CENTRAL COOPERATIVA DE EDUCACIÓN

COEDUCAR

POLÍTICA PARA LA SEGURIDAD DE LA INFORMACIÓN

Diciembre de 2019

Tabla de contenido

POLÍTICA PARA LA SEGURIDAD DE LA INFORMACIÓN

En virtud del fuerte compromiso de CENTRAL COOPERATIVA DE EDUCACIÓN, en adelante COEDUCAR con el adecuado tratamiento de datos personales, garantizando además de la salvaguarda y seguridad de la información, e ejercicio del Habeas Data, la empresa establece la presente Política aplicables para la seguridad de la información en la organización.

1. Objetivo

La presente Política establece las directrices generales para la Seguridad de la Información al interior de COEDUCAR, con el objetivo de brindar las condiciones de seguridad necesarias que impidan la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento a la información que es tratada por COEDUCAR.

2. Alcance

Esta Política de Seguridad de la Información será aplicada en todos los aspectos administrativos, de gestión, logísticos y de control fijados por la empresa, que deben ser cumplidos por los directivos, funcionarios, contratistas, terceros que presten sus servicios, empleados de terceros, proveedores que estén regulados por términos contractuales, y en general todas aquellas personas que tengan algún tipo de relación con la manipulación de información en COEDUCAR.

3. Políticas específicas para el tratamiento de datos personales

A continuación, encontrará algunas Políticas específicas, implementadas en COEDUCAR, para el manejo de datos personales y para el manejo de la información de la organización.

3.1. Políticas específicas

3.1.1. Instalación de software

Propósito: Minimizar el riesgo de exposición y de infección por programa maligno, evitando a su vez posibles sanciones por el uso de software sin licenciar.

Política: Los trabajadores no deben instalar software en los dispositivos de la compañía sin la respectiva autorización. Las peticiones de instalación de software deben ser aprobadas por el departamento de tecnología y el proceso de instalación debe ser realizado por personal calificado.

Todo software que sea instalado debe tener licenciamiento comercial, ser de licenciamiento libre (open source, free, trial), o en su defecto la licencia debe provenir del departamento de tecnología.

3.1.2. **Uso de dispositivos de almacenamiento externo**

Propósito: Minimizar el riesgo de exposición de información de la empresa o de infección por programa maligno contenido en dispositivos externos de almacenamiento (Discos Duros externos, USBs, CDs, Diskettes, Teléfonos Celulares, Reproductores Multimedia, etc).

Política: Está prohibido el uso de dispositivos de almacenamiento personales dentro de la infraestructura tecnológica de la empresa. En caso de requerirse alguno de estos dispositivos, estos deben ser adquiridos por parte de la entidad y se deben solicitar a modo de préstamo a los jefes de área correspondientes.

En caso de que la información sea transferido a dispositivos diferentes, una vez se termine de realizar la labor requerida con el dispositivo se debe eliminar toda la información contenida en el mismo, devolver los dispositivos de la entidad y realizar una limpieza con un software de antivirus y retornarse al encargado.

3.1.3. **Uso del Internet empresarial y política de monitoreo**

Propósito: El propósito de esta política es definir los estándares para el monitoreo y limitación de la navegación por Internet desde cualquier dispositivo en la red empresarial. Estos estándares están diseñados para asegurar que los empleados utilicen el Internet de forma segura y responsable.

Política: La gerencia está en potestad de monitorear todas las comunicaciones entrantes y salientes dentro de la red de la organización. Esto incluye conocer la IP de origen, la fecha, la hora, el protocolo, el servidor o dirección de destino y los datos comunicados.

La gerencia puede bloquear los sitios de Internet que se consideren inapropiados para el ambiente empresarial. Se considera una falta disciplinaria bajo cualquier circunstancia el acceso a páginas y sitios web de contenido sexual explícito, sitios de juegos o apuestas, sitios relacionados con sustancias ilícitas, sitios de citas y redes sociales, sitios de fraude, (indicios de lavado de activos o financiación del terrorismo), contenidos SPAM o en relación a delitos tipificados por la ley colombiana, contenido racista o de alguna forma ofensivo y discriminatorio, contenido violento, y todo contenido que no esté relacionado con el desarrollo de las finalidades de la empresa sin que medie previa autorización.

Así mismo está totalmente prohibido el uso de la infraestructura empresarial para realizar ataques informáticos o similares. Además, está prohibido el uso del Internet en horas no autorizadas para acceder a contenido multimedia no asociado a la labor del empleado.

Cualquier intento por evadir los controles técnicos impuestos, será considerado en sí mismo una falta disciplinaria y causal de terminación de contrato, sin perjuicio de las acciones legales pertinentes por los daños causados a Coeducar.

3.1.4. **Manejo de claves**

Propósito: El propósito de esta política es establecer un estándar de generación de contraseñas seguras, la protección de dichas contraseñas y su frecuencia de cambio.

Política: Todas las contraseñas de nivel de sistema (root, administrador, usuarios de windows, etc, bases de datos), deben ser cambiadas al menos cada tres meses.

Todas las contraseñas de nivel de usuario (correo, cuentas personales), deben ser cambiadas al menos cada seis meses.

Todas las contraseñas utilizadas deben seguir las condiciones descritas a continuación: Contener al menos tres de los siguientes caracteres: Minúsculas, Mayúsculas, Números, Caracteres especiales (e.g. #$%&/(“!.;), la longitud de la contraseña debe ser de al menos 8 caracteres, la contraseña no debe estar compuesta únicamente de palabras de diccionario, se deben evitar contraseñas tradicionales como password, 123456, qwerty, asdfg, etc.

Como base del correcto manejo de claves y contraseñas se presentan una serie de recomendaciones para el manejo correcto de las mismas:

- Siempre utilice contraseñas diferentes para los servicios de la entidad y sus cuentas personales no relacionadas al ámbito laboral.
- No comparta sus contraseñas con ningún tercero, incluso si este pertenece a la organización.
- Las contraseñas nunca deben estar escritas en texto plano (jamás archivos llamados claves.txt y en el escritorio).
- No revele las contraseñas por medios de comunicación desprotegidos como correo, mensajería instantánea, SMS, etc.
- Evite utilizar la opción de recordar contraseña en navegadores y programas internos.

3.1.5. **Uso de correo electrónico y comunicaciones personales**

Propósito: Prevenir daños y perjuicios en la imagen o el nombre de la organización por el manejo incorrecto de los servicios de comunicación.

Política: Los diferentes medios de comunicación a disposición de los trabajadores no deben ser utilizados para la distribución de mensajes con contenido ofensivo, racista, discriminatorio, pornográfico, sexual, político, etc. Los empleados que reciban comunicaciones con este contenido deben eliminarlo inmediatamente y reportar el incidente si es de origen interno.

Utilizar los correos empresariales para comunicaciones personales está prohibido. En especial si es para la distribución de mensajes cadena, spam o de alguna forma comerciales.

Los empleados no deben esperar privacidad alguna en contenido que almacenen o envíen como parte de los servicios de comunicación de la compañía. El no cumplimiento de las condiciones mencionadas anteriormente es considerado una falta disciplinaria y puede ser objeto de sanción.

3.1.6. **Confidencialidad con terceros**

Propósito: Establecer los requerimientos de confidencialidad en las relaciones con proveedores, contratistas, en particular con empleados y los terceros en general.

Política: Para el desarrollo de las relaciones contractuales, comerciales y laborales, se debe exigir a los terceros la aceptación de los acuerdos de confidencialidad definidos por la organización. En dichos acuerdos se debe establecer el compromiso de salvaguardar la información, velar por su correcto uso, impedir el uso no autorizado de dicha información y guardar reserva. Se debe estipular a su vez la información que es objeto de protección dentro del acuerdo y su temporalidad.

Los acuerdos deben incluirse dentro de los contratos celebrados entre la organización y terceros, como parte integral del contrato o firmarse como un acuerdo independiente.

La aceptación de las condiciones de confidencialidad es indispensable para conceder al tercero el acceso a la información protegida.

3.1.7. **La seguridad física y ambiental**

Propósito: Evitar el acceso físico no autorizado, daños e interferencia para la información de la organización y las instalaciones de procesamiento de información.

Política: Los equipos de cómputo deben estar situados y protegidos para reducir los riesgos de las amenazas ambientales y los riesgos y las oportunidades de acceso no autorizado. El equipo deberá estar protegido contra fallas de energía y otras interrupciones causadas por fallas en el soporte de los servicios públicos. El cableado que transporta datos, energía y telecomunicaciones o el soporte de los servicios de información debe estar protegido contra la

intercepción, interferencia o daños. Los equipos de cómputo deben tener un correcto mantenimiento para asegurar su continua disponibilidad e integridad.

Los equipos, la información o el software no se sacarán de las instalaciones de la empresa sin la previa autorización. Se aplicará seguridad a los activos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.

Todos los elementos del equipo que contienen los medios de almacenamiento deberán ser verificados para garantizar que los datos sensibles y el software con licencia se han eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.

Los usuarios deberán asegurarse de que el equipo que no cuenta con vigilancia tenga la protección adecuada.

Los puestos de trabajo deben estar limpios de papeles, soportes de almacenamiento extraíbles y cuando un computador este desatendido deberá bloquearse la pantalla.

Cuando sea apropiado, papeles y medios de información deben estar asegurados en armarios especiales, especialmente en horas fuera de las normales de trabajo.

3.1.8. **Requisitos para el control de acceso**

Propósito: Limitar el acceso de la información y a las instalaciones de procesamiento de la información.

Política: Los responsables de las áreas seguras de la empresa tienen la obligación de vigilar y garantizar que se cumplan las siguientes medidas de seguridad:

- Todas las áreas que manejan información confidencial y sensible se catalogan como seguras y deben permanecer cerradas y custodiadas. Algunas de estas áreas son: Tecnología, recursos humanos, contabilidad, rectoría, secretaría y coordinación académica, admisiones, cartera, tesorería, Gerencia.
- El acceso a áreas seguras donde se procesa o almacena información confidencial y restringida, es limitado únicamente a personas autorizadas.
- El acceso a áreas seguras requiere esquemas de control de acceso, como tarjetas, llaves o candados.
- El responsable de un área segura debe asegurar que no ingresen cámaras fotográficas, videos, teléfonos móviles con cámaras, salvo se tenga una autorización expresa.
- Se utilizan planillas para registrar la entrada y salida del personal.

- Se restringe el acceso físico a dispositivos como: puntos de acceso inalámbricos, puertas de enlace a redes y terminales de red que estén ubicadas en las áreas seguras.
- Se utilizan planillas para registrar la entrada y salida de equipos de cómputo.

3.1.9. **Copias de seguridad (Backups)**

Propósito: Evitar la pérdida de información de la empresa.

Política: Las copias de seguridad de la información se tomarán de forma automática cada treinta (30) días, las cuales se almacenarán en Google Cloud y serán custodiadas por el usuario en primera instancia, en segunda instancia serán verificadas por el departamento de tecnologías quien generará una segunda copia general en Google Cloud.

Los funcionarios responsables de la gestión del almacenamiento y respaldo de la información deberán proveer los recursos necesarios para garantizar el correcto tratamiento de esta.

Los dueños o responsables de los activos de información tecnológicos y recursos informáticos deben definir las estrategias para la correcta y adecuada generación, retención, y rotación de las copias de respaldo de la información.

Los dueños o responsables de los activos de información tecnológicos y recursos informáticos deben velar por el cumplimiento de los procedimientos de respaldo de la información.

Nota: En algunos casos se podrá suministrar a determinadas áreas un disco físico para hacer una copia de la información del área que estará bajo la custodia y responsabilidad del Jefe de la misma.

3.1.10. **Registro de actividad y supervisión**

Propósito: Registrar eventos y generar evidencia.

Política: Se producirán revisiones regulares y cuidadosas a los registros de eventos que se graban de las actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

Los registros de información se protegerán contra la manipulación y el acceso no autorizado. Las actividades del administrador del sistema y de la red serán registradas.

Estos registros serán protegidos y regularmente revisados.

Los relojes de todos los sistemas de informática relevantes serán sincronizados a una fuente de tiempo de referencia única.

3.1.11. **Revisiones de la seguridad de la información**

Propósito: Garantizar que la seguridad informática sea implementada y aplicada de acuerdo con las políticas y procedimientos de la organización.

Política: Los sistemas de información son revisados regularmente a través de Auditorias, por la gerencia o por quien este delegue, para cerciorarse que se da cumplimiento a las políticas y normas de seguridad de la información de la entidad.

4. Proceso para la atención de incidentes

Toda vez que se presente algún incidente con la seguridad de la información tratada por COEDUCAR, deberá adelantarse el siguiente procedimiento:

4.1. Reporte del Incidente

Ocurrido el incidente de seguridad, la primera persona que tenga conocimiento del mismo y en el menor tiempo posible, deberá presentar un informe detallado del mismo, dirigido al área o persona encargada de la seguridad de la información, que en este caso sería el departamento de tecnologías, con copia a la gerencia.

4.2. Comunicación del Incidente ante la SIC

Todo incidente de seguridad de la información deberá ser reportado ante la Superintendencia de Industria y Comercio, específicamente ante el Registro Nacional de Bases de Datos (RNBD).

4.3. Reunión del comité de Seguridad de la información

El área o persona encargada de la seguridad de la información, el departamento de tecnologías conformara de forma extraordinaria una reunión de un Comité para la seguridad de la información, en el cual se desarrollarán los siguientes ítems:

4.3.1. **Emisión del concepto técnico**

Evaluados los Hechos del caso se deberá dar un concepto técnico que determina todas las contingencias surgidas en el caso en concreto.

4.3.2. **Identificación de la falencia**

Como resultado del concepto técnico, se deberá identificar plenamente la falencia que dio paso al incidente de seguridad de la información.

4.3.3. **Toma de medidas**

El comité deberá tomar las medias y los correctivos necesarios para evitar futuros incidentes.

5. Modificación de las políticas

COEDUCAR se reserva el derecho de modificar la presente Política de Seguridad de la Información en cualquier momento, comunicando de forma oportuna a todas aquellas personas que estén relacionadas o que participen en la manipulación de la información de la empresa para su correcta implementación.

6. Vigencia

La presente Política fue aprobada por el Consejo de Administración de Coeducar en reunión de fecha 16 de diciembre de 2020 según acta no. 252 y rige a partir de esta fecha

ALIRIO SUÁREZ MONSALVE
Gerente General