
digilogics

Control de acceso (POL-05)

1. Objetivo

Establecer las directrices para limitar el acceso a los activos de información de la organización.

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

- **Activo de información**: Se refiere a cualquier información o elemento (hardware, software, bases de datos, dispositivos de almacenamiento, edificios, personas, documentos, conocimiento, etc.) que tenga valor para la organización.
- **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.
- **Usuario:** persona que utiliza un dispositivo o equipo de cómputo, software y/o aplicación, realiza múltiples operaciones.

4. Política

A.5.15 Control de acceso

Para otorgar 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 (software)
b) Limitar los accesos a áreas donde se resguarden activos de información.
c) Asignar roles y perfiles de acuerdo a funciones.
d) Los requerimientos para la asignación o retiro de los derechos de acceso, deberán ser solicitados por el jefe inmediato al administrador técnico de seguridad por correo electrónico.

A.5.16 Gestión de la identidad

- Todo colaborador tendrá acceso a los sistemas de información dependiendo de las necesidades de su puesto.
- Por cada servicio o aplicativo, son generadas cuentas diferentes o una misma cuenta, esto dependerá del tipo de perfil de puesto.
- las cuentas que ya no se requieren deben desactivarse o eliminarse a su debido tiempo.
- Se guardará registro del acceso a los aplicativos o servicios en el documento **Administración y control de accesos.**

A.5.17 Información de autenticación

- La administración de contraseñas, se gestiona por medio del documento **Administración y control de accesos.**

- La asignación de contraseñas debe cumplir las siguientes reglas:

    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 mínimo una letra mayúscula y una minúscula, cifras y caracteres especiales. Por ejemplo: oNQZnz$Hx2.
    4. Una contraseña segura no debe contener información personal que es fácil de averiguar. Por ejemplo: nombre, apellidos o fecha de nacimiento, palabras simples, frases hechas, conjuntos de símbolos fáciles de adivinar como password, contraseña, abcd, qwerty, asdfg, 1234567.
    5. Modos de generar una contraseña:
        - El primer dígito es el número de caracteres del usuario.
        - El segundo dígito es “c” si el número en el primer paso es impar y “t” su es par.
        - El tercer digito es la última letra del nombre del usuario.
        - El cuarto dígito es “$” si la letra en el paso anterior es una vocal y “%” si es una consonante.
        - Los tres últimos dígitos son las tres primeras letras del nombre del usuario.
        - Incluir un carácter aleatorio al final de la contraseña.
        - En este ejemplo, utilizando el algoritmo propuesto, la contraseña para Twitter sería “7cr%twig”,
- La asignación de información secreta de autenticación se realizará a través de **la Carta de Autorización.**
- Los usuarios al firmar su carta de autorización se hacen responsables 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.
- 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.
- Las siguientes acciones deben ser aplicadas por todos los usuarios:

    a) Desconectarse y cerrar adecuadamente las sesiones en servidores, equipos de cómputo y aplicaciones al final de su jornada laboral.
    b) Los equipos de cómputo deben contar con la configuración automática de bloqueo de pantalla usando protector de pantallas.

A.5.18 Derechos de acceso

- No se deben usar cuentas genéricas ni compartidas.
- 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.
- El responsable de cada área o jefe inmediato del colaborador es quien solicita por correo electrónico al administrador técnico de seguridad de la información la alta, baja o modificación de cuentas de usuarios y sus respectivos permisos.

- 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** para el control total de las claves de acceso.
- El administrador técnico de seguridad se encargará de cambiar cada 3 meses, los permisos de acceso de usuario de cada colaborador.
- El administrador técnico de seguridad de la Información debe actualizar el documento **Administración y control de accesos** siempre que existan altas, bajas, modificaciones en usuarios y aplicativos.
- Los derechos de acceso son otorgados mediante la **Carta autorización de accesos.**

  El administrador técnico de seguridad de la Información debe realizar una verificación periódica a los elementos descritos en el documento **Administración y control de accesos**, por lo menos una vez cada tres meses, considerando los siguientes aspectos:

  a) Actualización de la lista de colaboradores dados de alta en los registros, altas y bajas realizadas durante el periodo, remoción de los derechos de acceso y nuevas configuraciones.
  b) Actualización de la lista del software con respecto al perfil de puesto.
  c) Actualización de cuentas de usuario y claves de acceso, con respecto a la frecuencia de actualización de los mismos.