Primeros pasos del Marco de privacidad de NIST: una guía rápida para las pequeñas y medianas empresas

¿Qué es el Marco de privacidad de NIST y cómo lo puede usar mi organización?

El Marco de privacidad de NIST[1] es una herramienta voluntaria que puede ayudar a su organización a crear o mejorar un programa de privacidad. La gestión de riesgo de privacidad puede ayudarlo a crear confianza en sus productos y servicios, comunicar mejor sobre sus prácticas de privacidad y cumplir sus obligaciones de cumplimiento. Una buena ciberseguridad es importante, pero no puede abordar todos los riesgos de privacidad.

Comience utilizando el marco de privacidad siguiendo un modelo sencillo con las fases "En sus marcas, listos, fuera" y alinee a su empresa o agencia con las cinco áreas de gestión de riesgo de privacidad: identificación, gobernanza, control, comunicación y protección.

01 EN SUS MARCAS...

Prepárese para crear o mejorar su programa de privacidad utilizando el marco de privacidad para construir una base sólida para identificar y gestionar los riesgos de privacidad.

"Es difícil justificar la construcción de un programa de privacidad... el Marco de privacidad de NIST ha sido una de las herramientas que hemos podido usar, incluso cuando no podemos contar con un gran equipo de privacidad."

JAIME LEES
DIRECTORA DE DATOS
GOBIERNO DEL CONDADO DE ARLINGTON

Identificación:

- Identifique los datos que procesa (como recolección, uso, intercambio, almacenamiento) y mapee su flujo a través de sus sistemas en todo el ciclo de vida de los datos —desde la recolección a la eliminación. Esto no tiene que ser perfectamente exhaustivo, especialmente al principio, pero es una base para comprender sus riesgos de privacidad.
- Lleve a cabo una evaluación de riesgos de privacidad[2] utilizando su mapa de datos para evaluar cómo sus actividades de procesamiento de datos pueden crear problemas para personas (como vergüenza, discriminación o pérdidas económicas). Luego evalúe el efecto a su organización si esos problemas ocurrieran (como pérdida de la confianza del cliente o daños de imagen/reputación) que pudieran afectar su rentabilidad.
- Pregunte sobre opciones para contratos y productos y servicios que utiliza para operar su empresa para garantizar que estén configurados para reflejar sus prioridades de privacidad.

Gobernanza:

- La cultura de privacidad comienza en la cima. Determine en qué valores de privacidad (por ejemplo, autonomía humana, anonimato, dignidad, transparencia, control de datos) se enfoca su organización. Conecte los valores y políticas de privacidad de su organización con su evaluación de riesgos de privacidad para fomentar la confianza en sus productos y servicios.
- Conozca sus obligaciones legales relativas a la privacidad para que pueda construir productos y servicios que las cumplan.
- Ayude a su fuerza laboral a conocer sus roles y responsabilidades para que puedan tomar mejores decisiones sobre cómo gestionar riesgos de privacidad efectivamente en el diseño y despliegue de sus productos y servicios.
- Periódicamente, reevalúe para ver si sus riesgos de privacidad han cambiado. Esto puede ocurrir cuando hace mejoras a sus productos y servicios, cambia su procesamiento de datos o aprende sobre nuevas obligaciones legales.

[1] https://www.nist.gov/privacy-framework
[2] https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources

02

LISTOS ...

Ahora que conoce sus riesgos de privacidad y obligaciones legales y tiene una estructura de gobernanza, su organización puede enfocarse en las políticas y capacidades técnicas para sus sistemas, productos y servicios.

Control:

- ¿Está recolectando, intercambiando o almacenando datos que no necesita? Considere cómo sus políticas lo ayudan a usted o a otras organizaciones a mantener control sobre los datos y cómo las personas también podrían tener un rol.
- Tome en cuenta sus obligaciones legales y riesgos de privacidad cuando decida sobre la funcionalidad de sus servicios, productos, sistemas o procesamiento de datos. Considere un diseño flexible para que pueda responder de manera más costo-efectiva ante preferencias cambiantes de privacidad de clientes y un entorno legal dinámico.
- ¿Qué tipos de procesamiento de datos hace? Mientras más pueda lograr desconectar los datos de las personas y dispositivos, mayores serán las ganancias de privacidad. Considere cómo distintas medidas técnicas como la desidentificación, la descentralización de procesamiento de datos u otras técnicas pueden permitirle lograr sus objetivos empresariales o de agencia mientras protege la privacidad.

Protección:

- Controle quién puede iniciar sesión en su red y utilizar sus computadoras y otros dispositivos.
- Utilice software de seguridad para proteger los datos.
- Cifre los datos sensibles, en reposo y en tránsito.
- Realice respaldos periódicos de datos.
- Actualice el software de seguridad de manera regular, automatizando esas actualizaciones si fuera posible.
- Tenga políticas formales para disponer de manera segura los datos y dispositivos viejos.

"Si tiene que establecer un programa de privacidad, el Marco de privacidad de NIST es el lugar perfecto para comenzar."

JEEWON SERRATO
ASOCIADA
BAKERHOSTETLER

"El marco de privacidad puede ser un diferenciador de mercado para la organización para poder crecer su negocio."

MARY N. CHANEY, ABOGADA, CISSP, CIPP
DIRECTORADE INFORMACIÓN DE SEGURIDAD Y PRIVACIDAD
ESPERION THERAPEUTICS, INC.

Comunicación:

- Cree políticas para comunicar interna y externamente sobre sus actividades de procesamiento de datos.
- Incremente la transparencia y la comprensión del cliente brindando avisos e informes claros y accesibles o implementando alertas, avisos u otras señales para informar a las personas sobre sus actividades de procesamiento de datos y las elecciones que ellos tienen.
- ¿Realiza encuestas o grupos focales para obtener información para el diseño de servicios o productos? Incluya la privacidad para que pueda aprender más sobre las preferencias de privacidad de sus clientes.
- Considere qué hará en caso de una violación a los datos. ¿Cómo realizará notificaciones o cualquier recurso, como monitorear o congelar crédito? monitorear o congelar crédito?

03

¡FUERA!

Ahora es el momento avanzar desde donde se encuentra hoy hacia donde desea estar.

- ¿Cómo se compara su programa con lo que hemos sugerido aquí?
- Priorice los resultados de su objetivo y cree un plan de acción.
- Converse sobre su plan como una organización y utilícelo para trabajar hacia la adquisición de recursos y la construcción de la fuerza laboral necesaria para alcanzar sus metas.
- ¡Ponga su plan en marcha! ¡Está en camino de crear más confianza en sus productos y servicios, comunicarse más efectivamente sobre la privacidad con sus asociados y clientes y cumplir sus obligaciones de cumplimiento!

NIST National Institute of Standards and Technology
U.S. Department of Commerce