POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA PROVEEDORES

1. OBJETIVO

El objetivo de este documento es establecer las directrices y requisitos de seguridad de la información aplicables a los proveedores de servicios, independientemente del tipo de servicio prestado, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información de EM&E y sus clientes.

2. ALCANCE

La siguiente política se aplica a todos los proveedores que tengan acceso a la información de EM&E e intercambien, procesen, almacenen, modifiquen o creen nueva información confidencial propiedad de EM&E., o los que utilicen su infraestructura tecnológica, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información.

3. PRINCIPIOS GENERALES DE SEGURIDAD PARA PROVEEDORES

3.2. PRESTACIÓN DE SERVICIOS A EM&E

Las actividades desarrolladas por el personal perteneciente a empresas proveedoras se realizarán de acuerdo a lo establecido en el correspondiente contrato regulador, así como a las normas y procedimientos establecidos a tal efecto entre EM&E y el proveedor.

La empresa proveedora deberá asegurar que todo su personal que preste servicios para EM&E cuente con la formación y capacitación apropiada para el desarrollo del servicio contratado, tanto a nivel específico en las materias correspondientes a la actividad asociada a la prestación del servicio como de manera transversal en materia de seguridad de la información.

Cualquier tipo de intercambio de información que se produzca entre EM&E y el proveedor se entenderá realizado dentro del marco establecido por el contrato de prestación de servicios, de modo que dicha información no podrá ser utilizada en ningún caso fuera de dicho marco, ni para fines diferentes a los asociados a dicho contrato.

3.3. CONFIDENCIALIDAD DE LA INFORMACIÓN

Todas las relaciones con proveedores de servicios que tengan acceso a la información de EM&E estarán amparadas por los contratos de prestación de servicios y los acuerdos de confidencialidad (NDA) correspondientes.

Cualquier información, documentación, programa y/o aplicación, método, estrategia de negocio y actividad relacionadas con EM&E a las que tengan acceso los proveedores de servicios con objeto de realización del servicio serán considerados, por defecto, información confidencial. Sólo se podrá considerar como información no confidencial aquella información de EM&E a la que haya tenido acceso a través de los medios de difusión pública de información.

La información a la que tenga acceso el proveedor únicamente podrá ser utilizada para los fines descritos en el contrato de prestación de servicios.

El proveedor mantendrá el correspondiente deber de secreto durante la duración del servicio y después de que finalice la relación con EM&E.

El incumplimiento de estas obligaciones puede constituir un delito de revelación de secretos, previsto en el artículo 197 del Código Penal, que puede dar derecho a exigir compensaciones.

Para garantizar la seguridad de los datos de carácter personal, la salida de soportes informáticos que contengan datos este carácter fuera de las instalaciones de EM&E, deberá ser autorizada por EM&E y se realizará según el protocolo de protección de datos definido.

3.4. 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 EM&E para el desarrollo de sus funciones. Queda estrictamente prohibido el uso de programas informáticos en los sistemas de información de EM&E sin la correspondiente licencia.

Igualmente, 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.

3.5. INTERCAMBIO DE INFORMACIÓN

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

En relación al intercambio de información dentro del marco contractual existente entre las partes, se considerarán no autorizadas las siguientes actividades:

- Transmisión o recepción de material protegido por Copyright infringiendo la Ley de Protección Intelectual.
- Transmisión o recepción de toda clase de material pornográfico, mensajes o de una naturaleza sexual, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.
- Transferencia de información confidencial a terceras partes no autorizadas.
- Transmisión o recepción de ficheros que infrinjan la normativa de protección de datos de carácter personal.
- Todas las actividades que puedan dañar la imagen y reputación de EM&E están prohibidas.

Al término del servicio o ante el pedido efectuado en cualquier momento por EM&E, cesará inmediatamente el uso de toda información proporcionada y el proveedor entregará toda la información que posea, independientemente del soporte en que se encuentre, y destruirá toda copia que haya realizado.

3.6. USO APROPIADO DE LOS RECURSOS

Los recursos dispuestos para los proveedores de servicio serán utilizados exclusivamente para cumplir con las obligaciones y propósitos para la que fueron proporcionados En ningún caso podrán ser utilizados para actividades no relacionadas con el propósito del servicio o para la comisión de actividades que pudieran ser consideradas ilícitas. EM&E se reserva el derecho de implementar los mecanismos de control que considere oportunos para verificar el uso apropiado de estos recursos

Cualquier fichero introducido en la red de EM&E 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 esta política y en la normativa interna de la organización.

3.7. RESPONSABILIDAD DEL USUARIO

Los proveedores de servicios deberán asegurarse de que todo el personal que desarrolla labores para EM&E y pueda acceder a los sistemas de información, respete los siguientes principios básicos dentro de su actividad:

- Cada persona con acceso a información de EM&E 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 persona con acceso a información de EM&E deberá seguir la política de contraseñas.
- Cualquier persona con acceso a información de EM&E deberá velar porque los equipos queden protegidos cuando vayan a quedar desatendidos.
- Cualquier persona con acceso a información deberá respetar la política de mesas limpias, 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.

- Todo el personal que acceda a la información y/o los sistemas de EM&E deberá contar con la autorización necesaria.

3.8. REQUISITOS DE SEGURIDAD PARA LOS DISPOSITIVOS

Todos los dispositivos con acceso a información de EM&E deberán cumplir 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.
- Todos los dispositivos estarán adecuadamente protegidos frente a malware. Se mantendrán al día con las últimas actualizaciones de seguridad disponibles. El software antivirus deberá estar siempre habilitado.
- Los dispositivos deberán permanecer actualizados con la última versión disponible de parches de seguridad para el software y sistema operativo instalado.
- Los dispositivos no dispondrán de ninguna herramienta o ficheros contrarios a la política de seguridad de EM&E o que pueda interferir con el software corporativo.

3.9. COMUNICACIÓN DE INCIDENCIAS

Todos los proveedores deberán comunicar inmediatamente, cualquier incidencia, debilidad o amenaza que pudiera afectar la confidencialidad, integridad o disponibilidad de la información de EM&E al Departamento de IT a través del correo electrónico soporte@eme-es.com o al responsable que lo ha contratado.

4. PRINCIPIOS ESPECÍFICOS DE SEGURIDAD PARA PROVEEDORES

4.1. SEGURIDAD FÍSICA

Todos los proveedores que presten los servicios desde la sede del proveedor deberán garantizar que se cumplen las medidas de seguridad física siguientes:

- Contar con algún sistema de control de acceso que garantice la prevención ante robo, destrucción o interrupción del servicio.
- Contar con sistemas de detección y respuesta automática ante condiciones ambientales adversas, principalmente incendios.
- Si se mantiene algún tipo de copia de información de EM&E, lo sistemas que alberguen y/o procesen dicha información deberán estar ubicados en un área especialmente protegida.

4.2. SEGURIDAD DE SISTEMAS

Todos los proveedores cuyos servicios se presten mediante el uso de su infraestructura TIC deberán garantizar que se cumplen las consideraciones siguientes:

- Los sistemas de información que alberguen o procesen información responsabilidad de EM&E estarán adecuadamente protegidos frente a software malicioso. Se mantendrán los sistemas al día con las últimas actualizaciones de seguridad disponibles, en los entornos de prueba, desarrollo y producción. Además, el software antivirus deberá estar siempre habilitado.
- El proveedor establecerá una política de copias de seguridad que garantice la salvaguarda de cualquier dato o información relevante para el servicio prestado.
- En relación con la utilización del correo electrónico, no se permitirá la transmisión de información confidencial de EM&E salvo que la comunicación electrónica esté cifrada y el envío este expresamente permitido.
- El acceso a los sistemas de información que alberguen o procesen información de EM&E deberá realizarse siempre de forma autenticada, al menos mediante la utilización de un identificador usuario unipersonal y una contraseña asociada.
- Se deberá cumplir lo establecido en el punto Requisitos de seguridad para los dispositivos.

4.3. SEGURIDAD DE RED

Todos los proveedores cuyos servicios se presten mediante el uso de su infraestructura TIC deberán garantizar que se cumplen las siguientes medidas de seguridad red:

- Todas las redes por las que circule la información deberán estar correctamente gestionadas y controladas, asegurándose de que no existen accesos no controlados ni conexiones cuyos riesgos no estén apropiadamente gestionados.
- 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 TIC de EM&E deberán estar apropiadamente protegidas.

4.4. GESTIÓN DE CAMBIOS

Todos los proveedores de servicios que impliquen el acceso a los sistemas de información de EM&E deberán garantizar que se cumplen las siguientes consideraciones:

- Todos los cambios en la infraestructura TIC con la que presta el servicio están controlados y autorizados, garantizándose que no forma parte de esta, ningún componente no controlado.
- Todos los cambios que se lleven a cabo deberán realizarse siguiendo un procedimiento formalmente establecido y documentado.

5. ACTUALIZACIÓN DE LA POLÍTICA

Debido a la evolución de la tecnología, las amenazas de seguridad y a los nuevos requerimientos legales, EM&E se reserva el derecho a modificar esta política cuando considere necesario. Los cambios realizados serán comunicados a todos los proveedores de servicios a los que les aplique utilizando los medios que se consideren pertinentes. Es responsabilidad de cada empresa garantizar la lectura, conocimiento y cumplimiento de esta política por parte de su personal.

En Alcalá de Henares a 10 de octubre de 2022

Javier Escribano Ruiz
Presidente