POLÍTICA PARA LA SEGURIDAD DE LA INFORMACIÓN

En virtud del fuerte compromiso de BONDS AND CREDIT LTDA con el adecuado tratamiento de datos públicos, privados y sensibles, garantizando además de la salvaguarda y seguridad de la información, y ejercicio del Habeas Data, la empresa establece la presenta 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 BONDS AND CREDIT LTDA, 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 BONDS AND CREDIT LTDA.

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 BONDS AND CREDIT LTDA.

3. POLÍTICAS ESPECÍFICAS PARA EL TRATAMIENTO DE DATOS PERSONALES.

1. 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.

2. 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. REQUISITOS PARA EL CONTROL DE ACCESO

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

Política

Los trabajadores tienen la obligación de vigilar y garantizar que se cumplan las siguientes medidas de seguridad:

- 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, requieren 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 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.

4. ACCESO A DATOS SENSIBLES DE LOS EMPLEADOS.

Propósito: Garantizar que los datos sensibles relacionados con los datos de la salud, creencias religiosas, políticas, sexuales, planes de desarrollo, reconocimiento, y pago de beneficios legales y extralegales, entre otros de los trabajadores, solo puedan ser conocidos por el personal competente y pertinente en virtud de sus funciones, teniendo en cuenta el principio de Acceso Restringido.

Política:

Las finalidades para las que son tratados los datos sensibles en la empresa son limitadas y especificadas en las respectivas autorizaciones otorgadas por el titular de la información.

De forma general, el tratamiento de datos sensibles en la empresa estará limitado únicamente a la Gerencia General y al área Administrativa y Financiera, atendiendo las finalidades particulares autorizadas por el titular.

La empresa de forma particular y en los respectivos manuales de funciones según el cargo, determinará aquellos cargos particulares que podrán tener acceso a datos de carácter sensible, sin que ese acceso signifique una violación a la política de seguridad de acceso restringido.

Igualmente, aplican los mecanismos de seguridad identificados previamente como de acceso restringido a los datos personales.

5. SEGURIDAD DE LA INFORMACIÓN EN TORNO AL RECURSO HUMANO

El tratamiento de los datos personales, antes, durante y después de la relación laboral, se regirá por las siguientes reglas:

- BONDS AND CREDIT LTDA, informará a las personas interesadas en participar en un proceso de selección, las reglas aplicables al tratamiento de los datos personales que suministre el interesado durante el respectivo proceso de selección, así como de aquellos datos que se obtengan durante la realización del mismo.
- El tratamiento de los datos suministrados por los interesados en las vacantes de BONDS AND CREDIT LTDA, y los obtenidos del proceso de selección, será únicamente la informada en la autorización al aspirante.
- La empresa realizará estudios de seguridad previos a la contratación de nuevo personal para la empresa.
- La empresa contará con un proceso de eliminación de las hojas de vida de los candidatos (titulares) sobre los que ya no se tenga interés en conservar contacto.
- Una vez seleccionado un aspirante para ocupar un cargo en BONDS AND CREDIT LTDA, se celebrará el respectivo contrato de trabajo, acuerdo de confidencialidad y se le asignará cuando el cargo lo requiera, un usuario con un perfil definido relacionado directamente con el cargo a desempeñar, el cual le permitirá el acceso a la información personal tratada por la empresa, cuando el cargo así lo requiera.
- Seleccionado el candidato para el cargo, la empresa almacenará los datos personales del trabajador en una carpeta identificada con el nombre de cada persona. A esta carpeta solo tendrá acceso el área Administrativa y Financiera, con la finalidad de gestionar la relación laboral entre la empresa y el empleado.

- Para cuando BONDS AND CREDIT LTDA, requiera contratar servicios externos para el tratamiento de datos, durante la relación contractual con los trabajadores, podrá requerirse la transferencia de datos personales a un tercero que se denominará Encargado, Para este caso, la empresa seguirá los lineamientos para la selección de Encargados en la transmisión de datos personales contenidos en esta política.
- Una vez se termine el contrato de trabajo, la empresa suscribirá un acuerdo de confidencialidad con el extrabajador para salvaguardar la confidencialidad de la información personal manipulada por el extrabajador; así como solicitará la entrega formas de perfiles y contraseñas que le hayan sido asignadas durante la ejecución del contrato de trabajo.
- Terminada la relación laboral, BONDS AND CREDIT LTDA igualmente procederá a almacenar los datos personales de sus exempleados en un archivo general, sometiendo tal información a medidas y niveles de seguridad, atendiendo la calidad de los datos que dicho archivo puede contener.

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.

7. SELECCIÓN DE ENCARGADOS PARA TRANSMISIÓN DE DATOS PERSONALES

Propósito: Garantizar que en los eventos en los que se realicen transmisiones de datos personales, se elija el encargado teniendo en cuenta las prerrogativas que trata la normativa sobre protección de datos personales.

Política

Cuando BONDS AND CREDIT LTDA como responsable del tratamiento de datos personales, cuando realice Transmisión de datos personales, es de imperativo cumplimiento por parte de la empresa, seguir los siguientes lineamientos:

- Determinar cuál será el alcance del tratamiento que se permitirá realizar al Encargado.
- Evaluar la competencia y capacidad del Encargado para realizar el tratamiento que se le encomendará.
- Revisar el manual de políticas de tratamiento de datos personales propias del Encargado.
- Examinar las medidas de seguridad implementadas por el Encargado para el tratamiento de los datos personales, y su compatibilidad con los estándares determinados por BONDS AND CREDIT LTDA.
- Suscribir un contrato de transmisión de datos personales.
- Realizar auditorías para medir el nivel de protección de los datos personales en la ejecución del contrato de transmisión.

8. 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 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 BONDS AND CREDIT LTDA, deberá adelantarse el siguiente procedimiento:

1. **Reporte del Incidente:** Ocurrido el incidente de seguridad, la primera persona que tenga conocimiento del mismo, deberá informar inmediatamente al área Administrativa y Financiera a la persona encargada de la seguridad de la información, así como en el menor tiempo posible presentar un informe detallado sobre los hechos que del mismo se conocen.

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-. El reporte de los incidentes es una obligación del área Administrativa y Financiera, que deberá realizarlo una vez haya sido notificado de la ocurrencia del mismo por parte de cualquier área de la compañía.

3. **Reunión del comité de Seguridad de la información:** El área Administrativa y Financiera conformara de forma extraordinaria una reunión con la Gerencia, o el máximo órgano social, según corresponda para la seguridad de la información, en el cual se desarrollarán los siguientes ítems.

    a. **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.
    b. **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.
    c. **Toma de Medidas:** El comité deberá tomar las medias y los correctivos necesarios para evitar futuros incidentes.

5. MODIFICACIÓN DE LAS POLÍTICAS

BONDS AND CREDIT LTDA 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 rige a partir del 16 de enero de 2024.