EDICIÓN 1 FECHA: 12/08/2024 PE_05-RCE08	**PROCESO DE GESTION DE LA TECNOLOGIA E INFORMACION.** **Política de Privacidad**	

TABLA DE CONTENIDO

1. OBJETIVO **2**

2. ALCANCE **2**

3. RESPONSABILIDADES **2**

4. GENERALIDADES **2**

4.1Recopilación y Uso de Información Personal 2

4.2. Principios de Seguridad de la Información 2

4.3 Medidas de Seguridad 3

4.2. Protección de Datos Personales 3

4.3. Terceros y Transferencia de Datos 4

4.4. Evaluación de Riesgos 4

4.5. Incidentes de Seguridad 4

4.6 almacenamiento información sensible: 5

1. OBJETIVO

El propósito de esta política es garantizar que la información personal y los datos confidenciales sean gestionados de manera segura y se protejan contra accesos no autorizados, pérdida, alteración o divulgación no deseada. Esto incluye la implementación de medidas de seguridad y controles para cumplir con la ISO 27001, que define los requisitos para un sistema de gestión de seguridad de la información (SGSI).

2. ALCANCE

Esta política aplica a todos los empleados, contratistas, proveedores y cualquier tercero que tenga acceso a la información personal o confidencial en CONEXIONES EMPRESARIALES SAS También se aplica a todos los sistemas de información, infraestructuras tecnológicas y procesos que gestionan, almacenan o procesan dicha información.

3. RESPONSABILIDADES

- Coordinador de SGI (sistema de Gestión Integral):
- Todas las partes interesadas que tienen acceso a información resguardada por CONEXIONES EMPRESARIALES SAS

4. GENERALIDADES

4.1Recopilación y Uso de Información Personal

Recopilamos información personal y datos confidenciales de nuestros clientes, empleados y usuarios para los siguientes fines:

- Proveer nuestros servicios de manera eficiente.
- Cumplir con nuestras obligaciones legales y contractuales.
- Mejorar nuestros servicios y procesos internos.
- Realizar análisis internos de seguridad y calidad.

La información personal solo será recopilada y utilizada conforme a los principios de **necesidad, relevancia, y proporcionalidad**, garantizando que se recabe solo lo que sea necesario para el cumplimiento de nuestras actividades comerciales.

4.2. Principios de Seguridad de la Información

De acuerdo con la **ISO 27001**, seguimos una serie de principios de seguridad de la información, que incluyen:

- **Confidencialidad**: Nos aseguramos de que la información solo sea accesible para aquellos autorizados a tener acceso a ella.
- **Integridad**: Garantizamos que la información se mantenga exacta, completa y sin alteraciones no autorizadas.
- **Disponibilidad**: Aseguramos que la información esté disponible y accesible cuando sea necesario.

4.3 Medidas de Seguridad

Implementamos una serie de controles técnicos y organizativos para proteger la información personal y los datos confidenciales, que incluyen:

- **Controles de acceso**: Solo personas autorizadas tienen acceso a los datos personales según sus roles y responsabilidades, implementando la **gestión de acceso basada en roles**
- **Cifrado**: Todos los datos sensibles se cifran durante su almacenamiento y transmisión para garantizar su confidencialidad.
- **Monitoreo y auditoría**: Se realizan auditorías periódicas y monitoreo continuo de nuestros sistemas para detectar cualquier actividad sospechosa o no autorizada.
- **Entrenamiento en seguridad de la información**: Todos nuestros empleados y colaboradores reciben capacitación regular sobre las mejores prácticas en seguridad de la información y privacidad de datos.

4.2. Protección de Datos Personales

La protección de datos personales es una prioridad para nosotros. Cumplimos con todas las leyes y regulaciones locales e internacionales de protección de datos personales, como el **Reglamento General de Protección de** y otras normativas aplicables en nuestras regiones de operación.

Los usuarios tienen derecho a:

- Acceder a sus datos personales.
- Corregir o actualizar sus datos personales.
- Solicitar la eliminación de sus datos personales.
- Oponerse al procesamiento de sus datos personales bajo ciertas condiciones.

4.3. Terceros y Transferencia de Datos

No compartimos ni vendemos información personal a terceros sin el consentimiento explícito de los usuarios, salvo que sea necesario para cumplir con obligaciones legales o contractuales.

En caso de que sea necesario transferir datos a terceros proveedores o servicios externos, aseguramos que dichos terceros estén sujetos a acuerdos de protección de datos adecuados, cumpliendo con los estándares de seguridad definidos en esta política y la **ISO 27001**.

En CONEXIONES EMPRESARIALES SAS , hemos implementado una serie de controles técnicos y organizativos para proteger la seguridad y la reserva de los datos asegurando que los mismos estén protegidos contra alteraciones, pérdidas, tratamientos indebidos o accesos no autorizados. A continuación, describo los principales controles que hemos establecido:

- Cifrado de datos
- Control de accesos
- Registro de actividades
- Monitoreo
- Backup
- Protección de amenazas
- Políticas de seguridad
- Comunicación
- Evaluación de Riesgos
- Restricción de dispositivos extraíbles (USB, CD, DVD, etc.)

4.4. Evaluación de Riesgos

Realizamos evaluaciones de riesgos regulares sobre el procesamiento de datos personales y la seguridad de la información para identificar posibles vulnerabilidades y tomar medidas correctivas apropiadas. Esto incluye la identificación de amenazas potenciales, la evaluación de sus impactos y la implementación de controles de seguridad adecuados.

4.5. Incidentes de Seguridad

En caso de que se produzca un incidente de seguridad o violación de la privacidad de los datos, seguimos un protocolo definido para la gestión de incidentes, que incluye:

- Notificación inmediata a las partes afectadas.
- Investigación del incidente para determinar su impacto.
- Toma de medidas correctivas para mitigar los efectos y prevenir futuros incidentes.

- Notificación a las autoridades competentes si el incidente así lo requiere según la legislación aplicable.

4.6 almacenamiento información sensible:

El almacenamiento de información sensible en la nube puede ser seguro si se implementan adecuadas prácticas de seguridad y control:

I. Cifrado de Datos (En reposo y en tránsito)
contamos con un Proveedor de Servicios en la Nube Confiable que cumple con altos estándares de seguridad y privacidad

- En tránsito: Asegúrate de que todos los datos que se transmiten a la nube estén cifrados usando protocolos seguros, como TLS (Transport Layer Security), para evitar que los datos sean interceptados durante su transmisión.
- En reposo: Los datos sensibles almacenados en la nube deben estar cifrados mediante algoritmos robustos, nuestro proveedor de la nube nos ofrece opciones de cifrado para garantizar que los datos estén protegidos incluso si son accesibles por terceros no autorizados, Se utiliza AES-256 en bases de datos en AWS (RDS y S3). Cifrado en tránsito: TLS 1.2+ para proteger la transmisión de datos entre clientes y servidores
- Gestión de accesos con IAM: Roles y permisos mínimos necesarios (principio de menor privilegio).
- Autenticación multifactor (MFA) para accesos administrativos.
- Firewall y seguridad perimetral: Uso de VPC Security Groups.
- Configuración de listas blancas para permitir conexión de usuarios por IP.
- Monitoreo y detección de actividad sospechosa en bases de datos con AWS Cloud Watch y Cloud Trail

A través de la implementación de estos controles técnicos y organizativos, buscamos garantizar que los datos personales sean tratados de manera segura, protegidos contra accesos no autorizados, alteraciones o pérdidas, y que podamos responder rápidamente ante cualquier incidente que pueda comprometer su integridad. Nos comprometemos a mantener la confidencialidad, disponibilidad y integridad de los datos personales en todo momento, cumpliendo con las normativas y regulaciones vigentes en materia de protección de datos.

II. Control de Acceso y Autenticación

Implementa un control de acceso estricto para garantizar que solo personas autorizadas puedan acceder a la información sensible. Esto incluye:

- Autenticación multifactor Requiere múltiples factores para verificar la identidad de los usuarios, como contraseñas.
- Control de acceso basado en roles Configura permisos de acceso según los roles de los usuarios dentro de la organización, asegurando que solo los empleados o colaboradores con la necesidad de acceder a la información puedan hacerlo.
- No se permite el guardar información sensible y datos en equipos físicos, todo debe estar resguardado en la Nube.

a) Backup y Recuperación de Datos

los datos sensibles almacenados en la nube tengan copias de seguridad automáticas y estén protegidos de posibles fallos de hardware, pérdida de datos o ataques. Los datos están respaldados de manera cifrada y guardados y distribuidas para evitar riesgos de pérdida de información.

b) Monitorización y Auditoría

Implementa sistemas de monitoreo y auditoría para revisar continuamente el acceso y las actividades relacionadas con la información sensible. Los registros de actividad deben estar disponibles para detectar posibles accesos no autorizados, alteraciones o brechas de seguridad.

c) Protección de la Información con Contraseñas Fuertes

Las contraseñas utilizadas para acceder a los sistemas en la nube deben ser fuertes, es decir, combinando letras mayúsculas, minúsculas, números y caracteres especiales. Además, es recomendable actualizar las contraseñas regularmente y no compartirlas.

III. Implementación de Políticas de Seguridad Internas

Definimos y comunicamos nuestras políticas claras sobre el manejo de la información donde nuestra responsabilidad es proteger y garantizar el buen manejo de datos e información de nuestros clientes y la nuestra propia.

IV. Protección Contra Amenazas Externas (Firewall y Antimalware)

Configura mecanismos de seguridad adicionales, como firewalls y antivirus para proteger los datos contra posibles amenazas externas que puedan comprometer la seguridad de la información en la nube.

V. 9. Evaluaciones de Riesgos Continuas

Realiza evaluaciones de riesgos periódicas para identificar vulnerabilidades en los sistemas y protocolos de seguridad que se utilizan para almacenar la información sensible. Basado en los resultados de la evaluación, ajusta y refuerza las medidas de seguridad.

VI. 10. Cierre de Cuenta o Eliminación Segura de Datos

Cuando los datos ya no sean necesarios, asegúrate de que el proceso de eliminación sea seguro y conforme a las mejores prácticas. La eliminación de datos sensibles debe ser definitiva (borrado completo y no recuperable) para evitar cualquier acceso no autorizado posterior.

VII. Control Técnico

En CONEXIONES EMPRESARIALES SAS contamos con varios controles técnicos y organizativos implementados para prevenir la fuga de información a través de dispositivos extraíbles (USB, CD, DVD, etc.). Las medidas específicas que hemos implementado incluyen:

1. Desactivación de puertos USB y otros dispositivos extraíbles:
   - Hemos desactivado el acceso a puertos USB y otros dispositivos de almacenamiento extraíbles en los equipos que no requieren su uso, minimizando la posibilidad de fuga de información. Solo los empleados que necesiten utilizar estos dispositivos para su trabajo tienen acceso a ellos de manera controlada.
2. Política de Control de Acceso:
   - Implementamos políticas de control de acceso que permiten restringir el uso de dispositivos extraíbles. Solo los usuarios autorizados y con un propósito específico tienen acceso a dichos dispositivos.
3. Cifrado de Datos:
   - Todos los datos sensibles almacenados en dispositivos extraíbles deben ser cifrados mediante un cifrado de alta seguridad (por ejemplo, AES-256) antes de ser copiados a estos dispositivos. Esto garantiza que, incluso si un dispositivo es perdido o robado, la información almacenada en él está protegida.
4. Monitoreo y Registro de Actividades:
   - Utilizamos herramientas de monitoreo que registran todas las actividades relacionadas con dispositivos extraíbles. Esto nos permite auditar el acceso y uso de dispositivos como USBs, CDs o DVDs, y detectar cualquier comportamiento sospechoso o no autorizado.
5. Software de Prevención de Pérdida de Datos (DLP):
   - Hemos implementado sistemas de Prevención de Pérdida de Datos (DLP) que supervisan el uso de dispositivos extraíbles. Estos sistemas bloquean la transferencia de datos confidenciales o sensibles a dispositivos no autorizados.
6. Bloqueo de Copias No Autorizadas:

- En sistemas específicos, hemos implementado tecnologías de bloqueo de copias no autorizadas, que evitan que los empleados copien datos a dispositivos extraíbles sin los permisos adecuados.

7. Autenticación y Autorización Rigurosa:
   - Implementamos sistemas de autenticación multifactor (MFA) para garantizar que solo los usuarios autorizados puedan acceder a los sistemas y a la información. Además, se utiliza un control de acceso basado en roles (RBAC), que limita el acceso a los sistemas según las funciones específicas de los empleados, asegurando que solo tengan acceso a la información necesaria para realizar su trabajo.
8. Monitoreo y Auditoría Continuos:
   - Utilizamos herramientas avanzadas de monitoreo y auditoría para realizar un seguimiento continuo de las actividades dentro de nuestros sistemas de cómputo. Estos sistemas permiten detectar de manera temprana actividades sospechosas, como intentos de acceso no autorizado, modificaciones no registradas en la información o el uso indebido de los sistemas.
   - Los registros de auditoría contienen información detallada sobre qué usuarios han accedido a qué datos, qué acciones han realizado y cuándo, lo que nos permite detectar patrones inusuales de comportamiento.
9. Prevención de Pérdida de Datos (DLP):
   - Hemos implementado herramientas de Prevención de Pérdida de Datos (DLP) que monitorizan, filtran y bloquean el intento de transferir datos sensibles fuera de los sistemas internos de la organización. Estas herramientas son capaces de detectar comportamientos inusuales o no autorizados, como la descarga masiva de datos o el envío de información sensible a destinos no permitidos.
10. Protección contra Malware y Ataques Externos:
    - Se utilizan firewalls, antivirus y sistemas de detección de intrusos (IDS/IPS) para proteger nuestros sistemas de ataques externos o de malware que puedan intentar explotar vulnerabilidades y obtener acceso no autorizado a la información.
11. Control de Dispositivos Externos:
    - para evitar el abuso de los sistemas mediante dispositivos extraíbles (USB, discos duros externos, etc.), implementamos políticas que restringen el acceso a estos dispositivos y requieren la autorización explícita para su uso. Además, los dispositivos autorizados son cifrados para garantizar que los datos no puedan ser acusados indebidamente en caso de robo o pérdida.

12. Sistema de Alerta Temprana:
    - Hemos implementado un sistema de alertas automáticas que notifica a los administradores de sistemas en caso de detectar accesos anómalos, intentos de manipulación de datos o actividades fuera de los patrones normales de trabajo.
    -

VIII. Controles Organizativos:

1. Políticas Internas de Seguridad:
   - Contamos con políticas claras que regulan el uso de dispositivos extraíbles dentro de la organización. Estas políticas definen las responsabilidades de los empleados y los procedimientos a seguir para la autorización y el uso de dispositivos externos, garantizando que solo aquellos empleados con necesidades justificadas puedan acceder a estos dispositivos.
2. Capacitación y Concientización:
   - Proporcionamos capacitación regular a nuestros empleados sobre las mejores prácticas en seguridad de la información, incluyendo la protección contra la fuga de datos a través de dispositivos extraíbles. La capacitación incluye las implicaciones de seguridad y las consecuencias del uso indebido de estos dispositivos.
3. Revisión de Dispositivos Extraíbles:
   - Realizamos auditorías periódicas para revisar el uso de dispositivos extraíbles dentro de la organización, asegurándonos de que todos los controles estén siendo seguidos correctamente.
4. Acuerdos de Confidencialidad:
   - Todos los empleados y colaboradores firman acuerdos de confidencialidad que especifican la prohibición de la transferencia no autorizada de información sensible a dispositivos extraíbles. Estos acuerdos son parte de nuestro proceso de incorporación y de los contratos continuos con los empleados.
5. Evaluaciones Regulares de Riesgos:
   - Llevamos a cabo evaluaciones de riesgos periódicas para identificar posibles vulnerabilidades en los sistemas y procesos. A partir de estas evaluaciones, tomamos medidas correctivas para mitigar los riesgos y reforzar los controles existentes.
6. Revisión de Accesos y Privilegios:
   - Realizamos revisiones periódicas de los accesos y privilegios de los usuarios a los sistemas. Esto incluye verificar que los accesos estén alineados con las funciones laborales de cada empleado y que no haya accesos innecesarios a información sensible o crítica.
   - Investigación de Incidentes:
   - En caso de detectar un posible abuso de los sistemas o manipulación indebida de la información, contamos con un proceso de investigación de incidentes que incluye la recopilación de evidencia, el análisis del incidente y la toma de las acciones correctivas necesarias, como la suspensión de accesos o la implementación de medidas disciplinarias estipulado en el acuerdo de confidencialidad FCE-19-PA01 Acuerdo de confidencialidad.

7. Para identificar y mitigar el abuso de los sistemas de cómputo
    - detectar accesos inapropiados o manipulación indebida de la información, implementamos una combinación de herramientas y prácticas de monitoreo en AWS
8. Registro y Monitoreo Continuo:
    - AWS CloudWatch: Monitoreamos métricas de rendimiento y comportamiento anómalo en la infraestructura, como picos inusuales en el uso de CPU, memoria o tráfico de red.
    - AWS CloudTrail: Auditamos eventos y accesos en la plataforma, rastreando quién hizo qué acción, cuándo y desde dónde.
9. Alertas y Detección de Anomalías:
    - Se configuran alertas automáticas en AWS CloudWatch para detectar sobre cargas en los recursos de la plataforma.
    - Se implementan tableros de control por servicio con métricas clave para visualizar tendencias y detectar cambios abruptos en el uso de los recursos.
10. Respuestas a Incidentes y Trazabilidad:
    - Se mantiene un proceso de detección y respuesta a incidentes, con acciones predefinidas en caso de actividad sospechosa.
    - Los registros de CloudTrail permiten la trazabilidad completa de eventos, facilitando auditorías y análisis forenses si es necesario.