**Privacidad de la información: Regulación y cumplimiento normativo**

La seguridad y la privacidad están estrechamente relacionadas. Como recordarás, las personas tienen derecho a controlar cómo se recopilan y utilizan sus datos personales. Por su parte, las organizaciones tienen la responsabilidad de proteger la información que recopilan para evitar que se vea comprometida o sea mal utilizada. Como profesional de la seguridad, desempeñarás un rol fundamental en estas iniciativas.

Anteriormente, aprendiste cómo las regulaciones y el cumplimiento normativo ayudan a reducir el riesgo de seguridad. Para repasar, consulta [la lectura sobre cómo los controles de seguridad, los marcos y las regulaciones de cumplimiento normativo](https://www.coursera.org/learn/fundamentos-de-la-ciberseguridad/supplement/xu4pr/controles-marcos-y-cumplimiento) se combinan para gestionar la seguridad y minimizar el riesgo. En esta lectura, aprenderás cómo las regulaciones de privacidad de la información afectan las prácticas de manejo de datos. También conocerás algunas de las regulaciones de seguridad más influyentes en el mundo.

Diagrama, Icono

Descripción generada automáticamente

**Seguridad de la información versus privacidad de la información**

La seguridad y la privacidad son dos términos que se usan con frecuencia indistintamente fuera de este ámbito. Aunque ambos conceptos están relacionados, representan funciones específicas:

* **La privacidad de la información** se refiere a la protección contra el acceso y la difusión no autorizados de datos.
* **La seguridad de la información** (InfoSec) se refiere a la práctica de mantener los datos, en todas sus formas, alejados de usuarios no autorizados.

La diferencia clave: la privacidad consiste en proporcionar a las personas el control sobre su información personal y acerca de cómo se comparte. La seguridad, en cambio, se trata de proteger las decisiones de las personas y mantener su información a salvo de posibles amenazas.

Por ejemplo, una empresa minorista puede desear recopilar ciertos tipos de información personal sobre sus clientes con fines de marketing, como edad, género y ubicación. Antes de reunir esta información privada, es importante que se informe a los clientes sobre cómo se utilizará. Además, los clientes deben tener la opción de negarse a compartir sus datos si así lo desean.

Una vez que la empresa obtiene el consentimiento para recopilar información personal, puede implementar controles de seguridad específicos para proteger esos datos privados y evitar accesos, uso o divulgaciones no autorizadas. La compañía también debe contar con controles de seguridad para respetar la privacidad de todas las partes interesadas y de quienes optaron por no participar.

**Nota:** Tanto la privacidad como la seguridad son esenciales para mantener la confianza de los clientes y la reputación de la marca.

**Por qué es importante la privacidad en la seguridad**

La importancia de la privacidad en la seguridad de los datos comenzó a ganar mucha atención a finales de la década de 1990. En ese momento, las empresas tecnológicas pasaron repentinamente de procesar los datos de las personas a almacenarlos y utilizarlos con fines comerciales. Por ejemplo, si una persona buscaba un producto en línea, las empresas almacenaban y compartían información sobre el historial de búsqueda de ese usuario con otras organizaciones. Esto permitía a las compañías ofrecer experiencias de compra personalizadas de forma gratuita.

Con el paso del tiempo, esta práctica dio lugar a un debate global sobre si estas organizaciones tenían derecho a recopilar y compartir los datos privados de las personas. Además, la cuestión de la seguridad de los datos se convirtió en una preocupación creciente: a medida que las organizaciones recopilaban más datos, estos se volvían más vulnerables a ser objeto de abusos, uso indebido o robo.

Muchas organizaciones se preocuparon por la privacidad de los datos y comenzaron a ser más transparentes acerca de cómo recopilaban, almacenaban y utilizaban  la información. También comenzaron a implementar más medidas de seguridad para proteger la privacidad de los datos de las personas. Sin embargo, debido a la falta de reglas claras, las protecciones se aplicaban de manera inconsistente.

**Nota:** Cuantos más datos se recopilan, almacenan y utilizan, más vulnerables son a las filtraciones y amenazas.

**Regulaciones importantes sobre privacidad**

Las empresas deben cumplir con ciertas leyes para operar. Como recordarás, las **regulaciones** son normas establecidas por un gobierno u otra autoridad para controlar la forma en que se realiza algo. En particular, las regulaciones de privacidad existen para proteger a los usuarios de que su información sea recopilada, utilizada o divulgada sin su consentimiento. Además, estas regulaciones suelen describir las medidas de seguridad que deben implementarse para mantener la información privada protegida de amenazas.

Tres de las regulaciones de la industria más influyentes que todo profesional de la seguridad debe conocer son:

* Reglamento General de Protección de Datos (RGPD)
* Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI-DSS)
* Ley de Transferencia y Responsabilidad de los Seguros Médicos (HIPAA)

**Reglamento General de Protección de Datos (RGPD)**

El Reglamento General de Protección de Datos (RGPD) es un conjunto de normas y regulaciones desarrollado por la Unión Europea (UE) que otorga a los propietarios de los datos el control total sobre su información personal. Según el RGPD, se considera información personal el nombre, la dirección, el número de teléfono, la información financiera e información médica de una persona, entre otras.

Esta normativa es aplicable a cualquier empresa que maneje datos de ciudadanos o habitantes de la UE, sin importar dónde opere dicha compañía. Por ejemplo, una organización con sede en los Estados Unidos que maneja los datos de las visitas provenientes de la UE en su sitio web está sujeta a las disposiciones del RGPD.

**Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI-DSS)**

El Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI-DSS) refiere a un conjunto de normas de seguridad establecidas por importantes organizaciones de la industria financiera. Esta regulación tiene como objetivo asegurar las transacciones con tarjetas de crédito y débito contra el robo de datos y el fraude.

**Ley de Transferencia y Responsabilidad de los Seguros Médicos (HIPAA)**

La Ley de Transferencia y Responsabilidad de los Seguros Médicos (HIPAA) es una ley de los Estados Unidos que obliga a proteger la información sensible de salud de la gente. En virtud de la HIPAA, se prohíbe la divulgación de la información médica de una persona sin su conocimiento y consentimiento.

**Nota**: Estas regulaciones influyen en el manejo de datos en muchas organizaciones del mundo, a pesar de que fueron elaboradas por países o mercados específicos.

Existen otras leyes de cumplimiento normativo en materia de seguridad y privacidad. Cuáles de ellas debe seguir tu organización dependerá de la industria y del ámbito en el que se desempeñe. Independientemente de las circunstancias, el cumplimiento normativo es importante para todas las empresas.

**Evaluaciones y auditorías de seguridad**

Las empresas deben cumplir con regulaciones que son importantes para el sector o industria en la que se desempeñan. Al hacerlo, validan que han alcanzado un nivel mínimo de seguridad, al mismo tiempo que demuestran su compromiso con mantener la privacidad de los datos.

El cumplimiento de las normas suele ser un proceso continuo y de dos partes, que implica auditorías y evaluaciones de seguridad:

* Una **auditoría de seguridad** es una revisión de los controles de seguridad, políticas y procedimientos de una organización frente a un conjunto de expectativas.
* Una **evaluación de seguridad** es una revisión para determinar la resistencia de las actuales medidas de seguridad frente a las amenazas.

Por ejemplo, si una regulación establece que se debe habilitar la autenticación de múltiples factores (MFA) en todas las cuentas de administrador, se podría realizar una auditoría para verificar el cumplimiento de esas cuentas de usuario. Después de la auditoría, el equipo interno podría realizar una evaluación de seguridad que determine que muchos usuarios están utilizando contraseñas poco seguras. Basándose en su evaluación, el equipo podría decidir habilitar la MFA en todas las cuentas de usuario para mejorar su postura de seguridad general.

**Nota:** El cumplimiento de regulaciones legales, como el RGPD, puede ser verificado durante las auditorías.

Como analista de seguridad, es probable que participes de auditorías y evaluaciones de seguridad. Las empresas suelen realizar auditorías de seguridad con menos frecuencia, aproximadamente una vez al año. Estas auditorías pueden ser realizadas tanto internamente como  por diferentes grupos externos de terceros.

En cambio, las evaluaciones de seguridad se realizan con mayor frecuencia, generalmente cada tres a seis meses. Estas evaluaciones suelen ser realizadas por personal interno, en general como preparación para una auditoría de seguridad. Ambas evaluaciones son de suma importancia para asegurar que tus sistemas están protegiendo eficazmente la privacidad de todas las partes.

**Conclusiones clave**

Cada vez más empresas están dando prioridad a proteger y regular el uso de datos confidenciales para mantener la confianza de los clientes. Los profesionales de la seguridad deben pensar en los datos y en la necesidad de privacidad desde esta perspectiva. Las organizaciones suelen utilizar evaluaciones y auditorías de seguridad para identificar posibles fallas en sus planes de seguridad. Sin embargo, ignorar o posponer la corrección de los resultados de una evaluación, puede tener graves consecuencias para la empresa, como multas o filtraciones de datos.

Marcar como completo

Me gusta

No me gusta

Informar de un problema