A.9 Control de acceso (POL-05)

A.9 Control de acceso (POL-05)

1. Objetivo

Establecer las directrices para limitar el acceso a la información y a las instalaciones de procesamiento de información.

2. Alcance

Es de aplicación general a toda la organización y a los usuarios de recursos informáticos (equipo de cómputo y servidor) propiedad de DIGILOGICS.

3. Términos y Definiciones

- **Usuario:** persona que utiliza un dispositivo o equipo de cómputo, software y/o aplicación, realiza múltiples operaciones.
- **Clave de acceso o password:** es una combinación de letras y/o números que brinda, a quien lo conoce, la posibilidad de acceder a un recurso.
- **Privilegios o permisos de acceso**: conjunto de permisos dados a un usuario o a un sistema para acceder a un determinado recurso.
- **Red:** conjunto de computadoras y otros equipos interconectados, que comparten información, recursos y servicios.

4. Política

A.9.1 Requisitos del negocio para el control de acceso

A.9.1.1 Política de control de acceso

Para la aplicación de controles de acceso a los activos de información pertenecientes a DIGILOGICS, se tomarán en cuenta los siguientes aspectos:

a) Identificar los requerimientos de seguridad de las aplicaciones.
b) Los controles de acceso a los servicios de información, se asignarán con base en los roles y perfiles de los usuarios, según el servicio requerido.
c) Los requerimientos para la validación y retiro de los derechos de acceso, por evento vía correo electrónico.

A.9.1.2 Acceso a las redes y los servicios de la red

- Todos los servicios de información tendrán un registro de altas, bajas y cambios. Esto quedará declarado en el documento **Administración y control de accesos (POL-05.FO-01).**
- Todo colaborador tiene acceso a los sistemas de información dependiendo de las necesidades de su puesto, esto queda definido en el documento **Administración y control de accesos (POL-05.FO-01).** Se entregará una **Carta autorización de accesos (POL-05.FO-02)** con el tipo de nivel de acceso a cada usuario informático, los cuáles, deberán firmar de enterados.
- El Administrador Técnico de Seguridad en conjunto con el Oficial de Seguridad de la Información se encargarán de cambiar cada 6 meses, los permisos de acceso de usuario de cada colaborador. Los cambios de acceso y privilegios a cada usuario quedarán registrados en el documento **Carta autorización de accesos (POL-05.FO-02).**

A.9 Control de acceso (POL-05)

A.9.2 Gestión del acceso de usuarios

A.9.2.1 Registro y cancelación de usuarios

El proceso formal de registro de cuentas de usuario para los sistemas y servicios de Información será:

1. El Administrador técnico de seguridad deberá verificar siempre el puesto y roles a desempeñar del usuario, haciendo una vinculación con el acceso a la red y sistemas requeridos por el perfil de puesto.
2. Verificar con el usuario el acceso a los sistemas informáticos, garantizando el acceso seguro.
3. Entrega y firma de la **Carta autorización de accesos (POL-05.FO-02).**

El proceso formal de cancelación de cuentas de usuario para los sistemas y servicios de Información será:

1. Recursos materiales solicita la cancelación de usuario por correo electrónico al Administrador técnico de seguridad de la información.
2. El Administrador técnico de seguridad de la información realizará respaldo de la información del dispositivo del usuario.
3. Cancelación de los accesos a usuario.

A.9.2.2 Provisión de acceso de usuarios

- A todo colaborador desde el primer momento en que va iniciar labores se le otorga el usuario y claves de acceso, esto según su puesto. Se guardará registro de esta actividad en el documento **Administración y control de accesos (POL-05.FO-01).**
- Por cada servicio o aplicativo, son generadas cuentas diferentes o una misma cuenta, esto dependerá del tipo de perfil de puesto. Se guardará registro del acceso a los aplicativos o servicios en el documento **Administración y control de accesos (POL-05.FO-01).**
- El responsable de cada área es quien solicita por correo electrónico al Administrador técnico de seguridad de la información cuando solicite nuevos permisos a otros aplicativos o servicios.
- La Administración Técnica de Seguridad de la Información debe actualizar el documento **Administración y control de accesos (POL-05.FO-01).** siempre que existan altas, bajas, modificaciones en usuarios y aplicativos.
- La Dirección general también contará con acceso al documento **Administración y control de accesos (POL-05.FO-01).**
- En caso de que un usuario cambie sus claves de acceso a las aplicaciones o servicios que utiliza, debe de darlas a conocer al Administrador técnico de seguridad de la información. Éste debe actualizar el documento **Administración y control de accesos (POL-05.FO-01)** para el control total de las claves de acceso.

A.9.2.3 Gestión de derechos de acceso privilegiado

- La Administración Técnica de Seguridad de la Información tiene la responsabilidad de mantener regulado y controlado el uso y asignación de los privilegios otorgados a los usuarios.

- La solicitud de una cuenta de usuario privilegiado debe ser emitida formalmente por un humano vía correo electrónico, acompañada por el perfil de puesto del nuevo usuario. Debe cumplir con lo establecido en el punto 4.2.1 de la presente política.
- Las cuentas de usuario privilegiado sólo deben ser otorgadas al usuario final y únicamente para el cumplimiento de sus funciones.
- El Administrador técnico de seguridad de la información deberá ejecutar las siguientes actividades para la modificación de usuario:

    1. Solicitud formal vía correo electrónico por el responsable de área para la modificación de accesos y privilegios.
    2. El Administrador de seguridad de la información, deberá ingresar al panel de administración del servidor.
    3. Se modificarán los campos referentes a lo solicitado.
    4. Una vez completados los datos, se deberá el documento **Administración y control de accesos (POL-05.FO-01).**
    5. El usuario firma la **Carta autorización de accesos (POL-05.FO-02)** verificando los cambios a sus accesos y privilegios.

- Los accesos realizados con cuentas de usuario privilegiados deben ser registrados y controlados cada 6 meses.
- Una cuenta de usuario privilegiado sólo podrá ser utilizada en la actividad de administración o configuración del sistema para la cual se requieren dichos privilegios. No podrá ser utilizada en actividades rutinarias para la que exista un perfil de menores privilegios que lo permita.
- Las cuentas de usuario privilegiado tipo ADMIN, ROOT o similares, definidas por defecto, en sistemas y componentes, no pueden ser usadas. Siempre que sea posible las mismas deben ser eliminadas o deshabilitadas, además de modificadas sus contraseñas por omisión. Se debe contar con un mecanismo de recuperación de acceso privilegiado, dicho mecanismo debe mantener las garantías de reserva.
- El acceso privilegiado debe realizarse desde dispositivos debidamente fortalecidos para tal fin.

A.9.2.4 Gestión de información secreta de autenticación de los usuarios

- La administración de contraseñas, se gestiona por medio del documento **Administración y control de accesos (POL-05.FO-01).**
- La asignación de contraseñas debe cumplir conforme a lo siguiente:

    1. La contraseña debe tener al menos 8 caracteres.
    2. Si es usuario de Windows, asegúrese de que en las configuraciones de su sistema operativo esté establecido que la longitud mínima de contraseña no es menos de 8 dígitos.
    3. La contraseña debe contener por lo mínimo una letra mayúscula y una minúscula, cifras y caracteres especiales. Por ejemplo: oNQZnz$Hx2.
    4. Una contraseña segura no debe contener información personal que es fácil de averiguar. Por ejemplo: nombre, apellidos o fecha de nacimiento, palabras simples, frases hechas, conjuntos de símbolos fáciles de adivinar como password, contraseña, abcd, qwerty, asdfg, 1234567.

- La asignación de información secreta de autenticación se debe realizar a través de la **Carta de Autorización (POL-05.FO-02). V3.**

A.9.2.5 Revisión de los derechos de acceso de usuarios

- La Administración Técnica de Seguridad de la Información en conjunto con el Oficial de Seguridad de la Información deben realizar una verificación periódica a los elementos descritos en el documento **Administración y control de accesos (POL-05.FO-01)**, por lo menos una vez cada tres mes.

A.9.2.6 Eliminación o ajuste de los derechos de acceso

- La remoción de los derechos de acceso debe de hacerse de manera inmediata a la salida definitiva del personal (despido o renuncia), cambios de puesto o responsabilidades, área de Recursos humanos debe regular este proceso y notificar al Administrador técnico de seguridad de la información para que actualice el documento **Administración y control de accesos (POL-05.FO-01).**

A.9.3 Responsabilidades del usuario

A.9.3.1 Uso de la información secreta de autenticación

- Todo el personal de DIGILOGICS es responsable de su contraseña, la cual es confidencial y debe mantenerse secreta.
- Los lineamientos para la gestión básica de contraseñas son los siguientes:

  a) No se usan cuentas genéricas ni compartidas.
  b) Si el usuario realiza la modificación de su clave de acceso para los sistemas o aplicativos que lo requieran, debe notificar inmediatamente al Administrador de seguridad de la información.
  c) El usuario es el único responsable de su clave y por ende cualquier uso inadecuado de sus privilegios de acceso y claves, el usuario será sancionado. Para evitar esto, el usuario debe de reportar al Administrador de seguridad de la información de forma inmediata cualquier sospecha de que su clave ha sido revelada, vulnerada o compartida de manera no intencionada.

A.9.4 Control de acceso a sistemas y aplicaciones

A.9.4.1 Restricción de acceso a la información

- Los sistemas de información de DIGILOGICS se deben segregar para evitar accesos no autorizados; el uso de cuentas compartidas no es permitido.
- Las limitaciones a los usuarios están definidas por el control de privilegios de acceso que cada cuenta tiene, el fin es evitar accesos totales a utilerías, códigos fuentes o elementos de administrador de cuentas y equipos.
- Los tipos de acceso para cada usuario, están definidos en el documento **Administración y control de accesos (POL-05.FO-01).**

A.9.4.2 Procedimientos de inicio de sesión seguros

- Todo usuario en cada ingreso o inicio de sesión debe registrar su usuario y contraseña proporcionado por el la Administración Técnica de Seguridad de la Información o en su caso, la definida por el mismo usuario si es un aplicativo o un servicio.
- El primer acceso de los usuarios ser realizará en presencia del Administrador Técnico de Seguridad de la Información, garantizando así un acceso seguro.
- Las siguientes políticas deben ser aplicadas por todos los usuarios:

  a) Cerrar todas las sesiones en sistemas y servicios de información al finalizar su jornada laboral.
  b) Desconectarse y cerrar adecuadamente las sesiones en servidores, equipos de cómputo y aplicaciones al final de su jornada laboral.
  c) Los equipos de cómputo deben contar con la configuración automática de bloqueo de pantalla usando protector de pantallas.
  d) El tiempo de bloqueo de pantalla para cualquier dispositivo no puede sobrepasar el minuto de estar desatendido.

A.9.4.3 Sistemas de administración de contraseñas

- El resguardo y protección de las cuentas y claves de acceso descritas en el documento **Administración y control de accesos (POL-05.FO-01)**, es responsabilidad de la Administración Técnica de Seguridad de la Información. Su manejo es de acuerdo a la política de **Gestión de activos (POL-04).**
- El acceso a la ubicación de resguardo del documento **Administración y control de accesos (POL-05.FO-01)** se encuentra restringido a los colaboradores.
- La configuración y creación de contraseñas seguras, están definidos en el punto 4.2.4 de la presente política.

A.9.4.4 Uso de privilegios de los programas y utilidades

- Las cuentas de administrador y sus privilegios están definidos y aprobados por el Administrador Técnico de Seguridad y en casos específicos por la Alta Dirección, el acceso por omisión es de usuarios comunes sin privilegios de administración, dejando indicado esto en el documento Administración Control de Accesos, donde se debe definir los privilegios o permisos de acceso que debe contar cada cuenta de usuario.
- Para el acceso a la aplicación de videos “YouTube” está restringido a sólo material relacionado con el perfil del usuario.
- Otras aplicaciones de streaming de video se encuentran restringidos.
- El acceso a las aplicaciones de streaming musicales no están restringidos, pero sólo podrán ser escuchados por medio de auriculares.
- El acceso a redes sociales como Facebook, Instagram, Twitter, Snapchat, TikTok, Tinder, Bumble, y similares, es acceso restringido.
- Las descargas de servicios en la nube que permitan el intercambio de archivos libre, se encuentran prohibidos.
- Queda estrictamente prohibido el ingreso a páginas pornográficas.
- No es permitido la descarga de archivos de páginas no seguras.
- Para el uso de aplicaciones específicas o acceso temporal a páginas de internet, se requiere la autorización del Oficial de Seguridad de la Información.

ESTE PUNTO ES DE APLICACIÓN A TODOS LOS NIVELES DE LA ORGANIZACIÓN SIN EXCEPCIÓN.

5. Control de Versiones

Número de Versión	Fecha de Actualización	Descripción del Cambio
3	Marzo, 2021	Se actualizo el punto A.9.2.4