



Medidas Técnicas, Organizativas y Físicas

Sistema de Protección de Datos

BUSINESS & MICE COLOMBIA

Tabla de contenido

1. Introducción 1.1

Objetivo del Manual 1.2 Alcance 1.3 Marco Normativo 1.4 Relación con la Política de Tratamiento de Datos Personales

2. Principios y Lineamientos Generales

2.1 Principios de Tratamiento 2.2 Responsabilidades del Responsable y Encargado 2.3 Derechos de los Usuarios

3. Medidas de Seguridad Implementadas

3.1 Medidas Técnicas 3.2 Medidas Organizativas 3.3 Medidas Físicas

4. Seguridad del Dominio Web 4.1

Certificado SSL/TLS 4.2 Protección Hotlink 4.3 Firewall de Aplicaciones Web (ModSecurity) 4.4 Bloqueador de IPs 4.5 Evidencias Revisadas en Auditoría

5. Procesos de Auditoría e Inspección

5.1 Auditoría Interna 5.2 Auditoría Externa 5.3 Aspectos Revisados 5.4 Evidencias y Registros

6. Gestión de Autorizaciones y Consentimientos

6.1 Autorización para Tratamiento de Datos 6.2 Autorizaciones para Imágenes y Datos Audiovisuales 6.3 Autorizaciones para Menores de Edad

7. Gestión de Consultas, Reclamos y Supresión de Datos

7.1 Procedimiento de Consultas 7.2 Procedimiento de Reclamos 7.3 Eliminación y Revocatoria

8. Relación con Terceros y Proveedores

8.1 Transmisión y Transferencia de Datos 8.2 Contratos y Cláusulas de Protección 8.3 Verificación de Medidas de Seguridad

9. Gestión de Incidentes de Seguridad

9.1 Identificación 9.2 Registro 9.3 Acciones Correctivas 9.4 Reporte a Autoridades

1. Información del documento

Nombre del documento:	Medidas Técnicas, Organizativas y Físicas Sistema de Protección de Datos
Versión:	1.0

1. Alcance del Sistema de Protección de Datos

Este manual aplica a todos los procesos donde BUSINESS & MICE COLOMBIA recolecta, almacena, usa, circula o suprime datos personales, incluyendo:

- Bases de datos físicas y digitales.
- Información de clientes, prospectos, proveedores, empleados y asistentes a eventos.
- Datos audiovisuales captados durante actividades corporativas.
- Procesos internos administrativos, comerciales, operativos y de archivo.
- Transmisión y transferencia de datos a terceros autorizados.

2. Objetivo de las Inspecciones y Auditorías

Las auditorías internas y externas buscan verificar:

- Cumplimiento de la Ley 1581 de 2012 y Decreto 1377 de 2013.
- Aplicación de los principios de legalidad, finalidad, libertad, veracidad, transparencia, seguridad y confidencialidad.
- Implementación de medidas técnicas, organizativas y físicas para proteger los datos.
- Correcta gestión de autorizaciones, consultas, reclamos y supresión de datos.
- Funcionamiento de los controles de acceso, almacenamiento y circulación restringida.
- Cumplimiento de deberes del Responsable y del Encargado del Tratamiento.

3. Medidas Técnicas a Verificar

3.1 Seguridad de la Información

- Controles de acceso a bases de datos (usuarios, roles, permisos).
- Autenticación segura en sistemas internos.



- Registro de actividad (logs) y trazabilidad.
- Copias de seguridad y recuperación ante incidentes.
- Protección contra acceso no autorizado, pérdida o adulteración de datos.

“Guardar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado...”

3.2 Infraestructura Tecnológica

- Servidores y equipos con antivirus, firewall y actualizaciones vigentes.
- Cifrado de información sensible en tránsito y reposo.
- Protocolos de transmisión segura a terceros.
- Control de dispositivos externos (USB, discos, almacenamiento portátil).

4. Medidas Organizativas a Verificar

4.1 Procedimientos y Políticas

- Existencia y divulgación de la Política de Tratamiento de Datos.
- Procedimientos para consultas, reclamos y supresión.
- Manual interno de atención de solicitudes.

“Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley...”

4.2 Gestión de Autorizaciones

- Evidencia de autorizaciones previas, expresas e informadas.
- Formatos físicos o digitales de consentimiento.
- Autorizaciones para uso de imágenes en eventos.
- Autorizaciones para menores de edad y personas con discapacidad.

4.3 Capacitación y Competencias

- Capacitación del personal en protección de datos.
- Protocolos de manejo seguro de información.
- Compromisos de confidencialidad firmados.

4.4 Relación con Encargados y Terceros

- Contratos con cláusulas de protección de datos.
- Validación de medidas de seguridad de proveedores.
- Control de transmisión y transferencia de datos.



5. Medidas Físicas a Verificar

5.1 Control de Acceso Físico

- Oficinas con acceso restringido.
- Archivos físicos bajo llave.
- Control de ingreso de visitantes.
- Custodia de documentos sensibles.

5.2 Manejo de Documentos

- Almacenamiento seguro de contratos, autorizaciones y registros.
- Protocolos de destrucción segura de documentos.
- Señalización de áreas con información confidencial.

6. Aspectos Revisados en Auditorías Internas

- Cumplimiento de principios de tratamiento.
- Actualización y veracidad de los datos.
- Evidencia de autorizaciones y registros de consentimiento.
- Procedimientos de respuesta a consultas y reclamos.
- Gestión de incidentes de seguridad.
- Evaluación de proveedores encargados del tratamiento.
- Revisión de bases de datos y su clasificación (públicos, privados, sensibles).
- Verificación de medidas técnicas y físicas implementadas.

7. Aspectos Revisados en Auditorías Externas

- Cumplimiento normativo frente a SIC.
- Evidencia documental de políticas y procedimientos.
- Pruebas de seguridad tecnológica.
- Revisión de contratos con terceros.
- Validación de medidas de protección de datos sensibles.
- Revisión de reportes de incidentes y acciones correctivas.
- Evaluación de prácticas de recolección en eventos corporativos (incluyendo imágenes y videos).

8. Reportes y Acciones Correctivas

- Registro de hallazgos y no conformidades.
- Planes de acción con responsables y fechas.
- Seguimiento y cierre de acciones.
- Actualización de políticas y procedimientos cuando sea necesario.



“Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.”

9. Vigencia y Actualización

Este manual debe revisarse mínimo una vez al año o cuando:

- Cambie la normatividad.
- Se modifiquen procesos internos.
- Se incorporen nuevas tecnologías o proveedores.
- Se presenten incidentes de seguridad relevantes.

10. Seguridad del Dominio Web y Controles de Protección Digital

Como parte de las medidas técnicas y administrativas descritas en la Política de Tratamiento de Datos Personales —

“La información sujeta a tratamiento... se deberá manejar con las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros...” — BUSINESS & MICE COLOMBIA implementa controles específicos de seguridad en su infraestructura web y en el dominio institucional.

Estas medidas son verificadas durante auditorías internas y externas para garantizar la protección de los datos personales y la integridad de los servicios digitales.

10.1 Certificado SSL/TLS

El dominio oficial de BUSINESS & MICE COLOMBIA cuenta con **certificación SSL/TLS activa**, lo que garantiza:

- Cifrado de la información transmitida entre el usuario y el servidor.
- Protección contra interceptación de datos (MITM).
- Autenticación del dominio y confianza del navegador.
- Cumplimiento de buenas prácticas de seguridad web.

Durante auditoría se verifica:

- Vigencia del certificado.
- Correcta instalación y configuración.
- Ausencia de contenido mixto (mixed content).
- Redirección automática de HTTP a HTTPS.



10.2 Protección Hotlink

El dominio tiene habilitada la **protección contra hotlink**, evitando que terceros utilicen:

- Imágenes
- Videos
- Recursos digitales
- Archivos corporativos

sin autorización, lo cual protege la propiedad intelectual y evita consumo indebido de recursos del servidor.

Durante auditoría se revisa:

- Configuración del servidor o CDN.
- Lista de dominios permitidos.
- Bloqueo de solicitudes externas no autorizadas.

10.3 ModSecurity (WAF)

El servidor cuenta con **ModSecurity**, un firewall de aplicaciones web (WAF) que protege contra:

- Inyecciones SQL
- Cross-Site Scripting (XSS)
- Intentos de explotación de vulnerabilidades
- Escaneo automatizado de bots
- Manipulación de formularios o endpoints

Durante auditoría se valida:

- Reglas activas y nivel de sensibilidad.
- Registros de eventos y bloqueos.
- Actualización de reglas OWASP.
- Integración con el hosting o panel de control.

10.4 Bloqueador de IPs

El dominio implementa un **sistema de bloqueo de IPs** para prevenir accesos no autorizados, ataques o comportamientos sospechosos.

Controles revisados en auditoría:

- Listas de IPs bloqueadas y motivo del bloqueo.
- Listas blancas (whitelists) autorizadas.
- Registros de intentos de acceso fallidos.
- Automatización de bloqueo por comportamiento anómalo.

10.5 Evidencias Revisadas en Auditoría

Durante inspecciones internas y externas se solicita evidencia de:

- Panel de seguridad del hosting.
- Logs de ModSecurity y del servidor.
- Reportes de certificados SSL/TLS.
- Configuración de hotlink protection.
- Registros de bloqueo de IPs.
- Políticas de actualización y mantenimiento.

10.6 Relación con la Política de Tratamiento de Datos

Estas medidas complementan los principios de seguridad y confidencialidad establecidos en la Política:

“Guardar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado...”

“La información sujeta a tratamiento... se deberá manejar con las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad...”