ANEXO I

**FORMULARIO DE NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD DE UN PRESTADOR DE SERVICIOS DE CONFIANZA CUALIFICADO Y NO CUALIFICADO**

**FOR-ICPP-03**

**Versión 1.0**

**CONTROL DOCUMENTAL**

| **Documento** | |
| --- | --- |
| **Título:** Formulario de notificación de incidentes de seguridad de un prestador de servicios de confianza cualificado y no cualificado | **Nombre Archivo:**  FOR-ICPP-03 Vers 1.0 |
| **Código:** FOR-ICPP-03 | **Soporte Lógico:** https://www.acraiz.gov.py/ |
| **Fecha:** 06 / 10 /2022 | **Versión:** 1.0 |

| **Registro de cambios** | | |
| --- | --- | --- |
| **Versión** | **Fecha** | **Motivo de cambio** |
| 1.0 | 06 / 10 /2022 | ‘Versión inicial |

| **Distribución del documento** |
| --- |
| Ministerio de Industria y Comercio (MIC) |
| Prestadores de Servicios de Confianza (PSC) |
| Documento Público |

| **Control del documento** | |
| --- | --- |
| **Elaborado por: LUJAN OJEDA** |  |
| **Verificado por: JENNY RUÍZ DÍAZ** |  |
| **Aprobado por: LUCAS SOTOMAYOR** |  |

| **FORMULARIO DE NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD DE UN PRESTADOR DE SERVICIOS DE CONFIANZA CUALIFICADO Y NO CUALIFICADO** |
| --- |

**PRESTADOR DE SERVICIOS DE CONFIANZA**

| **DATOS DEL PRESTADOR** | |
| --- | --- |
| NOMBRE/RAZÓN SOCIAL: | |
| RUC: | |
| DOMICILIO: | |
| CIUDAD: | |
| NOMBRE DE DOMINIO DE INTERNET: | |
| CORREO ELECTRÓNICO: | |

| **DATOS DE LOS SERVICIOS AFECTADOS** | | |
| --- | --- | --- |
| Tipo del servicio | Cualificado | Nombre de los servicios |
|  |  |  |

| **DATOS DEL INCIDENTE** | |
| --- | --- |
| *Descripción del incidente* | |
|  | |

| **IMPACTO DEL INCIDENTE DE SEGURIDAD** | |
| --- | --- |
| Número total de usuarios |  |
| Número de usuarios afectados |  |
| Fecha y hora del incidente |  |
| Duración del incidente (en horas) |  |
| Duración de indisponibilidad del servicio (si aplica) |  |

| **IMPACTO EN DATOS PERSONALES** | |
| --- | --- |
| Descripción | |
|  | |

| **CAUSAS** | | |
| --- | --- | --- |
| ***Categoría*** | | **Marcar con una X** |
| *Error humano* | |  |
| *Fallo en los sistemas* | |  |
| *Desastre natural* | |  |
| Acciones maliciosas | |  |
| Fallos de terceros | |  |
| **Causa concreta** | | **Marcar con una X** |
| Ataque de denegación de servicio | |  |
| Software malicioso y virus | |  |
| Robo o pérdida de equipos | |  |
| Robo o pérdida de datos | |  |
| Corte de corriente | |  |
| Fallo de hardware | |  |
| Error de software | |  |
| Cambio/actualización defectuosa de hardware | |  |
| Cambio/actualización defectuosa de software | |  |
| Alteración de datos personales | |  |
| Escuchas | |  |
| Criptoanálisis | |  |
| Sobrecarga | |  |
| Error de política o procedimiento | |  |
| Apagado por razones de seguridad | |  |
| Otra, en este caso indicar cuál | |  |

| ***Detalle de la causa*** | |
| --- | --- |
| ***Descripción*** | |
|  | |

| **ACTIVOS AFECTADOS** | **NIVEL** | **MARCAR CON UNA X** | | |
| --- | --- | --- | --- | --- |
| Tipo de activo | Impacto (\*) | Confidencialidad | Integridad | Disponibilidad |
| Plataforma de la AC |  |  |  |  |
| Plataforma de la AV |  |  |  |  |
| Plataforma de Sello de tiempo |  |  |  |  |
| Plataforma de AR |  |  |  |  |
| Plataforma de generación de firma/sello |  |  |  |  |
| Plataforma de validación de firma/sello |  |  |  |  |
| Plataforma de conservación de firma/sello |  |  |  |  |
| Plataforma de servicio de entrega electrónica |  |  |  |  |
| Plataforma de red |  |  |  |  |
| Archivo |  |  |  |  |
| Hardware |  |  |  |  |
| Software |  |  |  |  |

(\*) Deberá indicarse si el impacto corresponde a un nivel bajo, medio o alto

| **SEVERIDAD DEL INCIDENTE SEGÚN EL ESCENARIO** | | **MARCAR CON UNA X** |
| --- | --- | --- |
| *Escenarios (severidad)* | |  |
| *GENÉRICOS:* | |  |
| *Autenticación. ataque por diccionario/phishing/escucha/duplicación/secuestro de sesión/hombre en medio* | |  |
| *Impacto en plataforma software* | |  |
| *Impacto en plataforma hardware* | |  |
| *Compromiso de claves privadas* | |  |
| *Uso inadecuado de algoritmos* | |  |
| *Uso no intencionado de certificados para otros propósitos* | |  |
| *Compromiso de dispositivo de almacenamiento de claves* | |  |
| *Compromiso de datos personales y/o logs* | |  |
| *Compromiso de red* | |  |
| *Compromiso de herramientas o plataforma de soporte* | |  |
| *ESPECÍFICOS POR SERVICIO* | |  |
| Certificados. Registro. Impersonación/repudio | |  |
| Certificados. Emisión. Divulgación/alteración/emisión no autorizada | |  |
| Certificados. Dispositivos. robo/descubrimiento/duplicación/escucha/cracking/phishing/ingeniería social | |  |
| Certificados. Almacenamiento de credenciales. divulgación/alteración/duplicación | |  |
| Certificados. Servicios de verificación. divulgación/alteración/ no disponibilidad | |  |
| Certificados. Servicios de emisión, revocación y reemisión. divulgación/alteración/acceso no autorizado/debilidad del protocolo | |  |
| Certificados. Servicios de revocación y destrucción. retrasos/uso tras desmantelamiento | |  |
| Validación. respuesta incorrecta | |  |
| Validación. inconsistencia entre CRL y OSP/Ataque de reproducción/ no disponibilidad | |  |
| Sellos de tiempo. no sincronización | |  |
| Sellos de tiempo. sesgo de reloj/sellado de tiempo local | |  |
| Sellos de tiempo. no disponibilidad/emisión fraudulenta | |  |
| Entrega electrónica certificada. no disponibilidad | |  |
| Entrega electrónica certificada. evidencias incorrectas/ dirección de envío incorrecta/almacenamiento deficiente/ evidencia no entregada | |  |
| Firma/sello. no disponibilidad/respuesta incorrecta/ no sincronización | |  |
| Verificación de firma/sello. Creación incorrecta | |  |
| Verificación de firma/sello. No disponibilidad/respuesta incorrecta/ no sincronización | |  |
| Verificación de firma/sello. Validación incorrecta | |  |
| Verificación de firma/sello. tiempos largos de respuesta | |  |
| Preservación. No disponibilidad/derechos de acceso/integridad de los datos/formatos de los datos | |  |
| Preservación. validación incorrecta de firmas/sellos | |  |
| Otro, especificar | | |

| **ACCIONES. DESCRIPCIÓN** | | |
| --- | --- | --- |
| Medidas tomadas para mitigar el incidente | | |
|  | | |
| Medidas tomadas o planeadas para evitar incidentes similares | | |
|  | | |

| **NOTIFICACIONES ADICIONALES EFECTUADAS POR EL PRESTADOR** | |
| --- | --- |
|  | |

| **OBSERVACIONES** | |
| --- | --- |
|  | |

**Consideraciones generales:**

* De corresponder la presentación, todos los documentos deberán ser adjuntados en formato PDF, firmados con firma electrónica cualificada del representante legal o representante debidamente autorizado y remitirse vía correo electrónico a la dirección de correo institucional [info-dgce@mic.gov.py](mailto:info-dgce@mic.gov.py).
* Los documentos reproducidos al formato electrónico deberán presentarse correctamente digitalizados y legibles