

CONSIDERANDO

Que la información es uno de los activos más valiosos para Consultoría y Capacitación HSEQ S.A.S., y su adecuada protección es esencial para garantizar la confianza de sus clientes, colaboradores y colaboradoras, proveedores y demás partes interesadas.

Que la creciente digitalización, el intercambio de datos sensibles y la normatividad vigente exigen el establecimiento de políticas claras, éticas y responsables sobre el manejo, almacenamiento, uso y protección de la información.

Que Consultoría y Capacitación HSEQ S.A.S., en el marco de su Código de Conducta y Ética Empresarial, se compromete a adoptar una cultura organizacional basada en la integridad, la confidencialidad, la transparencia y el cumplimiento legal.

Artículo 1. OBJETIVO

Establecer los lineamientos generales para la gestión segura, ética y responsable de la información, garantizando su confidencialidad, integridad y disponibilidad, de acuerdo con los principios del Código de Conducta y Ética Empresarial.

Artículo 2. ALCANCE

Esta política aplica a todos los colaboradores y colaboradoras, directivos, contratistas, consultores, proveedores y cualquier parte interesada que, directa o indirectamente, maneje información relacionada con Consultoría y Capacitación HSEQ S.A.S.

Artículo 3. MARCO NORMATIVO

Esta política se fundamenta en las siguientes disposiciones legales y normativas:

- Ley 1581 de 2012 – Protección de Datos Personales (Colombia)
- Decreto 1377 de 2013
- Ley 1266 de 2008 – Habeas Data
- ISO/IEC 27001 – Sistema de Gestión de Seguridad de la Información
- Normas internas del Código de Conducta y Ética Empresarial de HSEQ S.A.S.

Artículo 4. PRINCIPIOS EMPRESARIALES

1. Confidencialidad: Proteger la información sensible de accesos no autorizados.
2. Integridad: Garantizar que la información no sea modificada de forma indebida.
3. Disponibilidad: Asegurar que la información esté accesible cuando sea requerida por usuarios autorizados.
4. Transparencia: Actuar con claridad en el manejo de la información ante los titulares de los datos.
5. Legalidad: Cumplir con la legislación vigente en materia de protección de la información.
6. Ética: Utilizar la información de manera responsable, respetando los valores organizacionales.

Artículo 5. DEFINICIÓN

Seguridad de la información: Conjunto de prácticas, políticas, procesos y herramientas destinados a proteger la información contra accesos no autorizados, alteraciones, pérdidas o divulgación indebida.

Artículo 6. COMPROMISOS DE CONSULTORÍA Y CAPACITACIÓN HSEQ S.A.S.

La organización se compromete a:

- Establecer controles para mitigar riesgos asociados a la seguridad de la información.
- Garantizar la formación continua de su personal en buenas prácticas de protección de datos.
- Establecer comportamientos adecuados sobre el manejo y uso de los diferentes medios tecnológicos y no tecnológicos en los cuales se almacena, transmite o procesa información.
- Contribuir a la continuidad del negocio frente a los diferentes incidentes.
- Generar un ambiente de confianza a las partes interesadas.

Artículo 7. RESPONSABILIDADES

Todos los colaboradores y colaboradoras del Grupo Empresarial HSEQ S.A.S tienen la responsabilidad de proteger la información de la compañía en cualquiera de sus formas: digital, impresa o verbal. El mal uso, la divulgación no autorizada o la pérdida de esta información puede comprometer los intereses del Grupo y afectar su reputación, operación y cumplimiento legal.

1. Acceso y uso de la información

- La información debe ser utilizada únicamente para fines laborales autorizados.
- El acceso a la información será asignado por el responsable del proceso, de acuerdo con las funciones y necesidades del cargo.
- Evitar prácticas o usos inapropiados de las redes sociales que puedan comprometer la seguridad y privacidad de la información de la organización.
- La información interna no podrá ser compartida, transferida o comercializada con terceros sin autorización expresa y justificada.

2. Responsabilidad individual

- Cada colaborador es responsable del manejo seguro de la información que utiliza.
- La información almacenada en equipos corporativos no se considera privada y podrá ser auditada si se requiere.
- Está prohibido utilizar cuentas o accesos de otros colaboradores, así como compartir contraseñas.

3. Uso de recursos tecnológicos

- Los equipos de cómputo, redes, dispositivos móviles, bases de datos, aplicaciones y demás recursos tecnológicos deben utilizarse de forma responsable y exclusiva para fines laborales.
- El mal uso o daño a estos equipos, por descuido o negligencia, será responsabilidad del usuario, incluyendo posibles compensaciones a la empresa.

- Está prohibido el acceso a aplicaciones, páginas webs o contenidos que no tengan relación con la actividad laboral.
- Los dispositivos tecnológicos y de información que CONSULTORÍA Y CAPACITACIÓN HSEQ SAS pone a disposición de sus colaboradores son de uso exclusivo para el desarrollo de la actividad laboral encomendada por la organización.
- Está prohibida la conexión de dispositivos externos a la red o dispositivos susceptibles de captar información de los dispositivos tecnológicos de CONSULTORÍA Y CAPACITACIÓN HSEQ SAS.
- Las aplicaciones informáticas de comunicación y el acceso a internet deben ser utilizados exclusivamente para el desarrollo de las actividades laborales. Asimismo, a la red WIFI corporativa únicamente podrán conectarse los dispositivos corporativos autorizados por la organización.
- No deben conectarse a ella los dispositivos personales, móviles personales, ni dispositivos de los proveedores.
- Utilizar el correo electrónico exclusivamente para las actividades propias del desempeño de las funciones o actividades laborales y no se debe utilizar para otros fines.
- Utilizar el correo electrónico de manera ética, razonable, eficiente, responsable, no abusiva y sin generar riesgos para la operación de equipos o sistemas de información ni para la imagen de la organización.
- Abstenerse de enviar correos que promuevan la discriminación basada en raza, nacionalidad, género, edad, estado marital, orientación sexual, religión o discapacidad, o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluidas el lavado de activos, que contengan amenazas o mensajes violentos.
- Abstenerse de enviar, reenviar o intercambiar correos, mensajes, chats, mensajes de whatsapp no deseados o considerados como SPAM, cadena de mensajes o publicidad o con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, racista, o cualquier contenido que represente riesgo de virus.
- Todos los equipos tecnológicos asignados al colaborador deberán ser entregados al Líder de Servicios para su custodia en caso de inicio de periodo de vacaciones o terminación del contrato laboral. Durante la ausencia del colaborador, el Líder de Servicios será responsable de verificar y atender oportunamente los mensajes o llamadas de los clientes, con el fin de garantizar la continuidad en la prestación del servicio.
- Hacer buen uso de los recursos tecnológicos asignados por la organización. En ningún momento pueden ser usados para beneficio propio o para realizar prácticas ilícitas o malintencionadas que atenten contra otros, colaboradores y terceros, legislación vigente o políticas ni lineamientos de seguridad de la información establecidas por la organización.
- Solo el personal autorizado por la Dirección Administrativa podrá modificar, reubicar o intervenir equipos de cómputo.

4. Seguridad de accesos

- Las contraseñas son asignadas por la empresa y tienen carácter personal e intransferible. Cada colaborador o colaboradora es responsable del uso adecuado de su cuenta de acceso. Está prohibido compartir, divulgar o reutilizar estas credenciales. La empresa podrá actualizar o renovar las contraseñas según sus protocolos de seguridad.
- Cada colaborador es responsable de las actividades realizadas bajo su usuario.

- Está prohibido intentar vulnerar controles de seguridad, acceder a información de otros usuarios o instalar software malicioso.

5. Reporte de incidentes

- Toda situación que represente una amenaza a la seguridad de la información (virus, intentos de acceso no autorizado, pérdidas, daños, vulnerabilidades) debe ser reportada de inmediato al área de Tecnología y al jefe directo.
- En caso de retiro de la empresa, los colaboradores deben entregar todos los equipos y recursos tecnológicos que les hayan sido asignados.

Artículo 8. CANALES DE COMUNICACIÓN Y ATENCIÓN

Los colaboradores y partes interesadas podrán reportar situaciones que afecten la seguridad de la información o incumplimientos éticos a través de los siguientes canales:

Correo electrónico institucional: soporte@consultoriaycapacitacionhseq.com

Línea ética y de atención: 3212820679

Artículo 9. PROTECCIÓN DEL DENUNCIANTE

CONSULTORÍA Y CAPACITACIÓN HSEQ S.A.S. garantiza la confidencialidad de la identidad del denunciante, así como su protección frente a represalias o consecuencias negativas derivadas de su buena fe al reportar posibles incidentes o irregularidades.

Artículo 10. VIGENCIA Y SEGUIMIENTO

Esta política entra en vigencia a partir de la fecha de aprobación y será revisada anualmente o cada vez que las circunstancias lo ameriten. La Gerencia General será responsable de su cumplimiento y actualización.

Artículo 11. FIRMA Y PUBLICACIÓN

Esta política será firmada por el representante legal y difundida a través de los medios oficiales de la empresa para conocimiento de todos los interesados.

J.E.M

Jorge Eduardo Méndez
Gerente y Representante Legal