V.1. Brechas en la protección de datos y confidencialidad de la información (clientes, proveedores, terceros, empleados/as, empresa).

Descripción del asunto

La gestión de datos, imágenes e información personal y confidencial resulta relevante para todas las empresas del sector tecnológico, y de interés para sus proveedores, clientes y usuarios, por ejemplo, toda vez que las buenas prácticas en el manejo y uso de este tipo de contenidos, disminuye el riesgo de vulneración de derechos como la privacidad, el buen nombre, honor, honra y reputación.

Ante la gran capacidad actual para producir, almacenar y procesar datos (big data), aumenta también la necesidad de hacer un uso responsable de los mismos, ya que la gran mayoría de estos datos son datos privados (de personas empleadas, proveedores, clientes, usuarios, etc.). Usar de manera ilegítima o no autorizada estos datos, significa no asegurarse de que se cuenta con un consentimiento previo, libre e informado, donde la persona tenga control y conocimiento de lo que acepta. Pero, además, implica que se reflexione sobre el posible mal uso que se pueda dar a estos datos. Si bien los metadatos pueden aportar beneficios, algunos tipos de metadatos, tomados en conjunto, pueden revelar información personal y dar indicación del comportamiento, las relaciones sociales, las preferencias privadas e incluso la identidad de una persona.

Conexión con el asunto:

Algunas posibles causas internas	Algunas posibles causas externas
○ Falta de integridad del personal involucrado en los procesos de registro, gestión y confidencialidad de datos. ○ Falta de capacitación a personas empleadas sobre buenas prácticas de registro, gestión y confidencialidad de datos suministrados por terceros. ○ Ineficacia en los procedimientos y políticas sobre protección, gestión y confidencialidad de los datos. ○ Posibles brechas de ciberseguridad de las bases de datos. ○ Aplicación de la regulación local vs. el derecho internacional de los derechos humanos. ○ Ausencia de mecanismos de denuncia que generen confianza y una remediación efectiva.	○ Reclamación, por parte de los organismos públicos, de datos privados de las personas empleadas, proveedores, clientes, y terceras personas. ○ Contextos donde la regulación es laxa y/o no protege derechos básicos. ○ Elevado desarrollo y sofisticación de los delitos de ciberseguridad. ○ Mala prácticas en la gestión de datos y la confidencialidad de la información por parte de terceros (clientes, proveedores, socios…).

Impactos en las personas	Riesgos para Indra
○ Fraudes y suplantación de identidad. ○ Divulgación o uso no autorizado y no permitido de datos personales y privados. ○ Intromisión en la vida privada de las personas. ○ Afectación en la dignidad de la persona. ○ Daños a la reputación, honra y buen nombre. ○ Impactos en otros derechos afectados.	○ Mala reputación / Riesgo reputacional. ○ Riesgos operacionales (multas, paralización de servicios…). ○ Pérdida de grupos de interés (personas empleadas, proveedores, clientes…). ○ Desconfianza del mercado / inversores. ○ Presión y mayor observancia de las ONGs. ○ Conflictos (internos y externos). ○ Demandas judiciales.

Derechos afectados	
○ Privacidad. ○ Buen nombre, honra y reputación. ○ Habeas data - Protección de datos. ○ Derecho a la información.	○ Consentimiento previo, libre e informado. ○ Dignidad. ○ Pleno desarrollo de la personalidad individual. ○ Libertad individual.