1. INFORMACIÓN GENERAL

Objetivo	Establecer las directrices de seguridad para asegurar la protección de la confidencialidad, integridad y disponibilidad de los activos de información que están a disposición de los proveedores para el desarrollo de los acuerdos contractuales establecidos con Controles Empresariales.
Alcance	Las directrices establecidas en este documento son de obligatorio cumplimiento para todos los proveedores que acceden a información de la organización y tienen relación contractual directa.
Responsable	Oficial de privacidad y seguridad de la información
Documentos asociados y registros	N/A

2. DEFINICIONES

Activo de información	Cualquier elemento que tenga valor para la organización desde el punto de vista del manejo, manipulación, gestión y/o custodia de información, incluyendo el Recurso Humano..
Código malicioso (malware)	Malware o código malicioso es cualquier software intencionalmente diseñado para causar daño hacia un computador, servidor o red de datos, también son considerados códigos maliciosos si actúan ocultos o en secreto contra los intereses de los usuarios..

3. NORMATIVA

3.1. GENERAL

El proveedor es responsable por el conocimiento y debida aplicación de los siguientes requisitos de seguridad de la información

- Definir, aprobar, formalizar, publicar y comunicar hacia todos los empleados las políticas y directrices corporativas relacionadas con la seguridad de la información, esta política debe ser creada considerando las disposiciones legales y de entes de control aplicables. Con base en esta política se deberán establecer los estándares, técnicas o procedimientos necesarios para implementar adecuadamente la política de seguridad al interior de la organización.

Carrera 16 Nº 75 - 50, Bogotá • PBX: +57 (601) 546 2720 +57 (601) 546 2727 • FAX: +57 (601) 211 6435
www.controlesempresariales.com • servicioalcliente@coem.co
Bogotá Barranquilla Bucaramanga Cali Cartagena Medellín Neiva Pereira Perú

- Garantizar la identificación, el análisis, la evaluación y el tratamiento de los riesgos propios y de sus terceros subcontratados que hacen parte de la cadena de suministros de los servicios prestados a Controles Empresariales.

- Exigir el manejo adecuado y seguro de la información a los terceros subcontratados, cuando estos pueden o tiene el acceso a la información de Controles Empresariales. Contar con la metodología y los procedimientos adecuados para identificar y gestionar oportunamente los riesgos sobre la información cuando esta es conocida y manejada por terceros.

- Informar a Controles Empresariales por medio del supervisor del contrato, los riesgos que se hayan identificados sobre los servicios prestados, esto con el fin de actualizar el panorama de riesgos y tener el entendimiento de los impactos que estos tendrán sobre las operaciones de Controles Empresariales.

- Elaborar e implementar planes de acción sobre los riesgos que puedan afectar el normal desarrollo de los servicios prestados a Controles Empresariales.

- Brindar a los empleados vinculados a los servicios que son prestados a Controles Empresariales, la educación y la formación apropiada en seguridad de la información, cuyos programas deberán dictarse por lo menos una vez al año y ser impartidas en el proceso de inducción de los nuevos colaboradores. Los programas de capacitación deberán evidenciarse a través de los registros de participación y evaluación.

- Contar con un proceso formal para el registro de usuario (cuentas) y la cancelación oportuna de este, esto con el propósito de asegurar la asignación de los derechos o permisos de acceso a las aplicaciones o a los sistemas que manejen o almacenen información de Controles Empresariales, de igual forma se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado. Este requisito aplica para aquellos proveedores que presten servicios de suministro o administración de sistemas tecnológicos de información al exterior de Controles Empresariales.

- Restringir el acceso de los proveedores subcontratados a la información y a los sistemas utilizados por Controles Empresariales, estos permisos de acceso deben considerar: la autorización, la necesidad por conocer la información y el nivel de privilegios acorde con las labores realizadas. Los acuerdos contractuales establecidos y aceptados entre proveedor y proveedores subcontratados debe contener las obligaciones y responsabilidad en cuanto al manejo seguro de la información de los clientes.

Carrera 16 Nº 75 - 50, Bogotá • PBX: +57 (601) 546 2720 +57 (601) 546 2727 • FAX: +57 (601) 211 6435
www.controlesempresariales.com • servicioalcliente@coem.co
Bogotá Barranquilla Bucaramanga Cali Cartagena Medellín Neiva Pereira Perú

- El acceso a los sistemas informáticos de los clientes de Controles Empresariales debe contar siempre con la autorización y acompañamiento de los responsables de dichos sistemas por parte de los clientes, los permisos de acceso otorgados deben ser retirados una vez finalizada la prestación de los servicios contratados.

- Contar con un sistema interactivo de gestión de contraseñas, que asegure la calidad de estas cuando son utilizadas en la autenticación de los usuarios ante los sistemas o las aplicaciones. Este sistema puede considerar la verificación de la complejidad, la longitud mínima exigida, la vigencia, la restricción del uso de contraseñas anteriores, entre otros.

- Se debe evitar el uso de claves compartidas, genéricas o para grupos. La identificación y autenticación en los dispositivos y sistemas de cómputo de las entidades deberá ser única y personalizada.

- Las aplicaciones o sistemas de información utilizados para la prestación de servicios en Controles Empresariales. deberán disponer de herramientas o recursos criptográficos, que permitan cifrar y proteger la información sensible, personal o confidencial de Controles Empresariales, de sus clientes y colaboradores.

- Implementar un comprensivo y aprobado proceso de gestión de incidentes sobre los sistemas y la información, que incluya: la identificación, respuesta, recuperación y la revisión posterior a la implementación de los planes de acción o tratamiento. Los eventos que afecten la operación de los servicios prestados a Controles Empresariales. deben ser notificados a través del supervisor del contrato.

- Sincronizar todos los relojes de los sistemas de información o aplicaciones utilizadas dentro de los servicios prestados a Controles Empresariales. Se deberá tener como referencia la hora oficial suministrada por Instituto Nacional de Metrología.

- El acceso a las instalaciones y oficinas debe ser controlado en pro de proteger la información sensible o confidencial y prevenir el robo de documentos y equipos.

- El acceso a las áreas de procesamiento de datos, los centros de cableado y a las zonas de alto uso de información confidencial deber ser restringido y monitoreado.

- Contar con los mecanismos de seguridad apropiados para evitar el ingreso y la proliferación de software malicioso (malware) proveniente del ciberespacio que puedan llegar a afectar la disponibilidad de la plataforma tecnológica y la confidencialidad de los datos allí almacenados.

Carrera 16 Nº 75 - 50, Bogotá • PBX: +57 (601) 546 2720 +57 (601) 546 2727 • FAX: +57 (601) 211 6435
www.controlesempresariales.com • servicioalcliente@coem.co

- Permitir la realización coordinada de revisiones o auditorías gestionadas directamente desde Controles Empresariales.

- Contar con herramientas de protección ante virus y malware, dichos recursos deben estar permanentemente actualizados, permitiendo el aislamiento y control de los equipos infectados. Contar con procedimientos para el despliegue y la aplicación de los parches o actualizaciones de los sistemas y las aplicaciones.

- La transferencia de información entre el proveedor y Controles Empresariales debe realizarse a través de canales seguros de comunicaciones, si es vía correo se debe hacer a través de cuentas corporativas privadas, en los casos que se transmita información personal o confidencial se aplicarán controles de seguridad adicionales como el cifrado de los mensajes. Los mecanismos de seguridad a utilizar serán acordados entre las partes.

- Toda modificación o cambio para realizar en los sistemas informáticos de los clientes de CoEm debe ser notificado previamente a la persona de CoEm responsable por el relacionamiento con el cliente y siempre debe contar con el aval y autorización del mismo cliente siguiente el conducto regular establecido para la aprobación e implementación de los cambios en la infraestructura tecnológica.

- Garantizar la continuidad del servicio y la integridad de los datos durante las interrupciones que afecten los servicios prestados a Controles Empresariales, tales como las provocadas por fallas o no acceso a la infraestructura física donde se presta el servicio, fallas en el suministro de energía eléctrica, los imperfectos o las fallas en los equipos de cómputo, fallas de los sistemas telefónicos o en los canales de comunicaciones, ausencia de personas críticas para la operación del servicio, ausencia o incumplimiento de los terceros requeridos para la presentación del servicio.

- De acuerdo con lo establecido en la Ley 1581 de 2012 y el decreto reglamentario 1377 de 2013, debe cumplir con los requisitos de seguridad correspondientes según aplique en la función de encargado y/o responsable del tratamiento de datos personales.

Carrera 16 Nº 75 - 50, Bogotá • PBX: +57 (601) 546 2720 +57 (601) 546 2727 • FAX: +57 (601) 211 6435
www.controlesempresariales.com • servicioalcliente@coem.co
Bogotá Barranquilla Bucaramanga Cali Cartagena Medellín Neiva Pereira Perú

4. CONTROL DE VERSIONES

Versión	Fecha de modificación (dd/mm/aaaa)	Realizado	Observaciones	Estado
V1	17/07/2020	Líder SIG	Versión Inicial	Vencido
V2	3/05/2023	Oficial de Privacidad y Seguridad de la Información	Modificaciones de acuerdo a la nueva versión de la norma ISO 27001	Aprobado

Carrera 16 Nº 75 - 50, Bogotá • PBX: +57 (601) 546 2720 +57 (601) 546 2727 • FAX: +57 (601) 211 6435
www.controlesempresariales.com • servicioalcliente@coem.co
Bogotá Barranquilla Bucaramanga Cali Cartagena Medellín Neiva Pereira Perú