Un marco de información para la responsabilidad digital corporativa

Colegio de Registradores de España, 22 de abril de 2024
Acto 20 aniversario de XBRL España

Enrique Bonsón. Universidad de Huelva. Observatorio BIDA-AECA.

Un marco de información para la responsabilidad digital corporativa

- Concepto y función de la RDC. El contexto informativo.

- El marco de información:

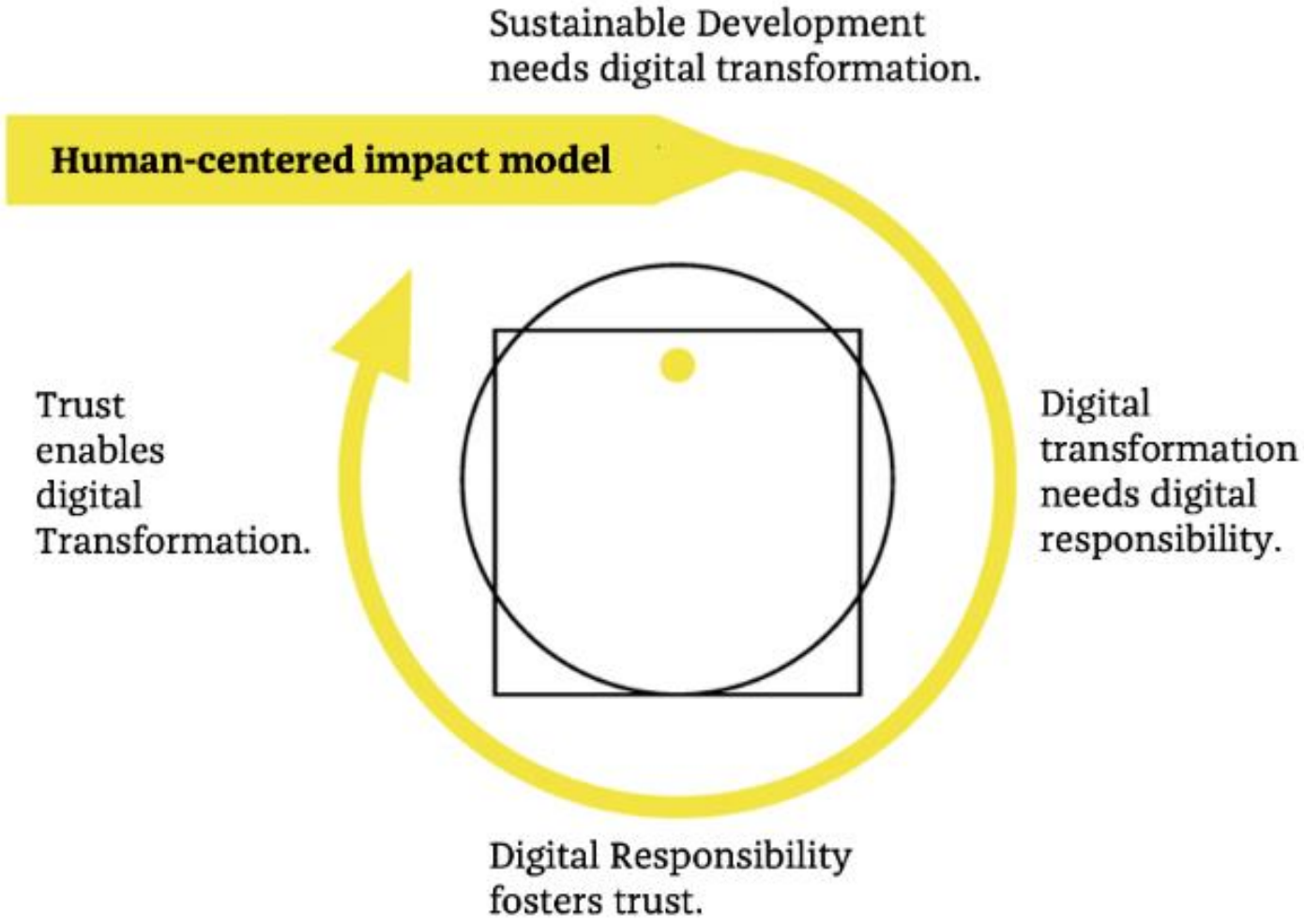
  - Enfoque RDC y acciones AESG
  - Riesgos digitales
  - Ciberseguridad
  - Protección de datos y privacidad
  - IA fiable: Algoritmos y equidad de datos

Concepto de RDC

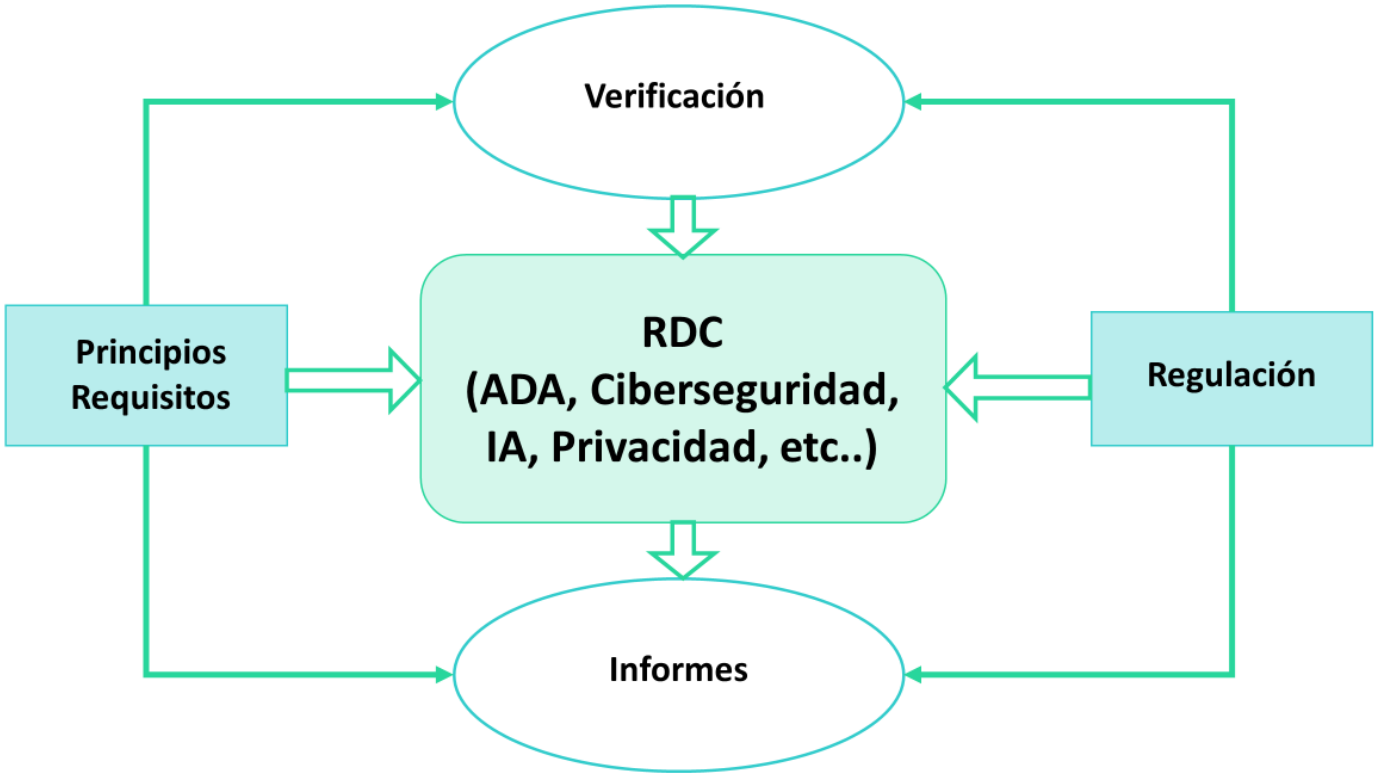
La responsabilidad digital corporativa es una orientación corporativa hacia el uso legal y ético de los datos y las tecnologías digitales de manera que se protejan los derechos de las personas en torno a los datos y las decisiones algorítmicas que les afectan y se genere confianza en relación con la seguridad, la utilidad y la eficiencia de la tecnología empleada (AECA, 2022).

La RDC es relevante porque reconoce que el uso de las tecnologías puede tener impactos significativos en la sociedad, y que las empresas deben usarlas de manera responsable. Al adoptar un enfoque de responsabilidad digital, las empresas pueden generar confianza y contribuir a un futuro digital más sostenible y equitativo.

La responsabilidad digital genera confianza (Identityvalley.org)



El contexto de la información sobre RDC



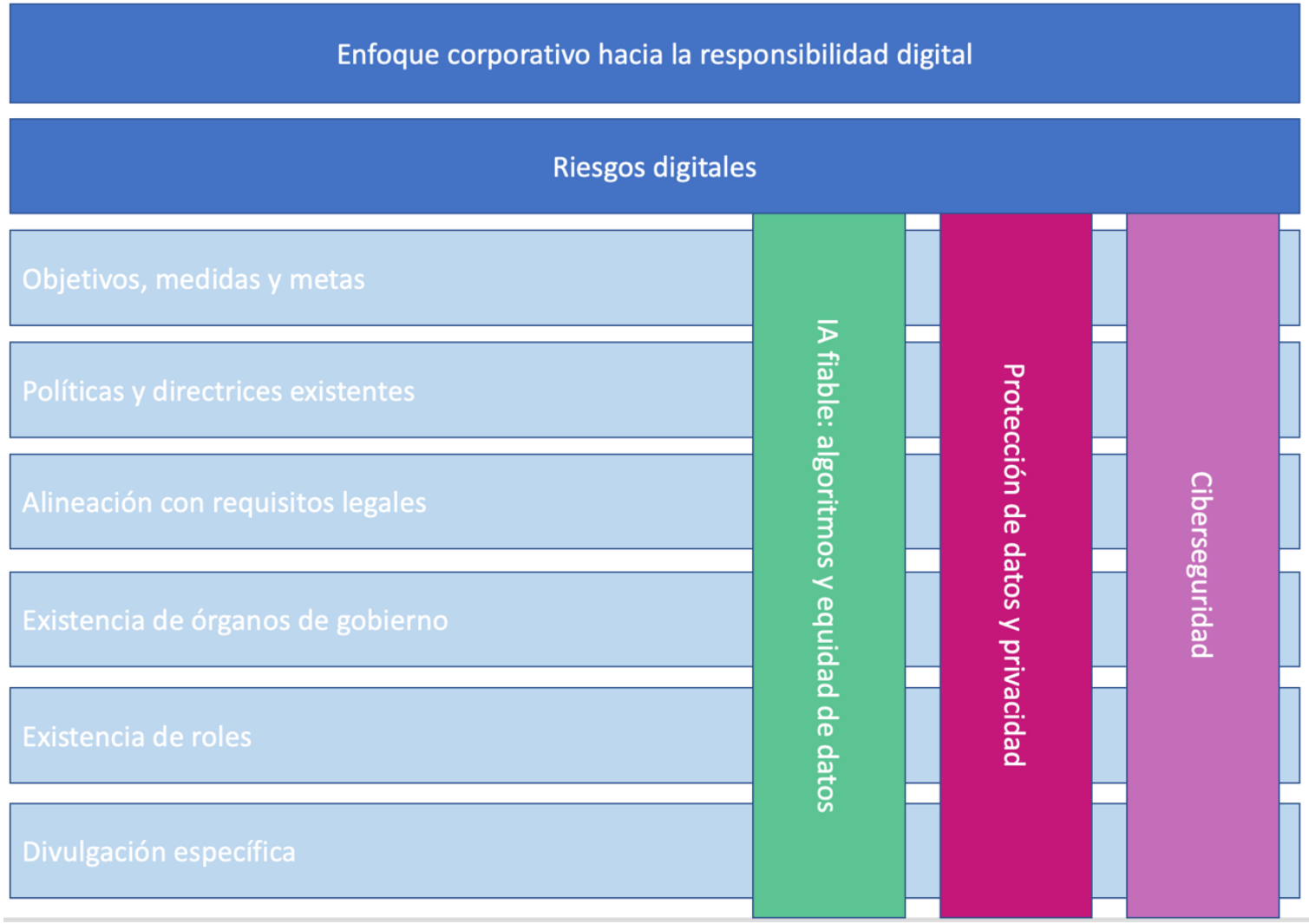
Metodología

1. **Comparación, contraste y organización de elementos.** Los temas y las mejores prácticas extraídas de diversas fuentes se compararon y organizaron en un conjunto preliminar de elementos propuestos para el marco.

2. **Validación mediante cuestionario.** Para asegurar que los elementos propuestos estuvieran bien fundamentados y alineados con las expectativas de las partes interesadas, se distribuyó un cuestionario diseñado para solicitar retroalimentación e ideas de expertos, académicos, representantes de la industria, organizaciones de la sociedad civil y otras partes interesadas relevantes.

3. La **propuesta final** surgió como resultado de la retroalimentación recibida a través del cuestionario que fue cuidadosamente analizada e incorporada al marco, mejorando su integridad y relevancia. Esta propuesta fue **aprobada por la Comisión de NTyC de AECA**.

El marco de información sobre RDC



Enfoque RDC y acciones AESG

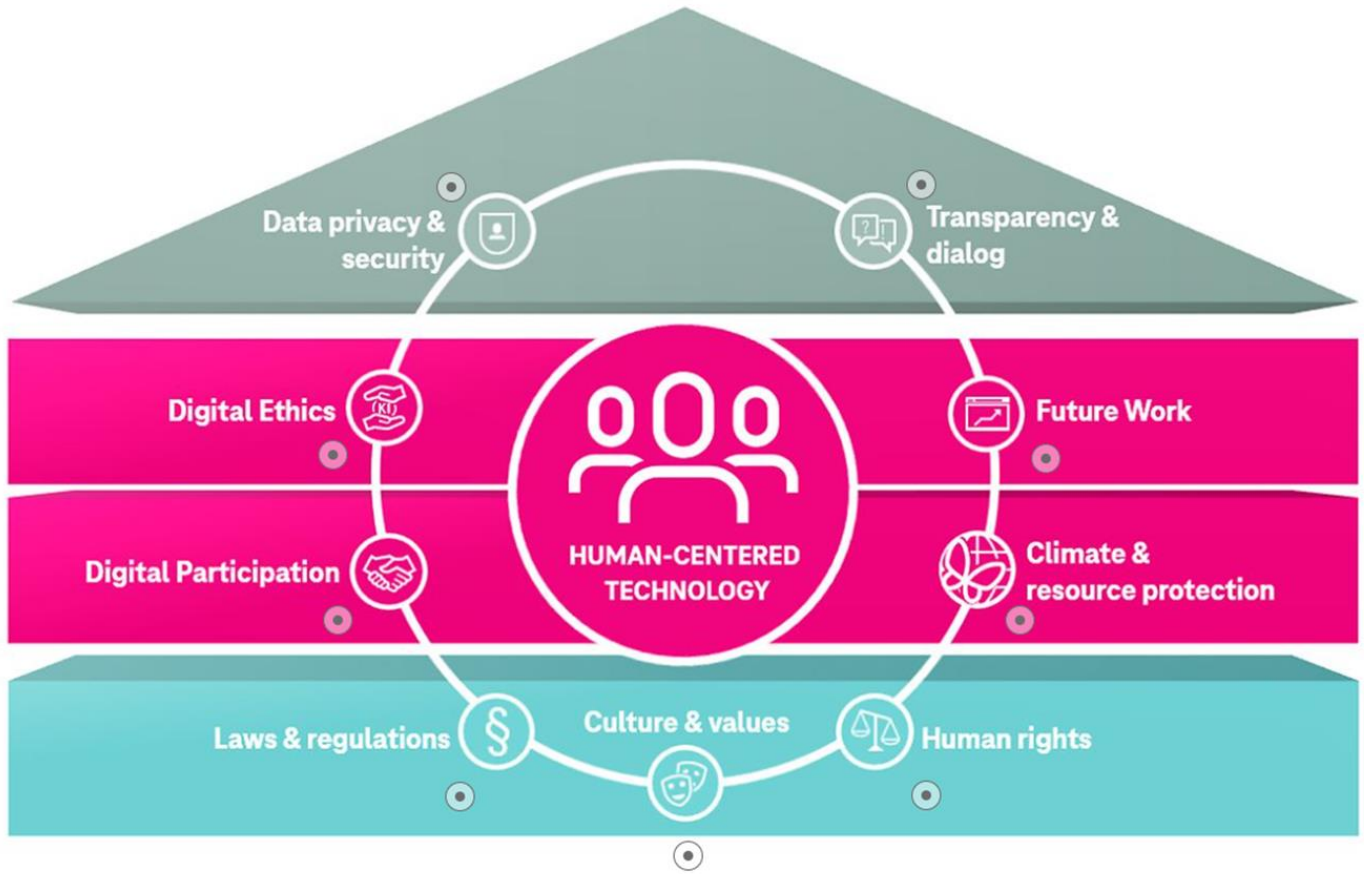
Marco para la divulgación de información sobre responsabilidad digital corporativa (RDC)
1. Enfoque corporativo hacia la responsabilidad digital
Declaración sobre cómo la responsabilidad digital está arraigada en la empresa.
La RDC como parte integrante de un plan de negocios socialmente responsable.
La RDC como parte de la visión/cultura de la empresa.
Acciones relacionadas con las dimensiones AESG (ambiental, económica, social y gobierno corporativo)
Soluciones digitales aplicadas para proteger el **medio ambiente**, buscar la neutralidad de carbono, reducir residuos, etc.
Utilización de tecnologías verdes **(green computing)**. Recursos de computación que minimicen el consumo energético y el impacto ambiental (computación en nube o teletrabajo), productos informáticos ecológicos y reciclaje.
Valor económico creado por tecnologías digitales. Inversiones relacionadas con la digitalización.
Inversiones relacionadas con la digitalización. Inversiones realizadas en esfuerzos de digitalización, incluida la infraestructura tecnológica, investigación y desarrollo y las inversiones en capital humano para la transformación digital.
Iniciativas **sociales** como herramientas de salud y seguridad basadas en nuevas tecnologías para empleados, iniciativas de capacitación en **alfabetización digital** para empleados y usuarios externos, relacionadas, entre otras cosas, con el RGPD, ciberseguridad/phishing/ciberacoso, etc., **inclusión digital:** iniciativas para personas con necesidades especiales, iniciativas para inspirar a las mujeres a trabajar en tecnología.
Soluciones digitales que conduzcan a la mejora y uso eficiente de datos para una mejor **gobernanza.**

Company Corporate Responsibility Investor Relations Media Careers Blog.Telekom

Search Deutsch

The House of Digital Responsibility

Click the hot spots on the infographic to learn more about each topic.



Contributions to E²SG

No. of employees trained in digital proficiency or digital soft skills

No. of educational and training initiatives in digital literacy for external stakeholders

No. of workshops increasing digital literacy

No. of upskilled employees

Digital literacy

No. of adjusted tech products and services to people with special needs

No. of applications developed to improve customer experience

No. of wifi spots installed in the community

Digital Inclusion

Customer satisfaction increase/decrease due to e.g. new digital platform

% decrease of health and safety incidents after incorporating digital solutions/apps

Digital for good

% of carbon footprint/water consumption/waste reduction after applying digital solutions

Environmental

Level of automation of management processes;

Estimated time saved (compared to the non-digital processes)

Governance

% of revenue increase due to digital solutions

% of costs savings due to digital solutions

Economic

Riesgos digitales

2. Riesgos digitales
Descripción de los riesgos y análisis de impactos.
Planes de mitigación e identificación de oportunidades.

Riesgos relacionados con violaciones de datos, ciberataques, fallas tecnológicas, cambios regulatorios y cualquier otra amenaza digital.

Para cada riesgo digital identificado, describir las posibles consecuencias de estos riesgos en las operaciones, estabilidad financiera, reputación y partes interesadas.

Estrategias o planes para mitigar los riesgos digitales. Medidas para prevenir, gestionar y recuperarse de amenazas digitales, protocolos de seguridad, capacitación de empleados, planes de respuesta a incidentes y asociaciones con expertos en ciberseguridad.

Oportunidades derivadas de los riesgos digitales.

Riesgos digitales. Ibex 35, 2022 (Bonsón et al. 2024)

Categories	% sentences
Cybersecurity risk	58,85%
Technological risk	35,26%
Privacy risk	9,94%
Digital transformation risk	0,64%
Artificial Intelligence risk	0,32%
Digital risk	0,00%

Categories	% comps.
Cybersecurity risk	85,71%
Technological risk	62,86%
Privacy risk	34,29%
Digital transformation risk	2,86%
Artificial Intelligence risk	2,86%
Digital risk	0,00%

Ciberseguridad

3. Ciberseguridad
Objetivos, medidas y metas en ciberseguridad.
Políticas y directrices existentes relacionadas con la ciberseguridad.
Alineación con **requisitos legales** (Directiva EU 2022/2555, Reglamento EU 2019/881) o **estándares** como ISO 27001 y 27002.
Existencia de **órganos de gobierno** en materia de ciberseguridad.
Existencia de **roles** como director de seguridad de la información (CISO) o director de infraestructuras y sistemas de ciberseguridad.
Infraestructuras y sistemas de ciberseguridad
Acciones contra DDoS, ransomware, FluBot, etc.
Controles internos, monitorización continua y procesos de verificación externa.

Protección de datos y privacidad

4. Protección de datos y privacidad
Objetivos, medidas y metas en protección de datos y privacidad.
Políticas y directrices existentes relacionadas con la protección de datos y la privacidad.
Alineación con **requisitos legales** como el RGPD o **estándares** como ISO 27701.
Existencia de **órganos de gobierno** en materia de protección de datos y privacidad.
Existencia de **roles** como director de protección de datos (DPO) o director de datos.
Ecosistema de gobernanza de datos personales, intercambio mutuo de datos, identificación de partes involucradas y el propósito de la recopilación de datos.
Controles internos, monitorización continua y procesos de verificación externa.

IA fiable: Algoritmos y equidad de datos

5. IA fiable: Algoritmos y equidad de datos
Objetivos, medidas y metas para garantizar una IA fiable
Políticas y directrices existentes para una IA fiable.
Alineación con **requisitos legales y directrices**, como el marco regulatorio de la UE sobre IA (2021-2023) o las directrices éticas para una IA fiable (2019)
Existencia de **órganos de gobierno** para la IA.
Existencia de **roles** como director de IA (CAIO).
Para cada algoritmo que pueda tener un alto impacto (riesgo).
Descripción del algoritmo: tipo, datos de entrada, diseño, supervisión humana, etc.
Declaración de que el sistema cumple con las regulaciones relacionadas con la IA o, si corresponde, que se garantiza la no discriminación algorítmica, la transparencia, la auditabilidad y la explicabilidad del algoritmo, así como su accesibilidad, usabilidad y confiabilidad.
Mecanismos para que los usuarios reciban explicaciones significativas.
Controles internos, monitorización continua y procesos de verificación externa.

Próximos pasos

- Opinión emitida nº 4. Comisión de NTyC de AECA.
- Divulgación
- Revisión de informes RDC
- Identificación de buenas prácticas
- Definición de KPIs
- European reporting Lab

Hacia un marco de información para la responsabilidad digital corporativa

Colegio de Registradores de España, 22 de abril de 2024
Acto 20 aniversario de XBRL España

Enrique Bonsón. bonson@uhu.es