Política de gestión de Incidentes

POL-SI-05

Sistemas de la Información

Histórico de versiones

Versión	Fecha	Autor	Validador	Aprobador	Cambios
1.0	Junio 2020	Departamento IT	Departamento IT	Departamento IT	Versión inicial

Contenido

1 INTRODUCCIÓN

1.1 Objeto y Contenido

Asegurarnos de que todos los miembros de la organización conocen y aplican un procedimiento rápido y eficaz para actuar ante cualquier incidente en materia de seguridad de la información. Este procedimiento incluirá medidas para comunicar de forma correcta los incidentes a quien corresponda tanto dentro como fuera de la empresa. También incluirá los mecanismos para registrar los incidentes con sus pruebas y evidencias con objeto de estudiar su origen y evitar que ocurran en un futuro.

1.2 Ámbito de Aplicación

Esta política afecta a cualquier persona o empresa que acceda a la Información de Doctaforum Medical Marketing S.L., en adelante, la Compañía.

Las empresas pertenecientes a Doctaforum Medical Marketing S.L. seguirán las directrices de la Compañía así como los documentos que emanen de éstas.

1.3 Distribución

Una vez aprobado por el Comité, se divulgará a todos los empleados afectados, a través del sistema de gestión documental establecido.

1.4 Entrada en vigor

El presente documento entrará en vigor una vez aprobado formalmente y en la fecha que se indica en su cabecera.

1.5 Revisión del Documento

El presente documento deberá ser revisado con una periodicidad anual, salvo la necesidad de un cambio sobre el mismo.

2 PROCESO DE COMUNICACIÓN DE INCIDENTES

En el caso de que un usuario sospeche que ha sufrido cualquier incidente de seguridad, deberá notificarlo al responsable de sistemas de forma inmediata describiendo de forma detallada el suceso o sospecha.

3 PROCESO DE GESTIÓN DE INCIDENTES

Ante la llegada de un incidente de seguridad, el departamento de sistemas lo analizará y clasificará según su criticidad basándose en la siguiente tabla:

Gravedad incidente	Descripción
Baja	Fallo o malfuncionamiento puntual, recepción de correo de Phishing u otras incidencias que no pongan en riesgo la integridad de los datos de la compañía.
Media	Incidentes que puedan causar o hayan causado la indisponibilidad temporal de datos de la compañía o sistemas incluidos en los BIA, sin indicios de fuga de información ni fallo de integridad de los datos.
Alta	Incidentes que puedan causar o hayan causado fallos en la integridad de datos o la fuga de ellos.

Tras su categorización, se tomarán las medidas oportunas para la erradicación, contención y remediación del incidente usando para ello todas las herramientas de seguridad y control de las que se dispongan.

En el caso de indecentes de gravedad **Alta**, con afectación la integridad de la información o fuga de datos, se notificará de inmediato el suceso al DPO. En caso de que los datos afectados sean o tengan relación con algún cliente o proveedor, estos también serán informados mediante los canales de comunicación establecidos con cada uno de ellos.

Tras la resolución de incidentes de criticidad **Media** o **Alta**, se estudiarán las medidas preventivas aplicables para la prevención de incidentes de características similares.