AUDITORÍA DE CIBERSEGURIDAD 2022

TÉRMINOS DE REFERENCIA

11 de noviembre de 2022

Dirección de Transformación Digital

CONTENIDO

INTRODUCCIÓN

Acción Contra el Hambre es una organización internacional no gubernamental, privada, apolítica, aconfesional y no lucrativa, creada en 1979 en Francia para intervenir en todo el mundo. Su vocación es luchar contra el hambre, el sufrimiento físico y las situaciones de desamparo que amenazan la vida de hombres, mujeres y niños.

La necesidad de esta auditoría nace de las directrices trazadas por el Plan Estratégico Nacional para 2018 de Acción Contra el Hambre España en el que se considera necesario realizar una auditoría de ciberseguridad de forma periódica para mejorar la seguridad de sus sistemas de información.

Nuestros Principios[1]

Área de transparencia[2]

Memoria 2021[3]

OBJETIVO

Realizar un análisis de riesgos, vulnerabilidades y carencias en materia de ciberseguridad que puedan amenazar la disponibilidad de los servicios, la integridad de los sistemas y la confidencialidad de la información con el fin de asegurar la continuidad de las operaciones y el correcto funcionamiento de Acción Contra el Hambre España.

[1] https://www.accioncontraelhambre.org/es/nuestros-principios
[2] https://www.accioncontraelhambre.org/es/sobre-nosotros/transparencia
[3] https://www.accioncontraelhambre.org/sites/default/files/documents/memoria_anual_2021.pdf

ALCANCE

La auditoría debe realizar una revisión completa de la infraestructura tanto física como en la nube, sistemas de información, servicios, equipamiento, políticas, medidas y procedimientos de seguridad de Acción Contra el Hambre España.

Se deben evaluar los siguientes puntos:

1. Gestión y protección de identidades y credenciales de acceso, revisión de políticas y medidas de seguridad como SSO, Acceso Condicional, MFA o SSPR.
2. Gestión y protección de Acceso Privilegiado.
3. Análisis de la seguridad de la infraestructura de red y redes inalámbricas.
4. Medidas para la mitigación de vulnerabilidades y bastionado de servidores.
5. Seguridad de dispositivos móviles, MS Defender y medidas de seguridad de Windows 10/11.
6. Seguridad de los servicios y las aplicaciones web mediante pruebas de intrusión.
7. Revisión del programa de concienciación en ciberseguridad para usuarios, simulación de ataques de ingeniería social.
8. Mitigación de riesgos relacionados con acciones maliciosas por parte del personal de la organización.
9. Gestión de incidentes de seguridad.
10. Recuperación ante desastres y plan de continuidad de negocio.

UBICACIÓN

La auditoría deberá llevarse a cabo en las oficinas de la sede central de Acción contra el Hambre en la calle Duque de Sevilla 3 de Madrid. Al menos en aquellos puntos en los que sea indispensable para la correcta realización de las tareas programadas.

Las pruebas que no lo requieran podrán realizarse de forma remota.

PERSONAL INVOLUCRADO

Acción contra el Hambre designará una persona referente para la gestión del proyecto, quien se encargará de coordinar esfuerzos entre las diferentes partes y facilitar la información necesaria para el correcto desarrollo de la auditoría.

RESULTADOS ESPERADOS

Informe con los resultados de la auditoría de ciberseguridad identificando las diferentes vulnerabilidades, posibles carencias y la gravedad del riesgo que éstas suponen. Dentro del documento se deben definir medidas y propuestas de mejora para la prevención y la mitigación de los riesgos y vulnerabilidades identificadas.

CÓMO APLICAR

Se deberá presentar:

1. Una propuesta técnica que incluya:
    a. La metodología que se utilizará para analizar todos los puntos del alcance que aparecen en estos términos de referencia además de cualquier otro que no esté indicado y pueda ser relevante.
    b. Un plan de trabajo que detalle el desarrollo y la duración de las acciones definidas a llevar a cabo.
    c. Detalle de los recursos necesarios para el correcto desarrollo de la auditoría, tanto humanos como tecnológicos. Indicar los perfiles profesionales participantes en la auditoría, así como las herramientas a utilizar.
    d. Cumplimentar y adjuntar a la propuesta el CUESTIONARIO DE EVALUACIÓN DE ENCARGADO DE TRATAMIENTO, que se adjunta en las últimas páginas de estos Términos de Referencia (Pag. 7 a 11).

2. Una propuesta financiera que incluya:
    a. Un desglose del coste de cada actividad con IVA incluido. Indicando además el coste total.
    b. Propuesta de condiciones de pago que podrán ser negociables.
    c. Será imprescindible emitir factura/s con IVA.

Tanto la propuesta técnica como la financiera deberán ser enviadas con la referencia "ESMD01961 Auditoría de Ciberseguridad 2022 – Propuesta – Nombre de la empresa que presenta la oferta" en el asunto del e-mail a njamil@accioncontraelhambre.org con copia a jdelaplaza@accioncontraelhambre.org, mmartin@accioncontraelhambre.org

Una reunión de clarificación técnica podrá ser agendada si fuese necesario para asegurar la calidad de la propuesta a enviar entre el 14 y el 18 de noviembre, a excepción del día 15, por no disponibilidad del equipo técnico.
Para solicitud de reunión, envíe un email con la referencia "ESMD01961 Auditoría de Ciberseguridad 2022 – Clarificaciones - Nombre de la empresa que solicita la reunión" en el asunto del e-mail a njamil@accioncontraelhambre.org con copia a jdelaplaza@accioncontraelhambre.org y mmartin@accioncontraelhambre.org.

Recepción de propuestas no más tarde del 27 de noviembre de 2022 a las 23:59 hora de Madrid.

INFORMACIÓN SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL (En cumplimiento del Reglamento UE 2016/679 de Protección de Datos)	
Nota: en caso de enviar los datos para cotizar, está aceptando los términos descritos en la cláusula de protección de datos.	
Responsable del tratamiento	Denominación social: ACCIÓN CONTRA EL HAMBRE. NIF: G-81164105. Dirección: Calle Duque de Sevilla, nº 3, 28002 de Madrid. Teléfono: 34 91 391 53 00. Email: procurement@accioncontraelhambre.org
Finalidades	Gestión de su solicitud como proveedores de la Organización.
	Tratamiento de sus datos para la comprobación de que usted no figura en listados privados, o listados publicados por organismos oficiales nacionales o internacionales, tales como listas de sancionados, personas con responsabilidad pública, etc.
Legitimación y conservación	Base jurídica del tratamiento: ▪ Interés legítimo de las partes.
	Salvo en los casos que se manifieste la voluntariedad, los datos son necesarios para llevar a cabo las finalidades descritas y su ausencia conllevará la imposibilidad de mantener la relación deseada con la Organización.
	Los datos se conservarán mientras se mantenga la relación y, una vez extinguida, durante el plazo previsto de prescripción de las acciones que resulten de aplicación.
Destinatarios de cesiones y transferencias internacionales de datos	▪ Entidades subvencionadoras con la finalidad de justificar que se ha llevado a cabo una selección. ▪ Otras ONG con la finalidad de compartir datos de proveedores que facilitan la provisión de ciertos bienes y servicios. ▪ Otras sedes de la organización, así como los países en que las mismas intervienen con la finalidad de compartir datos de proveedores que facilitan la provisión de ciertos bienes y servicios. Sólo se comunicarán los datos necesarios para el cumplimiento de estas finalidades.
	Sus datos podrán ser transferidos a los países donde todas las sedes de la Organización desarrollen sus operaciones y/o donde otras ONG desarrollen sus operaciones, así como las entidades subvencionadoras. Alguno de estos países podría no ofrecer un nivel de protección de los datos equiparable a la normativa europea. Se trata de un requisito previo para poder participar en los procedimientos de aprovisionamiento de la Organización, debido a la naturaleza internacional de la misma y del procedimiento de aprovisionamiento.
	No se prevén otras transferencias internacionales de los datos.
Derechos de los interesados	Puede ejercitar sus derechos de acceso, rectificación, supresión, portabilidad y la limitación u oposición dirigiéndose por escrito a la dirección de correo electrónico procurement@accioncontraelhambre.org
	Tiene derecho a reclamar ante la Autoridad de Control (Agencia Española de Protección de Datos: www.agpd.es).

CUESTIONARIO DE EVALUACIÓN DE EMPRESA PROVEEDORA

CUESTIONARIO DE EVALUACIÓN DE ENCARGADO DE TRATAMIENTO

Nombre del Proveedor	NIF
Datos de contacto para protección de datos	
Nombre:	Departamento:
e-mail:	Teléfono:
Descripción de los servicios a prestar	

¿Dónde y cómo se va a realizar el tratamiento de datos?
☐ En las instalaciones y con los sistemas de información del proveedor.
☐ En las instalaciones y con los sistemas de información de la entidad.
☐ En acceso remoto a los sistemas de información de la entidad.

¿Se van a tratar categorías especiales de datos? (Datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.)
☐SI ☐NO

N.º	Aspecto evaluado	SI/NO	Observaciones/evidencias
1	Sistema de gestión de protección de datos y seguridad de la información.		
1a	¿Se ha comunicado al personal su funciones y obligaciones respecto al tratamiento de datos personales?		
1b	¿Se dispone de políticas de uso de recursos (correo electrónico, internet…)?		

1c	¿Se dispone de un sistema de control de acceso a la información mediante identificadores inequívocos y robustos, con perfiles de acceso y cambio periódico?		
1d	¿Se dispone de un sistema de control de acceso físico a instalaciones?		
1e	¿Se dispone de software de seguridad (antivirus, firewall, antimalware…)?		
1f	¿Se dispone de un procedimiento de gestión de soportes?		
1g	¿Se dispone de un procedimiento de copias de seguridad?		
1h	¿Se dispone de un procedimiento de encriptado de comunicaciones y de terminales portátiles?		
1i	¿Se dispone de un plan de contingencias?		

1j	¿Se dispone de un procedimiento de controles periódicos/auditorías/evaluaciones de impacto?		
1k	¿Se dispone de un procedimiento de tratamiento, archivo y almacenamiento de documentación en papel?		
2	¿Los trabajadores y personal externo que participan en el tratamiento han recibido formación en protección de datos?		
3	¿Los trabajadores y personal externo que participan en el tratamiento han firmado un compromiso de confidencialidad?		
4	¿Se dispone de Delegado de Protección de Datos o figura similar en caso de que no sea obligatorio su nombramiento?		
5	¿Se dispone de un sistema de gestión de incidentes de seguridad de protección de datos, incluido el procedimiento de notificación de violaciones de seguridad al interesado/responsable?		
6	¿Se dispone de un Registro de Actividades de Tratamiento?		

7	¿Se dispone de un procedimiento de subcontratación, incluyendo evaluación del subcontratista y contrato?		
8	¿Se dispone de un procedimiento de atención de ejercicio de derechos de los interesados?		
9	¿Se dispone de un procedimiento de tratamiento de datos a la finalización del servicio (devolución, destrucción o traspaso a otro proveedor)?		
10	¿El proveedor está adherido a un Código de Conducta?		
11	¿Se dispone de una Certificación en Protección de Datos?		
12	¿Se dispone de una Certificación en Seguridad de la Información (ISO o similares)?		

13	Mejoras aportadas /otras medidas informadas por el proveedor

Se le informa de que sus datos personales, así como los que se deriven de la relación comercial, serán tratados con la finalidad de mantenimiento de la misma. La base jurídica para el tratamiento de los datos es la correcta ejecución del acuerdo. Dichos datos son necesarios, de tal forma que de no ser facilitados no se podrá crear la relación deseada entre las partes. Los datos se conservarán mientras se mantenga la relación contractual y no se solicite su supresión, y, en cualquier caso, en cumplimiento de plazos legales de prescripción que le resulten de aplicación. No están previstas cesiones ni transferencias internacionales de sus datos, salvo obligación legal. Podrá ejercitar sus derechos de acceso, rectificación, supresión, portabilidad y la limitación u oposición dirigiéndose por escrito a la dirección del Responsable del Tratamiento (pdatos.tic@accioncontraelhambre.org). Asimismo, tiene derecho a reclamar ante la Autoridad de Control (Agencia Española de Protección de Datos: www.agpd.es).

Datos del Responsable del Tratamiento: ACCIÓN CONTRA EL HAMBRE; NIF: G-81164105; Calle Duque de Sevilla, nº 3, 28002 de Madrid; + 34 91 391 53 00.

****

A rellenar por acción contra el Hambre

Cuestionario realizado por:	
Nombre:	Departamento:
e-mail:	Fecha:
Resultado de la evaluación:	
¿Procede la contratación?	
☐SI ☐NO	
Cuestionario validado por (Comité de Protección de Datos o un miembro de éste) *(sólo se exige esta validación cuando se traten datos de categoría especial o, cuando el proveedor no esté establecido en la UE o en países que ofrecen protección equiparable y no se trate de contrataciones de evaluadores y/o consultores de proyectos.)*	
Nombre:	Departamento:
e-mail:	Fecha:
Firma	