Documento sobre seguridad de la información y cumplimiento de la Ley N° 29733, Ley de Protección de Datos Personales.

I. INTRODUCCIÓN

El presente documento forma parte de los elementos de seguridad y protección de los datos personales sobre los cuales Cintac mantiene un interés y ejerce un uso conforme a las disposiciones aplicables en la materia:

- Ley N° 29733, Ley de Protección de Datos Personales.
- Decreto Supremo N° 016-2024-JUS, que aprueba el Reglamento de la Ley N° 29733.
- Resolución Directoral N° 019-2013-JUS/DGPDP, que aprueba la Directiva de Seguridad de la Información Administrada por los Bancos de Datos Personales.

Los datos personales, así como la información en general, son elementos importantes para el funcionamiento de una organización y más si se trata de información comercial o de índole confidencial. Dichos activos incluyen diversos datos de titularidad de trabajadores, postulantes y proveedores que se originan o producen como parte de la ejecución de las obligaciones contraídas por Cintac.

En este sentido, el presente documento proporciona las reglas que debe cumplir el personal expresamente habilitado para acceder, manipular y transmitir cierto tipo de información de manera tal que se asegure su correcto tratamiento bajo el amparo de la legislación antes indicada.

II. ÁMBITO DE APLICACIÓN

A continuación, se describirá el ámbito de aplicación que corresponde al presente documento:

- **¿Quiénes deben cumplir con lo dispuesto en el presente documento?**

  Las medidas y procedimientos a los que se hace referencia en este documento son de obligatorio cumplimiento para todo el personal de Cintac

que realice algún tipo de uso sobre la información referida en el acápite precedente.

Las personas con acceso a información de Cintac se encuentran obligadas a cumplir con lo dispuesto en el presente documento. Estas personas se clasifican en dos (02) categorías:

a) **Administradores:** Personas específicamente designadas por Cintac para supervisar la correcta gestión y utilización de la información que se encuentra comprendida en el ámbito de aplicación del presente documento.

Los Administradores tienen a su cargo: (i) fiscalizar el cumplimiento del presente documento; (ii) supervisar el uso que el Usuario efectúe con la información contenida o destinada a ser contenidos en las Bases de Datos de Cintac; (iii) presentar un reporte dirigido al equipo de tecnologías de la información detallando los problemas que pueda identificar durante la aplicación del presente documento; (iv) proponer las modificaciones y mejoras al presente documento; y, (v) autorizar el acceso a las Bases de Datos.

NOTA: Los Administradores, dada la cercanía con los activos informativos, podrán recaer en los miembros de las áreas: i) legal; y/o, (ii) tecnologías de la información. Siendo preferentemente que sea designado a un miembro del área legal.

b) **Usuarios:** Todo personal -distinto de los Administradores- que se encuentre previamente autorizado por los Administradores para acceder a la información comprendida en el ámbito de aplicación del presente documento y que, por tanto, accede o puede acceder a soportes físicos o digitales que contienen dicha información.

III. SOBRE EL RESPONSABLE DE SEGURIDAD Y CUMPLIMIENTO DEL PRESENTE DOCUMENTO

Cintac designará al "Responsable de Seguridad" (quien podrá ser uno de los Administradores). Esta persona será el coordinador de los distintos Administradores y el encargado de la correcta aplicación del presente

documento. Para el desempeño de sus labores, el Responsable de Seguridad contará con el apoyo de la Gerencia General de Cintac.

Todos los Usuarios reciben capacitaciones anuales en materia de Seguridad de la Información para comprender su importancia, su aplicación en Cintac y tomar conciencia sobre las medidas de seguridad aplicables.

IV. MEDIDAS DE SEGURIDAD

- **Acceso a la Información**

1. Únicamente el Usuario tendrá acceso a la información. Los Administradores designarán a aquel personal de Cintac que tendrá la calificación de Usuario respecto de la información a su cargo.

2. Los Usuarios únicamente tendrán acceso a aquella información que sea necesaria para el desempeño normal de sus labores y/o funciones. En este sentido, los Administradores deberán identificar cuál es el tipo de información a los que puede acceder y los usos que podrán efectuar cada uno de los Usuarios.

3. Cada Usuario será responsable por la seguridad tanto de la información como de los soportes físicos que la contenga y que se encuentren bajo su custodia.

4. Se deberá tener especial cuidado con el acceso que se otorgue a la información que tenga la calificación de sensible. Cualquier solicitud de acceso referida a este tipo de información por parte de los Usuarios, y la correspondiente autorización por parte de los Administradores, deberá estar adecuadamente sustentada y documentada.

- **Gestión de Contraseñas y acceso a los sistemas informáticos de Cintac**

5. Todo acceso a la información mediante los sistemas de informáticos de Cintac debe realizarse previa identificación mediante un usuario y contraseña cuya obtención será coordinada con el Administrador. Las contraseñas deben ser elaboradas procurando que éstas no posean caracteres fácilmente identificables. Su uso estará exclusivamente asociado

a un Usuario y, por tanto, se encuentra prohibido compartir el usuario y contraseña con otras personas.

6. Cualquier incidencia relacionada con los usuarios y/o contraseñas debe ser comunicada de inmediato al Responsable de Seguridad.

7. La gestión de contraseñas permite discriminar el tipo de información a los que podrá acceder determinado usuario. Sin embargo, al poder estar los equipos de cómputo conectados con otros ordenadores y/o al internet, es posible que terceros intenten acceder indebidamente a los sistemas informáticos de Cintac.

   En este sentido, usuario deberá comunicar inmediatamente al Responsable de Seguridad cualquier acceso no autorizado o anomalía que hubiera detectado. Será el Responsable de Seguridad quien adoptará las medidas correctivas del caso, informando de dicha situación a los socios de Cintac.

8. **Política de usuarios y contraseñas:** El proceso de asignación de usuario y contraseña antes descrito comprende lo siguiente:

   a) Registro del día y hora en que se realizó la asignación.
   b) Registro de quién autorizó dicho usuario y contraseña.
   c) La contraseña es entregada con texto recordatorio de mantenerla en secreto.
   d) La contraseña está habilitada para ser cambiada por el usuario.
   e) La contraseña debe ser de al menos 8 dígitos, alfanuméricas (mayúsculas, minúsculas y números) y debe incluir un caracter especial.
   f) La contraseña deberá ser cambiada en el lapso de 1 hora en caso de que su confidencialidad se vea comprometida.
   g) La contraseña no deberá constar en medios escritos (o en medios no cifrados en general).

9. Cada Usuario tendrá trazabilidad sobre sus interacciones, pues se llevará un registro del horario de acceso, hora de salida, acción relevante realizada con cada documento y motivo de acceso. Los accesos deben ser personales y no asignados de forma grupal.

10. Asimismo, y a fin de reducir los riesgos antes descritos, se encuentra prohibida la instalación de cualquier *software* que no haya sido previamente autorizado por el Administrador.

11. Además, se cuenta con controles especiales para usuarios remotos y computación móvil, de forma que se cumpla con los mismos niveles de seguridad que el Usuario que se encuentra presencialmente en las instalaciones de Cintac.

12. El Administrador podría determinar que corresponde retirar algún acceso a la información mediante los sistemas informáticos si el Usuario dejara de prestar sus servicios a Cintac, si cambiara de rol dentro de Cintac (y por lo tanto ya no necesite tener acceso a la información), o de identificarse un incumplimiento de las medidas de seguridad. En estos casos, se podrá deshabilitar el usuario y contraseña asignado al Usuario y será suprimido del sistema. Además, se llevará un registro que permita visualizar: i) el día y la hora del retiro del usuario y contraseña; ii) quién fue la persona encargada que llevó a cabo este proceso; y, iii) qué privilegios fueron retirados.

- **Ubicación y acceso al soporte utilizado para conservar la información**

13. En caso los equipos informáticos y los documentos físicos ubicados dentro de las instalaciones de Cintac contenga información descrita en el ámbito de aplicación del presente documento, únicamente podrán ser accedidos por usuarios cumpliendo las condiciones descritas en la sección anterior.

14. Los equipos informáticos y documentos físicos deben estar ubicados en espacios seguros y que impidan el ingreso y/o acceso no controlado de terceros. Se entenderá como tercero toda persona que no mantenga algún tipo de vinculación laboral y/o contractual con Cintac o que, incluso teniendo algún vínculo laboral y/o contractual, no sea considerada como Usuario.

15. Para la conservación en ambientes físicos de la información se siguen los parámetros de la NTP ISO/IEC 17799 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de Seguridad de la Información. Así, entre otros, se cumplen con los siguientes estándares:

a) Los archivadores se encuentran protegidos con sistemas de acceso por puertas.
b) Por protocolo, las puertas se cierran con llave cuando no se usan los documentos.
c) La zona de almacenamiento cuenta con protección contra daños ambientales.
d) Todo documento que es copiado pasa por un proceso de supervisión, pues la copia debe ser previamente autorizada por el Administrador. Se cuenta con trazabilidad sobre las copias pues el sistema de impresoras y fotocopiado permite conocer quién lo copió, cuántas copias obtuvo y la descripción del archivo copiado.

16. Cada equipo informático debe estar etiquetado con un código que permita su identificación inmediata. Del mismo modo, los soportes físicos deberán estar debidamente catalogados de manera tal que permitan identificar su ubicación y contenido.

17. En caso los soportes físicos o digitales en los que se encuentren la información requieran de algún tipo de intervención por parte de terceros (situación que puede presentarse, por ejemplo, cuando los equipos de cómputo y servidores son objeto de mantenimiento), se requerirá la autorización previa del Administrador quien, a su vez, deberá verificar que el tercero con acceso a tales soportes físicos o digitales, no tenga acceso efectivo a la información contenida en ellos.

18. Para el traslado de los soportes que contengan información comprendida dentro del ámbito de aplicación del presente documento hacia un local distinto al cual se encuentran físicamente dichos soportes, deberá adoptarse las precauciones que sean razonables para evitar cualquier pérdida de información o acceso no autorizado por parte de terceros.

19. Sin que la presente lista exhaustiva, se adoptarán las siguientes medidas: (i) cualquier traslado de los soportes requerirá autorización previa por parte del Administrador; (ii) se deberá llevar un registro que detalle los soportes que son objeto de traslado, la persona designada para llevar a cabo el traslado, y de la persona que recibió los soportes; y, (iii) deberá verificarse que tanto el medio de transporte como el local a donde serán trasladados

los soportes estén adecuadamente acondicionado para impedir el acceso de terceros.

- **Conservación y respaldo**

20. Se cuenta con un sistema de almacenamiento y respaldo informático que permite la recuperación completa de la información ante una eventual interrupción o daño. Este sistema de almacenamiento cuenta con una localización diferente y a suficiente distancia de la localización principal que es respaldada.

- **Integridad de la red y control de incidentes**

21. Los sistemas digitales utilizados por Cintac son seguros, cuentan con antivirus instalados para la protección frente a software malicioso y reciben mantenimiento preventivo conforme a las recomendaciones del proveedor de software. Además, los sistemas permiten la encriptación de la información si esta será transmitida electrónicamente a terceros, así como cuando es almacenada por proveedores de *hosting* y *cloud computing*.

22. En el eventual e improbable caso de que ocurra un incidente de seguridad que comprometa la información comprendida dentro del ámbito de aplicación del presente documento, se cuenta con un protocolo y metodología de gestión de riesgos para informar al titular de los datos personales que fueron comprometidos de manera inmediata. La información se encuentra clasificada según el nivel de riesgo que implicaría un posible incidente de seguridad, por lo que se tiene claridad y trazabilidad sobre esta información ante un eventual incidente.

- **Ingreso de nueva información y modificación de la existente**

23. Cualquier incorporación de nueva información o la modificación o eliminación de los ya contenidos en las Bases de Datos, únicamente podrá ser realizado por el Administrador para dicho fin específico.

24. En caso la información deje de ser útil o necesaria para Cintac, será eliminada, así como todas sus copias o reproducciones.

25. Los datos relacionados serán eliminados únicamente previa autorización del Administrador y se cuenta con un equipo especializado autorizado encargado de la eliminación de esta información.

26. Una vez que la información sea suprimida, el sistema no permitirá recuperarla.

V. CONSULTAS VINCULADAS CON LA IMPLEMENTACIÓN DEL PRESENTE DOCUMENTO

Los Administradores son los responsables de absolver cualquier pregunta que los Usuarios tengan respecto a la aplicación del presente documento. Las consultas serán dirigidas al correo institucional del Administrador vinculado a la consulta.

De ser necesario, los Administradores contarán con el apoyo del Responsable de Seguridad.

VI. CONTROL PERIÓDICO DEL CUMPLIMIENTO DEL PRESENTE DOCUMENTO

El Responsable de Seguridad deberá realizar las gestiones necesarias para que, una vez por año, se lleve a cabo un control sobre el nivel de cumplimiento de las reglas contenidas en el presente documento.

Se otorga un énfasis especial a la auditoría sobre el funcionamiento del sistema de privilegio de accesos, administración de derechos y perfiles y el sistema de respaldo.

VII. MODIFICACIONES AL PRESENTE DOCUMENTO

El Responsable de Seguridad, por iniciativa propia o por sugerencia de los Administradores, podrá solicitar modificaciones al presente documento; las cuales serán analizadas y, de ser el caso, aprobadas por Cintac.

ANEXO: REVISIÓN DE MEDIDAS DE SEGURIDAD

- ***Acceso a la Información***

N°	Medida	Verificación Sí/No
1	Se ha designado al personal de Cintac con la calificación de Usuario respecto de la información a su cargo.	
2	Se requiere que cualquier solicitud de acceso a datos personales por parte de los Usuarios, y la correspondiente autorización por parte de los Administradores, deba estar adecuadamente sustentada y documentada.	

- ***Gestión de contraseñas y acceso a los sistemas informáticos de Cintac***

N°	Medida	Verificación Sí/No
1	Todo acceso a la información mediante los sistemas de informáticos de Cintac se realiza previa identificación mediante un usuario y contraseña.	
2	Las contraseñas deben ser elaboradas procurando que éstas no posean caracteres fácilmente identificables.	
3	La gestión de contraseñas permite discriminar el tipo de información a los que podrá acceder determinado Usuario.	
3	Se ha informado al usuario que se encuentra obligado a informar inmediatamente al Responsable de Seguridad cualquier acceso no autorizado o anomalía que hubiera detectado.	
	Sobre la política de usuarios y contraseñas de Cintac	
4	El proceso de asignación de usuario y contraseña comprende lo siguiente: • Registro del día y hora en que se realizó la asignación.	

- Registro de quién autorizó dicho usuario y contraseña.
- La contraseña es entregada con texto recordatorio de mantenerla en secreto.
- La contraseña está habilitada para ser cambiada por el usuario.
- La contraseña debe ser de al menos 8 dígitos, alfanuméricas (mayúsculas, minúsculas y números) y debe incluir un carácter especial.
- La contraseña deberá ser cambiada en el lapso de 1 hora en caso de que su confidencialidad se vea comprometida.
- La contraseña no deberá constar en medios escritos (o en medios no cifrados en general).

5	Se tiene trazabilidad sobre las interacciones de cada Usuario.
6	Se lleva un registro del horario de acceso, hora de salida, acción relevante realizada con cada documento y motivo de acceso.
7	Los accesos son personales y no asignados de forma grupal.
8	Se encuentra prohibida la instalación de cualquier *software* que no haya sido previamente autorizado por el Responsable de Seguridad.
9	Se cuenta con controles especiales para usuarios remotos y computación móvil, de forma que se cumpla con los mismos niveles de seguridad que el Usuario que se encuentra presencialmente en las instalaciones de Cintac.
10	Se puede deshabilitar el usuario y contraseña asignado al Usuario y suprimirlo del sistema cuando este dejara de prestar sus servicios a Cintac, si cambiara de rol dentro de Cintac (y por lo tanto ya no necesite tener acceso a la información), o de identificarse un incumplimiento de las medidas de seguridad.
11	Se lleva un registro que permite visualizar: i) el día y la hora del retiro del usuario y contraseña; ii) quién fue

la persona encargada que llevó a cabo este proceso; y, iii) qué privilegios fueron retirados.

- ***Ubicación y acceso al soporte utilizado para conservar la información***

N°	Medida	Verificación Sí/No
1	En caso los equipos informáticos y los documentos físicos ubicados dentro de las instalaciones de Cintac contenga información descrita en el ámbito de aplicación del presente documento, únicamente pueden ser accedidos por Usuarios cumpliendo con la gestión de contraseñas.	
2	Los equipos informáticos y documentos físicos están ubicados en espacios seguros que impiden el ingreso y/o acceso no controlado de terceros.	
3	Para la conservación en ambientes físicos de la información, entre otros, se cumplen los siguientes estándares: • Los archivadores se encuentran protegidos con sistemas de acceso por puertas. • Por protocolo, las puertas se cierran con llave cuando no se usan los documentos. • La zona de almacenamiento cuenta con protección contra daños ambientales. • Todo documento que es copiado pasa por un proceso de supervisión, pues la copia debe ser previamente autorizada por el Administrador. Se cuenta con trazabilidad sobre las copias pues el sistema de impresoras y fotocopiado permite conocer quién lo copió, cuántas copias obtuvo y la descripción del archivo copiado.	
4	Cada equipo informático está etiquetado con un código que permita su identificación inmediata.	
5	Los soportes físicos están debidamente catalogados de manera tal que permitan identificar su ubicación y contenido.	

6	En caso los soportes físicos o digitales en los que se encuentren la información requieran de algún tipo de intervención por parte de terceros (situación que puede presentarse, por ejemplo, cuando los equipos de cómputo y servidores son objeto de mantenimiento), se requiere la autorización previa del Administrador.	
7	Para el traslado de los soportes que contengan información comprendida dentro del ámbito de aplicación del presente documento hacia un local distinto al cual se encuentran físicamente dichos soportes, se adoptan las precauciones que sean razonables para evitar cualquier pérdida de información o acceso no autorizado por parte de terceros.	
8	Se adoptan las siguientes medidas: (i) cualquier traslado de los soportes requiere autorización previa por parte del Administrador; (ii) se lleva un registro que detalle los soportes que son objeto de traslado, la persona designada para llevar a cabo el traslado, y de la persona que recibió los soportes; y, (iii) se verifica que tanto el medio de transporte como el local a donde serán trasladados los soportes estén adecuadamente acondicionado para impedir el acceso de terceros.	

- ***Conservación y respaldo***

N°	Medida	Verificación Sí/No
1	Se cuenta con un sistema de almacenamiento y respaldo informático que permite la recuperación completa de la información ante una eventual interrupción o daño.	
2	Este sistema de almacenamiento cuenta con una localización diferente y a suficiente distancia de la localización principal que es respaldada	

- ***Integridad de la red y control de incidentes***

N°	Medida	Verificación Sí/No
1	Los sistemas digitales utilizados por Cintac son seguros, cuentan con antivirus instalados para la protección frente a software malicioso y reciben mantenimiento preventivo conforme a las recomendaciones del proveedor de software.	
2	Los sistemas permiten la encriptación de la información si esta será transmitida electrónicamente a terceros, así como cuando es almacenada por proveedores de *hosting* y *cloud computing*.	
3	En el eventual e improbable caso de que ocurra un incidente de seguridad que comprometa la información comprendida dentro del ámbito de aplicación del presente documento, se cuenta con un protocolo y metodología de gestión de riesgos para informar a los titulares de datos personales que fueron comprometidos de manera inmediata.	

- ***Ingreso de nueva información y modificación de la existente***

N°	Medida	Verificación Sí/No
1	En caso la información deje de ser útil o necesaria para Cintac, es eliminada, así como todas sus copias o reproducciones.	
2	Los datos relacionados son eliminados únicamente previa autorización del Administrador.	
3	Se cuenta con un equipo especializado autorizado encargado de la eliminación de esta información.	
4	Una vez que la información es suprimida, el sistema no permite recuperarla.	

- ***Adicional: Sobre la videovigilancia***

N°	Medida	Verificación Sí/No

1	Se ha colocado en todos los ambientes en donde se realice videovigilancia un cartel informativo que advierta a cualquier tipo de persona que sus actividades se encuentran siendo videovigiladas.
2	El cartel informativo cumple con los requisitos mínimos exigidos por la Directiva para el Tratamiento de Datos Personales mediante Sistemas de Videovigilancia.
3	Las cámaras de videovigilancia no deberán captar o grabar imágenes, videos o audios del interior de baños, espacios de aseo, vestuarios, vestidores y en general espacios protegidos por el derecho a la intimidad personal.
4	Las grabaciones realizadas no serán compartidas ni visualizadas por terceros. Únicamente se podrá realizar su compartición en los siguientes supuestos: • Se está frente a la comisión de un delito o haya indicios razonables del hecho delictivo; • Cuando se haya emitido una resolución judicial que lo autorice; o, • Cuando se necesario para el ejercicio de las funciones de una entidad pública, como en el caso de las autoridades competentes en materia laboral.