POLÍTICA DE GESTIÓN DE ACCESOS

El Centro de Arbitraje Latinoamericano e Investigaciones Jurídicas -CEAR LATINOAMERICANO- establece la presente política con el propósito de garantizar que el acceso a la información, por parte de los usuarios, sea gestionado, controlado y autorizado exclusivamente por los propietarios de los activos de información. Su objetivo es salvaguardar la seguridad de la organización ante accesos no autorizados.

En este sentido, la organización ha definido las siguientes cláusulas:

1. REQUISITOS GENERALES DE CONTROL DE ACCESOS

1.1. El control de acceso a los sistemas de información debe realizarse mediante códigos de identificación y contraseñas únicas para cada usuario.

1.2. El Área de Administración es la única encargada de administrar los usuarios y contraseñas de todos los equipos de la organización.
Nota: La creación y/o cambio de usuarios y contraseñas será realizada por el Encargado de TI.

1.3. El nivel de acceso a los sistemas de información se otorgará en función de:

- Funciones del usuario.
- Perfiles de acceso estandarizados.
- Solicitud, autorización y administración de acceso.
- Segregación de funciones.
- Revisión periódica de privilegios.

1.4. Los sistemas de información deben bloquearse automáticamente después de un número máximo de intentos de acceso fallidos, para evitar ataques cibernéticos. El número máximo de intentos, así como el periodo transcurrido entre cada intento, debe ser configurable por cada sistema.

1.5. Toda aplicación informática deberá generar *logs* para intentos fallidos de inicio de sesión.

1.6. Cada equipo de cómputo debe ser asignado a un responsable, quien deberá garantizar su uso adecuado.

1.7. El Oficial de Seguridad de la Información puede realizar inspecciones y auditorías inopinadas en los equipos de la organización.

Av. Sánchez Carrión Nº 615
Edif. Vértice 22 Oficina 306 - Jesús María - Lima
51-(1) 397 8586 / 51-(1) 957 540 053
arbitraje@cearlatinoamericano.pe
Web: www.cearlatinoamericano.pe

1.8. En lo posible se deben usar sistemas o técnicas criptográficas (Cloudflare, discos duros encriptados, encriptado SSL) para proteger la información crítica y sometida a alto riesgo, cuando otras medidas o controles no proporcionen la protección adecuada.

2. ACCESO A REDES Y SERVICIOS DE RED

2.1. La organización debe establecer diferentes segmentos de red, dependiendo de la criticidad de las aplicaciones.

2.2. Los visitantes de la organización solo pueden usar la red WiFi: "Cear-Invitados".

2.3. Los perfiles de acceso deben considerar los servicios de red y conexiones a las redes a los que un usuario puede tener acceso.

2.4. Todos los dispositivos (equipos, móviles, laptops) que accedan a la red deben estar registrados en la base de datos de direcciones MAC.

2.5. Para la conexión de equipos a la red se debe considerar:

- Limitar los intentos fallidos de conexión; tras alcanzar el límite, el usuario será deshabilitado temporalmente.
- Asignar identificadores únicos a los equipos que se conecten a la red, conforme a los lineamientos establecidos.

3. GESTIÓN DE ACCESO DE USUARIO

3.1. Las cuentas deben ser utilizadas exclusivamente para actividades laborales y no para propósitos personales, ilegales o no éticos.

3.2. La creación, modificación o eliminación de cuentas de acceso debe ser autorizada por el Área de Administración.

3.3. En casos de cese o licencia, los permisos de acceso deben ser retirados o bloqueados.

3.4. En casos de rotación de personal, los accesos deben ser modificados según el nuevo rol, previa gestión del Jefe de Administración, Finanzas y RRHH.

3.5. El Responsable de TI debe administrar, llevar el control de la gestión de los accesos y validar la deshabilitación de los accesos en los principales sistemas del personal cesado.

3.6. Las contraseñas de acceso deben cambiarse cada seis (6) meses.

3.7. Para la creación y cambio de contraseña, se deben considerar las siguientes directrices:

Av. Sánchez Carrión Nº 615
Edif. Vértice 22 Oficina 306 - Jesús María - Lima
51-(1) 397 8586 / 51-(1) 957 540 053
arbitraje@cearlatinoamericano.pe
Web: www.cearlatinoamericano.pe

- Las cuentas de sistemas y red, la contraseña debe tener mínimo 8 caracteres y máximo 12 caracteres, combinando mayúsculas, minúsculas, números y caracteres especiales.
- No debe considerarse nombres, palabras comunes, ni datos personales.
- Al cambiarla, no debe considerarse las últimas dos (2) contraseñas utilizadas.
- Las cuentas genéricas deben tener contraseñas de al menos 12 caracteres y, de ser posible, diferentes para cada sistema y servidor.

3.8. Si se sospecha que una cuenta ha sido comprometida, el usuario debe reportarlo al Oficial de Seguridad de la Información y este debe cambiar la contraseña de inmediato.

3.9. Las contraseñas no deben almacenarse en mecanismos automáticos de conexión que las guarden en el equipo.

4. REVISIÓN DE DERECHOS DE ACCESO

4.1. El Jefe de Administración, Finanzas y RRHH, junto con el Oficial de Seguridad de la Información, debe revisar periódicamente los derechos de acceso y revocar aquellos que hayan caducado, no estén en uso o no correspondan a la función actual del colaborador.

5. RESTRICCIÓN DE ACCESO A LA INFORMACIÓN

5.1. El propietario de cada activo de información debe garantizar que los usuarios accedan a la información según su perfil de usuario y nivel de clasificación. En la generación de perfiles, se debe controlar los derechos de acceso a lectura, escritura, borrado y ejecución, analizado entre la organización y el área usuaria.

5.2. Se prohíbe almacenar información de la organización en sitios web de almacenamiento externo o convertidores de documentos. Únicamente se permite el uso de OneDrive en las cuentas asignadas.

5.3. Todos los trabajadores deben mantener el acceso a la información restringido a las personas autorizadas.

5.4. Los derechos/privilegios del SISTELAR, cuentan con derechos de acceso para cada tipo de usuario.

Roles Internos:

- Mesa de Partes Virtual
- Secretaría General
- Secretaría Arbitral

Av. Sánchez Carrión Nº 615
Edif. Vértice 22 Oficina 306 - Jesús María - Lima
51-(1) 397 8586 / 51-(1) 957 540 053
arbitraje@cearlatinoamericano.pe
Web: www.cearlatinoamericano.pe

- Administración
- Profesionales (Árbitros, Adjudicadores, Peritos)
- Admin del Sistema

Roles Externos:

- Partes (Contratista y Entidad)
- Terceros
- Procuraduría

6. PROCEDIMIENTOS DE INGRESO SEGURO

6.1. El trabajador debe asumir la responsabilidad sobre su cuenta de usuario y proteger el acceso a su estación de trabajo mediante el uso de protectores de pantalla o *logout* del sistema.

6.2. En la organización debe restringirse y controlarse estrechamente el uso de programas utilitarios que puedan vulnerar los controles del sistema y las aplicaciones.

6.3. Si el sistema lo permite se debería utilizar el doble factor de autenticidad (2FA).

7. CONTROL DE ACCESO AL CÓDIGO FUENTE DE LOS PROGRAMAS

7.1. El acceso al código fuente de los programas debe estar restringido únicamente a personal autorizado para su edición o modificación.

7.2. En caso de aplicaciones desarrolladas por proveedores externos, se deben revisar las condiciones establecidas en el contrato.

Firmado por la Gerente General: Verónica Sandoval Larraín.

CEAR LATINOAMERICANO S.A.C.
VERONICA SANDOVAL LARRAIN
Gerente General

Av. Sánchez Carrión Nº 615
Edif. Vértice 22 Oficina 306 - Jesús María - Lima
51-(1) 397 8586 / 51-(1) 957 540 053
arbitraje@cearlatinoamericano.pe
Web: www.cearlatinoamericano.pe