Tel.: 2295-3386 Fax.: 2257-0412 Correo: tecnologia-info@poder-judicial.go.cr

Lineamiento	L-SGSI-010	**Fecha:**	14/08/2018	**Página #:**	1 de 5
Título:	Lineamiento de Control de Acceso				

Lineamiento de Control de Acceso

1.0 PROPÓSITO

El propósito de este documento es establecer los lineamientos de acceso a los diversos sistemas, equipos, instalaciones e información, con base en los requerimientos de seguridad y objetivos de la institución.

2.0 ALCANCE

Este lineamiento aplica para todas las personas que laboran para el Poder Judicial y abarca todos los sistemas, equipos, instalaciones e información custodiados por la Dirección de Tecnología de Información y Comunicaciones.

3.0 TÉRMINOS Y DEFINICIONES

Para mayor claridad sobre el contenido de este lineamiento, se debe tener en cuenta los siguientes términos y definiciones:

- Acceso remoto: conexión a un equipo de cómputo interno desde una ubicación externa a donde éste se encuentra.
- Área segura: áreas que contienen información sensible o crítica, incluyendo las instalaciones para el procesamiento de la información.
- Autenticación: proceso realizado por un sistema de información para confirmar la identidad de una persona.
- Credenciales: combinación de la identidad de una persona y su información de autenticación, por ejemplo, el nombre de usuario y contraseña.
- Instalación para el procesamiento de la información: cualquier sistema, servicio o infraestructura tecnológica que procese y/o almacene información, o la ubicación física que los alberga.
- Separación de funciones: control administrativo utilizado para prevenir el hecho que una persona realice una actividad crítica de forma individual.
- Sesión: conexión lógica entre dos o más dispositivos o entre una computadora y un usuario, necesaria para el intercambio de información.

Tel.: 2295-3386 Fax.: 2257-0412 Correo: tecnologia-info@poder-judicial.go.cr

4.0 RESPONSABILIDADES

Con el fin de cumplir con los requisitos de este lineamiento se describen las siguientes responsabilidades:

1) Dirección de Tecnología de Información y Comunicaciones

a. Elaborar e implementar los procedimientos y mecanismos para la gestión de las cuentas de usuario en la plataforma tecnológica.

b. Configurar los grupos y derechos de acceso de las personas usuarias dentro de la plataforma tecnológica.

c. Definir en conjunto con el Departamento de Servicios Generales, las áreas seguras donde se procesa, almacena y transfiere información sensible o crítica custodiada por la DTIC, así como las personas autorizadas para acceder a éstas.

d. Gestionar continuamente los controles de acceso a la plataforma tecnológica y áreas seguras definidas por la DTIC.

2) Persona o entidad dueña del servicio y/o la información

a. Autorizar y revisar los accesos a la información, plataforma tecnológica y áreas seguras.

b. Reportar cualquier falla, anomalía o incidente con el proceso de control de acceso, que ponga en riesgo la seguridad de la información.

c. Aplicar cuando corresponda los mecanismos de bloqueo de cuentas de usuario, definidos por la Dirección de Tecnología.

5.0 PAUTAS

1) Gestión de cuentas de usuario

a. Todas las personas deben tener una cuenta de usuario o identificador único para acceder a la plataforma tecnológica del Poder Judicial, de manera que las acciones realizadas con una determinada cuenta puedan ser asociadas directamente a la persona a quien fue asignada.

b. Se deben generar cuentas o identificadores que revelen la menor cantidad de información acerca de la persona usuaria. Estos no deben divulgar información sobre sus funciones dentro de la institución, salvo aquellos casos donde se necesite identificar obligatoriamente la unidad o área a la que pertenece.

c. El acceso a la plataforma tecnológica se debe suministrar, revisar y revocar de acuerdo con los procedimientos que establezca la Dirección de Tecnología de Información y Comunicaciones.

Tel.: 2295-3386 Fax.: 2257-0412 Correo: tecnologia-info@poder-judicial.go.cr

d. Se otorgarán permisos de administrador en los equipos tecnológicos, sólo a los usuarios que, por su función, requieran de este tipo de acceso.

e. Cuando se requiera otorgar acceso a otras entidades a la plataforma tecnológica del Poder Judicial, la institución debe gestionar la autenticación y verificar la identidad de la persona usuaria externa antes de suministrar los accesos a los sistemas y/o servicios.

f. Los accesos requeridos por entidades externas a la plataforma tecnológica y áreas seguras del Poder Judicial, deben ser definidos y documentados en los acuerdos o contratos entre las partes.

g. Los accesos de las personas usuarias se deben otorgar estrictamente a la plataforma tecnológica, áreas seguras e información del Poder Judicial que sean necesarios para que lleven a cabo sus actividades asignadas y tomando en cuenta la separación de funciones críticas. Para lo cual es necesario que los diferentes sistemas de información de la institución cuenten con su respectivo módulo para la administración de la seguridad.

2) Gestión de sesiones

a. Los sistemas y equipos tecnológicos del Poder Judicial deben contar con mecanismos para bloquear y finalizar las sesiones de usuario de manera automática, después de períodos de inactividad definidos o por limitaciones de horario y considerando la naturaleza de las funciones de la persona usuaria.

b. Donde sea posible, se debe definir y limitar el número de sesiones concurrentes permitidas en los sistemas y equipos tecnológicos, tomando en cuenta las funciones y necesidades de usuarios específicos.

c. Las sesiones Web establecidas entre las personas usuarias y los equipos servidores del Poder Judicial deben protegerse, con el fin de conservar la confidencialidad de las credenciales de acceso, si éstas fuesen interceptadas por un atacante.

3) Gestión de contraseñas

a. Todas las contraseñas de las cuentas de usuario y administrativas de la infraestructura tecnológica del Poder Judicial deben cumplir con los requisitos definidos en el Lineamiento para el Uso de las Credenciales de Usuario y Contraseñas.

b. Los sistemas y equipos tecnológicos del Poder Judicial deben contar con mecanismos de bloqueo de cuentas de usuario, para limitar los intentos de inicio de sesión inválidos.

c. Las cuentas de usuario que hayan sido bloqueadas por cualquier motivo, sólo serán habilitadas nuevamente por la Dirección de Tecnología de Información y Comunicaciones o quien ésta designe como responsable.

Tel.: 2295-3386 Fax.: 2257-0412 Correo: tecnologia-info@poder-judicial.go.cr

4) Acceso remoto e inalámbrico

a. El acceso remoto a la infraestructura tecnológica del Poder Judicial por parte de la persona usuaria interna, debe realizarse por medio de herramientas que garanticen la confidencialidad e integridad de los datos en los canales de comunicación.

b. Cuando se requiera acceder remotamente a un equipo de cómputo para llevar a cabo labores de soporte, el acceso por parte de la persona técnica debe realizarse mediante las herramientas autorizadas por la Dirección de Tecnología de Información y Comunicaciones, y previa autorización y notificación a la persona usuaria.

c. El acceso a la plataforma tecnológica del Poder Judicial a través de redes inalámbricas debe ser limitado estrictamente a dispositivos autorizados.

d. El acceso remoto a la infraestructura tecnológica del Poder Judicial por parte de terceras personas no está permitido.

5) Acceso al código fuente

a. Se debe restringir el acceso al código fuente de los programas desarrollados y adquiridos por el Poder Judicial.

6) Acceso físico

a. El acceso físico a las áreas seguras debe ser controlado, con el fin de prevenir que una persona no autorizada tenga acceso a la plataforma tecnológica e información de la institución.

b. Se debe contar con un listado de las personas que están autorizadas para acceder a cada área segura definida.

6.0 MEDICIÓN DEL CUMPLIMIENTO

El cumplimiento de este lineamiento se verificará mediante diferentes métodos, entre los que se destacan: recorridos periódicos, auditorías internas y externas, reportes de las jefaturas, o cualquier otro mecanismo definido por la Dirección de Tecnología de Información y Comunicaciones.

7.0 EXCEPCIONES

Tel.: 2295-3386 Fax.: 2257-0412 Correo: tecnologia-info@poder-judicial.go.cr

Cualquier excepción a este lineamiento debe ser aprobado previamente por Consejo Superior o quien éste designe como responsable para la aprobación del mismo.

8.0 INCUMPLIMIENTOS

Cualquier persona que labore, visite o brinde apoyo al Poder Judicial y que no cumpla con lo aquí estipulado, queda sujeta a las sanciones disciplinarias y/o legales que los órganos correspondientes determinen. La Dirección de Tecnología de Información y Comunicaciones elaborará un informe donde se incluya un análisis de los riesgos derivados del incumplimiento, así como del posible impacto asociado.

9.0 DOCUMENTACIÓN RELACIONADA

- Normas técnicas para la gestión y control de las Tecnologías de Información de la Contraloría General de la República.
- Política de Seguridad de la Información.
- Reglamento del Gobierno, de la Gestión y el uso de los Servicios Tecnológicos del Poder Judicial.

10.0 HISTORIAL DE VERSIONES

Fecha	Revisión #	Descripción del cambio	Responsable