POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA PROVEEDORES EXTERNOS

El Grupo de Computación Avanzada del IFCA, emite, difunde, implementa revisa periódicamente esta política de seguridad de la información en el ámbito de la norma ISO 27001.

Una vez recibida, el proveedor externo acusará recibo y entendimiento de la misma. Caso de no recibir comentarios a partir de una semana de la fecha de envío, se entenderá por aceptada.

a) Identificación y documentación de los tipos de proveedores.

Esta política se aplicará a:

- Servicios de Tecnologías de la Información.
- Servicios de logística.
- Suministradores de componentes de la infraestructura de TI y proveedores representantes de los mismo.
- Mantenedores de infraestructuras.

b) Proceso y ciclo de vida normalizados para la gestión de las relaciones con los proveedores;

El proceso de contratación con proveedores será nuestro procedimiento interno de compras donde habitualmente se solicitará una garantía entre 3 y 5 años 3 a 5 años.

El IFCA se reserva el derecho a modificar este documento cuando sea necesario.

Se gestionará esta política y las relaciones con nuestros proveedores externos con frecuencia mínima durante el ciclo de renovación de contratos.

Los cambios realizados serán divulgados a todas las empresas proveedoras 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 por parte de su personal, así como de cumplir y respetar dichas políticas.

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

c) tipos de acceso a la información que se permitirá a los diferentes tipos de proveedores, con su supervisión y su control del acceso.

Los proveedores se podrán conectar a nuestra infraestructura desde nuestras instalaciones con supervisión, admitiendo conexiones remotas.

Toda información, documentación, programas y/o aplicaciones, métodos, organización, estrategias de negocio y actividades relacionadas con IFCA o con sus proyectos, a las que tenga acceso los proveedores con objeto de la realización del servicio serán considerado información confidencial y el 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 IFCA.

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.

El IFCA podrá solicitar el borrado seguro de los dispositivos que hayan tenido acceso a la Información de IFCA.

d) los requisitos mínimos de seguridad de la información por cada tipo de información y tipo de acceso para servir de base para cada uno de los acuerdos con los proveedores en consonancia con las necesidades y requisitos de negocio de la organización y su perfil de riesgo;

Cualquier tipo de intercambio de información que se produzca entre IFCA 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.

IFCA 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 servicio, se considerarán no autorizadas las siguientes actividades:

1. Transmisión o recepción de material protegido por los derechos de autor infringiendo la Ley de Propiedad Intelectual.
2. 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.
3. Transmisión o recepción de información sensible, salvo que la comunicación electrónica esté cifrada y el envío esté autorizado por escrito.
4. Transferencia de información protegida a terceras partes no autorizadas.
5. Transmisión o recepción de aplicaciones no relacionadas con el negocio.
6. Participación en actividades de Internet, como grupos de noticias, juegos u otras que no estén directamente relacionadas con la prestación del servicio.
7. Todas las actividades que puedan dañar la imagen y reputación de IFCA están prohibidas en Internet y en cualquier otro lugar.

e) los procesos y procedimientos para supervisar el cumplimiento de los requisitos de seguridad de la información establecidos para cada tipo de proveedor y cada tipo de acceso, incluyendo la revisión por terceros y la validación de los productos;

Los proveedores de servicios deberán permitir que el IFCA o la unidad técnica de la Universidad de Cantabria, o empresas subcontratadas, lleve a cabo las auditorías de seguridad solicitadas, colaborando con el equipo auditor y facilitando todas las evidencias y registros que le sean requeridos sin demora injustificada. El alcance, profundidad de cada auditoría, así como su número, será establecido expresamente por el IFCA o la unidad técnica de la UC.

f) Controles de exactitud y completitud, para garantizar la integridad de la información o del tratamiento de la información proporcionados por cualquiera de las partes.

Los medios de comunicación serán los autorizados por el procedimiento integrado de comunicaciones internas y externas del IFCA, que será comunicado al proveedor externo cuando proceda, por email o por teléfono.

g) Tipos de obligaciones que sean aplicables a los proveedores para proteger la información de la organización.

Los proveedores de servicios proporcionarán al IFCA siempre que se requiera, la relación de personas, perfiles, funciones y responsabilidades asociados al servicio prestado, e informará de cualquier cambio (alta, baja, sustitución 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 previsto tanto en las materias correspondientes a la actividad como asocia da 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 contenido en esta política.

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

1. Cada persona con acceso a información de IFCA 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 conocida por el propio usuario sin que sea revelada al resto del personal bajo ningún concepto.
2. Los usuarios no deberán utilizar ningún identificador de otro usuario, aunque dispongan de la autorización del propietario.
3. Los usuarios conocen y aplican los requisitos y procedimientos existentes en torno a la información manejada.
4. Cualquier usuario con acceso a información de IFCA deberá seleccionar contraseñas de calidad (al menos 12 caracteres, contener letras mayúsculas, minúsculas, dígitos y caracteres especiales, según lo definido en nuestra política criptográfica, que el proveedor externo debe conocer.
5. Cualquier persona con acceso a información de IFCA deberá velar por que los equipos queden protegidos cuando vayan a quedar desatendido.
6. 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 reducirlos 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.)
7. Las personas con acceso a sistemas de información de IFCA nunca deberán, sin autorización por escrito efectuar pruebas para detectar y/o explotar una supuesta debilidad o incidencia de seguridad.
8. Ninguna persona con acceso a sistemas de información de IFCA intentará sin autorización expresa y por escrito por ningún medio, transgredir los sistemas de seguridad y las autorizaciones. Se prohíbe la captura de trafico de red por parte de los usuarios, salvo que se estén llevando a cabo tareas de auditoría autorizadas por escrito.

h) Gestión de incidencias y contingencias asociadas al acceso de los proveedores, incluyendo responsabilidades, tanto del IFCA, como de los proveedores.

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 IFCA o que haya podido afectar través computing.security@ifca.unican.es

Los recursos corporativos de IFCA a los que tengan acceso los proveedores de servicios serán utilizados exclusivamente para cumplir con las obligaciones es 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, daños a terceros, incumplimientos de la normativa de protección de datos etc.

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

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

En caso de apreciar que algún proveedor de servicios, o su personal, utiliza incorrectamente recursos o información del IFCA, se le comunicará tal circunstancia al proveedor para que realice las acciones oportunas. El IFCA 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 IFCA 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 malware.

i) Acuerdos de resiliencia y, si fuesen necesarios, acuerdos de recuperación y de contingencia para asegurar la disponibilidad de la información o el tratamiento de la información proporcionada por cualquiera de las partes.

Estableceremos los acuerdos de resiliencia, contingencia y recuperación cuando sea necesario.

j) Sesiones de concienciación para el personal de la organización que participa en compras con respecto a las políticas, procesos y procedimientos aplicables.

Se usará el código de conducta del CSIC y de la UC para nuestro personal y el del proveedor.

k) Sesiones de concienciación para el personal de la organización que interactúa con el personal de los proveedores con respecto a las reglas apropiadas referentes al acuerdo y a las actuaciones según el tipo de proveedor y el nivel de acceso de proveedores a los sistemas y la información de la organización.

Se usará el código de conducta del CSIC y de la UC para nuestro personal y el del proveedor.

l) Condiciones bajo las que los requisitos y controles de seguridad de la información se documentarán en un acuerdo firmado por ambas partes.

Los acuerdos firmados por ambas partes incluirán los controles y requisitos de seguridad, bajo los criterios de la UC y el CSIC e incluirán requisitos sobre

<u>Seguridad física</u>

Todos los proveedores de servicios cuyos servicios se presten desde la sede del proveedor cumplirán los siguientes requisitos:

- 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 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.
- Los edificios o instalaciones deberían contar con sistemas automáticos de detección y respuesta automática ante condiciones ambientales adversas (fuego principalmente).
- Si se mantiene algún tipo de copia de información responsabilidad del IFCA, los sistemas que alberguen y/o procesen dicha información deberán estar ubicados en un área especialmente protegida, que incluya al menos las medidas de seguridad:
  - 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.

m) Gestión de las migraciones necesarias de información, instalaciones de tratamiento de la información y cualquier otra cosa que necesite ser migrada, y garantizar que la seguridad de información se mantenga durante todo el período de transición.

Caso de que se realicen por el proveedor, este deberá respetar la política criptográfica del IFCA.

Firma: Resp. Servicio de Computación

I. CABRILLO
Firmado por CABRILLO BARTOLOME JOSE IBAN - ***0368** el día 30/09/2021 con un certificado

FECHA: 2021-09-30