Seguridad de la Información para Proveedores

Edición: 1

indra

Contenido

1 Objetivo

El objetivo principal de este documento es mitigar los riesgos posibles asociados al acceso a la información, sistemas de información o recursos de Indra por parte de proveedores de servicios, independientemente del tipo de servicio proporcionado, o de relación que le una con Indra (legal, contractual o de cualquier otra índole no laboral), con el fin de proteger la confidencialidad, integridad y disponibilidad de la información de Indra y sus clientes.

Indra se reserva el derecho a modificar este documento cuando sea necesario. Los cambios realizados serán divulgados a todas las empresas proveedoras de servicios a las que les aplique utilizando los medios que se consideren pertinentes. Es responsabilidad de cada empresa proveedora garantizar la lectura y conocimiento de las políticas de seguridad más recientes de Indra por parte de su personal, así como de obtener su compromiso de cumplir y respetar dichas normas.

En caso de incumplimiento de cualquiera de estas obligaciones, Indra se reserva el derecho de adoptar las medidas sancionadoras que se consideren pertinentes en relación con la empresa contratada, y que pueden llegar a la resolución de los contratos que tenga vigentes con dicha empresa.

2 Principios generales de seguridad

Los proveedores de servicios proporcionarán a Indra siempre que se requiera, la relación de personas, perfiles, funciones y responsabilidades asociados al servicio prestado, e informará de cualquier cambio (alta, baja, sustitución o cambio de funciones o responsabilidades) que se produzca en dicha relación.

Los proveedores de servicios deberán asegurar que todo su personal tiene la formación y capacitación apropiada para el desarrollo del servicio provisto, tanto a nivel específico en las materias correspondientes a la actividad asociada a la prestación del servicio, como en materia de seguridad de la información.

Como mínimo, los proveedores de servicios deberán asegurarse que todo el personal asociado al servicio conoce y se compromete a cumplir lo recogido en esta política. Indra podrá solicitar en cualquier momento evidencias del proceso de información.

Los proveedores de servicios deberán permitir que Indra lleve a cabo las auditorías de seguridad solicitadas, colaborando con el equipo auditor y facilitando todas las evidencias y registros le sean requeridos.

El alcance y profundidad de cada auditoría será establecido expresamente por Indra en cada caso. Las auditorías se llevarán a cabo siguiendo la planificación que se acuerde en cada caso con el proveedor del servicio.

Indra se reserva el derecho de realizar auditorías extraordinarias adicionales, siempre que se den causas específicas que lo justifiquen.

2.1 Confidencialidad de la información

Toda información, documentación, programas y/o aplicaciones, métodos, organización, estrategias de negocio y actividades relacionadas con Indra o con su negocio, a las que tenga acceso los proveedores de servicios con objeto de realización del servicio serán considerados información confidencial, en función de lo cual, el acceso, intercambio y tratamiento de dicha información, se realizará siempre de acuerdo a las finalidades previstas descritas en el contrato de prestación de servicios y manteniendo el correspondiente deber de secreto durante la duración del servicio y después de que finalice la relación con Indra.

Todos los recursos e información a la que haya podido tener acceso o que haya sido necesaria elaborar, modificar o copiar para el correcto desempeño del servicio serán devueltos a la finalización de este. Indra podrá solicitar el borrado seguro de los dispositivos que hayan tenido acceso a la Información de Indra.

2.2 Propiedad Intelectual

Se garantizará el cumplimiento de las restricciones legales al uso del material protegido por la normativa de propiedad intelectual. Los proveedores de servicios únicamente podrán utilizar material autorizado por Indra para el desarrollo de sus funciones. Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia en los sistemas de información de Indra.

Asimismo, queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual sin la debida autorización por escrito.

Indra únicamente autorizará el uso de material producido por él mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

2.3 Intercambio de información

Cualquier tipo de intercambio de información que se produzca entre Indra y los proveedores de servicios se entenderá que ha sido realizado dentro del marco establecido por el contrato de prestación de servicios correspondiente, de modo que dicha información no podrá ser utilizada fuera de dicho marco ni para otros fines.

La distribución de información ya sea en formato electrónico o físico se realizará mediante los recursos determinados en el contrato de prestación de servicios para tal cometido y para la finalidad exclusiva de facilitar las funciones asociadas a dicho contrato.

Indra se reserva, en función del riesgo identificado, la implantación de medidas de control, registro y auditoría sobre estos recursos de difusión. En relación con el intercambio de información dentro del marco del contrato de prestación de servicios, se considerarán no autorizadas las siguientes actividades:

- Transmisión o recepción de material protegido por los derechos de autor infringiendo la Ley de Protección Intelectual.
- Transmisión o recepción de toda clase de material pornográfico, de naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.
- Transmisión o recepción de información sensible, salvo que la comunicación electrónica esté cifrada y el envío esté autorizado por escrito.
- Transferencia de información protegida a terceras partes no autorizadas.
- Transmisión o recepción de aplicaciones no relacionadas con el negocio.
- Participación en actividades de Internet, como grupos de noticias, juegos u otras que no estén directamente relacionadas con la prestación del servicio.
- Todas las actividades que puedan dañar la imagen y reputación de Indra están prohibidas en Internet y en cualquier otro lugar.

2.4 Uso apropiado de los recursos corporativos de Indra

Los recursos corporativos de Indra a los que tengan acceso los proveedores de servicios serán utilizados exclusivamente para cumplir con las obligaciones y propósitos de la provisión del servicio.

Bajo ningún concepto podrán ser utilizados para actividades no relacionadas con el propósito del servicio o para la comisión de actividades que pudieran ser consideradas ilícitas, como daños contra la propiedad intelectual de terceros, incumplimientos de la normativa de protección de datos etc.

Los proveedores de servicios se comprometen a utilizar los recursos corporativos de Indra a los que tenga acceso de acuerdo con las políticas de seguridad de Indra.

Con el fin de velar por el correcto uso de los mencionados recursos, Indra podrá implementar los mecanismos de control y auditoría que considere oportunos, ya sea de forma periódica o cuando por razones específicas de seguridad o del servicio resulte conveniente.

En caso de apreciar que algún proveedor de servicios, o su personal, utiliza incorrectamente recursos o información de Indra, se le comunicará tal circunstancia al proveedor para que realice las acciones oportunas. Indra se reserva el derecho de ejercer las acciones que legalmente le amparen para la protección de sus derechos.

Cualquier fichero introducido en la red de Indra o en cualquier equipo conectado a ella a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual, protección de datos de carácter personal, y control de virus y programa maligno.

2.5 Responsabilidades del usuario

Los Proveedores de servicios deberán asegurarse de que todo el personal que en el desarrollo de sus funciones para Indra puedan tener acceso a la información, sistemas de información o recursos de Indra respete los siguientes principios básicos dentro de su actividad:

- Cada persona con acceso a información de Indra es responsable de la actividad desarrollada por su identificador de usuario y todo lo que de él se derive. Por lo tanto, es imprescindible que cada persona mantenga bajo control los sistemas de autenticación asociados a su identificador de usuario, garantizando que la clave asociada sea únicamente conocida por el propio usuario, no debiendo revelarse al resto del personal bajo ningún concepto.
- Los usuarios no deberán utilizar ningún identificador de otro usuario, aunque dispongan de la autorización del propietario.
- Los usuarios conocen y aplican los requisitos y procedimientos existentes en torno a la información manejada.
- Cualquier usuario con acceso información de Indra deberá seleccionar contraseñas de calidad (al menos 8 caracteres, contener letras mayúsculas, minúsculas, dígitos y caracteres especiales, que no contengan ningún tipo de información fácilmente adivinable) https://www.osi.es/es/contrasenas.
- Cualquier usuario con acceso información de Indra deberá cambiar las contraseñas por defecto y las temporales en el primer inicio de sesión, y como mínimo una vez cada 90 días y o cuando exista un posible indicio de conocimiento por parte de otros usuarios.
- Cualquier persona con acceso a información de Indra deberá velar por que los equipos queden protegidos cuando vayan a quedar desatendidos.
- Cualquier persona con acceso a información deberá respetar las normas de escritorio limpio, con el fin de proteger los documentos en papel, soportes informáticos y dispositivos portátiles de almacenamiento y reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo (Almacenamiento bajo llave, bloqueo de equipos desatendidos, protección de los puntos de recepción y envío de información, destrucción segura, etc.)
- Las personas con acceso a sistemas de información de Indra nunca deberán, sin autorización por escrito, realizar pruebas para detectar y/o explotar una supuesta debilidad o incidencia de seguridad.
- Ninguna persona con acceso a sistemas de información de Indra intentará sin autorización expresa y por escrito por ningún medio transgredir el sistema de seguridad y las autorizaciones. Se prohíbe la captura de tráfico de red por parte de los usuarios, salvo que se estén llevando a cabo tareas de auditoría autorizadas por escrito.

2.6 Requisitos de seguridad para los dispositivos

Todos los dispositivos con acceso a información de Indra, independientemente de la propiedad de estos, deberán cumplir con las políticas de seguridad establecidas por Indra, en especial se tendrán en cuenta las siguientes consideraciones:

- El acceso a los sistemas deberá realizarse siempre de forma autenticada, al menos mediante la utilización de un identificador personal y una contraseña asociada.
- Todo el software instalado o contenido en el dispositivo debe estar licenciado, dentro del ciclo de vida del producto y en un estado acorde a la licencia de uso.
- Los dispositivos deberán permanecer actualizados con la última versión disponible de parches de seguridad para el software y sistema operativo instalado.
- Los dispositivos deben contar con un sistema de protección anti-malware instalado, activo y actualizado a su última versión disponible, tanto del motor como del fichero de firmas.
- Debe activarse el bloqueo de pantalla para que este salte a los 10 minutos de inactividad. El desbloqueo deberá conllevar el uso de contraseñas, patrones de desbloqueo o mecanismos equivalentes, que garanticen que el dispositivo no podrá ser utilizado por un usuario no autorizado.
- Los dispositivos no dispondrán de ninguna herramienta o ficheros contrarios a la política de seguridad de Indra o que pueda interferir con el software corporativo. Este punto incluye, aquellos que traten de descubrir información distinta de la del propio usuario o realizar accesos no autorizados, como por ejemplo sniffers, herramientas de escaneo de redes, descubrimiento de contraseñas, etc.

2.7 Comunicación de incidentes de seguridad

Los proveedores de servicios se comprometen a comunicar de manera inmediata cualquier incidente, debilidad o amenaza (observada o sospechada) que detecte en los sistemas de información de Indra o que haya podido afectar a información propiedad de Indra o de sus clientes al **Departamento de Seguridad de la Información** a través del Usuario Genérico Indra CSIRT csirt@indra.es, o a través del Responsable del servicio.

En el caso de personal del proveedor desplazado en Indra, cualquier incidente, debilidad o amenaza relacionada con la información o los recursos de Indra deberá ser comunicada a través del Usuario Genérico Indra CSIRT csirt@indra.es o del centro de atención al usuario (CAU) de Indra.

3 Principios específicos de seguridad

3.1 Seguridad física

Obligados: Todos los proveedores de servicios cuyos servicios se presten desde la sede del proveedor.

- Los edificios o instalaciones deben ser físicamente sólidos (por ejemplo: no deberían existir huecos en el perímetro o áreas dónde pudieran producirse rupturas fácilmente); los muros externos de las instalaciones deberían ser de construcción sólida.
- Todas las puertas externas deberían estar adecuadamente protegidas contra los accesos no autorizados a través de mecanismos de control, por ejemplo, barras, alarmas, cerraduras, tornos, cámaras de vigilancia etc.
- Cuando sea posible, se recomienda establecer barreras físicas que requieran la identificación del empleado mediante algún método de identificación y autenticación (tarjetas de identificación, tarjetas electrónicas, identificación biométrica, etc.) para prevenir los accesos físicos no autorizados.
- Los edificios o instalaciones deberían contar con sistemas automáticos de detección y respuesta automática ante condiciones ambientales adversas (fuego principalmente). Cuando no se pueda disponer de un sistema de extinción automática de incendios, deben contarse con medidas de extinción manual, que deben ser conocidas por todo el personal de la empresa.
- Se deben establecer las condiciones ambientales básicas de temperatura, higiene, aislamiento eléctrico y sonoro, y otras medidas similares de acuerdo con los requerimientos específicos del equipamiento informático.
- Si se mantiene algún tipo de copia de información responsabilidad de Indra, los sistemas que alberguen y/o procesen dicha información deberán estar ubicados en un área especialmente protegida, que incluya al menos las siguientes medidas de seguridad:
    - Tener un sistema de control de acceso independiente al de la sede.
    - Existirá un registro de acceso realizados.
    - El acceso por parte de personal externo se asignará únicamente cuando sea necesario y se encuentre autorizado, y siempre bajo la vigilancia de personal autorizado.
    - El personal externo no podrá permanecer ni ejecutar trabajos en las áreas especialmente protegidas sin supervisión.
    - Contar con algún tipo de protección frente a fallos de alimentación.

3.2 Seguridad en desarrollo.

Obligados: Todos los proveedores de servicios que realicen trabajos de desarrollo y/o pruebas de aplicaciones para Indra.

- Los entornos con los que se lleven a cabo dichas actividades deberán estar aislados entre sí y también aislados de los entornos de producción.
- Todos los accesos a los sistemas de información que alberguen o procesen información deberán estar protegidos, al menos, por un “cortafuegos”, que limite la capacidad de conexión a ellos.
- Todo el proceso de desarrollo de software externalizado será controlado y supervisado por Indra.

- Las especificaciones de los aplicativos deberán contener expresamente los requisitos de seguridad a cubrir en cada caso.
- Se incorporarán los mecanismos de identificación, autentificación, control de acceso, auditoría e integridad en todo el ciclo de vida de diseño, desarrollo, implantación y operación de los aplicativos.
- Las aplicaciones que se desarrollen deberán incorporar validaciones de los datos de entrada que verifiquen que los datos son correctos y apropiados y que eviten la introducción de código ejecutable.
- Los procesos internos desarrollados por las aplicaciones deberán incorporar todas las validaciones necesarias para garantizar que no se producen corrupciones de la información.
- Siempre que sea necesario se deberán incorporar funciones de autenticación y control de integridad en las comunicaciones entre los diferentes componentes de las aplicaciones.
- Se deberá limitar la información de salida ofrecida por las aplicaciones, garantizando que sólo se ofrece aquella pertinente y necesaria.
- El acceso al código fuente de los aplicativos deberá estar limitado al personal del servicio.
- En el entorno de pruebas sólo se utilizarán datos reales cuando hayan sido apropiadamente disociados o siempre que se pueda garantizar que las medidas de seguridad aplicadas sean equivalentes a las existentes en el entorno de producción.
- Durante las pruebas de los aplicativos se verificará que no existen canales de fuga de información no controlados, y que por los canales establecidos sólo se ofrece la información prevista.
- Solo se transferirán al entorno de producción aquellos aplicativos que hayan sido expresamente aprobados.

3.3 Seguridad de sistemas

Obligados: Todos los proveedores de servicios cuyos servicios se presten mediante el uso de su infraestructura TIC.

3.3.1 Gestión de activos

- Los proveedores de servicios deberán contar con un registro de activos actualizado en el que se puedan identificar los activos utilizados para la prestación del servicio.
- Los proveedores de servicios deberán notificar a Indra las bajas de los activos utilizados para la prestación del servicio. Si dicho activo contiene otra propiedad de Indra (hardware, software u otro tipo de activos), deberá ser entregado a Indra previamente a llevar a cabo la baja para que Indra proceda a la retirada de los activos de su propiedad.
- Siempre que un activo haya contenido información considerada sensible, Los Proveedores de servicios deberá llevar a cabo las bajas de activos garantizando la eliminación segura de dicha información, aplicando funciones de borrado seguro o destruyendo físicamente el activo, para que la información que haya contenido no pueda ser recuperable.
- Todos los activos utilizados para la prestación del servicio deberán tener un responsable, que se deberá asegurar de que dichos activos incorporan las medidas de seguridad mínimas establecidas por Indra, y que al menos deben ser las especificadas en la presente normativa:

- Cumplir lo establecido en el punto Requisitos de seguridad para los dispositivos.
    - Deberán registrar los eventos más significativos en torno a su funcionamiento. Estos registros de actividad estarán contemplados dentro de la normativa de copias de seguridad del proveedor. En especial, se registrarán todos los eventos realizados con permisos privilegiados.
    - Los relojes de los sistemas estarán sincronizados entre sí y con la hora oficial.
    - El Proveedor del servicio garantizará que la capacidad de los sistemas se gestiona adecuadamente, evitando potenciales paradas o malos funcionamientos de dichos sistemas por saturación de recursos.
    - Los errores y fallos registrados en la actividad de los sistemas se analizan, adoptándose las medidas necesarias para su subsanación.
- El Proveedor establecerá una normativa de copias de seguridad que garantice la salvaguarda de cualquier dato o información relevante para el servicio prestado, con una periodicidad semanal.

3.3.2 Gestión de la continuidad

- Los proveedores de servicios deberán contar con un plan de continuidad y un plan para la recuperación de TI en caso de desastre que permita la prestación del servicio aun en caso de contingencias. Este plan deberá ser desarrollado en función de una evaluación de riesgos (al menos una vez al año) para identificar los riesgos que podrían causar una interrupción de las operaciones y asegurarse de que se ponen en funcionamiento los controles apropiados para gestionarlos y controlarlos.
- Los proveedores de servicios pondrán a prueba el plan de continuidad y el plan de recuperación para confirmar que sirven para recuperar el servicio en los plazos de tiempo acordados. Estas pruebas se realizarán anualmente o justo después de que se realicen cambios, mejoras o modificaciones importantes que afecten a los servicios.

3.3.3 Seguridad de red

- Todas las redes deberán estar adecuadamente gestionadas y controladas, asegurándose de que no existen accesos no controlados ni conexiones cuyos riesgos no estén apropiadamente gestionados por él, estableciéndose los oportunos sistemas de monitorización y auditoría de seguridad necesarios para garantizar la seguridad de las conexiones.
- Los servicios disponibles en las redes a través de las que circule la información deberán limitarse en la medida de lo posible.
- Las redes que permitan el acceso a la infraestructura Indra deberán estar apropiadamente protegidas, debiéndose cumplir las siguientes premisas:
    - Deberán ser comunicadas y autorizadas por la Unidad Sistemas de Información (SITI).
    - El acceso de usuarios remotos a la red de Indra estará sujeto al cumplimiento de procedimientos de autenticación previa y validación del acceso por SITI.
    - Estas conexiones se realizarán por tiempo limitado y mediante la utilización de redes privadas virtuales o líneas dedicadas.
    - En estas conexiones no se permitirá ningún tipo de equipo de comunicaciones (tarjetas, módems, etc.) que posibilite conexiones alternativas no controladas.

3.3.4 Gestión de cambios

- Los Proveedores de servicios deberán garantizar que todos los cambios en la infraestructura TIC con la que presta el servicio están controlados y autorizados, garantizándose que no forma parte de la infraestructura TIC ningún componente no controlado.
- Se deberán verificar que todos los nuevos componentes introducidos en la infraestructura TIC utilizada para la prestación del servicio funcionan adecuadamente y cumplen los propósitos para los que fueron incorporados.
- Todos los cambios que se lleven a cabo se deberán realizar siguiendo un procedimiento formalmente establecido y documentado, que garantice que se siguen los pasos apropiados para realizar el cambio.
- El procedimiento de gestión de cambios deberá garantizar que se minimizan los cambios sobre los componentes críticos, limitándose a los estrictamente imprescindibles.
- Se deberán verificar todos los cambios sobre los componentes críticos, para comprobar que no se producen efectos adversos colaterales o no previstos sobre el funcionamiento de dichos componentes o sobre su seguridad.
- Se deberán analizar las vulnerabilidades técnicas que presenten las infraestructuras utilizadas para la prestación del servicio, informando a Indra de todas aquellas asociadas a los componentes críticos, con el fin de gestionar conjuntamente dichas vulnerabilidades.

Avda. de Bruselas, 35
28018 Alcobendas
Madrid, España
T +34 91 480 50 00

indracompany.com