POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN RECURSOS HUMANOS

El objetivo de esta política es garantizar la seguridad de la información en todas las etapas del proceso laboral en el Centro de Arbitraje Latinoamericano e Investigaciones Jurídicas -CEAR LATINOAMERICANO-, abarcando la vinculación, ejecución y desvinculación del personal.

Para ello, se establecen las siguientes disposiciones:

1. BÚSQUEDA Y SELECCIÓN DE NUEVO PERSONAL

1.1. El Área de Recursos Humanos (RRHH) debe seguir los lineamientos establecidos en el **PR-07 Procedimiento de Recursos Humanos** para la evaluación de los candidatos a colaboradores de la organización.

1.2. El legajo de postulantes debe almacenarse en la plataforma OneDrive, dentro de la carpeta del área de RRHH, a la cual solo tendrá acceso el Área de Recursos Humanos (RRHH).

1.3. Los currículums vitae (CV) de los postulantes se almacenarán exclusivamente para fines laborales tanto de manera física como también en la carpeta One Drive del área de RRHH por un tiempo máximo de 10 años.

1.4. El Área de Recursos Humanos (RRHH) debe realizar la debida diligencia de los postulantes seleccionados, en cumplimiento de las leyes, reglamentos y requisitos de la organización. Se deberá garantizar la privacidad y la protección de los datos personales del postulante, considerando lo siguiente:

- Verificación y disponibilidad de referencias laborales.
- Comprobación de documentos de identificación, tales como currículum vitae, certificados académicos y profesionales.
- Evaluaciones adicionales, tales como antecedentes penales, policiales y/o verificaciones a través del Certijoven o Certiadulto.
- Firma de acuerdo de confidencialidad.
- Autorización de uso de imagen y voz (en caso aplique).
- Documentación de la debida diligencia.

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

2. TÉRMINOS Y CONDICIONES DEL EMPLEO

2.1. El Área de Recursos Humanos (RRHH) debe garantizar que todos los colaboradores firmen un acuerdo de confidencialidad y no divulgación al momento de su contratación. Dicho acuerdo debe especificar el período de vigencia y las acciones a tomar en caso de incumplimiento.

2.2. El Jefe de Administración, Finanzas y RRHH debe asegurarse de que todos los colaboradores conozcan y acepten las políticas de Seguridad de la Información de la organización. (al momento de la inducción de ingreso al personal se debe difundir las políticas del sistema integrado de gestión del CENTRO)

3. DURANTE EL EMPLEO

3.1. El Oficial de Seguridad de la Información debe coordinar con el Área de Recursos Humanos (RRHH) para garantizar que los empleados que ingresen a la organización conozcan sus roles y responsabilidades en materia de Seguridad de la Información.

3.2. Todos los jefes de área deben asegurar que el personal y terceros a su cargo cumplan con las políticas y procedimientos de Seguridad de la Información establecidos en la organización, así como con sus roles y responsabilidades.

3.3. Cada colaborador está obligado a reportar al Oficial de Seguridad de la Información cualquier incidente o evento de seguridad de la información del que tenga conocimiento, utilizando los medios y procedimientos establecidos en el **PR-24 Procedimiento de Gestión de Incidentes de Seguridad de la Información**.

4. CONCIENCIA, EDUCACIÓN Y CAPACITACIÓN SOBRE LA SEGURIDAD DE LA INFORMACIÓN

4.1. Se deben realizar charlas de inducción y sensibilización dirigidas al personal de la organización, en las que se difundan temas relacionados con la Seguridad de la Información, su contribución a la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI), los beneficios de un mejor desempeño y las consecuencias del incumplimiento de los requisitos establecidos en el SGS.

4.2. La asistencia del personal a las charlas de inducción y sensibilización en Seguridad de la Información debe ser registrada de manera formal.

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

5. PROCESOS DISCIPLINARIOS

5.1. La organización ha establecido que toda violación a las normas internas, incluidas las políticas y procedimientos de Seguridad de la Información, será sujeta a sanciones disciplinarias, tales como:

5.1.1. Llamada de atención verbal

- Aplicable para faltas leves o cuando es la primera infracción.
- Se deja constancia informal, aunque puede anotarse en una bitácora de RR.HH.

5.1.2. Amonestación escrita

- Cuando hay reincidencia de faltas leves o se incurre en una falta moderada.
- Se entrega al trabajador una carta firmada y se archiva en su legajo personal.

5.1.3. Suspensión temporal sin goce de haber

- Para faltas moderada. La suspensión puede ser por uno o varios días, según la falta.
- Debe estar debidamente motivada y documentada, cumpliendo con el debido proceso.

5.1.4. Cambio de puesto o reasignación

- En casos donde el trabajador representa un riesgo en su puesto actual.
- Se puede aplicar con acuerdo previo o como medida temporal.

5.1.5. Terminación del contrato de trabajo por falta grave (despido)

Para casos de violaciones serias, como:

- Robo de información
- Filtración intencional de datos confidenciales
- Incumplimiento reiterado de políticas internas
- Uso indebido de recursos tecnológicos
- Incumplimiento grave de obligaciones contractuales

5.2. El área de RRHH ha definido como falta leve, moderada o grave de la siguiente manera:

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

5.2.1. Faltas Leves

Son acciones que no causan un daño directo o significativo a los activos de información, pero que incumplen disposiciones establecidas y pueden generar riesgos si se repiten. Ejemplos:

- No bloquear la pantalla del equipo al ausentarse del puesto de trabajo.
- Dejar documentos impresos en áreas comunes sin custodia.
- Utilizar contraseñas débiles, pese a la capacitación o política interna.
- No reportar inmediatamente un incidente menor (como un correo sospechoso).
- Descuidar el uso de dispositivos de almacenamiento (USB) sin cifrado, sin que haya fuga.

5.2.2. Faltas Moderadas

Acciones que comprometen la confidencialidad, integridad o disponibilidad de la información de forma parcial, sin haber intencionalidad comprobada, pero con riesgo relevante para la organización.

Ejemplos:

- Compartir credenciales de acceso con otro colaborador (aunque no se haya producido un incidente).
- Instalar software no autorizado en el equipo de la organización.
- Utilizar canales no aprobados para transmitir información sensible (por ejemplo, WhatsApp personal).
- Eliminar o modificar información sin autorización previa.
- Reincidencia en faltas leves.

5.2.3. Faltas Graves

Acciones que causan o tienen alta probabilidad de causar un daño severo, deliberado o negligente, a los activos de información, reputación o cumplimiento legal de la organización.

Ejemplos:

- Filtrar o divulgar información confidencial o sensible sin autorización.
- Acceder intencionalmente a información fuera del ámbito de funciones.
- Manipular, borrar o sustraer información crítica de forma no autorizada.
- Realizar actividades fraudulentas usando los sistemas de la organización.
- Utilizar los sistemas corporativos para fines ilegales.

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

- Reincidencia en faltas moderadas.
- Vandalismo en la organización / daño intencional de los activos de la información.

6. TERMINACIÓN O CAMBIO DE RESPONSABILIDADES DEL EMPLEO

6.1. El Área de Recursos Humanos (RRHH) es responsable del proceso de finalización del empleo del colaborador, debiendo coordinar con el jefe inmediato y, de ser necesario, con el Oficial de Seguridad de la Información.

6.2. El Jefe de Administración, Finanzas y RRHH debe informar oportunamente a los responsables de los procesos de cese sobre la finalización del contrato del colaborador, a fin de tomar las medidas preventivas y correctivas necesarias.

6.3. Los jefes de área deben notificar de manera inmediata al Área de Recursos Humanos (RRHH) sobre cualquier cese imprevisto de personal.

6.4. El encargado de TI y/o el Jefe de Administración, Finanzas y RRHH deben actualizar los accesos del colaborador conforme a los perfiles de usuario definidos en el procedimiento control de acceso.

6.5. En caso de terminación del contrato, el Jefe de Administración, Finanzas y RRHH debe iniciar oportunamente las acciones para la devolución de activos de información.

6.6. En caso de que un colaborador cambie de funciones, se deben seguir los procedimientos establecidos para garantizar la entrega de activos, la actualización de accesos, la transferencia de información y la posterior asignación de recursos acorde a su nuevo rol.

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