Última actualización: enero de 2017

Marco NYMITY de Gobernanza en Privacidad y Protección de Datos

Menú de mecanismos para demostrar la responsabilidad: políticas de protección de datos, procedimientos, prácticas y otras medidas organizacionales o técnicas

NYMITY
innovating compliance

1. Mantenga una estructura de gobernanza

Asegúrese de que haya personas encargadas de protección de datos, responsabilidad de directivos y procedimientos de reporte a la gerencia

Actividades de Gestión de Información

- Asigne responsabilidades en protección de datos personales a un individuo (ej. Oficial de Protección de Datos, Asesor de Protección de Datos, CPO)
- Involucre a los Directivos en la gestión de protección de datos (ej. a la Junta Directiva o al Consejo Ejecutivo)
- Nombre un Oficial de Protección de Datos (OPD) independiente y con funciones de supervisión
- Asigne responsabilidades en materia de protección de datos a través de toda la organización (ej. Red de Protección de Datos)
- Mantenga roles y responsabilidades para las personas responsables de protección de datos (ej. descripción de puestos de trabajo)
- Mantenga comunicaciones regulares entre el Área de Protección de Datos, la Red de Protección de Datos y otras personas responsables en la materia
- Involucre en los asuntos de protección de datos a las partes interesadas dentro de la organización (ej. seguridad de la información, marketing, etc.)
- Reporte periódicamente a los stakeholders internos sobre el estado del programa de protección de datos (ej. Junta Directiva, Consejo de Administración)
- Reporte periódicamente a los stakeholders externos sobre el estado del programa de protección de datos (ej. autoridades de protección de datos, terceros, clientes)
- Lleve a cabo una Evaluación Corporativa de Riesgo en materia de protección de datos
- Integre la protección de datos en las evaluaciones y reportes de gestión de riesgos del negocio
- Mantenga una Estrategia de Protección de Datos
- Mantenga una misión/visión del programa de protección de datos
- Exija que los empleados reconozcan y se adhieran a las políticas de protección de datos

2. Mantenga un inventario de datos personales y mecanismos de transferencia de datos

Mantenga un inventario de sus bases de datos personales, o de los flujos de datos personales, incluyendo transferencias internacionales, con un listado de categorías de datos

Actividades de Gestión de Información

- Mantenga un inventario de bases de datos (qué datos personales son almacenados y en dónde)
- Clasifique los datos personales tratados por tipo (ej. sensibles, privados, semi-privados, públicos)
- Obtenga la aprobación de la autoridad de protección de datos para el tratamiento (cuando la aprobación sea necesaria)
- Registre las bases de datos ante la autoridad de protección de datos (cuando el registro sea necesario)
- Mantenga diagramas de flujo para los flujos de datos personales (ej. entre sistemas, entre procesos, entre países)
- Mantenga registros de los mecanismos usados para hacer transferencias internacionales de datos (ej. cláusulas contractuales estándar, normas corporativas vinculantes o aprobación de la autoridad de protección de datos)
- Use Normas Corporativas Vinculantes como un mecanismo de transferencia de datos
- Use contratos como mecanismo de transferencia de datos (ej. cláusulas contractuales estándar o contratos de transmisión y/o remisión de datos)
- Use las Reglas de Flujo Transfronterizo de Datos de APEC como mecanismo de transferencia de datos
- Use las aprobaciones de las autoridades de protección de datos como mecanismo de transferencia de datos
- Use la adecuación de terceros países o una de las medidas alternativas (ej. consentimiento, ejecución de contrato, interés público), como mecanismo de transferencia
- Use el Escudo de la Privacidad EU – EE.UU (EU-US Privacy Shield) como mecanismo de transferencia de datos

3. Mantenga una Política Interna de Protección de Datos

Mantenga una política de protección de datos personales que cumpla con los requerimientos legales y que establezca los riesgos operacionales y el riesgo de daños a los individuos

Actividades de Gestión de Información

- Mantenga una política de protección de datos personales
- Mantenga una política de protección de datos de empleados
- Mantenga un Código de Conducta organizacional que incluya aspectos de protección de datos
- Documente las bases legales del tratamiento de datos personales
- Integre la ética en el tratamiento de datos personales (ej. Códigos de Conducta, políticas y otras medidas)

4. Integre la protección de datos en las operaciones

Mantenga políticas y procedimientos operacionales consistentes con la política de protección de datos personales, los requerimientos legales y los objetivos del sistema de gestión de riesgo operativo

Actividades de Gestión de Información

- Mantenga políticas/procedimientos para la recolección y uso de datos personales sensibles (incluyendo datos biométricos)
- Mantenga políticas/procedimientos para la recolección y uso de datos personales de niños y menores de edad
- Mantenga políticas/procedimientos para velar por la calidad de los datos
- Mantenga políticas/procedimientos para anonimizar los datos personales
- Mantenga políticas/procedimientos para revisar los tratamientos hechos total o parcialmente por medios automatizados
- Mantenga políticas/procedimientos para usos secundarios de datos personales
- Mantenga políticas/procedimientos para obtener válidamente el consentimiento
- Mantenga políticas/procedimientos para la destrucción segura de datos personales
- Integre la protección de datos en el uso de cookies y de mecanismos de rastreo y localización
- Integre la protección de datos en las prácticas de retención de registros
- Integre la protección de datos en las prácticas de marketing directo
- Integre la protección de datos en las prácticas de marketing vía correo electrónico
- Integre la protección de datos en las prácticas de marketing vía telefónica (telemercadeo)
- Integre la protección de datos en las prácticas de publicidad digital (ej. en línea, dispositivos móviles)
- Integre la protección de datos en las prácticas de contratación de empleados
- Integre la protección de datos en las prácticas de la organización de uso de redes sociales
- Integre la protección de datos en las políticas/procedimientos BYOD (dispositivos personales en el lugar de trabajo)
- Integre la protección de datos en las prácticas de salud y seguridad
- Integre la protección de datos en la interacción con los comités de trabajo
- Integre la protección de datos en las prácticas para el monitoreo de empleados
- Integre la protección de datos en las prácticas de uso de sistemas de video-vigilancia
- Integre la protección de datos en el uso de dispositivos de geo-localización (de rastreo y/o localización)
- Integre la protección de datos en las políticas/procedimientos de acceso a las cuentas corporativas de correo electrónico de los empleados (ej. vacaciones, permisos, terminación)
- Integre la protección de datos en los procedimientos para llevar a cabo investigaciones internas
- Integre la protección de datos en las prácticas de revelación de información a las autoridades
- Integre la protección de datos en las prácticas de investigación (ej. investigación científica e histórica)

5. Mantenga un programa de capacitación y concientización

Provea capacitación continua y programas de concientización para promover el cumplimiento de la política de protección de datos y mitigar los riesgos operacionales

Actividades de Gestión de Información

- Lleve a cabo entrenamientos en protección de datos
- Lleve a cabo entrenamientos en protección de datos con contenidos específicos para los distintos puestos de trabajo
- Lleve a cabo regularmente capacitaciones de actualización
- Incorpore la protección de datos en otros programas operacionales de capacitación tales como recursos humanos, seguridad, call center
- Lleve a cabo capacitaciones que respondan a temas y asuntos de actualidad
- Desarrolle un boletín de protección de datos o incorpore la materia en las comunicaciones corporativas existentes
- Mantenga un repositorio de información sobre protección de datos (ej. una intranet sobre protección de datos)
- Publique materiales para crear conciencia sobre protección de datos (ej. carteleras y videos)
- Lleve a cabo eventos de concientización sobre protección de datos (ej. un día/semana anual de protección de datos)
- Mida la participación en las actividades de entrenamiento en protección de datos (ej. número de participantes, resultados)
- Haga efectivo el requisito de completar el entrenamiento en protección de datos
- Proporcione educación continuada y entrenamiento al personal del Área de Protección de Datos y/o para los Oficiales de Protección de Datos
- Mantenga certificados a los responsables en materia de protección de datos y provéales educación profesional continuada

6. Gestione los riesgos de seguridad de la información

Mantenga un programa de seguridad de la información basado en requerimientos legales y evaluaciones de riesgos periódicas

Actividades de Gestión de Información

- Integre el riesgo de protección de datos en las evaluaciones de riesgo de seguridad
- Integre la protección de datos en una política de seguridad de la información
- Implemente medidas de seguridad tecnológicas (ej. detección de intrusos, firewalls, monitoreo)
- Mantenga medidas para encriptar los datos personales
- Mantenga una política sobre los usos aceptables de los recursos de información
- Mantenga procedimientos para restringir el acceso a información personal (ej. acceso basado en roles o separado según funciones)
- Integre la protección de datos en una política de seguridad corporativa (protección de las instalaciones físicas y de activos tangibles)
- Mantenga medidas de seguridad de recursos humanos (ej. preselección, valoración de desempeño)
- Mantenga planes de back-up y continuidad del negocio
- Mantenga una estrategia de prevención de pérdida de datos
- Lleve a cabo exámenes regulares de las condiciones de seguridad de los datos personales
- Mantenga una certificación de seguridad (ej. ISO)

7. Gestione los riesgos con terceros

Celebre contratos y acuerdos con terceros que sean consistentes con la política de protección de datos, con los requerimientos legales y con los niveles de riesgo operacional tolerables

Actividades de Gestión de Información

- Mantenga requerimientos de protección de datos personales para terceros (ej. clientes, proveedores, encargados, afiliados)
- Mantenga procedimientos para celebrar contratos o convenios con todos los encargados
- Lleve a cabo procesos de debida diligencia (due diligence) de las prácticas de protección de datos y seguridad de la información de los potenciales proveedores/encargados
- Lleve a cabo procesos de debida diligencia de los terceros que suministran información personal a la organización
- Mantenga un procedimiento de evaluación de riesgos de protección de datos de sus proveedores/distribuidores
- Mantenga una política para contratar a los prestadores de servicios en la nube
- Mantenga procedimientos que establezcan las acciones por incumplimientos contractuales
- Lleve a cabo análisis continuos de debida diligencia sobre las prácticas de protección de datos y seguridad de la información de proveedores/encargados
- Revise los contratos de largo plazo para detectar riesgos de protección de datos nuevos o en evolución

8. Mantenga avisos de privacidad

Mantenga avisos de privacidad disponibles para los titulares que sean consistentes con la política de protección de datos, con los requerimientos legales y con los niveles tolerables de riesgo operacional

Actividades de Gestión de Información

- Mantenga un aviso de privacidad que detalle las prácticas de la organización en el manejo de datos personales
- Ponga a disposición un aviso de privacidad en todos los puntos en los que se recolecten datos personales
- Ponga a disposición el aviso de privacidad en medios visibles como letreros y carteles
- Ponga a disposición el aviso de privacidad en las comunicaciones de marketing (ej. correos electrónicos, folletos, ofertas)
- Ponga a disposición el aviso de privacidad en los contratos y términos de uso
- Mantenga guiones para uso de los empleados para explicar o dar a conocer el aviso de privacidad
- Mantenga una certificación de privacidad o un sello de confianza para incrementar la confianza de los clientes

9. Responda a las peticiones y quejas de los individuos

Mantenga procedimientos efectivos para interactuar con los titulares respecto de su información personal

Actividades de Gestión de Información

- Mantenga procedimientos para dar respuesta a las peticiones, quejas y reclamos
- Mantenga procedimientos para dar respuesta a las solicitudes de acceso a datos personales
- Mantenga procedimientos para responder solicitudes o para proveer mecanismos para que los individuos actualicen o corrijan sus datos personales
- Mantenga procedimientos para contestar solicitudes de eliminación de información (opt-out) o para restringir u objetar el tratamiento
- Mantenga procedimientos para responder las solicitudes de información
- Mantenga procedimientos para responder las solicitudes sobre portabilidad de datos
- Mantenga procedimientos para responder las solicitudes relacionadas con derecho al olvido o borrado de datos
- Mantenga preguntas y respuestas frecuentes para responder las inquietudes de los individuos
- Investigue las razones de fondo de las quejas de protección de datos
- Monitoree y reporte las mediciones de las quejas de protección de datos (ej. número, razones de fondo)

10. Monitoree las nuevas prácticas operacionales

Monitoree las prácticas operacionales para identificar nuevos procesos o cambios materiales en los procesos existentes y garantice la implementación de los principios de Privacy by Design (Privacidad por Diseño)

Actividades de Gestión de Información

- Integre la Privacidad por Diseño en el desarrollo de sistemas y productos
- Mantenga guías y formatos para las Evaluaciones de Impacto de Privacidad (PIAs por sus siglas en inglés) y las Evaluaciones de Impacto de Protección de Datos (EIPDs)
- Lleve a cabo PIAs/EIPDs para nuevos programas, sistemas y procesos
- Lleve a cabo PIAs/EIPDs cuando haga cambios a los programas, sistemas o procesos existentes
- Involucre a los interesados externos (ej. individuos, activistas de protección de datos) como parte del proceso de PIA/EIPD
- Monitoree y tome medidas para enfrentar problemas de protección de datos detectados durante las PIAs/EIPDs
- Reporte el análisis y los resultados del PIA/EIPD a la autoridad de protección de datos (en caso de ser requerido) y a los interesados externos (si resulta apropiado)

11. Mantenga un programa de gestión de incidentes y vulneraciones de datos

Mantenga un programa efectivo de gestión de incidentes y vulneraciones de datos personales

Actividades de Gestión de Información

- Mantenga un plan de respuesta a incidentes de datos personales
- Mantenga un protocolo de notificación (a los titulares afectados) y de reportes (a las autoridades de protección de datos, centrales de riesgo, policía, etc.) sobre incidentes
- Mantenga un registro para rastrear incidentes
- Monitoree y reporte las mediciones de incidentes de datos personales (ej. naturaleza del incidente, riesgo, razón de fondo)
- Lleve a cabo pruebas periódicas del plan de respuesta a incidentes
- Involucre a un proveedor de respuesta de incidentes
- Involucre a un equipo de investigación forense
- Obtenga un seguro con cobertura de incidentes de datos personales

12. Monitoree las prácticas de manejo de datos

Verifique que las prácticas operacionales cumplan con la política de protección de datos y las políticas y procedimientos operacionales, y mida y genere reportes sobre su efectividad

Actividades de Gestión de Información

- Lleve a cabo autoevaluaciones de gestión de datos personales
- Lleve a cabo auditorías internas del programa de protección de datos (ej. auditoría operativa del Área de Protección de Datos)
- Lleve a cabo revisiones frecuentes e integrales de los procedimientos
- Lleve a cabo evaluaciones a la medida con base en eventos externos, tales como quejas o incidentes
- Involucre a un tercero para llevar a cabo auditorías/evaluaciones
- Monitoree y reporte las mediciones del programa de protección de datos
- Mantenga documentación como evidencia para probar el cumplimiento legal y/o la responsabilidad demostrada (accountability)
- Mantenga certificaciones, acreditaciones o sellos de protección de datos para demostrarle a las autoridades de protección de datos el cumplimiento legal

13. Haga seguimiento a criterios externos

Haga un seguimiento continuo a nuevos requerimientos de cumplimiento, expectativas y buenas prácticas

Actividades de Gestión de Información

- Identifique de manera continua los requerimientos sobre cumplimiento legal (compliance) (ej. leyes, jurisprudencia, regulación, etc.)
- Mantenga suscripciones a un servicio de reporte de cumplimiento o a una actualización de una firma de abogados para mantenerse informado sobre nuevos desarrollos
- Participe en conferencias de protección de datos, eventos de asociaciones de industria o grupos de expertos
- Reporte el seguimiento a nuevas leyes, regulaciones, enmiendas u otras fuentes de derecho
- Consulte la opinión de abogados expertos en relación con los cambios regulatorios
- Documente las decisiones adoptadas frente a nuevos requerimientos incluyendo su implementación o cualquier razón para no implementar cambios
- Identifique y gestione los conflictos entre legislaciones

El Marco NYMITY de Gobernanza en Privacidad y Protección de Datos se desarrolló con base en la investigación global de Nymity sobre responsabilidad demostrada (*accountability*).
El Marco es un listado comprensivo de más de 130 Actividades de Gestión de Información (AGI) distribuidas en 13 Categorías de Gestión de Datos (CGD).