberán probar y auditar las copias de seguridad y las pruebas de restauración realizadas.

Las pruebas de restauración se realizarán al menos una vez cada tres meses, mediante la implementación del proceso de recuperación de datos y la verificación de que todos los datos han sido recuperados satisfactoriamente.

## **Comunicación de la Política**

### **Este documento deberá ser del conocimiento de:**

- » Todo el personal jurisdiccional, administrativo y de soporte de la Institución.
- » Todo el personal de la Dirección de Tecnología de la Información y Comunicación.
- » Contraloría General.

Los responsables de las áreas son responsables del cumplimiento de las políticas que apliquen para todo personal interno y externo con acceso a los activos de información bajo su responsabilidad.

## GRUPO DE TRABAJO ESPECIALIZADO TRANSFORMACIÓN DIGITAL

Coordinado por República Dominicana  
Período 2023-2024

**Martín García Díaz**

**Nicaragua**

Director General de la División General  
de Tecnología de la Información y comunicaciones

**Mario Enrique Oregel Torres**

**Guatemala**

Gerente de Área de la Gerencia de Informática

**Pablo Ernesto Santana Parada**

**El Salvador**

Director de Desarrollo Tecnológico e información

**Kattia Morales Navarro**

**Costa Rica**

Directora de Tecnología de la Información y  
Comunicaciones

**Maritere Colón Domínguez**

**Puerto Rico**

Jueza Superior  
Directora Administrativa de los Tribunales Auxiliar

**Edgar Rodríguez y Katya Quiel**

**Panamá**

Director de Modernización y Desarrollo Institucional;  
directora de Informática

**Lourdes Carolina Munguía Díaz**

**Honduras**

Jueza Coordinadora del Juzgado de Letras del Trabajo

**República Dominicana**

**Arelis S. Ricourt Gómez,**

Jueza Presidente Cámara Civil  
Corte Apelación de La Vega

**Edynson Francisco Alarcón Polanco**

Juez Presidente Cámara Civil  
Corte Apelación Distrito Nacional

**Katerine A. Rubio Matos**

Jueza de Paz

**Welvis Beltrán**

Director de Tecnología