NORI ZUZENDUA: CYBERZAINTZA, EUSKAL ZIBERSEGURTASUNAREN AGENTZIA

DIRIGIDO A: CYBERZAINTZA, AGENCIA VASCA DE CIBERSEGURIDAD

IZAPIDE MOTA / TIPO DE TRÁMITE

☐ Zibersegurtasuneko babeserako berariazko datuen fitxari alta ematea. / Alta ficha datos específicos para la protección en ciberseguridad.

☐ Zibersegurtasuneko babeserako berariazko datuen fitxa aldatzea. / Modificación ficha datos específicos para la protección en ciberseguridad.

IDENTIFIKATZE / IDENTIFICACIÓN

Establezimenduaren izena / Nombre del establecimiento	
Helbidea / Dirección	

KONTAKTU-PUNTUA INTZIDENTE ETA ALERTETARAKO / PUNTO DE CONTACTO PARA INCIDENTES Y ALERTAS

Erakundearen intzidenteak eta zibersegurtasun-alertak jakinarazteko harremanetarako gune arduraduna. / Punto de contacto responsable de la notificación de incidentes y alertas de ciberseguridad de la organización	
Izena / Nombre	
e-mail	
Tel	

Kontaktu sekundarioa, kontaktu-puntu nagusia falta bada. / Contacto secundario en caso de ausencia del punto de contacto principal	
Izena / Nombre	
e-mail	
Tel	

APLIKATUTAKO SEGURTASUN-KONTROLAK / CONTROLES DE SEGURIDAD APLICADOS

Honako hauek baditu adierazi / Se indicará si dispone de:

☐ Informazioaren segurtasunari buruzko politika orokorra.

Política general de seguridad de la información.

Informazioaren segurtasunari buruzko politika espezifikoak. / Políticas específicas de seguridad de la información.

☐ Eguneratzeak kudeatzeko politika espezifikoa.

Política específica de gestión de actualizaciones.

☐ Pasahitzak kudeatzeko politika espezifikoa.

Política específica de gestión de contraseñas.

☐ Hornitzaileekiko harremanetarako informazioaren segurtasunari buruzko politika espezifikoa.

Política específica ca de seguridad de la información para las relaciones con proveedores.

☐ Kalteberatasun teknikoak kudeatzea.

Gestión de las vulnerabilidades técnicas.

☐ Informazioaren eta lotutako beste aktiboen inbentarioa: aktiboen identifikazioa.

Inventario de información y otros activos asociados: identificación de los activos.

☐ Babes edo segurtasun kopiak (backup).

Copias de respaldo o de seguridad (backup).

☐ Programa maltzurren aurka babesteko mekanismoak. (antibirusa, EDR, etab.).

Mecanismos de protección contra programas maliciosos. (Antivirus, EDR, etc.).

☐ Posta elektronikoa babesteko mekanismoak.

Mecanismos de protección de correo.

☐ Sarea segmentatzeko mekanismoak.

Mecanismos de segmentación de red.

☐ Sarea kontrolatzeko mekanismoak (Firewall, IDS, IPS, NAC, etab.).

Mecanismos de control de red (Firewall, IDS, IPS, NAC, etc.).

☐ Urruneko sarbide mekanismoak (VPN, urruneko mahaigaina, etab.).

Mecanismos de acceso remoto (VPN, escritorio remoto, etc.).

☐ Aplikazioen segurtasun-mekanismoak (WAF, APIen segurtasuna, etab.).

Mecanismos de seguridad de aplicaciones (WAF, seguridad de API, etc.).

☐ Faktore anitzeko autentifikazio-mekanismoak.

Mecanismos de autenticación multi-factor.

☐ Segurtasun-auditoretza teknikoak.

Auditorías técnicas de seguridad.

Segurtasuneko azken auditoria teknikoaren data. / Fecha de la última auditoría técnica de seguridad. __/__/____

☐ Erakundeko langileak zibersegurtasunaren arloan kontzientziatzea.

Concienciación al personal de la organización en materia de ciberseguridad.

Langileak zibersegurtasun inguruan kontzientziatzeko azken ekimenaren data: / Fecha de la última iniciativa de concienciación al personal en materia de ciberseguridad. __/__/____

☐ Zibersegurtasuneko intzidentea kudeatzeko ariketa edo simulazioa.

Ejercicio o simulacro de gestión de incidente de ciberseguridad.

Zibersegurtasuneko intzidentea kudeatzeko azken ariketaren edo simulazioaren data. / Fecha del último ejercicio o simulacro de gestión de incidente de ciberseguridad. __/__/____

☐ Erreferentziazko hornitzaile bat zibersegurtasun intzidenteei erantzuteko.

Un proveedor de referencia en materia de respuesta a incidentes de ciberseguridad.

DATA ETA SINADURA / FECHA Y FIRMA