ó



# RESPUESTAS ANTE INCIDENTES DE SEGURIDAD DIGITAL EN EL PROGRAMA NACIONAL DE ASISTENCIA SOLIDARIA "PENSIÓN 65"

Instructivo N°002-2024-PENSIÓN65

Versión N° 1

Aprobado mediante Resolución de Dirección Ejecutiva N° D000055-2024-MIDIS/P65-DE

| Etapa | Responsable | Cargo | Visto Bueno y sello: |
|---|---|---|---|
| Formulado por: | Daniel Torres Marquina | Jefe(a) de la Unidad de Tecnologías de la Información | Firmado digitalmente por TORRES MARQUINA Juan Daniel FAU 20547960051 soft<br>Motivo: Soy el autor del documento<br>Fecha: 28.05.2024 15:14:19 -05:00<br>Fecha: |
| Revisado por: | Raquel Gutiérrez Sánchez | Jefe(a) de la Unidad de Planeamiento, Presupuesto y Modernización | Firmado digitalmente por GUTIERREZ SANCHEZ Raquel Esther FAU 20547960051 hard<br>Motivo: Soy el autor del documento<br>Fecha: 28.05.2024 16:24:02 -05:00<br>Fecha: |
| | Hugo Aliaga Gastelumendi | Jefe(a) de la Unidad de Asesoría Jurídica | Firmado digitalmente por ALIAGA GASTELUMENDI Hugo Armando FAU 20547960051 soft<br>Motivo: Soy el autor del documento<br>Fecha: 28.05.2024 17:31:12 -05:00<br>Fecha: |
| Aprobado por: | Julio Mendigure Fernández | Director(a) Ejecutivo(a) | Firmado digitalmente por MENDIGURE FERNANDEZ Julio FAU 20547960051 soft<br>Motivo: Soy el autor del documento<br>Fecha: 28.05.2024 17:46:19 -05:00<br>Fecha: |

## HOJA DE CONTROL DE CAMBIOS

| Versión | Fecha | Documento sustento | Textos modificados | Responsable |
|---|---|---|---|---|
| 01 | 23/04/2024 | INFORME NºD00084-2024-MIDIS/P65-UTI | Documento inicial | Unidad de Tecnologías de la Información |
| | | | | |
| .. | | | | |
| … | | | | |
| … | | | | |
| | | | | |

Notas:

1/ Señalar el informe que sustenta la formulación del documento normativo y/o el informe que sustenta la modificación de la nueva versión del documento.
2/ Señalar los artículos, numerales, literales, anexos, etc. que genera la modificación del documento.
3/ Señalar la unidad de organización que formula la nueva versión del documento.

# RESPUESTAS ANTE INCIDENTES DE SEGURIDAD DIGITAL EN EL PROGRAMA NACIONAL DE ASISTENCIA SOLIDARIA "PENSIÓN 65"

## INDICE

| | |
|---|---|
| **1.** | **OBJETIVO** |
| | Establecer actividades para la respuesta efectiva ante incidentes de seguridad digital que comprometan la operatividad de los sistemas y servicios del Programa, a través de la contención y/o recuperación de la información en el marco de la ciberseguridad. |
| **2.** | **ÁMBITO DE APLICACIÓN** |
| | El presente documento es de cumplimiento del Equipo de Respuestas ante incidentes de seguridad digital (CSIRT) de la Unidad de Tecnologías de la Información. |
| **3.** | **BASE LEGAL** |
| 3.1 | Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado. |
| 3.2 | Ley N° 27444, Ley del Procedimiento Administrativo General. |
| 3.3 | Ley N° 29733, Ley de Protección de Datos Personales. |
| 3.4 | Ley Nº 30096 Delitos Informáticos. |
| 3.5 | Ley 27269, Ley de Firmas y Certificados Digitales y su reglamento según Decreto Supremo Nº052-2008-PCM. |
| 3.6 | Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital. |
| 3.7 | Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo. |
| 3.8 | Decreto Supremo N° 081-2011-PCM, que crea el Programa Nacional de Asistencia Solidaria "Pensión 65" y modificatorias. |
| 3.9 | Decreto Supremo N° 103-2022-PCM, que aprueba la Política Nacional de Modernización de la Gestión Pública al 2030. |
| 3.10 | Resolución Ministerial N° 273-2017-MIDIS, que aprueba el Manual de Operaciones del Programa Nacional de Asistencia Solidaria "Pensión 65". |
| 3.11 | Resolución Ministerial N° 002-2021-MIDIS, aprueba los Lineamientos de Seguridad de la Información del MIDIS. |
| 3.12 | Resolución Ministerial Nº 004-2016-PCM. Aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2º Edición", en todas las entidades integrantes del Sistema Nacional de Informática. |
| 3.13 | Resolución de Dirección Ejecutiva N° 000179-2023-MIDIS/P65-DE, que aprueba la conformación del Equipo de Respuestas a Incidentes de Seguridad Digital del Programa Nacional de Asistencia Solidaria "Pensión 65" que forma parte de la Oficina de Tecnologías de la Información. |
| **4.** | **DOCUMENTOS DE REFERENCIA** |
| 4.1 | Política de Seguridad de la Información – Pensión 65<br><br>La información contenida en el presente documento se alinea a la Política de Seguridad de la Información, basada en la NTP ISO/IEC 27001:2014; por lo que su uso estará sujeto a las condiciones de Confidencialidad, Integridad y Disponibilidad de la información utilizada para los procesos que el presente documento contenga. |
| 4.2 | Protección de datos personales<br><br>La información de datos personales que se utilice como insumo y/o se genere como parte del proceso en el presente documento se alinea a lo dispuesto en la Ley Nº29733 Ley de Protección de Datos Personales, por lo que su uso, manejo y disposición estará sujeto a las |

| | |
|---|---|
| | condiciones de Confidencialidad, Integridad y Disponibilidad de los datos personales utilizados. |
| **5.** | **DEFINICIONES Y/O ABREVIATURAS** |
| **5.1** | **ABREVIATURAS** |
| 5.1.1 | **UTI**: Unidad de Tecnologías de la Información. |
| 5.1.2 | **CNSD:** Centro Nacional de Seguridad Digital |
| 5.1.3 | **CSIRT** - **Computer Security Incident Response Team**: Equipo de Respuestas a Incidentes de Seguridad Digital del Programa Nacional de Asistencia Solidaria "Pensión 65". |
| **5.2** | **DEFINICIONES** |
| 5.2.1 | **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. |
| 5.2.2 | **Ataque:** Intento de destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo. |
| 5.2.3 | **Ataque cibernético o ciberataque:** Es un intento deliberado de acceder, dañar, robar o destruir información o sistemas informáticos mediante el uso de tecnología y recursos digitales. Estos ataques pueden ser llevados a cabo por individuos malintencionados, grupos organizados, o incluso entidades estatales con diversos objetivos, que pueden incluir el robo de datos, el sabotaje, el espionaje, el fraude financiero, el secuestro de datos (ransomware), entre otros. |
| 5.2.4 | **Autenticación:** Garantía de que una característica reivindicada de una entidad es correcta. |
| 5.2.5 | **Centro Nacional de Seguridad Digital:** Gestiona, dirige, articula y supervisa la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital a nivel nacional como componente integrante de la seguridad nacional, a fin de fortalecer la confianza digital. |
| 5.2.6 | **Ciberamenaza (o amenaza cibernética):** Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar un ciberataque. |
| 5.2.7 | **Ciberseguridad:** Es el conjunto de políticas, conceptos de seguridad, recursos, controles de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, buenas prácticas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio. |
| 5.2.8 | **Colaboradores:** Son los servidores civiles, funcionarios, servicios de terceros, proveedores de servicio del Programa Nacional de Asistencia Solidaria "Pensión 65". |
| 5.2.9 | **Confiabilidad:** Propiedad de la conducta y resultados esperados consistentes. |
| 5.2.10 | **Confidencialidad:** Propiedad por la que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados. |
| 5.2.11 | **Consecuencia:** Resultado de un evento que afecta a los objetivos. |
| 5.2.12 | **Equipo de Respuesta ante Incidentes de Seguridad Digital:** Es un equipo técnico conformado principalmente por especialistas en seguridad de las tecnologías de la información o informática, responsable de la gestión de incidentes de seguridad digital que afectan los activos de una entidad pública o una red de confianza.<br>El Equipo es denominado como CSIRT de acuerdo al numeral 2.9 de la Guía para la Conformación e Implementación de Equipos de Respuestas ante Incidentes de Seguridad Digital, conforme a lo establecido en el Decreto Supremo N° 029-2021-PCM, |
| 5.2.13 | **Incidente de Seguridad de la Información:** Un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información. |
| 5.2.14 | **Incidente de Seguridad digital:** Ocurrencia de una situación que tiene posibles implicaciones de seguridad potenciales para el sistema, la información o su entorno y que puede requerir una acción adicional (monitorear, investigar o reaccionar). |

| | |
|---|---|
| 5.2.15 | **Mesa de Ayuda:** Es el punto de contacto inicial con los colaboradores, quienes hayan identificado o tengan sospecha de un incidente de seguridad digital. Es el responsable de informar lo reportado por los colaboradores a todo el equipo de CSIRT. |
| 5.2.16 | **No repudio:** Capacidad para demostrar la ocurrencia de un evento o acción reclamada y sus entidades de origen. |
| 5.2.17 | **Phishing:** es un tipo de estafa de ingeniería social que implica engañar a las personas para que compartan información confidencial o instalen malware. Los estafadores utilizan el phishing para engañar a las personas para que les proporcionen información personal y financiera, como números de cuentas bancarias.<br>Las víctimas reciben un mensaje de correo electrónico o un mensaje de texto que imita (o "suplanta su identidad") a una persona u organización de confianza, como un compañero de trabajo, un banco o una oficina de gobierno. |
| 5.2.18 | **Playbook de ciberseguridad:** Es un conjunto de herramientas, condiciones, lógica empresarial, flujos y tareas que se utilizan para responder a sucesos y amenazas de seguridad. |
| 5.2.19 | **Ransomware:** Es un tipo de malware (software malicioso, cualquier programa o archivo que sea intencionalmente dañino para una computadora, servidor, cliente o red), que cifra los datos de una organización y luego exige un rescate a la empresa para desbloquear los archivos cifrados. |
| 5.2.20 | **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información. Además, hay que considerar otras propiedades, como la autenticidad, la responsabilidad, el no repudio y la confiabilidad también pueden estar involucrados. |
| 5.2.21 | **Seguridad Digital:** En concordancia con el Decreto Supremo N° 050-2018-PCM, la Seguridad Digital en el ámbito nacional es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. |
| 5.2.22 | **SIEM** (Security Information and Event Management o la información sobre seguridad y gestión de eventos): Es una solución de seguridad que ayuda a las organizaciones a reconocer posibles amenazas y vulnerabilidades de seguridad antes de que tengan la oportunidad de interrumpir las operaciones comerciales. |
| 5.2.23 | **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotado por una o más amenazas. |
| **6.** | **DESARROLLO** |
| 6.1 | **Conformación del CSIRT** |
| 6.1.1 | El equipo del CSIRT, se conforma de acuerdo a la Resolución de Dirección Ejecutiva N° 000179-2023-MIDIS/P65-DE. |
| 6.2 | **Responsabilidades** |
| 6.2.1 | Las Responsabilidades del CSIRT se encuentran definidas en el Anexo N° 01 "Responsabilidades del equipo CSIRT". |
| 6.3 | **Disponibilidad** |
| 6.3.1 | El CSIRT se encuentra disponible en horario de Oficina 8:30 am a 5:30 pm, de lunes a viernes, y posterior al horario de Oficina en caso de que el incidente comprometa las operaciones, servicios y/o sistemas del Programa. |
| 6.4 | **Respuestas a Incidentes de seguridad digital** |
| | El proceso de la respuesta a incidentes de seguridad digital cuenta con las siguientes etapas:<br>a) Preparación<br>b) Identificación.<br>c) Contención y recuperación<br>d) Post – Incidente |

| | |
|---|---|
| 6.4.1 | La etapa a), se encuentra desarrollada en el numeral 6.6 como acciones previas importantes como medida de prevención.<br>Las etapas b), c) y d), se encuentran desarrolladas en el numeral 6.7, que se ha desarrollado como el Flujo de atención de incidentes de seguridad digital del CSIRT. |
| 6.5 | **Lecciones aprendidas** |
| 6.5.1 | Posterior a un ciberataque, es necesario realizar el análisis del incidente ocurrido independientemente de su gravedad y las interrupciones ocasionadas.<br><br>Para ello el/a Coordinador/a del CSIRT, convocará a reunión al equipo CSIRT y demás partes involucradas y relevantes del programa.<br>Procederán a revisar los factores que han condicionado el ataque (ejemplo: falta de actualización de los sistemas, etc.), al igual que aquellos que han funcionado correctamente y han evitado un mayor impacto del ataque ocurrido. A fin de mejorar la respuesta y reducir las posibles vías de entrada ante futuros ataques, pudiendo disminuir el tiempo de respuesta ante los mismos y corregir errores presentes en la estructura del programa. |
| 6.6 | **Preparación** |
| 6.6.1 | El/la Gestor/a de Infraestructura, Redes, y Base de Datos (CSIRT), realiza actividades para prevenir incidentes de seguridad digital como se indica a continuación:<br><br>✓ Realizar el monitoreo de la conectividad y recursos de los servidores, antivirus, equipos de comunicación y de seguridad.<br>✓ Implementar y/o coordinar la implementación de herramientas de correlación de eventos (SIEM) que permitan detectar y monitorear eventos de seguridad que pueden convertirse en incidentes.<br>✓ Realizar o coordinar el monitoreo de eventos que ocurran en los equipos de seguridad (eventos de los servidores, equipos de comunicación, entre otros disponibles).<br>✓ Mantener actualizados los parches de seguridad de los sistemas operativos y software de los equipos de comunicación, de seguridad y servidores. Para ello debe considerar las vulnerabilidades que hayan sido identificadas, como por ejemplo vulnerabilidades en los sistemas o aplicaciones web que se encuentren publicadas, entre otras detectadas.<br>✓ Mantener actualizado el antivirus en los equipos de cómputo y servidores, con las firmas de actualización al día.<br>✓ Coordinar la actualización de los sistemas de información con el personal de desarrollo de sistemas.<br>✓ Mantener actualizadas las licencias de los equipos de seguridad.<br>✓ Realizar el respaldo de la información y de las máquinas virtuales críticas.<br>✓ En coordinación con soporte tecnológico, mantener las actualizaciones de parches en equipos de cómputo.<br>✓ Mantener actualizado el inventario de los servidores, equipos de comunicación, de seguridad, UPS.<br><br>En caso de que existan inconvenientes para la realización de las actividades precedentes, debe emitir un informe detallado al/a la Jefe/a de la UTI para que proceda con las acciones que correspondan. |
| 6.6.2 | El/La Oficial de Seguridad y Confianza Digital, realiza las siguientes actividades como se indica a continuación:<br><br>✓ Coordinar con las unidades correspondientes, la sensibilización y capacitación a los usuarios de la entidad, los cuales incluyen:<br>- Personal Técnico: Al personal de UTI (Especialista de infraestructura, analistas y programadores, etc.), los cuales deben ser entrenados respecto a los temas técnicos |

| | | |
|---|---|---|
| | | en ciberseguridad, sistemas y servicios tecnológicos que deban asegurarse ante eventos que puedan comprometer las operaciones de la entidad.<br>- Usuarios y proveedores de servicio: A los usuarios (trabajadores bajo cualquier modalidad de contratación), a los proveedores bajo contrato, deben ser sensibilizados de acuerdo con las políticas y procedimientos de seguridad del programa, y respecto a las responsabilidades y uso apropiado de los servicios y sistemas de tecnologías de la información.<br>✓ Coordinar la realización de análisis de vulnerabilidad o Ethical Hacking o similares, a la infraestructura tecnológica del Programa.<br>✓ Realizar una revisión diaria de los boletines de seguridad periódicos que publica el Centro Nacional de Seguridad Digital, así como otras empresas tecnológicas donde se evalúan las amenazas observadas y recomendaciones de mitigación. Y en caso sea necesario, informar al CSIRT.<br>✓ Coordinar simulacros y ejercicios periódicos de ataques cibernéticos que puedan presentarse.<br>✓ Mantener actualizado el Instructivo considerando ciberataques más comunes o actuales. |
| 6.7 | **Flujo de atención de incidentes de seguridad digital del CSIRT** | |
| 6.7.1 | **Identificación** | |
| 6.7.1.1 | Gestor/a de Infraestructura, Redes, y Base de Datos (CSIRT) | Identificar la criticidad e impacto del Incidente.<br>**¿El incidente es de criticidad Media o Alta (Anexo N° 02)?**<br>Continuar en la actividad 6.7.2.1.<br>Caso contrario, procede a realizar acciones para atender el incidente de criticidad baja y registrar su solución. |
| 6.7.2 | **Contención y recuperación** | |
| 6.7.2.1 | Gestor/a de Infraestructura, Redes, y Base de Datos - CSIRT | Si el incidente es un ataque de Ransomware, iniciar las acciones indicadas en el Anexo N° 03: Playbook de atención frente a ataques de ransomware malware y/o ransomware.<br>Si el incidente es un ataque de Phishing, iniciar las acciones indicadas en el Anexo N° 04: Playbook de atención frente a ataques de Phishing.<br>Si el incidente es la extracción no autorizada de información, iniciar las actividades del Anexo N° 05: Playbook de atención frente a extracción no autorizada de información.<br>Si el incidente es otro tipo de ataque, tomar acción de acuerdo a la experiencia técnica del equipo CSIRT. |
| 6.7.2.2 | Gestor/a de Infraestructura, Redes, y Base de Datos - CSIRT | Reportar el estado del incidente al Oficial de Seguridad y Confianza Digital y Coordinador del CSIRT.<br>**¿El incidente ha sido resuelto?**<br>Si: Continuar en la siguiente actividad.<br>No: Continuar en la actividad 6.7.2.4 |
| 6.7.2.3 | Coordinador/a - CSIRT | **¿Datos personales han sido comprometidos?**<br>Si: Coordinar la comunicación interna con las Unidades de organización pertinentes.<br>No: Continuar en la actividad 6.7.3.1. |
| 6.7.2.4 | Gestor/a de Infraestructura, Redes, y Base de | **¿Requiere apoyo externo?**<br>Si: Continuar en la siguiente actividad.<br>No: Continuar en la actividad 6.7.3.10. |

| | | |
|---|---|---|
| | Datos - CSIRT | |
| 6.7.2.5 | Gestor/a de Infraestructura, Redes, y Base de Datos - CSIRT | Contactar con otros proveedores especializados, el Centro Nacional de Seguridad Digital u otras organizaciones de seguridad del estado peruano que puedan brindar apoyo técnico, y continuar en la actividad 6.7.2.12. |
| 6.7.2.6 | Gestor/a de Infraestructura, Redes, y Base de Datos - CSIRT | Continuar con la recuperación de los servicios, sistemas y continuar en la actividad 6.7.2.2. |
| 6.7.3 | **Post-Incidente** | |
| 6.7.3.1 | Coordinador/a - CSIRT | Comunicar el restablecimiento de los servicios a los colaboradores. |
| 6.7.3.2 | Gestor/a de Infraestructura, Redes, y Base de Datos - CSIRT | Realizar el seguimiento y monitoreo a los servicios y sistemas que fueron comprometidos, a fin de estar alertas a comportamientos anómalos. |
| 6.7.3.3 | Gestor/a de Infraestructura, Redes, y Base de Datos - CSIRT | Realizar el informe técnico detallado del incidente. |
| 6.7.3.4 | Gestor/a de Infraestructura, Redes, y Base de Datos - CSIRT | Subsanar las brechas de seguridad que hayan sido encontradas durante la respuesta al incidente de seguridad.<br><br>**Finalizar actividad.** |
| 6.7.3.5 | Oficial de Seguridad y Confianza Digital y Coordinador - CSIRT | Documentar el incidente coordinando con el/la Gestor/a de Infraestructura, Redes, y Base de Datos - CSIRT. |
| 6.7.3.6 | Oficial de Seguridad y Confianza Digital y Coordinador - CSIRT | Solicitar o coordinar la contratación de un análisis forense de ser necesario para determinar el origen y trazabilidad del incidente. |
| 6.7.3.7 | Oficial de Seguridad y Confianza Digital y Coordinador - CSIRT | Evaluar la oportunidad de mejora, de acuerdo a la respuesta al incidente de seguridad digital.<br><br>**Finalizar actividad.** |
| 7. | **PROCEDIMIENTO RELACIONADO** | |
| 7.1 | Procedimiento "Gestión de Incidentes de Seguridad de la Información en el Programa Nacional de Asistencia Solidaria "Pensión 65". | |
| 8. | **ANEXO** | |
| 8.1 | **Anexo N° 01** Responsabilidades del Equipo de Respuesta ante Incidentes de Seguridad Digital – CSIRT. | |
| 8.2 | **Anexo N° 02** Niveles de Criticidad. | |
| 8.3 | **Anexo N° 03** Playbook de atención frente a ataques de Ransomware. | |

| | |
|---|---|
| 8.4 | **Anexo N° 04** Playbook de atención frente a ataques de Phishing. |
| 8.5 | **Anexo N° 05** Playbook de atención frente a extracción no autorizada de información. |
| 8.6 | **Anexo N° 06** Flujo de atención de incidentes de seguridad digital del CSIRT. |

## Anexo N° 01

Responsabilidades del Equipo de Respuesta ante Incidentes de Seguridad Digital

| Rol o Función | Designado | Responsabilidades |
|---|---|---|
| Coordinador/a del CSIRT | Jefe/a de la Unidad de Tecnologías de la Información | Responsable de supervisar el cumplimiento de las funciones del equipo CSIRT.<br>Asegurar la ejecución de actividades de preparación, contención y recuperación ante incidentes de seguridad digital por parte del equipo CSIRT.<br>Coordinar con las Unidades correspondientes, respecto a las posibles repercusiones a la entidad, en caso de un incidente de seguridad digital que comprometa información sensible, los servicios y/o sistemas de información del Programa.<br>Coordinar con las autoridades internas y externas competentes, acerca de denuncias relacionadas a delitos informáticos que se realicen en el Programa.<br>Realizar reuniones periódicas (cada 20 días) con el equipo de respuesta a incidentes de seguridad digital.<br>Presentar informes a la Dirección Ejecutiva, relacionados a los incidentes de seguridad digital producidos en el Programa y la respuesta ante los mismos.<br>Coordinar con la Dirección Ejecutiva la necesidad de los recursos requerido para el desempeño del CSIRT (como capacitación, software, hardware, etc.) para que se ejecute la respuesta a incidentes de seguridad. |
| Soporte Tecnológico | Soporte Técnico o quien haga sus veces en la Unidad | Informar al equipo de CSIRT, los incidentes de seguridad digital, que sean reportados en la plataforma de mesa de ayuda (https://mesadeayuda.pension65.gob.pe/) por el personal del Programa.<br>Brindar el apoyo técnico al Gestor/a de Infraestructura, Redes, y Base de Datos, en cuanto al restablecimiento de los equipos de cómputo, en caso de corresponder.<br>Otros que le sean asignados por el Coordinador/a del CSIRT. |
| Gestor/a de Infraestructura, Redes, y Base de Datos | Especialista de Infraestructura y Base de Datos | Participar en la remediación del incidente de seguridad digital.<br>Informar al equipo de CSIRT acerca de cualquier debilidad o vulnerabilidad en la infraestructura tecnológica que haya encontrado, que comprometa las operaciones del Programa,<br>Aplicar las reglas de seguridad a nivel de la infraestructura tecnológica (servidores, sistema operativo, redes, etc.), on premise y/o en nube en el Programa.<br>Coordinar con el personal de desarrollo de sistemas de información, de corresponder, para realizar el restablecimiento de los mismos.<br>Coordinar con los proveedores que brindan soporte a la infraestructura tecnológica para su participación, de corresponder, antes, durante y después del incidente de seguridad digital.<br>Preservar las evidencias físicas y/o digitales que correspondan al incidente de seguridad digital.<br>Informar al Coordinador/a del CSIRT, acerca de sus actividades. |
| Oficial de Seguridad y Confianza Digital | Oficial de Seguridad y Confianza Digital | Clasificar y gestionar los incidentes de seguridad digital.<br>Realizar la comunicación del incidente al Centro Nacional de Seguridad Digital.<br>Hacer seguimiento a la remediación del incidente de seguridad digital.<br>Coordinar con el Centro Nacional de Seguridad Digital el apoyo en los incidentes de seguridad digital que se presenten, de corresponder.<br>Hacer seguimiento hasta la solución del incidente de seguridad digital.<br>Registrar los antecedentes, análisis del incidente y su detalle, en coordinación con el Gestor/a de Infraestructura, redes, y Base de Datos.<br>Coordinar capacitaciones relacionadas a ciberseguridad, para el equipo del CSIRT, como mínimo una vez al año. |

## Anexo N° 02

Niveles de Criticidad

| Nivel de Criticidad | Impacto |
|---|---|
| BAJA | No afecta la operatividad de los servicios o sistemas.<br><br>Se puede proceder como se considere de acuerdo con las fallas que se presenten. Quien atienda el incidente, puede realizar acciones como: reiniciar un componente tecnológico o destruir un documento. Así mismo, debe quedar un registro de estos incidentes, como medida de control y seguimiento, que puede ser utilizado posteriormente como base de consulta para la resolución de incidentes futuros.<br><br>Ejemplo: |
| MEDIA | Afecta la operatividad de los servicios o sistemas de una Unidad critica.<br><br>Son trabajos que deben ser realizados por el administrador del equipo, servidor, informando a sus propietarios como reiniciar un servicio de información, realizar cambios en las configuraciones, desconectar la red, reconstruir y recuperar la información, remover privilegios de los usuarios, etc.<br><br>Ejemplo: |
| ALTA | Afecta la operatividad de los servicios o sistemas en el Programa.<br><br>Son trabajos que deben ser realizados por el equipo técnico del CSIRT como:<br>● Reiniciar de manera completa más de un sistema de información.<br>● Desconectar por largos periodos de tiempo un recurso tecnológico para determinar la falla.<br>● Realizar la recuperación de más del 40% de los equipos servidores de los centros de datos.<br><br>Ejemplo: |

## Anexo N° 03:

Playbook de atención frente a ataques de Ransomware

| | |
|---|---|
| 1. | Aislar de la red, desconectando ya sea de manera física o lógica, las interfaces de red (alámbricas o inalámbricas) de los equipos Servidores de producción del Data Center y Endpoints.<br>En caso de que hayan sido afectados equipos de las Unidades Territoriales, coordinar con el personal de la Unidad para apagar los equipos, para su posterior revisión. |
| 2. | Coordinar con los proveedores de seguridad perimetral y antivirus, para verificar la red perimetral y los equipos afectados. Remitir las muestras o evidencias de malware que se puedan recuperar al proveedor de antivirus para su análisis. Todo esto en caso de corresponder. |
| 3. | De ser posible comprobar si el proceso del malware se encuentra en ejecución, pudiendo hacer uso de herramientas como Process Explorer, para finalizar su ejecución.<br><br>Arrancar el equipo en Modo Seguro. Realizar una copia de seguridad (imagen completa del equipo afectado) en un dispositivo de almacenamiento externo aislado, para su custodia.<br>En caso de que en el futuro se libere la clave de cifrado, se realice la recuperación de la información resguardada. |
| 4. | Valorar el escenario. Analizar la situación y el alcance de la infección para poder determinar cuál es el método idóneo de proceder a la hora de restaurar la normalidad de los sistemas informáticos afectados.<br><br>A continuación, se muestran todos los posibles escenarios, ordenados desde el más favorable (en el que se poseen copias de seguridad) hasta el más desfavorable (en el que no se poseen copias de seguridad y no se pueden recuperar los datos de otra forma):<br><br>- Se dispone de backups completos del equipo afectado: Es la situación más favorable, en la que se procederá a limpiar el equipo y después a restaurar la última copia de seguridad.<br>- Existe una herramienta que permite el descifrado: Este escenario ocurrirá normalmente cuando el ransomware no es demasiado reciente y ya ha sido analizado previamente junto con su código. De modo que existe una herramienta que permite descifrar los datos.<br>Los fabricantes de Antivirus y otras organizaciones ponen a disposición, herramientas de descrifrado como https://www.nomoreransom.org/, entre otros.<br>- Se dispone de Shadow Copies. En este caso, para volver a la normalidad, tan solo sería necesario restaurar las copias de seguridad que realiza Windows automáticamente de los ficheros, utilizando Shadow Explorer, por ejemplo. Sin embargo, el ransomware frecuentemente imposibilita esta acción.<br>- Se pueden recuperar los ficheros utilizando software forense. Lo más probable es que no se recupere el 100% de los datos, pero puede ser una forma efectiva de recuperar datos importantes.<br>- Si ninguno de los anteriores es posible, sólo queda conservar los ficheros cifrados para descifrarlos en un futuro. Es posible que en el futuro los ficheros puedan ser descifrados con una herramienta específica. De ser así, este escenario nos devolvería al escenario descrito en el apartado uno. Para poder seguir haciendo uso del equipo afectado, si se diera este escenario, se recomienda tomar las siguientes acciones:<br>  - En primer lugar, clonar el equipo para conservar la información cifrada, siempre de forma aislada.<br>  - En segundo lugar, evaluar la seguridad del equipo para averiguar los motivos por los que se ha infectado.<br>  - Finalmente, si es necesario formatear el equipo y cambiar todas las contraseñas que pudieran estar guardadas, como medida de seguridad.<br><br>- Si formatear no fuese posible, se deberá limpiar el equipo en la medida de lo posible, poniendo especial atención en los posibles ejecutables que hayan originado los procesos o servicios del malware, para evitar así que el ordenador vuelva a ser cifrado. |

## Anexo N° 04: Playbook de atención frente a ataques de Phishing

| | |
|---|---|
| 1. | Identificar el ataque de Phishing:<br>• Correos falsificados;<br>• Correos electrónicos desconocidos con enlaces a URL externas;<br>• Correos electrónicos que no se pueden reenviar;<br>• Correos electrónicos sospechosos, notificados por usuarios, internos, externos. |
| 2. | Informar a los colaboradores internos y/o externos de corresponder, para que no reenvíen o abran el correo remitido. |
| 3. | Identificar el alcance del ataque, ¿Quiénes recibieron el correo?, ¿Qué activos se han visto afectados? ¿Cuántas cuentas de correo han sido comprometidas? |
| 4. | Cambiar las contraseñas de los correos afectados en coordinación con los colaboradores. |
| 5. | Bloquear el correo original que envió el Phishing |
| 6. | En caso de que exista pérdida o vulneración de datos, iniciar las actividades del Anexo N° 05. |
| 7. | En caso de que exista activos afectados, al haber recibido un correo con malware y haberlo descargado, se debe identificar que sistemas o activos de información se han visto afectados, asegurar las copias para el análisis forense o evaluación posterior.<br>Iniciar la restauración de los sistemas o servicios.<br>En caso de que se haya identificado un ransomware, iniciar las actividades del Anexo N° 03. |
| 8. | Recopilar más información relacionada al incidente.<br>Identificar la IP de origen del envío del correo electrónico.<br>Evaluar si la IP puede ser bloqueada. |
| 9. | Preservar toda la evidencia para revisión y toma de acciones legales anticipadas de corresponder. |
| 10. | Bloquear el acceso a cualquier herramienta de acceso remoto (RAT) |
| 11. | En caso de que hayan remitido un link adjunto en el correo de Phishing, realizar pruebas en un ambiente controlado. |
| 12. | Monitorear para detectar actividades sospechosas. |
| 13. | Denunciar el caso del incidente a la DIVINDAT (División de Investigación de Delitos de Alta Tecnología), según corresponda. |

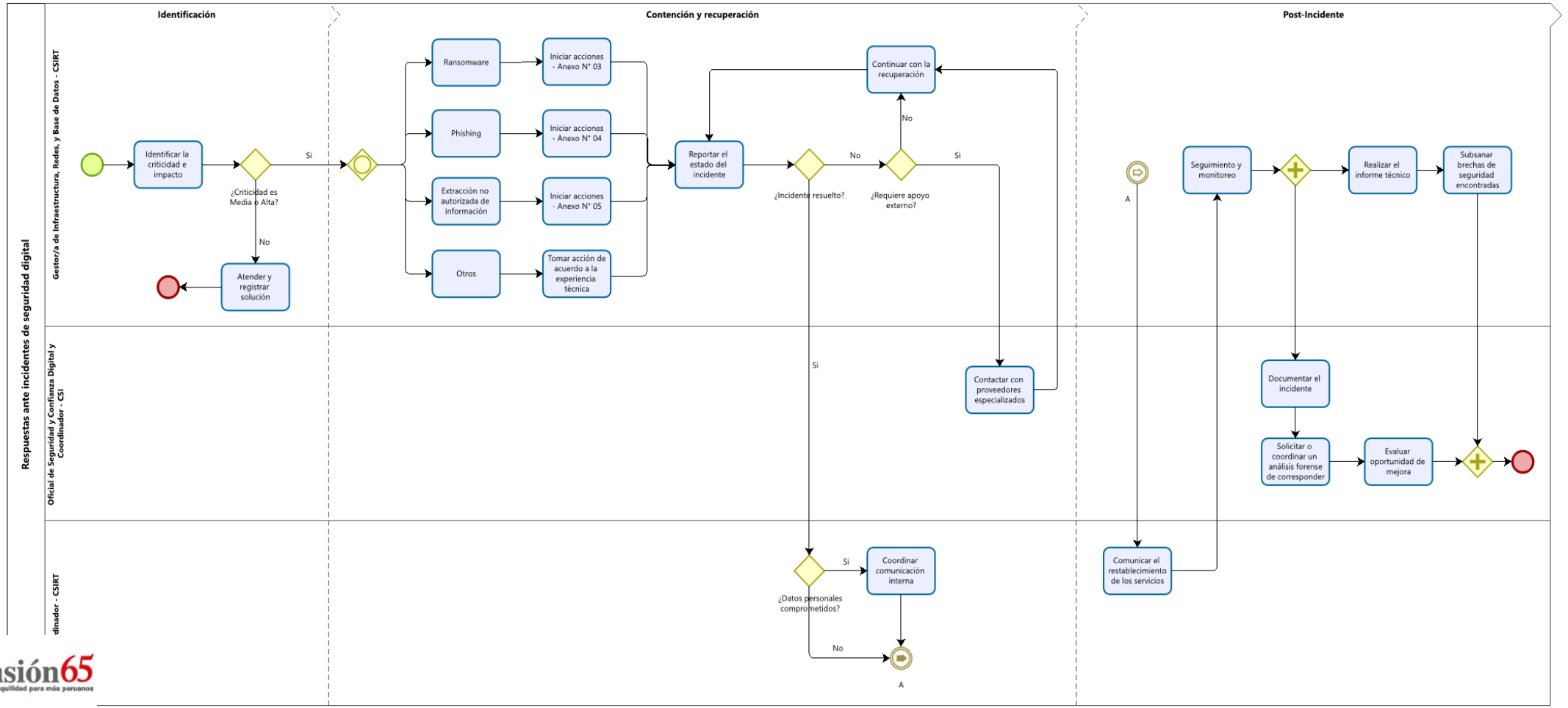
## Anexo N° 05:

Playbook de atención frente a extracción no autorizada de información

| | |
|---|---|
| 1. | Determinar la cantidad (tamaño en disco, número de registros, etc.) de información ha podido ser sustraída.<br>Establecer el tipo de datos que contiene la información que ha podido ser sustraída.<br>Debe considerarse especialmente si se han filtrado datos de carácter personal.<br>Determinar si la información es relativa al Programa o es externa, es decir, si por el contrario se trata de información que hace referencia a la institución o personal externo a la institución.<br>Establecer y acotar la causa principal de la filtración, si tiene un origen técnico, o humano. Si el origen es técnico, determinar los sistemas informáticos que están afectados o en los cuales se ha producido la brecha. Si es humano, iniciar el proceso para identificar cómo se ha producido la fuga y responsables de esa información. |
| 2. | Auditoría externa.<br>El objetivo de ésta será conocer el tamaño, gravedad y nivel de difusión de la filtración en el exterior de la institución. Hay que distinguir entre información que ha sido sustraída e información que se ha hecho pública, ya que no son necesariamente lo mismo<br>- Determinar el alcance de la publicación de la información sustraída (dónde se ha publicado, cuántos potenciales accesos habrá tenido, etc.). Este punto es crítico para cerrar la brecha de seguridad y mitigar la difusión de la información sustraída.<br>- Establecer qué información se ha hecho pública y determinar la cantidad (tamaño en disco, número de registros, etc.) de la información filtrada en el exterior de la organización.<br>- Recoger las noticias y otros contenidos que hayan aparecido en los medios de comunicación, así como en otros medios en internet sobre el incidente.<br>- Conocer las reacciones que se están produciendo en relación con el incidente. |
| 3. | Con la información obtenida se inicia el proceso de valoración del incidente, posibles consecuencias e impacto. Se establecen las tareas principales con una planificación detallada para cada una de ellas. Se debe considerar que al tratarse de una evaluación inicial las tareas se diseñan en función de la información disponible, que puede ser incompleta.<br>Dentro de las principales tareas que será necesario llevar a cabo, se encuentran las siguientes:<br><br>- Tareas para cortar la filtración y evitar nuevas fugas de información.<br>- Tareas de revisión de la difusión de la información y mitigación de la misma, en especial si ésta contiene datos de carácter personal o se trata de información confidencial.<br>- Tareas de actuación con los afectados por la fuga de información, ya sean internos o externos.<br>- Tareas para la mitigación de las consecuencias legales: posibles incumplimientos de normativa en materia de protección de datos de carácter personal o de otra normativa. También aquellas tareas encaminadas a la preparación de toda la información necesaria ante posibles denuncias por los afectados, otras organizaciones, etc.<br>- Tareas para la determinación de las consecuencias económicas, que puedan afectar a la organización y su posible mitigación.<br>- Tareas a cometer en los activos de la institución afectados, y su alcance, en relación con los activos de información, infraestructuras, personas, etc.<br>- Planificación del contacto y coordinación con fuerzas y cuerpos de seguridad, denuncia y otras actuaciones, en caso de ser necesario.<br>- Planificación de comunicación e información del incidente, tanto a nivel interno como externo, a medios de comunicación, y afectados, en caso de ser necesario. |
| 4. | El primer paso es reducir la brecha de seguridad y evitar que se produzcan nuevas fugas de información. Por este motivo, en algunos casos es posible que sea necesario desconectar un determinado servicio o sistema informático de internet o de la red interna. Ante esta situación debe primar el objeto del plan que no es otro que mitigar la fuga de información en el menor tiempo posible. Más adelante se aplicarán medidas más adecuadas o menos drásticas que la desconexión, pero siempre garantizando la seguridad. |

| | |
|---|---|
| | El siguiente paso es debemos minimizar la difusión de la información sustraída, en especial si se encuentra publicada en internet. Por este motivo, se contactará con los sitios que han publicado información y se solicitará su retirada, en especial si se trata de información sensible o protegida por la ley de protección de datos personales.<br>Junto con el paso anterior, si se considera necesario, se llevará a cabo la comunicación pertinente a los medios. Los medios de comunicación pueden aportar un mecanismo muy eficaz para hacer llegar tranquilidad a los afectados.<br>Como se indicó anteriormente debe de existir un único punto de contacto exterior desde la institución para evitar descoordinación |
| 5. | Evaluar el resultado y la efectividad de las acciones realizadas, en relación con las consecuencias y su impacto. Además, en caso de ser necesario, se deberá de hacer frente a otras consecuencias que hayan podido generarse durante la fase de mitigación del incidente, como pueden ser consecuencias legales, económicas, etc.<br>Iniciar el proceso de estabilización de la situación generada por el incidente. Se comenzará con un proceso de valoración global del mismo, que supondrá una auditoría más completa a partir de la cual se diseñan e implantan las medidas definitivas para evitar nuevas fugas y restablecer el normal funcionamiento de los servicios e infraestructuras de TI que pudieran haberse visto afectadas. |

## Anexo N° 06: Flujo de atención de incidentes de seguridad digital del CSIRT




pensión65 tranquilidad para más peruanos

Firmado digitalmente por TORRES MARQUINA Juan Daniel FAU 20547960051 soft
Motivo: Doy Visto Bueno
Fecha: 28-05-2024 15:15:37 -05:00