1. Introducción, Objetivo y Alcance

La seguridad de la información y la Ciberseguridad son el conjunto de medidas preventivas destinadas a resguardar y preservar la confidencialidad, integridad y disponibilidad de los activos de información que son procesados, almacenados y transportados, independientemente de su forma. Estas medidas son fundamentales para asegurar la continuidad de las operaciones en CUMBRA, el cumplimiento regulatorio y la protección de la reputación de la organización, así como reducir o minimizar impactos no deseados para el logro de los objetivos esperados. Para gestionar este proceso, la organización cuenta con un área de Seguridad de la Información y Ciberseguridad (en adelante Seguridad de información).

Esta área es liderada por el Oficial de Ciberseguridad, que reporta con la Gerencia Regional de Administración y Finanzas, quien a su vez tiene el reporte directo con la Gerencia General de CUMBRA y tiene como propósito principal, la protección de los activos de información mediante la gestión de los riesgos, principalmente los cibernéticos. Esta área brinda soporte a los procesos de negocio para mitigar impactos no deseados y asegurar la continuidad de sus operaciones y seguridad de la información de la organización.

En ese sentido, el objetivo de la presente política es establecer las medidas preventivas generales para cubrir los tres componentes fundamentales de la seguridad de la Información (confidencialidad, integridad y disponibilidad) y es de aplicación obligatoria para todos los colaboradores de CUMBRA.

Este documento aplica para CUMBRA Perú S.A., CUMBRA Ingeniería S.A., Ecología y Tecnología Ambiental S.A.C. y/o Vial y Vives-DSD S.A. (en su conjunto “CUMBRA”).

2. Medidas Preventivas

2.1. Concientización, educación y capacitación en Seguridad de la Información y Ciberseguridad:

a. El colaborador debe participar activamente y de manera obligatoria en las actividades del Programa de concientización y entrenamiento de Seguridad de la Información y Ciberseguridad.
b. El colaborador es responsable de adoptar y ejercer las buenas prácticas y recomendaciones emitidas en el Programa de concientización y entrenamiento de Seguridad de la Información y Ciberseguridad.
c. El colaborador es responsable de cumplir con las políticas y procedimientos difundidos por Seguridad de la información.

2.2. Uso y tratamiento de la información:

a. Cumplir con el procedimiento **IC-GI-PC-001 Gestión de Información Documentada**, que detalla el etiquetado de confidencialidad de la información acorde al tipo de información. En situaciones en las que entidades gubernamentales u otros casos especiales requieran documentación sin etiquetado, es necesario contar con la aprobación tanto del Dueño del Proceso asociado como del Oficial de Ciberseguridad.
b. Toda información generada por el colaborador durante y al término de su vínculo laboral es de propiedad exclusiva de la organización.
c. El colaborador es responsable de hacer buen uso de la información que custodia, resguardando su disponibilidad, integridad y confidencialidad, siguiendo las buenas prácticas y recomendaciones emitidas por Seguridad de la información.

d. El colaborador debe guardar absoluta reserva frente a la información que custodia, comprometiéndose a utilizarla para el desempeño de sus funciones.
e. Está prohibido utilizar la información de la organización para fines personales, ajenos a los aspectos laborales.
f. Está prohibido compartir y transferir información a terceros que no hayan sido autorizados, así como el almacenamiento en medios inseguros o no oficiales por la organización.

2.3. Control de acceso:

a. El usuario asignado al colaborador lo identifica dentro de un servicio informático (sistema de información, aplicación, plataforma, etc.) y todas las actividades que se realicen con este, están bajo su responsabilidad.
b. El colaborador es responsable de resguardar la disponibilidad, integridad y confidencialidad de los datos de su usuario y de la información creada, procesada, transmitida y almacenada a través de este.
c. Las contraseñas de usuario deben ser cambiadas al ser entregadas, de manera periódica y cada vez que los servicios informáticos lo soliciten. En caso de sospechar que una contraseña haya sido revelada o descubierta, debe ser cambiada de manera inmediata.
d. El colaborador es responsable de utilizar contraseñas robustas siguiendo las buenas prácticas y recomendaciones emitidas por Seguridad de la información.
e. Las cuentas y contraseñas son:

- Personales e intransferibles.
- Asignadas en base al rol y función que desempeña el colaborador.
- De uso estrictamente laboral y confidencial.

a. Está prohibido compartir/prestar usuarios y contraseñas entre colaboradores y a terceros.
b. Está prohibido utilizar post-it o archivos de texto para almacenar usuarios y contraseñas.

2.4. Servicios informáticos:

a. El acceso a los servicios informáticos: sistemas de información, aplicaciones, plataformas, correo electrónico corporativo, navegación a internet, carpetas compartidas, almacenamiento en nube, conexión remota segura y red inalámbrica, son otorgados para desempeñar y acompañar a las actividades relacionadas a las funciones del colaborador, de uso estrictamente laboral.
b. El colaborador es responsable de hacer buen uso de los servicios informáticos, resguardando la disponibilidad, integridad y confidencialidad de los accesos otorgados, siguiendo las buenas prácticas y recomendaciones emitidas por Seguridad de la Información.

2.5. Medios extraíbles:

a. Cumplir con el instructivo **IC-TI-IN-007 Lineamiento de seguridad para el acceso temporal a USB**, la cual detalla las medidas de control y seguimiento a excepciones de acceso para asegurar la confidencialidad y disponibilidad de la información.
b. El acceso a dispositivos extraíbles (memorias USB, discos duros externos, CDs/DVDs, etc.) se encuentra restringido. De existir una necesidad justificada, el colaborador debe generar un requerimiento a través del Portal de Soporte de Mesa de Ayuda, para solicitar una excepción a Seguridad de la Información, detallando el requerimiento (motivo de la excepción, periodo del requerimiento y hostname) y adjuntando el V°B° de la Gerencia respectiva, entendiendo y

asumiendo los riesgos asociados (consecuencias de conceder el permiso) para que se apruebe temporalmente el permiso.

c. De detectarse eventos de virus informáticos ocasionados por este medio, se revocará el acceso, quedando como inválida la excepción del permiso.

2.6. Protección contra malware (virus informático):

a. El dispositivo de cómputo asignado al colaborador está protegido a través del software de antivirus de la empresa.
b. Está prohibido el uso de otro software que ponga en riesgo la continuidad de las operaciones y seguridad de la información de la organización De ocurrir un incidente asociado a malware y/o virus informático, el dispositivo de cómputo debe ser desconectado de la red corporativa a la brevedad posible para salvaguardarla.

2.7. Escritorio y pantalla limpios:

a. El colaborador es responsable de bloquear su dispositivo de cómputo asignado al ausentarse o retirarse de su puesto trabajo.
b. El colaborador es responsable de mantener su escritorio de trabajo libre de documentos físicos y/o medios extraíbles que contengan información de la organización.
c. El colaborador debe utilizar la cadena de seguridad al ausentarse o retirarse de su puesto trabajo para resguardar su dispositivo de cómputo ante pérdida o robo.
d. El colaborador es responsable de mantener su escritorio de pantalla libre de archivos para resguardar la información contenida en su equipo de cómputo.
e. Para espacios libres o salas de reunión, el colaborador debe considerar lo expuesto en los numerales anteriores.

2.8. Eventos e incidentes de Seguridad de la Información y Ciberseguridad:

a. El colaborador es responsable de notificar los eventos e incidentes relacionados a Seguridad de la Información y Ciberseguridad, como comportamientos inusuales en su dispositivo cómputo (Malware y/o Virus Informático), correos de dudosa procedencia (Phishing o Spam), cambios y accesos no autorizados en los servicios informáticos, entre otros a través del Portal de Soporte de Mesa de Ayuda.

3. Cierre

De detectarse incumplimiento de las medidas preventivas descritas, o uso indebido de información, como almacenar y compartir en medios no autorizados, compartir o prestar usuarios y contraseñas, acceso a páginas web no permitidas, uso y descarga de software no autorizado y de ocio, u otras acciones que pongan en riesgo la continuidad de las operaciones y seguridad de la información de la organización, se notificará el incumplimiento al colaborador y a su jefe directo a través del correo corporativo con copia a la Gerencia de la que él colaborador pertenece y Gerencia Regional de Gestión Humana para la evaluación y aplicación de las medidas disciplinarias pertinentes, según lo estipulado en el Reglamento Interno de Trabajo y lo previsto la legislación laboral vigente.

Lo establecido en la presente política es de cumplimiento obligatorio. En caso de incumplimiento, se procederá a notificar al colaborador y a su jefe directo a través del correo electrónico, con copia a la Gerencia de Gestión Humana, para aplicar las medidas disciplinarias correspondientes, conforme a lo estipulado en el Reglamento Interno de Trabajo y la legislación laboral vigente.

Diego Aguirre Salmón
Gerente General

La versión vigente de este documento se encuentra en el Portal Regional. Accede a través de este código QR

IC-TI-PO-002