

## Resumen Políticas de Seguridad de la Información Proveedores externos

El objetivo del presente documento es mitigar los riesgos asociados a la Seguridad de la Información de Controles Administrativos Integrales S.A. de C.V., describiendo lo que se espera de todo el personal que pertenece a otras empresas proveedoras que trabajan para nosotros, y que en el desarrollo de sus funciones pueda tener acceso a la información, sistemas de información o recursos de la empresa en general, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información y sistemas manejados.

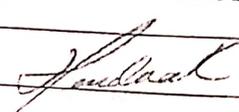
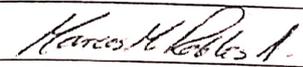
Con este documento se pretende fomentar el uso de buenas prácticas en materia de seguridad de la información, para ello, las empresas proveedoras a las que se les remita este documento se responsabilizan de informar de las políticas incluidas en el mismo a las personas que destinen a prestar sus servicios en nuestra empresa, así como cumplir y respetar dichas normas.

### Políticas referentes a un desarrollo interno sano:

1. Buscar conjuntamente la productividad y eficiencia.
2. Ejercer la autoridad con justicia y equidad en todos los asuntos que afecten a los trabajadores.
3. Reconocer y respetar la integridad de los trabajadores.
4. Cumplir estrictamente los compromisos legales y contractuales con un sentido de responsabilidad, equidad y justicia.
5. Crear las condiciones de trabajo seguras las cuales contribuyan a proteger la salud y las vidas de sus trabajadores.
6. Todo proveedor externo que realice algún trabajo dentro de nuestras instalaciones deberá contar con su Seguro Social vigente, de lo contrario no podrá prestar sus servicios dentro de la empresa.

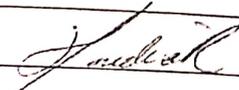
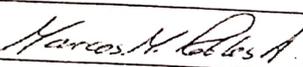
### Políticas referentes a la seguridad de la información:

7. En cada ocasión en que un proveedor requiera información, que sea adicional a aquella que el servicio se ha obligado a entregar en virtud del contrato respectivo, la Comisión de Seguridad de Información analizará los motivos de dicho requerimiento y procederá a aprobar o rechazar la entrega de la misma.
8. Todo proveedor externo deberá firmar su contrato por tiempo determinado, así como las Políticas de Seguridad de la Información para proveedores externos.
9. Ningún proveedor externo podrá extraer mercancía que sin previa autorización de la Dirección General o en su ausencia del encargado del departamento.
10. Se llevará un registro interno de las incidencias encontradas en mercancía o servicios de proveedores externos, mismas que serán documentadas y firmadas por el jefe inmediato, el proveedor y en caso de negativa de este con la firma de dos testigos, en los formatos establecidos por la empresa. Por lo anterior, toda pérdida deberá documentarse inmediatamente por el responsable de área, encargándose de llenar los formatos y documentos que para tal efecto el proceso respectivo indique, debiendo de estar firmados por el jefe inmediato, el proveedor externo y en caso de negativa por dos testigos; lo cual será reportado inmediatamente a la Tesorería y a Recursos Humanos.
11. El acceso físico por parte de los proveedores a los activos de información deberá ser controlado y supervisado por personal administrativo o técnico.
12. Las contraseñas asignadas son únicas, no deberán compartirse ni hacer mal uso de las mismas.

|        | Elaboró   | Revisó  | Autorizó  |
|--------|---|---|---|
| Puesto | Dirección de Recursos Humanos   | Dirección de Sistemas   | Dirección General   |
| Fecha  | 27 Noviembre 2020   | 27 Noviembre 2020   | 27 Noviembre 2020   |
| Firma  |  |  |  |

## Resumen Políticas de Seguridad de la Información Proveedores externos

13. De acuerdo a las reglas establecidas por la empresa, las puertas de cada área de trabajo deberán mantenerse cerradas y sólo se deberá permitir el acceso a la misma a personal Interno Autorizado para ello.
14. Todos y cada uno de los accesos a las diferentes áreas de trabajo, cuentan con control de acceso biomédico y serán registrados en una base de datos para deslindar responsabilidades (nombre, fecha y hora).
15. No se permite divulgar o hacer mal uso de la información de clientes.
16. No se permite divulgar o hacer mal uso de los manuales internos.
17. En situaciones en que proveedores requieran hacer instalaciones de activos de información de carácter tecnológico, tales como servidores, equipos de soporte, entre otros, será requisito base implementar configuraciones que cumplan con el estándar de seguridad establecido por Controles Administrativos Integrales S.A. de C.V. El departamento de Sistemas tendrá la responsabilidad de verificar y validar la configuración de los equipos instalados, así como también de reportar las debilidades y oportunidades de mejora al proveedor del servicio a través de los procedimientos internos establecidos para estos efectos.
18. En todo intercambio de información entre Controles Administrativos Integrales S.A. de C.V. y los proveedores de servicios o productos, se deberán implementar estándares y procedimientos formales asociados al intercambio de información, que permitan garantizar razonablemente la seguridad en el acceso y la transferencia de información.
19. De preferencia los proveedores que entreguen sus servicios a Controles Administrativos Integrales S.A. de C.V., sea cual fuere la modalidad de contratación utilizada, deberán contar con certificaciones vigentes relativas a la seguridad de la información aplicado a los procesos de servicios que deseen contratarse y sobre todo en los casos en que se externalice los procesos de tratamiento y resguardo de información.
20. El personal del proveedor que tenga acceso a información privilegiada que pueda ser clasificada como restringida o confidencial propiedad de Controles Administrativos Integrales S.A. de C.V. o de sus clientes deberá contar con acuerdos de confidencialidad debidamente firmados, así mismo revisar su vigencia y aplicabilidad al menos una vez al año.
21. Las actividades que el proveedor externo lleve a cabo deben ser única y exclusivamente aquellas para las que fue contratado y que se especifican en el contrato.
22. Todo proveedor que brinde un servicio o producto a Controles Administrativos Integrales S.A. de C.V. deberá apegarse de forma estricta a las Políticas de Seguridad de la Información, así como deberá asistir a las sesiones de inducción y/o capacitación a los que sea convocado.

|               | Elaboró   | Revisó  | Autorizó  |
|---------------|---|---|---|
| <b>Puesto</b> | Dirección de Recursos Humanos   | Dirección de Sistemas   | Dirección General   |
| <b>Fecha</b>  | 27 Noviembre 2020   | 27 Noviembre 2020   | 27 Noviembre 2020   |
| <b>Firma</b>  |  |  |  |