4to. Congreso Internacional de Protección de Datos Personales

Y

XIV Encuentro Iberoamericano de Protección de Datos

LUIS FERNANDO COTE PEÑA

GERENTE GENERAL Y DE OPERACIONES EN FERSACO S.A.S.

Consultores Especializados en Cumplimiento de Hábeas Data

FERSACO
Consultoría integral

www.fersaco.com

luisfernandocotep@fersaco.com

3157942668

¿POR QUÉ ACTUAR EN RELACIÓN CON LOS INCIDENTES?

Para Responsables y Encargados del tratamiento:

- *Existe el deber legal de informar las violaciones de los códigos de seguridad **.*

- *Les asiste la necesidad de disminuir el daño o peligro al interés tutelado ante tales violaciones, por ser este un criterio de graduación de sanciones **.*

**Ley 1581 de 2012 en concordancia con la Circular Externa 02 del 3 de Noviembre de 2015.*

Protegida con derechos de autor

GESTIÓN DE INCIDENTES

FERSACO
Consultoría integral
www.fersaco.com

Protegida con derechos de autor

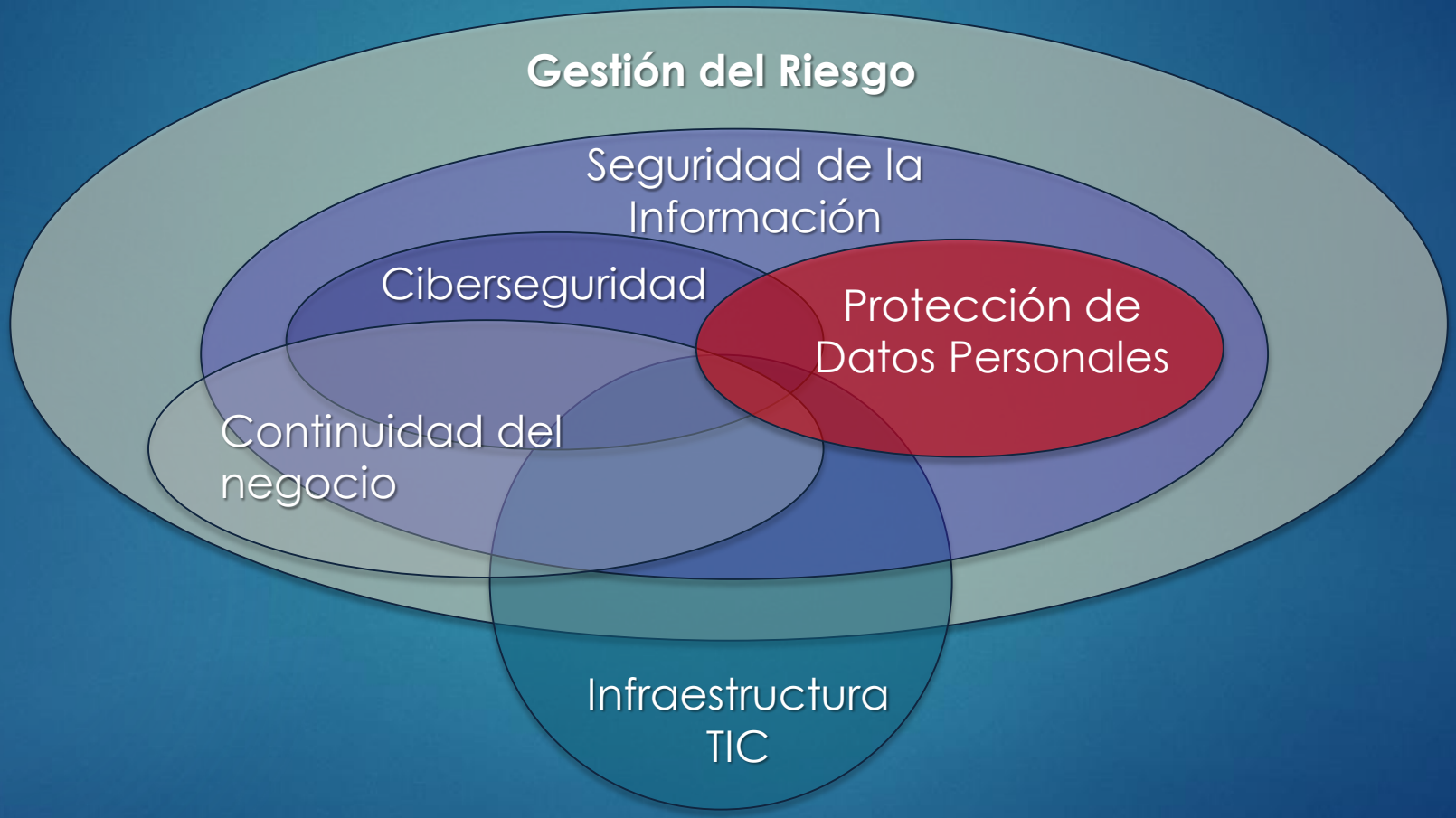
ACCIONES PREVIAS AL INCIDENTE

- Diseñar e implementar un SGSDP

Protegida con derechos de autor

ACCIONES PREVIAS AL INCIDENTE

- Comprender sistémicamente el riesgo de incidentes de Hábeas Data



*Interrelaciones Sistémicas (Adaptado de "Ciberseguridad en 9 pasos, el manual para la ciberseguridad de la información del Gerente" de Dejan Kosutic, 2012).

Protegida con derechos de autor

ACCIONES PREVIAS AL INCIDENTE

- Identificar en el SGSDP el diamante de la gestión de incidentes

Protegida con derechos de autor

ACCIONES PREVIAS AL INCIDENTE

- Registrar información en el RNBD

Paso 6 del RNBD*:
Medidas de seguridad de la información

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN PERSONAL	
¿Cuenta con una política y procedimientos implementados de gestión de incidentes de seguridad de la información personal?	☐
¿Tiene implementada una política para mejorar la seguridad de la información personal a partir de los incidentes o vulnerabilidades detectados?	☐

*Manual de Usuario del Registro Nacional de Bases de Datos – RNBD 2015, Página 39

Protegida con derechos de autor

RESUMEN DE ACCIONES PREVIAS AL INCIDENTE

QUÉ?	QUIÉN?	CÓMO?	CUÁNDO	DÓNDE?
Diseñar e Implementar el SGSDP	Alta Dirección, Equipo del proyecto, Comité de Protección de Datos	Se sugiere apalancarse en la serie 27000 de la ISO en especial la 27001:2013	Desde la expedición de la Ley 1266 de 2008 y 1581 de 2012	Transversal a la organización
Comprender sistémicamente el riesgo	Alta Dirección, Comité de Protección de Datos y CSIRT	Favoreciendo una cultura de gestión de riesgos	Permanentemen-te	Transversal a la organización
Identificar en el SGSDP el diamante de la gestión de incidentes	Comité de Protección de Datos y CSIRT	Identificar gobierno, activos, tipificación y protocolo	Desde la implementación del SGSDP	Al interior del Comité de Protección de Datos y del CSIRT
Registrar información en el RNBD	Administrador y/o el operativo del RNBD	Marcando en cada BD, en gestión de incidentes de seguridad, la existencia de las políticas exigidas	**Antes del 8 de noviembre de 2016**	Plataforma RNBD de la SIC

Protegida con derechos de autor

Protegida con derechos de autor

ACCIONES DURANTE EL INCIDENTE

- Atención y reconocimiento del incidente por el CSIRT

A. REPORTAR DE LA OCURRENCIA DEL INCIDENTE
B. ATACAR EL INCIDENTE
C. RESTABLECER LA OPERACIÓN

D. DOCUMENTAR EL INCIDENTE

1. **Tipo**
2. **Causa**
3. **Tipo y número de Titulares afectados**
4. **Tipo y número de registros de datos personales comprometidos**
5. **Activos comprometidos**
6. **Afectaciones probables a los Titulares**
7. **Afectaciones probables para la Organización**
8. **Medidas adoptadas**

E. REPORTAR AL COMITÉ DE PROTECCIÓN
F. INFORMAR AL ADMINISTRADOR O EL OPERATIVO DEL RNBD

Protegida con derechos de autor

RESUMEN DE ACCIONES DURANTE EL INCIDENTE

QUÉ?	QUIÉN?	CÓMO?	CUÁNDO	DÓNDE?
Reportar sobre incidente	Quien lo detecte	A través de los canales definidos en el protocolo de gestión de incidentes	Una vez detectado	AL CSIRT a través del Helpdesk, mail, teléfono o personalmente
Atacar el Incidente	CSIRT	Depende de la naturaleza del incidente	Inmediata-mente sea detectado	En los activos involucrados
Restablecer la operación	CSIRT	Depende de la naturaleza del ataque y del compromiso de operación	Inmediata-mente sea controlado	En las áreas afectadas
Documentar el incidente	CSIRT	Registrando, fecha de ocurrencia y/o detección tipo, causa, titulares, etc.	Inmediata-mente sea controlado	Registro de Incidentes del CSITR
Informar ocurrencia del incidente	CSIRT	Registrando, fecha de ocurrencia y/o detección tipo, causa, titulares, activos, afectaciones a los Titulares y organización y medidas adoptadas.	Inmediata-mente sea documenta-do	Comité de Protección de Datos
Reportar incidente	CSIRT	Tipo, causa, fecha de ocurrencia, total de titulares afectados, fecha de conocimiento, tipo de dato comprometido, etc.	**Inmediatamen-te sea documentado**	Usuario u operario Del RNBD

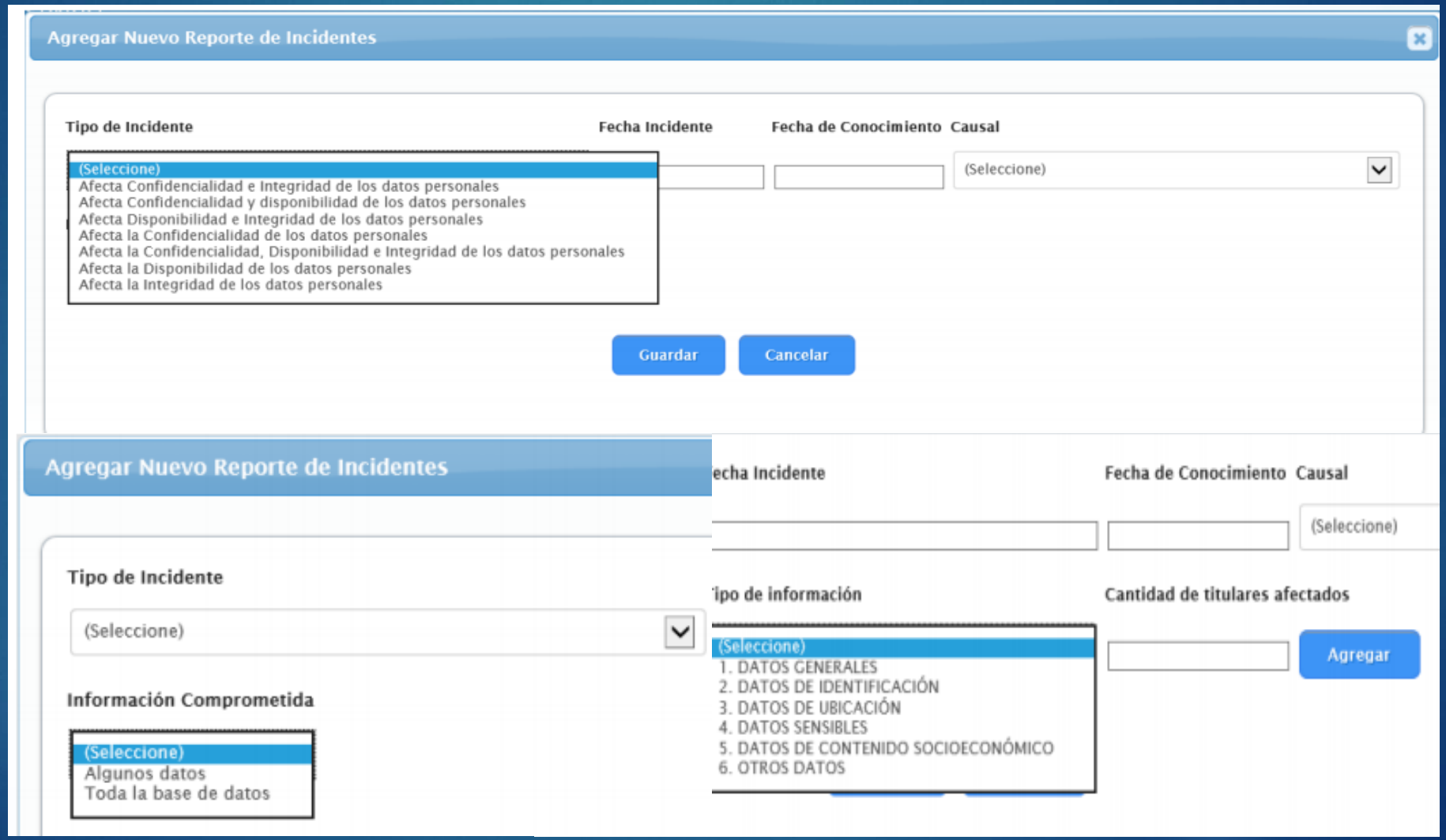
ACCIONES DESPUÉS DEL INCIDENTE

- Reportar a la SIC el incidente

Protegida con derechos de autor

ACCIONES DESPUÉS DEL INCIDENTE

- Reportar a la SIC



Protegida con derechos de autor

ACCIONES DESPUÉS DEL INCIDENTE

- Atender inmediatamente al Titular

COMUNICACIÓN INMEDIATA AL TITULAR AFECTADO:

1. Naturaleza de la violación
2. Fecha de ocurrencia y/o de conocimiento de ocurrencia
3. Datos comprometidos
4. Sus posibles afectaciones
5. Mecanismos adoptados en su favor
6. Contacto de atención

Protegida con derechos de autor

EXCEPCIONES ESPAÑOLAS AL DEBER DE INFORMAR AL TITULAR

Reglamento 2016/679 del PE/CE artículo 34

a. Datos afectados, estaban sometidos a medidas de protección técnicas y organizativas apropiadas, que protegen la confidencialidad, como el cifrado;
b. Posteriormente se adoptaron medidas que evitan alto riesgo para los derechos y libertades del interesado.
c. Si implica esfuerzo desproporcionado, caso en el cual se realiza comunicación pública o una medida semejante para informar efectivamente a los interesados.

**Nota: En Colombia no hay excepción reglada.*

Protegida con derechos de autor

ACCIONES DESPUÉS DEL INCIDENTE

- Aprender la lección

A. EVALUAR Y GESTIONAR CONOCIMIENTO DOCUMENTANDO:

1. Hechos generadores
2. Efectos del incidente
3. Medidas correctivas adoptadas
4. Incluso incidentes no resueltos

B. INCORPORAR INFORMACIÓN AL BANCO DE INCIDENTES

C. SOCIALIZAR CON ÁREAS INVOLUCRADAS

D. COMPARTIR CON OTROS CSIRT`S

FERSACO Consultoría integral

www.fersaco.com

Protegida con derechos de autor

RESUMEN DE ACCIONES DESPUÉS DEL INCIDENTE

QUÉ?	QUIÉN?	CÓMO?	CUÁNDO	DÓNDE?
Reportar a la SIC	Usuario Del RNBD	Tipo, causa, fecha de ocurrencia, total de titulares afectados, fecha de conocimiento, tipo de dato comprometido, compromiso total o parcial de datos.	"15 días hábiles siguientes al momento en que se detecten (se conozca) y sean puestos en conocimiento de la persona o área encargada de atenderlos"	En el RNBD
Aten-der Inmediatamente al titular	Comité de P de DP o quien haga sus veces	Informando, fecha de ocurrencia y/o detección tipo, causa, titulares, registros, activos, afectaciones probables a los Titulares y organización y medidas adoptadas.	Inmediatamente se recibe el reporte del CSIRT	A la dirección del Titular registrada en la BD de la organización
Apren-der la lección	CSIRT junto con el Comité de Protección de DP si fuere distinto	Evaluando el incidente documentado, incorporándolo al banco de incidentes, compartiéndolo con otros CSIRT´s y socializando las lecciones aprendidas.	Una vez restablecida la operación y mitigados los efectos del incidente	Comité de Protección de DP o CSITR, Funcionarios de Áreas afectadas.

Protegida con derechos de autor

"El asunto no es tanto la ausencia de incidentes como la confianza en que están bajo control: se sabe qué puede pasar y se sabe qué hacer cuando pasa."

(MAGERIT – versión 3, 2012, Pág. 7)

FERSACO
Consultoría integral

www.fersaco.com

Protegida con derechos de autor

GRACIAS

LUIS FERNANDO COTE PEÑA
GERENTE GENERAL Y DE OPERACIONES FERSACO S.A.S.
Consultores Especializados en Cumplimiento de Hábeas Data

www.fersaco.com
luisfernandocotep@fersaco.com
3157942668