

Seguridad de la Información para Proveedores

Guía básica

Versión 2.2

Dirección de Seguridad de la Información de Indra

indracompany.com



Índice

1	Propósito.....	3
2	Alcance	3
3	Descripción.....	3
3.1	Pautas mínimas de seguridad.....	3
3.1.1	Roles y responsabilidades.....	4
3.1.2	Política y procedimientos de Seguridad de la Información.....	4
3.1.3	Análisis de riesgos.....	5
3.1.4	Formación y concienciación en materia de Seguridad de la Información	5
3.1.5	Navegación segura por Internet	6
3.1.6	Seguridad en los Sistemas.....	7
3.1.7	Gestión de Incidentes	9
4	Comunicaciones	10
5	Control de cambios.....	10

1 Propósito

El presente documento tiene como objetivo proteger la información y garantizar un nivel mínimo de seguridad en los sistemas de información que proveedores y/o terceros manejan en el desempeño de sus funciones para Indra.

Así pues, se establecen unas pautas de Seguridad de la Información mínimas para proveedores o terceros prestadores de servicios que ayuden a garantizar la confidencialidad, integridad y disponibilidad de la información de Indra o de sus clientes.

2 Alcance

Este documento aplica a todos los proveedores o terceros prestadores de servicios que durante sus actividades traten información de Indra o de cualquiera de sus clientes, ya sea en formato físico como electrónico.

3 Descripción

Indra considera la información uno de sus activos más valiosos, por lo que tiene la responsabilidad de garantizar un nivel mínimo de Seguridad de la Información en todos sus procesos, tratando los riesgos de Seguridad de la Información que pudieran suponer graves consecuencias para la compañía. Si se llegase a materializar un incidente de seguridad, este podría tener graves consecuencias como, por ejemplo, sanciones legales y regulatorias, pérdidas económicas, daños operativos y a la reputación de la empresa.

El hecho de externalizar servicios supone un riesgo para la Seguridad de la Información ya que si un sistema de información o cierta información en la cadena de suministro se viese comprometida, esto podría generar retrasos y problemas, y es por ello por lo que este documento pretende mitigar los posibles riesgos asociados al acceso a 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, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información de Indra y sus clientes.

Esta guía básica nace para facilitar el cumplimiento de las políticas de seguridad internas de Indra, en concreto del **MAN-MNF-0858 Seguridad de la Información para Proveedores**, siendo responsabilidad de cada empresa proveedora garantizar la lectura y conocimiento en su versión más reciente por parte de su personal, así como de obtener su compromiso de cumplirla y respetarla.

El MAN-MNF-0858 desarrolla detalladamente todo a lo que debe comprometerse el proveedor de servicios o terceras partes prestadoras de servicios, mientras que esta guía pretende enfocarse en unos mínimos generales que se consideran esenciales para mitigar los riesgos de seguridad que Indra ha identificado con mayor impacto y probabilidad de que ocurran, identificados durante la realización de auditorías que realiza la compañía.

3.1 Pautas mínimas de seguridad

A continuación, se listan las pautas mínimas de seguridad para alcanzar una mejora sustancial del estado de la Seguridad de la Información de los proveedores de servicios de Indra:

3.1.1 Roles y responsabilidades

- Para garantizar la seguridad de la información en todas las partes de la empresa, se recomienda definir claramente cuáles son los roles y responsabilidades en materia de Seguridad de la Información. Se debe **identificar un responsable de Seguridad de la Información** nombrado por la alta dirección, que actúe como punto de contacto para todas las cuestiones relacionadas con la Seguridad de la Información. Entre algunas de sus funciones, este deberá de proporcionar toda la información necesaria a Indra cuando se produzca un incidente de seguridad en el que se haya comprometido información de Indra o de sus clientes, o haya un cambio relevante en el servicio prestado para que Indra pueda analizarlos y evaluar los riesgos de asociados.

3.1.2 Política y procedimientos de Seguridad de la Información

- **Dar a conocer a los proveedores el MAN-MNF-0858 Seguridad de la Información de Indra para Proveedores**, llevándose un registro de la difusión en el que conste que ha sido entendido y comprendido por todos los usuarios con acceso a información de Indra o de sus clientes. Dicho documento se puede consultar en el portal de [Indracompany](#) o en las referencias que aparecen dentro de las Condiciones generales de compra de Indra.
- Disponer de una **Política de Seguridad de la Información** donde se indiquen los objetivos que tiene la dirección de la empresa en materia de Seguridad de la Información, y **procedimientos de seguridad con las actividades necesarias de seguridad y de TI asignadas a los roles correspondientes**. Por ejemplo, procedimientos de configuración segura para la instalación de sistemas de información (creación de diferentes roles y asignación de las funcionalidades según necesidad, deshabilitación de las funciones no requeridas, seguir las pautas del fabricante...), sobre la gestión del inventario de activos, la gestión de los usuarios en los sistemas, control de accesos, gestión de logs, gestión de las copias de seguridad, etc., así como **procedimientos destinados a usuarios finales** que tengan acceso a información de Indra en papel o en formato electrónico, con instrucciones de uso seguro o buenas prácticas para el tratamiento de la misma o de los servicios y sistemas que la almacenan (por ejemplo, definición de una política de contraseñas seguras para acceder a los sistemas).
 - Dentro de estos procedimientos, se recomienda que exista un **procedimiento que detalle los procesos de autorización¹ respecto a los sistemas de información**, tanto para acciones realizadas por usuarios en el entorno de operación como para posibles acciones que tuviera que realizar un administrador del sistema. Este proceso de autorización debe cubrir, por ejemplo, entrada de equipos y aplicaciones en producción, establecimiento de comunicaciones con otros sistemas, utilización de servicios de terceros, entre otros.
 - Se presentan los siguientes recursos gratuitos del INCIBE (Instituto Nacional de Ciberseguridad de España) que pueden utilizarse para el desarrollo de políticas y procedimientos sobre los aspectos esenciales y elementos donde se debe aplicar seguridad y que deben estar bajo control: <https://www.incibe.es/protege-tu-empresa/herramientas/politicas>
- El proveedor debe **formalizar la actividad de firma de acuerdos de confidencialidad por parte de sus empleados y colaboradores**, y la aceptación de las condiciones y responsabilidades en materia de seguridad de la información, así como cumplir en específico los **acuerdos de confidencialidad de la información** que pudieran existir firmados en el contrato de prestación de servicios, y mantener el correspondiente **deber de secreto** durante la duración del servicio y después de que finalice la relación con Indra.

¹ Consultar propuesta de plantilla en Anexo A.

- En caso de que el **proveedor subcontrate parte de los servicios prestados a Indra**, es recomendable que el personal subcontratado también esté en conocimiento del MAN-MNF-0858 para garantizar la seguridad de la información en las actividades subcontratadas, y sea preferiblemente, un proveedor homologado por Indra o previamente autorizado por esta.
- Contar con documentación descriptiva o diagramas de la **arquitectura de los sistemas de información y/o servicios publicados² que traten o almacenen información de Indra**. Debería existir documentación que precise las áreas físicas donde se encuentran los sistemas, las características técnicas de éstos, los puntos de acceso a los mismos, los equipos existentes, las redes internas y conexiones al exterior, los sistemas de seguridad de los que se dispone, etc.
- En caso de que la **actividad/servicio proporcionado por el proveedor prevea el acceso o tratamiento de datos personales de INDRA o bajo responsabilidad de esta**, debe cumplir con lo especificado dentro de las Condiciones generales de compra de Indra, en concreto el apartado Confidencialidad y protección de datos personales, subapartado *Protección de datos personales* y las *Disposiciones especiales aplicables a órdenes de compra relacionadas con servicios que supongan el tratamiento de datos de carácter personal*.

3.1.3 Análisis de riesgos

- El proveedor debe identificar periódicamente, aunque sea de manera no formal, **las amenazas que podrían tener mayor probabilidad e impacto** de ocurrir y que pudieran poner en riesgo a Indra o información de sus clientes de alguna forma, tomando medidas para evitarlos o mitigarlos.

INCIBE dispone de una herramienta de autodiagnóstico especialmente diseñada para ayudar a empresas a realizar un análisis de riesgos, evaluar su estado de ciberseguridad y a avanzar hacia mayores niveles de protección. A través de una serie de preguntas y de manera rápida, se guía al usuario para que determine el estado en Seguridad de la Información de su empresa, qué riesgos amenazan su funcionamiento y qué aspectos se deben mejorar, para empezar a medir y mejorar.

Herramienta de análisis de riesgos gratuita:

<https://www.incibe.es/empresas/herramientas/conoces-tus-riesgos>.

3.1.4 Formación y concienciación en materia de Seguridad de la Información

- **Concienciar y sensibilizar en materia de Seguridad de la Información a los empleados periódicamente.** Se debe contar con planes de concienciación [que incluya normativa de seguridad relativa al buen uso de los sistemas y protección de la información, campañas de prevención de amenazas, envío de boletines, etc.] y llevar un registro de su ejecución que muestre que los empleados han recibido dicha concienciación y la han entendido. Un ejemplo de concienciación sería enseñar a los empleados a desconfiar y protegerse de correos electrónicos fraudulentos de destinatarios desconocidos o correos con adjuntos o enlaces sospechosos, verificando una serie de cosas.
- **Formar en materia de ciberseguridad** a todo el personal que provee servicios a Indra y/o maneja su información, ya que la mayoría de las situaciones que afectan a la continuidad del negocio se deben de alguna forma u otra a la falta de preparación en ciberseguridad de los empleados que manejan los dispositivos que almacenan la información, o por no dar contenido formativo relativo a la configuración de los sistemas a las personas responsables de ellos.

² Consultar propuesta de documentación en Anexo B.

A continuación, se presentan los siguientes recursos gratuitos que pueden utilizarse para enviar boletines sobre Seguridad de la Información, para concienciar y formar al personal, o para la consulta de información en materia de Seguridad de la Información:

- **INCIBE** (<https://www.incibe.es/>): El Instituto Nacional de Ciberseguridad de España es una sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial y consolidada como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos. Tiene recursos muy útiles sobre ciberseguridad y consejos para evitar o estar preparados ante las amenazas más comunes, como lo es el [Kit de concienciación](#), un conjunto de recursos didácticos y herramientas de entrenamiento para concienciar y entrenar a los empleados en el uso seguro de la tecnología, evitando incidentes de Seguridad de la Información.
- **CCN** (<https://www.ccn-cert.cni.es/>): El Centro Criptológico Nacional (CCN) es el Organismo responsable de coordinar la acción de los diferentes organismos de la Administración Pública que utilicen medios o procedimientos de cifra y garantizar la seguridad de las Tecnologías de la Información en ese ámbito. Resultan especialmente interesantes las [Guías CCN-STIC de Seguridad](#) públicas, las cuales son desarrolladas para mejorar el grado de ciberseguridad de las organizaciones. Periódicamente son actualizadas y completadas con otras nuevas, en función de las amenazas y vulnerabilidades detectadas por el CCN-CERT (Centro de Respuesta a incidentes de Seguridad de la Información del CCN).

3.1.5 Navegación segura por Internet

- **Disponer de mecanismos técnicos** adecuadamente configurados para realizar y comprobar la navegación por Internet, como puede ser una solución de proxy o con funcionalidades de proxy como puede tenerlas un firewall, que permita imponer restricciones de acceso a Internet en base a direcciones IP o datos de inicio de sesión, filtrar el contenido no adecuado de páginas web, bloqueo de sitios web maliciosos, o bloqueo de categorías completas (web con contenidos streaming, redes sociales, etc.) por política de empresa.

El anterior apartado recogía información sobre concienciación y formación en materia de Seguridad de la Información para los empleados, pero por hablar más específicamente sobre navegación segura en el presente apartado, aunque vaya dirigido al usuario final, se han decidido incluir aquí buenas prácticas para que los empleados con acceso a Internet puedan navegar de forma más segura:

- **Verificar que las webs son de confianza y seguras** antes de llevar a cabo alguna acción:
 - Entrar a sitios web **oficiales y conocidos**, fijarse en los iconos y diseño de la web, si existen errores ortográficos, si aparece información legal sobre la empresa, etc.
 - Revisar si aparece el **icono de un candado** a la izquierda de la barra de direcciones del navegador. Esto indica que la página web utiliza un certificado vigente que asegura que la web es la correcta, verificado por una empresa de confianza, y que además utiliza HTTPS, lo que permite que las comunicaciones vayan cifradas.
 - **Revisar si el enlace está bien escrito** (por ej., amaz0n.es cambiando la letra "o" por el número "0" no es el enlace oficial y correcto, y podría estar engañando al usuario para llevarlo a una página maliciosa), y en caso de que se vaya a hacer clic en un botón o hipervínculo adjunto en un correo, poner el cursor del ratón encima del mismo para saber a qué enlace redirige, evitando de este modo ser redirigidos a páginas web maliciosas o fraudulentas que manipulen al usuario para realizar acciones no deseadas.

- **Comprobar la reputación de la web** mirando comentarios y valoraciones en otros sitios de Internet.
- Tener **precaución al compartir información privada** en sitios web.
- **No guardar contraseñas en el navegador** cuando se da la opción de recordar contraseña en el mismo.
- **Eliminar cookies³ de sesión.** Se pueden borrar después de navegar, borrar el historial de navegación por completo o configurar el navegador para que se borren automáticamente. [Aquí](#) se puede encontrar información de cómo borrar las cookies en los principales navegadores web.
- **Actualizar los navegadores** [y el dispositivo donde está instalado] a la última versión y las extensiones [también conocidas como *plugins*] cuya instalación haya sido autorizada, así como desinstalar las que no se utilicen. Los navegadores suelen actualizarse automáticamente, pero todos tienen una opción para [buscar nuevas versiones o comprobarlo de manera manual](#). Por otro lado, aquí encontramos información de [cómo desinstalar extensiones que no se utilizan de los navegadores web](#).
- **Configurar seguridad y privacidad** en el navegador, aparte de configurar y revisar las cookies y *plugins*, se pueden configurar otras opciones como bloquear la geolocalización, el micrófono, desactivar la sincronización de contraseñas y bloquear *pop-ups*. Para encontrar estas opciones, se puede consultar información en los siguientes enlaces de los navegadores más utilizados: [Google Chrome](#), [Microsoft Edge](#), [Mozilla Firefox](#), [Opera](#) y [Safari](#).
- **Evitar**, en la medida de lo posible, la **navegación por Internet por motivos no profesionales**.
- **Difundir entre los empleados buenas prácticas para el uso de Internet.** Aquí hay algunos recursos interesantes para ello:
 - [Oficina de Seguridad del Internauta](#) de INCIBE
 - [Blog INCIBE: Navegación segura y privada para ti y tu empresa. Parte I](#)
 - [Blog INCIBE: Navegación segura y privada para ti y tu empresa. Parte II](#)

3.1.6 Seguridad en los Sistemas

- **Inventario de activos** registrado donde aparezcan los elementos (equipos, servidores, etc.) que contienen o tratan información de Indra con sus correspondientes características identificativas y poniendo a su responsable.
- Sistema operativo licenciado, con versiones del sistema operativo **actualizadas⁴ y soportadas⁵**, y con la **última versión de parches de seguridad** instalados.
- Actualización de los **programas instalados en los dispositivos a sus versiones más recientes** para reducir el número de vulnerabilidades, por ej., el paquete de Office, correo electrónico, software ERP, programas de diseño de planos y piezas, etc.

³ Las cookies son pequeños archivos de texto enviados al navegador que guardan información sobre la sesión con una web para facilitar las conexiones futuras y recordar datos de navegación como hábitos y preferencias. Si se [navega en modo privado o incógnito](#), se inicia sesión sin usar datos ya almacenados en el navegador y al terminar se borrarán las cookies, el historial de navegación y otros datos creados.

⁴ Ayuda para la actualización del S.O Microsoft Windows [aquí](#)

⁵ Buscar información sobre el soporte de otros productos y servicios de Microsoft [aquí](#)

- Instalación de un **antivirus**⁶ que siempre esté activo y actualizado a su última versión disponible.
- Realizar un **análisis técnico de vulnerabilidades** previamente a la puesta en producción del servicio o sistema que trate información de Indra. Valorar que se lleve a cabo un análisis de vulnerabilidades y una auditoría técnica de revisión de la configuración de la infraestructura cada cierto tiempo. De igual forma, ante cambios significativos en las infraestructuras y sistemas se recomienda la realización de una auditoría interna/externa de vulnerabilidades.
- Protección de los **accesos a los sistemas de información**:
 - Gestionar, identificar y revisar todos los **usuarios que acceden a la información** (quién es su responsable, qué rol tiene, qué permisos tiene ese rol etc.). Por ej., si un sistema de información trata información de Indra, ese sistema debe permitir la consulta solo de los usuarios que tengan autorizado el acceso a dicha información. Dichos usuarios deben poder ser dados de baja o deshabilitados en cualquier momento, al igual que se deben poder modificar sus permisos en caso de ser necesario.
 - **Limitar el número de intentos** fallidos de inicio de sesión en los PC y en general en todos los sistemas y aplicaciones.
 - **Crear contraseñas robustas**. A continuación, se deja una serie de recomendaciones a seguir para crearlas:
 - Que contengan mínimo 8 caracteres (preferiblemente 10), y se considere ampliar la longitud si además son cuentas con privilegios.
 - Que contengan caracteres de al menos tres grupos de los siguientes:
 - Letras Mayúsculas (A, B, C, D, ...)
 - Letras Minúsculas (a, b, c, d, ...)
 - Dígitos (0,1,2,3...)
 - ¡Caracteres especiales permitidos (! @ # \$ % & * _ + - = [] | ; < > ? , . /)
 - No contener el nombre del empleado, ni el nombre de la cuenta de usuario, ni el de la empresa, ni parte de los mismos.
 - No debe ser ningún dato personal (nombre, apellidos, fecha de nacimiento, DNI, ...).
 - No debe contener palabras incluidas en el diccionario, en ningún idioma (Por ejemplo, "casa" ni "house").
 - No utilizar contraseñas similares. Las contraseñas deben ser significativamente diferente de otras contraseñas anteriores.
 - Un buen consejo es utilizar palabras mal escritas o introducir números por determinadas letras. Por ejemplo, sustituye la letra "O" por un "cero", la "a" por un "dos" (Orden2d0r).
 - Mantener la confidencialidad de las contraseñas. No compartirlas con nadie, ni escribirlas en papel.
 - Los usuarios deben **cambiar las contraseñas que estén por defecto en el primer inicio de sesión y con una periodicidad determinada**, y/o cuando exista un posible indicio de conocimiento por parte de otros usuarios.

⁶ Las soluciones de hardware, software y servicios desarrollados o proporcionados por Kaspersky Lab (entre ellas su solución de antivirus) se encuentra actualmente prohibida a todas las agencias gubernamentales con sede en los Estados Unidos. Info. [aquí](#). Si se utiliza SO Windows 10, 11 o posterior, y Windows Server 2016, 2019, o posterior, el sistema ya incluye de forma gratuita Microsoft Defender Antivirus, que ofrece una protección avanzada y suficiente para la mayoría de los usuarios. No obstante, si se requiere un nivel de protección adicional o funcionalidades específicas, puede valorarse la instalación de otra solución antimalware complementaria o de una suite de seguridad más completa.

- **Bloquear las sesiones de usuario** o apagar el PC al dejarlo desatendido. En el [siguiente enlace](#) aparece información de cómo configurar el bloqueo automático fijando un tiempo en el S.O. Windows y cómo bloquear la pantalla manualmente. Para S.O. Mac consultarlo [aquí](#).
- **Configurar conexiones remotas seguras** que pudieran ser necesarias para que trabajadores, colaboradores externos o administradores de sistemas puedan acceder a recursos de la empresa para sus labores. **No debe estar permitido utilizar aplicaciones de conexión a escritorio remoto como el conocido RDP de Windows**, ya que estas herramientas pueden crear puertas traseras a través de las cuales podría comprometerse el servicio o las credenciales de acceso de usuario, y, por lo tanto, permitir el acceso a los equipos corporativos. Además, es altamente recomendable el uso de una **VPN**⁷ correctamente configurada. Para un acceso remoto seguro se aconseja ver las pautas de la siguiente [Guía sobre ciberseguridad en el teletrabajo de INCIBE](#).
- Almacenar los **registros de los accesos a los sistemas y aplicaciones que contienen información de Indra**, sobre todo los intentos de autenticación exitosos o fallidos, y si se mantienen en el tiempo de alguna forma o se sobrescriben en un corto periodo de tiempo.
- Se recomienda la **realización de copias de Seguridad de la Información periódicas** en un dispositivo diferente al sistema que la almacena, junto con un procedimiento de realización de dichas copias y verificación de recuperación de la información de las copias de respaldo.
- **Notificación de baja de activos.** Una vez finalizado el servicio contratado que se presta a Indra, se debe garantizar la Seguridad de la Información de Indra almacenada en los sistemas de información digitales o archivadores, no debiendo **acceder ya a información sensible de Indra o procediendo a su destrucción/devolución en caso de que Indra lo exija**. Por tanto, se debe:
 - señalar los activos de información que han de ser devueltos/destruidos si Indra lo exige
 - borrar la información sensible u obsoleta de Indra almacenada digitalmente en los sistemas de uso principal/diario o proceder a la destrucción del sistema si procediese
 - eliminar permisos de acceso a esos sistemas o carpetas con información que es obsoleta o ya no es útil de Indra

3.1.7 Gestión de Incidentes

- El proveedor debe disponer de un **procedimiento de gestión y respuesta ante incidentes** y un registro de estos. El [siguiente recurso](#) incluye una serie de controles para que la organización revise los puntos más relevantes a tener en cuenta en lo relativo a la respuesta a incidentes de ciberseguridad, y [este otro recurso](#) incluye una guía que atiende a buenas prácticas generalmente reconocidas en la gestión de incidentes y, como tales, pueden servir de referencia en el diseño e implementación de este servicio y su procedimiento asociado.
- Dicho procedimiento debe incluir la obligación de **comunicar de manera inmediata cualquier incidente, debilidad o amenaza** (observada o sospechada) que se detecte en los sistemas con información de Indra o que haya podido afectar a información propiedad de Indra o sus clientes (en un apartado de notificación de incidentes de seguridad a proveedores), al Departamento de Seguridad de la Información de Indra en csirt@indra.es con copia al responsable del servicio de Indra y/o al Focal Point asignado dentro de Indra.

⁷ Una VPN (Virtual Private Network) es una tecnología de red que permite una conexión virtual segura para acceder a los recursos de información privados o internos de una organización, utilizando como soporte de comunicaciones una infraestructura no confiable que generalmente suele ser Internet.

4 Comunicaciones

- Comunicación de **incidentes de seguridad** a: csirt@indra.es y al responsable de proyecto/servicio o focal point dentro de Indra.
- Comunicación de **cambios en la prestación del servicio** (cambios de usuarios que manejan información de Indra, actualizaciones en el producto desarrollado o solución prestada...), o **cambios en el Contacto de Seguridad del Proveedor** al que Indra deba dirigirse para temas de Seguridad de la Información a: responsable de proyecto/servicio o focal point.

5 Control de cambios

Fecha	Ed. / Rev.	Descripción de los cambios
Noviembre 2021	1.0	Edición inicial
Enero 2023	2.0	Actualización de contenido
Octubre 2024	2.1	Actualización por cambios menores
Octubre 2025	2.2	Cambio de formato del documento

Tech for the future

Generamos
confianza para
proteger e impulsar
tanto el presente,
como el futuro

Avda. de Bruselas, 35
28108 Alcobendas
Madrid, Spain
T +34 91 480 50 00

indracompany.com

