

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

INSTITUTO INTERNACIONAL DE ARTES CULINARIAS Y SERVICIOS

Agosto 2025

1. Contexto

La Política de Seguridad de la Información es un conjunto de reglas, principios y directrices que una organización define para proteger su información y los sistemas que la procesan, almacenan o transmiten. Estas políticas buscan garantizar la confidencialidad, integridad y disponibilidad de la información, además de asegurar el cumplimiento legal y la gestión adecuada de riesgos.

¿Para qué sirven estas políticas?

- Proteger los activos de información frente a amenazas internas y externas.
- Establecer responsabilidades claras para los usuarios y administradores de sistemas.
- Prevenir incidentes de seguridad, como fugas de datos, accesos no autorizados o pérdidas de información.
- Cumplir con la legislación vigente y marcos regulatorios.
- Fomentar una cultura organizacional de seguridad.

2. Alcance

Una Política de Seguridad de la Información puede abarcar diversas áreas, para efectos de la versión actual del documento se abordan los siguientes aspectos.

- A. Uso aceptable de los recursos tecnológicos.
- B. Control de acceso
- C. Gestión de contraseñas.

A. Política de Uso Aceptable de los Recursos Tecnológicos

1. Propósito

El objetivo de esta Política es establecer las normas para el uso adecuado, seguro y responsable de los recursos tecnológicos proporcionados por Culinary, garantizando la protección de los activos de información y el correcto funcionamiento de los sistemas.

2. Alcance

Esta Política se aplica a todos los empleados, contratistas, proveedores, consultores y cualquier persona que utilice los recursos tecnológicos de Culinary, incluyendo equipos informáticos, redes, software, correo electrónico, acceso a internet y sistemas de información.

3. Definición de Recursos Tecnológicos

Incluye, pero no se limita a:

- Computadoras de escritorio, portátiles, servidores, teléfonos móviles corporativos.
- Sistemas operativos, aplicaciones, plataformas de comunicación, correo electrónico, software licenciado.
- Redes corporativas, internet, Wi-Fi, almacenamiento en la nube, dispositivos de red.

4. Uso Aceptable

Está permitido el uso de los recursos tecnológicos de la organización para:

- Cumplir con las funciones laborales y responsabilidades asignadas.
- Comunicaciones internas y externas relacionadas con el trabajo.
- Acceso a sistemas autorizados de la empresa.
- Navegación en internet relacionada con temas profesionales o de formación.

5. Uso No Aceptable

Queda prohibido utilizar los recursos tecnológicos de la organización para:

- Acceder, descargar o distribuir contenido ilegal, ofensivo, discriminatorio o pornográfico.
- Utilizar software no autorizado o sin licencia.
- Ingreso y utilización de computadores personales en las dependencias del Instituto sin previa autorización.
- Compartir contraseñas o accesos personales sin autorización expresa.
- Realizar actividades personales que interfieran con las responsabilidades laborales.

- Participar en actividades que comprometan la seguridad, como hacking, instalación de malware o uso de proxies/VPNs sin autorización.
- Enviar correos electrónicos masivos no autorizados (spam).
- Usar los recursos para fines comerciales o personales fuera del ámbito laboral.

6. Seguridad y Confidencialidad

Todos los dispositivos deben tener contraseñas seguras y bloqueos automáticos.

Se deben aplicar medidas de seguridad como el cifrado de datos, actualización de software y uso de antivirus. La información confidencial debe ser protegida y no compartida sin autorización previa.

7. Monitoreo y Auditoría

La organización se reserva el derecho de monitorear, registrar y auditar el uso de sus recursos tecnológicos para garantizar el cumplimiento de esta Política, respetando las leyes de privacidad vigentes.

8. Responsabilidades del Usuario

Cada usuario es responsable de:

- Hacer uso responsable y ético de los recursos tecnológicos.
- Reportar cualquier incidente de seguridad o uso indebido al área de TI.
- Mantener la confidencialidad de la información a la que accede.
- No modificar ni intentar eludir las configuraciones de seguridad establecidas.

9. Sanciones por Incumplimiento

El incumplimiento de esta Política puede conllevar sanciones disciplinarias que van desde advertencias hasta la terminación del contrato laboral, según la gravedad del caso y las normativas internas.

10. Revisión de la Política

Esta Política será revisada anualmente o cuando haya cambios significativos en los recursos tecnológicos, en la normativa legal aplicable o en la estructura organizacional.

B. Política de Control de Accesos

1. Propósito

El propósito de esta Política es establecer los lineamientos que aseguren que el acceso a los sistemas de información, redes y recursos tecnológicos de Culinary esté restringido únicamente a usuarios autorizados, conforme a sus roles y responsabilidades, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información.

2. Alcance

Esta Política aplica a todos los empleados, contratistas, consultores, proveedores y cualquier otro usuario que requiera acceso a los sistemas, aplicaciones, datos o infraestructura tecnológica de Culinary.

3. Principios Generales

- El acceso a los sistemas se concederá únicamente bajo el principio de mínimos privilegios.
- Todo acceso debe estar autorizado, documentado y justificado.
- Se debe asegurar la identificación y autenticación del usuario previo al acceso.

4. Tipos de Acceso

4.1 Acceso Físico: Se debe restringir el ingreso a salas de servidores, centros de datos y equipos críticos mediante tarjetas, llaves, biometría u otros controles. Por tanto, el acceso debe estar limitado al personal autorizado y registrado. Los visitantes deberán ser acompañados por personal autorizado.

4.2 Acceso Lógico: Requiere autenticación mediante credenciales únicas (nombre de usuario y contraseña) o mecanismos más seguros como el doble factor de autenticación (2FA). Se debe asignar acceso por roles, funciones o perfiles definidos previamente. Finalmente, el acceso a sistemas críticos debe ser auditable.

5. Gestión de Cuentas de Usuario

Las cuentas de usuario deben crearse únicamente por solicitud formal y aprobación de un supervisor o responsable autorizado.

Las cuentas inactivas por más de 90 días estarán sujetas a desactivación.

Las cuentas de usuarios que finalizan su relación laboral con la organización serán desactivadas inmediatamente.

6. Revisión y Auditoría de Accesos

TI realizará una revisión semestral de los permisos de acceso para asegurar que estén alineados con las funciones actuales del usuario. Toda asignación, modificación o eliminación de acceso debe quedar registrada.

7. Control de Acceso Remoto

El acceso remoto a los sistemas de la organización debe realizarse a través de canales seguros (por ejemplo, VPN corporativa con autenticación fuerte). Se debe registrar y monitorear toda conexión remota.

8. Privilegios de Administrador

El acceso con privilegios elevados (administradores, root, etc.) debe ser concedido solo a personal autorizado y capacitado. Deben mantenerse registros de uso de estas cuentas, y en lo posible, utilizar cuentas nominativas (no compartidas) para fines de auditoría.

9. Uso de Cuentas Compartidas

El uso de cuentas compartidas está prohibido, salvo casos excepcionales debidamente documentados y controlados.

10. Responsabilidades del Usuario

Todos los usuarios son responsables de:

- Proteger sus credenciales de acceso.
- No compartir ni divulgar sus contraseñas.
- Notificar inmediatamente a TI sobre accesos sospechosos o compromisos de cuentas.

11. Sanciones por Incumplimiento

El incumplimiento de esta Política podrá dar lugar a sanciones disciplinarias, legales o contractuales, conforme a las normas internas y leyes aplicables.

12. Revisión y Actualización

Esta Política será revisada al menos una vez al año o cuando existan cambios en la infraestructura tecnológica, procesos de negocio o normativas legales.

C. Política de Gestión de Contraseñas

1. Propósito

Establecer los lineamientos y requisitos mínimos para la creación, uso, almacenamiento y renovación de contraseñas en Culinary, con el fin de proteger los sistemas de información y garantizar la confidencialidad, integridad y disponibilidad de los datos.

2. Alcance

Esta política aplica a todos los usuarios (empleados, contratistas, proveedores y terceros) que tengan acceso a sistemas, aplicaciones, servicios o redes de Culinary, tanto internos como remotos.

3. Requisitos de Creación de Contraseñas

Las contraseñas deben cumplir los siguientes criterios mínimos:

- Tener una longitud mínima de 12 caracteres.
- Incluir al menos una letra mayúscula, una letra minúscula, un número y un carácter especial (por ejemplo: !, @, #, \$, %, &, *).
- No contener palabras comunes, nombres propios, información personal (fecha de nacimiento, DNI, nombres de familiares).
- No reutilizar contraseñas utilizadas anteriormente.

4. Vigencia y Renovación

- Las contraseñas deben cambiarse cada 90 días.
- El sistema debe evitar el reuso de al menos las últimas 5 contraseñas.
- El cambio de contraseña será obligatorio ante sospechas de compromiso o incidentes de seguridad.

5. Gestión de Contraseñas por el Usuario

- Las contraseñas son personales e intransferibles.
- No deben compartirse, escribirse en papel, ni almacenarse en archivos sin cifrar.
- Está prohibido el uso de contraseñas idénticas para múltiples sistemas, especialmente entre cuentas personales y laborales.

6. Cuentas con Privilegios Elevados

Las cuentas administrativas (root, admin, superuser) deben usar contraseñas aún más robustas y estar protegidas con doble factor de autenticación (2FA) si existe la opción. El acceso debe ser auditable y controlado.

7. Responsabilidades del Usuario

Los usuarios son responsables de crear y mantener contraseñas seguras, cambiar sus contraseñas inmediatamente si sospechan de una vulneración, cumplir con esta Política y reportar cualquier incidente relacionado.

8. Sanciones por Incumplimiento

El incumplimiento de esta Política puede derivar en acciones disciplinarias, incluyendo la suspensión del acceso a sistemas, sanciones contractuales o incluso la terminación de la relación laboral, dependiendo de la gravedad del incidente.

9. Revisión y Actualización

Esta Política será revisada al menos una vez al año o cuando se produzcan cambios significativos en la tecnología, legislación o estructura organizativa.