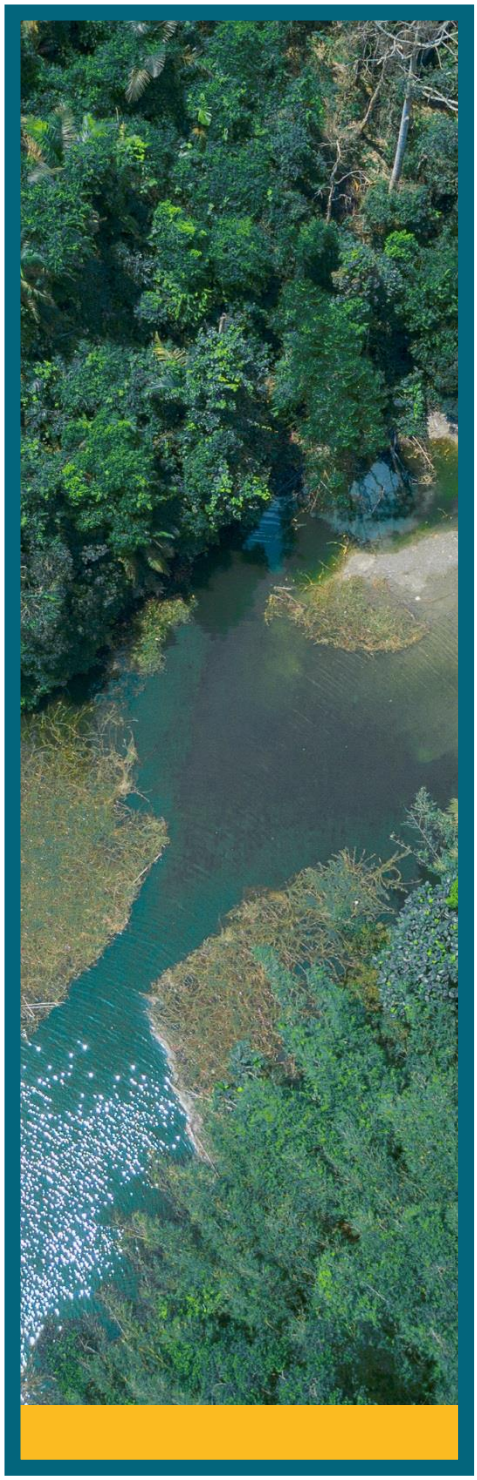

Política General

Política de Seguridad de la Información

Índice

1 Introducción

Indra considera la información como uno de sus activos más críticos, por esa razón las funciones relacionadas con la gestión de la Seguridad de la Información deben desarrollarse de un modo coordinado a través de la implantación de un modelo alineado con su cultura, procesos, estructura y estrategia.

Para tal propósito, Indra ha establecido un Modelo de Seguridad de la Información asegurando así que se identifican y valoran los riesgos de seguridad a los que está expuesto y, adopta en consecuencia, las estrategias de seguridad más eficaces y coherentes arreglo con la estrategia de negocio, mediante la utilización eficiente de los recursos y aportando el mayor valor posible a las partes interesadas.

Por ello, la Seguridad de la Información es una parte integral de todos los procesos y está incluida en la planificación estratégica de Indra.

2 Objeto

El objeto principal de la política de Seguridad de la Información de Indra es establecer un marco de actuación que permita proteger la información de Indra y otros grupos de interés.

Por esa razón, es necesario establecer las medidas oportunas en todos aquellos lugares donde se almacena, procesa o transmite con el fin de garantizar:

- Su confidencialidad, asegurando que sólo quienes estén autorizados puedan acceder a la información,
- Su integridad, asegurando que la información y sus métodos de proceso sea exactos y completos, evitando modificaciones no autorizadas y
- Su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

3 Alcance

La presente Política es de aplicación y obligado cumplimiento para todas las empresas del grupo Indra.

4 Principios

Para lograr el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información, se establecen los siguientes principios fundamentales:

- **Ciberhigiene**: Aplicar en todos los activos de la compañía unas medidas básicas que garanticen un nivel mínimo de seguridad.
- **Concienciación**: Ser conscientes de los riesgos de seguridad de la información, así como conocer y aplicar las prácticas necesarias para proteger la información.
- **Gestión del Riesgo de Seguridad**: Realizar una adecuada evaluación, gestión y tratamiento del riesgo de seguridad de la información para alcanzar un nivel aceptable de riesgo, priorizando las medidas y controles a implantar acorde a los riesgos identificados y los objetivos de negocio perseguidos.

- **Cumplimiento**: Cumplir con todas las obligaciones legales, regulatorias, sectoriales y contractuales que afecten a la seguridad de la información.

- **Seguridad desde el diseño**: Incorporar la seguridad de la información como un elemento esencial en el diseño y desarrollo de productos, soluciones y servicios

- **Gestión de Incidentes de Seguridad**: Actuar de manera adecuada y conjunta para prevenir, detectar y responder a los incidentes que puedan afectar a la seguridad de la información.

- **Mejora continua**: Mejorar la eficacia y eficiencia de los controles de seguridad implantados para adaptarse a la evolución de los riesgos y los nuevos entornos tecnológicos.

- **Reevaluación**: Revisar y evaluar la seguridad de los sistemas de información periódicamente, tanto de forma interna como externa, tomando las medidas necesarias para corregir las desviaciones que se puedan detectar.

5 Modelo de gobierno

Teniendo en cuenta las recomendaciones de las normas internacionales, Indra ha definido un Modelo de Gobierno de Seguridad de la Información que, a través de sus órganos de supervisión, asegura la coordinación de la Seguridad de la Información entre las unidades organizativas y su Dirección, encargados de velar por la aplicación de los principios fundamentales de Seguridad de la Información en Indra.

5.1 Órganos de supervisión

El gobierno de Seguridad de la Información consta de los siguientes órganos de supervisión:

- La Dirección de Seguridad de la Información o DSI, es el órgano encargado de garantizar la Seguridad de la Información, y sobre quien recae la gestión del Comité de Seguridad de la Información.

- El Comité de Seguridad de la Información o CSI, es el órgano encargado de gestionar la Seguridad de la Información del Grupo Indra. Su función principal es impulsar la Seguridad de la Información, con el compromiso y apoyo de la Dirección, definiendo los objetivos y planes de seguridad estratégicos, según las necesidades, objetivos y procesos de negocio.
  La asistencia al Comité de Seguridad de la Información es de obligado cumplimiento por todos sus miembros y son los encargados de establecer, desarrollar e implementar las decisiones acordadas.

Además, periódicamente, al menos anualmente, Chief Information Security Officer o CISO informa a los organismos independientes de la Comisión de Auditoría y Cumplimiento del Consejo y de la Unidad de Coordinación de Riesgos sobre su funcionamiento y posibles incidencias acontecidas durante el ejercicio

5.2 Roles y responsabilidades

Para el correcto funcionamiento e integración del Modelo de Gobierno de Seguridad de la Información en el Grupo Indra, se ha llevado a cabo la definición de una estructura organizacional con la asignación de roles sujetos a funciones y responsabilidades para la correcta ejecución de las actividades.

A continuación, se ilustran las dependencias y comunicaciones entre las unidades organizativas, órganos de supervisión y roles que lo componen.

Ilustración I - Estructura organizacional y roles

Las responsabilidades determinadas para cada rol dependerán de las metas establecidas para los diferentes procesos de seguridad pues éstas van a permitir detallar los roles y responsabilidades de las personas que se van a encargar de establecer y desarrollar cada una de estas actividades asociadas a la implementación de los procesos de Seguridad de la Información.

A continuación, se describen los roles que se identifican dentro del Modelo de Gobierno de Seguridad de la Información en Indra:

- Chief Information Security Officer o CISO, responsable de Seguridad de la Información del Grupo Indra, se encarga del desarrollo de la estrategia, objetivos y planes de Seguridad de la Información, en coordinación con todas las unidades organizativas.

- Local Information Security Officer o LISO, responsable de la coordinación de la Seguridad de la Información en cada una de las unidades organizativas, siguiendo las normativas, políticas y directrices marcadas desde la Dirección de Seguridad de la Información del Grupo Indra, garantizando así su cumplimiento, y aportando una visión global de la seguridad de la unidad organizativa, anticipando riesgos en función de sus particularidades y favoreciendo la toma de decisiones.

- Country Managers, representan al Grupo Indra en cada uno de los países donde éste tiene presencia. Son los responsables de la Seguridad de la Información en las unidades organizativas que están presentes en los países bajo su ámbito.

- Directores, responsables de la Seguridad de la Información en los Mercados y Áreas Corporativas que están bajo su ámbito. Las responsabilidades determinadas para cada rol dependerán de las metas establecidas para los diferentes procesos de seguridad pues éstas van a permitir detallar los roles y responsabilidades de las personas que se van a encargar de establecer y desarrollar cada una de estas actividades asociadas a la implementación de los procesos de Seguridad de la Información.

A nivel operativo, el gobierno de la Seguridad de la Información se traslada a un modelo de responsabilidad de Seguridad de la Información donde la seguridad es una responsabilidad compartida.

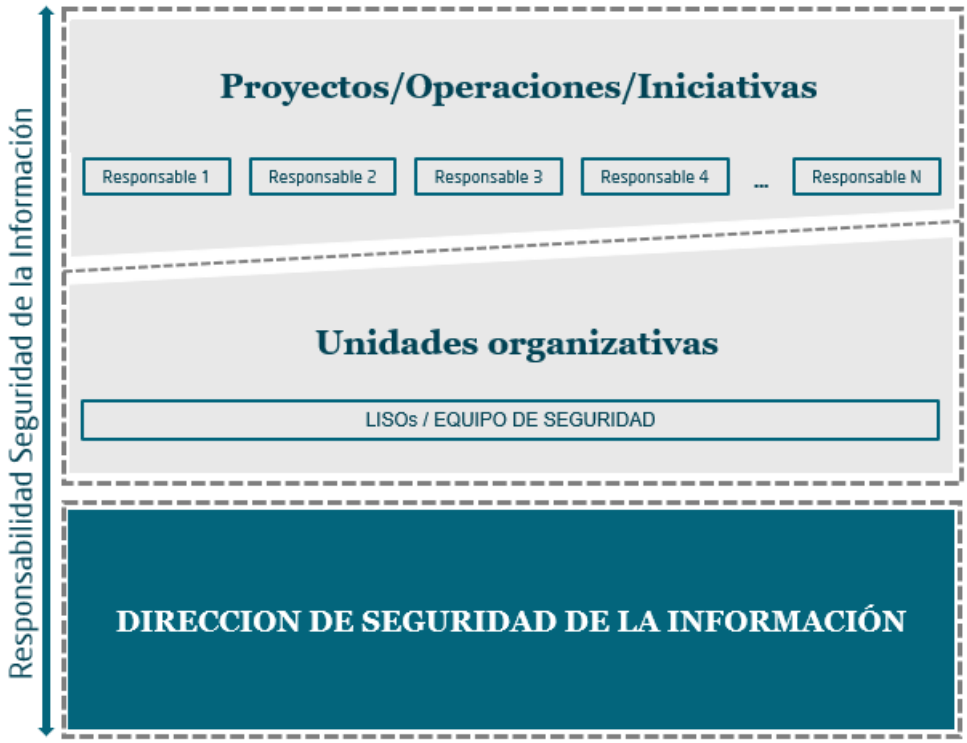

Ilustración II - Modelo de Responsabilidad de Seguridad de la Información

6 Canal para reporte de incidentes

En aras de garantizar la pronta detección y gestión eficaz de incidentes de seguridad, Indra tiene formalizado un equipo interno de gestión de incidentes “Indra CSIRT”, que presta sus servicios de acuerdo a los estipulado en el documento RFC2350 disponible en la web corporativa: https://www.indracompany.com/sites/default/files/d7/Documentos/Sobre-Indra/SeguridadInformacion/rfc2350.txt .

Cualquier evento sospechoso o vulnerabilidad que pueda afectar a los sistemas de información de Indra debe ser comunicado en csirt@indra.es.

7 Aprobación

Mediante la aprobación de esta política, el Consejo de Administración manifiesta su determinación y compromiso en alcanzar un nivel de seguridad adecuado a las necesidades del negocio que garantice la protección de los activos de forma homogénea en todas las empresas del Grupo Indra.