1. Objetivo

Establecer controles que limiten el acceso a la información y a los servicios tecnológicos únicamente a usuarios autorizados, de acuerdo con los requisitos del negocio y la seguridad de la información.

2. Alcance

Aplica a todo el personal que accede a recursos de información o tecnológicos en la organización, incluyendo redes WiFi, plataformas de almacenamiento en la nube, correos corporativos y sistemas de gestión.

3. Política de Control de Acceso (A.9.1.1)

- Solo el personal autorizado tiene acceso a recursos digitales como plataformas en la nube, sistemas de correo, infraestructura de desarrollo y archivos compartidos.
- Cada persona debe usar credenciales personales e intransferibles. Está prohibido compartir usuarios y contraseñas.
- El acceso se asigna de acuerdo con el rol del empleado, bajo el principio de **mínimo privilegio**.
- Se revisan accesos al menos una vez al año o ante cambios de rol, desvinculación de personal o detección de accesos innecesarios.

4. Acceso a Redes y Servicios en Red (A.9.1.2)

- El único medio autorizado para conectarse a servicios de la empresa es la **red WiFi corporativa** instalada en las oficinas.
- No se permite conectarse desde redes WiFi públicas o personales, salvo aprobación explícita del responsable de TI.
- La transferencia y almacenamiento de información se hace únicamente mediante **Google Drive** y **OneDrive**, bajo políticas de acceso restringido según área y función.
- Está prohibido el uso de VPNs, redes anónimas o cualquier forma de red alternativa sin autorización formal.

5. Control de acceso a sistemas y aplicaciones

Restricción de acceso a la información

Política:

- El acceso a la información y a las funciones de los sistemas de la organización estará limitado según el principio de mínimo privilegio.
- Sólo se otorgarán permisos necesarios para el desempeño de funciones específicas, y se documentará cada asignación.
- Cada usuario deberá acceder a las aplicaciones usando credenciales personales e intransferibles.

Demostración de cumplimiento:

- Control de accesos en Google Workspace, OneDrive y sistemas internos mediante cuentas nominativas.
  Se lleva un registro de usuarios activos, acceso a recursos compartidos y se revisan al menos una vez cada 6 meses.
- Acceso a plataformas como APIs y servicios de correo se otorga bajo solicitud autorizada y formato aprobado.

6 Procedimiento de ingreso seguro

Política

Cuando lo requiera la criticidad de la información o el riesgo asociado, el ingreso a los sistemas deberá realizarse mediante procesos de acceso seguro.

Controles implementados

- Autenticación mediante usuario y contraseña segura (mínimo 8 caracteres, con letras y números).

- Doble factor de autenticación (2FA) en correos, accesos a consola de servicios en la nube (ej: CPanel, CapRover,Google y OneDrive).
- Las contraseñas se actualizan cada 90 días o en caso de sospecha de compromiso. El acceso a sistemas desde redes no autorizadas está prohibido (solo desde la red WiFi interna autorizada).

7 Uso de programas utilitarios

Política:

- Solo se permite el uso de programas utilitarios que vienen preinstalados o que han sido aprobados por el área de operaciones y tecnología.
- El software antivirus provisto por el área de operaciones y TI (AVG) debe mantenerse actualizado automáticamente.
  No está permitido instalar herramientas adicionales (utilitarios de disco, redes, monitoreo, etc.) sin previa autorización.
- Se deberá evitar el uso de software portable o descargado desde sitios no verificados. Las actualizaciones del sistema operativo deben mantenerse activas para asegurar el correcto funcionamiento de las herramientas del sistema.

8 Responsabilidades

Los usuarios deben:

- Mantener sus contraseñas seguras y renovarlas cada 90 días. Reportar accesos no autorizados o pérdida de dispositivos de inmediato. El responsable de seguridad debe auditar accesos, definir políticas de asignación y revocación de permisos, y mantener un registro de los cambios.

CARLOS HUMBERTO TRONCOSO AYALDE
GERENTE GENERAL

VERSIÓN	CAMBIO	VIGENCIA
1	Primera versión	25/06/2024