FUNDACIÓN IBEROAMERICANA
DE CIENCIAS SOCIALES
Y DE LA SALUD

Calle Fuente del Rey 2 (esquina Carretera de Castilla)
28023. Madrid. España.
www.ficssalud.org

PROTECCIÓN DE DATOS
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Política de Seguridad de la Información de FUNDACIÓN IBEROAMERICANA DE CIENCIAS SOCIALES DE LA SALUD (FICSSALUD), conforme a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

INDICE:

1. INTRODUCCIÓN.

La Seguridad de la Información se caracteriza como la preservación de:

- su confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información;
- su integridad, asegurando que la información y sus métodos de proceso son exactos y completos;
- su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

FUNDACIÓN IBEROAMERICANA DE CIENCIAS SOCIALES DE DE LA SALUD (FICSSALUD) depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

2. OBJETIVOS.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

2.1. Prevención.

Todo el personal y servicios de FUNDACIÓN IBEROAMERICANA DE CIENCIAS SOCIALES Y DE LA SALUD (en adelante, FICSSALUD) deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello deben implementarse las medidas mínimas de seguridad determinadas conforme al análisis de riesgo preceptivo.

2.2. Detección.

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su

detención, la operativa y sistemas deben monitorizarse de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.

Se establecerá los mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una incidencia de seguridad.

2.3. Respuesta

FUNDACIÓN IBEROAMERICANA DE CIENCIAS SOCIALES DE DE LA SALUD (FICSSALUD) debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar puntos de contacto para las comunicaciones con respecto a incidentes detectados.
- Establecer protocolos para el intercambio de información relacionada con el incidente.

2.4. Recuperación.

Para garantizar la disponibilidad de los servicios críticos, FICSSALUD desarrollará planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

3. MARCO NORMATIVO.

FICSSALUD se esfuerza en cumplir con toda la legislación aplicable a su actividad para garantizar la protección e sus activos de información, como por ejemplo la siguiente:

- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

4. ORGANIZACIÓN DE LA SEGURIDAD.

4.1. Designación de responsables.

FICSSALUD designará al Responsable de Seguridad de la Información y al Delegado de Protección de Datos. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

4.2. Responsable de seguridad.

Las funciones del Responsable de Seguridad de la Información son las siguientes:

- Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas.
- Realizar o promover las auditorías periódicas para verificar el cumplimiento de los requisitos del mismo.
- Gestionar o promover la formación y concienciación en materia de seguridad TIC.
- Comprobar que las medidas de seguridad existente son las adecuadas para las necesidades de la entidad.
- Revisar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución, emitiendo informes periódicos sobre los más relevantes.

4.2. Delegado de Protección de Datos.

El Delegado de Protección de Datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

El Delegado de Protección de Datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

El responsable o el encargado del tratamiento publicarán los datos de contacto del Delegado de Protección de Datos y los comunicarán a la autoridad de control.

1. El Delegado de Protección de Datos tendrá como mínimo las siguientes funciones:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del Reglamento, La LOPD 3/2018 y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.
- Supervisar el cumplimiento de lo dispuesto en el presente Reglamento y la LOPD 3/2018, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación;
- Cooperar con la autoridad de control;
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa cuando una evaluación de impacto relativa a la protección de los datos muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo, y realizar consultas, en su caso, sobre cualquier otro asunto.

2. El Delegado de Protección de Datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

5. DATOS DE CARÁCTER PERSONAL.

FICSSALUD trata datos de carácter personal. El manual o documento de protección de datos, al que tendrán acceso sólo las personas autorizadas, recoge los tratamientos afectados y los responsables correspondientes. Todos los sistemas de información de FICSSALUD se

ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado manual.

6. GESTIÓN DE RIESGOS.

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se revisará:

- Regularmente, al menos una vez al año.
- Cuando cambie sustancialmente la información manejada.
- Cuando cambien los servicios prestados dentro del alcance.
- Cuando ocurra un incidente muy grave de seguridad.
- Cuando se reporten vulnerabilidades muy graves.

Los análisis de riesgos se llevarán a cabo siguiendo siempre una misma metodología, que estará procedimentada.

7. OBLIGACIONES DEL PERSONAL.

Todos los trabajadores de FICSSALUD tienen la obligación de conocer esta Política de Seguridad de la Información, que es de obligado cumplimiento, siendo responsabilidad de FICSSALUD disponer los medios necesarios para que la información llegue a los afectados.

Todo empleado es responsable de registrar y reportar las violaciones a la seguridad, confirmadas o sospechadas.

Todo empleado es responsable de preservar la confidencialidad, integridad y disponibilidad de los activos de información en cumplimiento de la presente política y de los procedimientos de seguridad internos.

Se sancionará cualquier violación a esta política y a cualquier política o procedimiento de seguridad que se haya comunicado.

FICSSALUD velará porque se brinde concientización y entrenamiento en materia de seguridad de la información a todo el personal.

8. TERCERAS PARTES.

Las terceras partes relacionadas con FICSSALUD, dentro del alcance, firmarán con la empresa un acuerdo que proteja la información intercambiada.

Cuando FICSSALUD utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha Política, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.