GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN EN EL PROGRAMA NACIONAL DE ASISTENCIA SOLIDARIA "PENSIÓN 65"

Procedimiento N°006-2024-PENSION65

Versión N° 01

Aprobado mediante Resolución de Dirección Ejecutiva N° D000054-2024-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	pensión65 tranquilidad para más peruanos Firmado digitalmente por TORRES MARQUINA Juan Daniel FAU 20547960051 soft Motivo: Soy el autor del documento Fecha: 28.05.2024 16:00:38 -05:00
Revisado por:	Raquel Gutiérrez Sánchez	Jefe(a) de la Unidad de Planeamiento, Presupuesto y Modernización	pensión65 tranquilidad para más peruanos Firmado digitalmente por GUTIERREZ SANCHEZ Raquel Esther FAU 20547960051 hard Motivo: Soy el autor del documento Fecha: 28.05.2024 16:24:27 -05:00
	Hugo Aliaga Gastelumendi	Jefe(a) de la Unidad de Asesoría Jurídica	pensión65 tranquilidad para más peruanos Firmado digitalmente por ALIAGA GASTELUMENDI Hugo Armando FAU 20547960051 soft Motivo: Soy el autor del documento Fecha: 28.05.2024 17:31:33 -05:00
Aprobado por:	Julio Mendigure Fernández	Director(a) Ejecutivo(a)	pensión65 tranquilidad para más peruanos Firmado digitalmente por MENDIGURE FERNANDEZ Julio FAU 20547960051 soft Motivo: Soy el autor del documento Fecha: 28.05.2024 17:43:08 -05:00

HOJA DE CONTROL DE CAMBIOS

Versión	Fecha	Documento sustento	Textos modificados	Responsable
01	23/04/2024	INFORME NºD00083-2024-MIDIS/P65-UTI	Documento de inicio	Unidad de Tecnologías de la Información
..				
…				
…				

pensión65 tranquilidad para más peruanos

Firmado digitalmente por TORRES MARQUINA Juan Daniel FAU 20547960051 soft
Motivo: Soy el autor del documento
Fecha: 28.05.2024 16:01:09 -05:00

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN EN EL PROGRAMA NACIONAL DE ASISTENCIA SOLIDARIA "PENSIÓN 65"

INDICE

1.	**OBJETIVO**
	Establecer el procedimiento que determine las actividades y responsabilidades para la identificación, evaluación, control y respuesta oportuna, así como la gestión de los incidentes de seguridad de la información, que puedan comprometer la integridad, confidencialidad o disponibilidad de la misma; a fin de prevenir y/o minimizar el impacto en las operaciones del Programa.
2.	**AMBITO DE APLICACIÓN**
	El presente documento es de cumplimiento obligatorio para todo el personal que labora o brinda servicios en el Programa Nacional de Atención Solidaria “Pensión 65”, independiente de la modalidad de contratación, así como también para los proveedores de servicios externos.
3.	**BASE LEGAL**
3.1	Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado y modificatorias; y su Reglamento aprobado mediante Decreto Supremo N° 030-2002-PCM.
3.2	Ley N° 27444, Ley del Procedimiento Administrativo General.
3.3	Ley 29733, Ley de protección de datos personales.
3.4	Ley Nº30096 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° 004-2013-PCM, que aprueba la Política Nacional de Modernización de la Gestión Pública.
3.8	Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412.
3.9	Decreto Supremo N° 081-2011-PCM, que crea el Programa Nacional de Asistencia Solidaria “Pensión 65” y sus modificatorias.
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 N° 159-2022-MIDIS, que aprueba el Catálogo de Documentos Oficiales del Ministerio de Desarrollo e Inclusión Social.
3.13	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.
3.14	Resolución Directoral N°102-2019-MIDIS/P65-DE, que reconforma el Comité de Gobierno Digital del Programa Nacional de Asistencia Solidaria “Pensión 65”.
3.15	Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD. Establece la Implementación y Mantenimiento del Sistema de Gestión de Seguridad de la Información en las Entidades Públicas.
3.16	Resolución de Dirección Ejecutiva N°D000179-2023-MIDIS/P65-DE, que conforma el Equipo de Respuestas ante Incidentes de Seguridad Digital del Programa “Pensión 65” que forma parte de la Oficina de Tecnologías de la Información, y determina sus funciones.
3.17	Resolución de Dirección Ejecutiva N°D00013-2024-MIDIS/P65-DE, que designa al/a la Jefe(a) de la Unidad de Asesoría Jurídica como Oficial de Datos Personales del Programa Nacional de Asistencia Solidaria “Pensión 65”.

4.	SIGLAS Y DEFINICIONES
4.1	**Siglas**
	UTI: Unidad de Tecnologías de la Información. **ERSI:** Equipo de respuesta a incidentes de Seguridad de la Información. **CSIRT:** Computer Security Incident Response Team
4.2	**Definiciones**
4.2.1	**Activo de Información:** Información que tiene valor para el Programa Nacional de Asistencia Solidaria "Pensión 65", pudiendo además ser aquel recurso (humano, tecnológico, etc.) que efectúa tratamiento directo o indirecto de la información que soporta uno o más procesos del Programa. Hace referencia a la información a los activos asociados a la información.
4.2.2	**Colaboradores:** Son los/as usuarios/as internos/as, externos/as, servicios de terceros y proveedores de servicios que laboran/brindan servicios al Programa o mantienen un vínculo de contratación.
4.2.3	**Confidencialidad:** Característica/propiedad por la cual la información no está disponible o revelada a individuos, entidades o procesos no autorizados.
4.2.4	**Datos personales:** Los datos personales son cualquier información que permite identificar a una persona. Por ejemplo, el nombre, los apellidos, la fecha de nacimiento, la dirección del domicilio, la dirección de correo electrónico, el número de teléfono, el número de RUC, el número de la placa del vehículo, la huella digital, el ADN, una imagen, el número del seguro social, etc. son datos que identifican a una persona, ya sea directa o indirectamente.
4.2.5	**Equipo de Respuesta de Seguridad de la Información (ERSI):** Equipo conformado por el/la Oficial de Confianza y Seguridad Digital, Propietario/a del Activo y profesionales internos o externos que se hayan designado o se designen o sean partes interesadas, para las acciones de respuesta al incidente de seguridad de la información.
4.2.6	**Computer Security Incident Response Team (CSIRT)**[1] por sus siglas en inglés**:** Es el equipo de Respuesta ante Incidentes de Seguridad Digital**,** equipo técnico de la Unidad de Tecnologías de la Información que responde ante incidentes de seguridad digital, descritos en el Anexo N° 02 c. Dicho equipo es conformado mediante Resolución de Dirección Ejecutiva.
4.2.7	**Evento:** Es cualquier ocurrencia observable en un sistema o red de información que indica una posible violación de la seguridad de la información. Por ejemplo, un ataque de piratas informáticos fallido.
4.2.8	**Disponibilidad:** Característica/propiedad por el cual la información permanece accesible y disponible para su uso cuando lo requiera la persona autorizada.
4.2.9	**Incidentes en la gestión de servicios de Tecnologías de la Información:** Son eventos relacionados específicamente a tecnologías que no llegan a ser incidentes de seguridad de la información. Por ejemplo: impresora no enciende, olvido de contraseña, monitor no enciende, etc.
4.2.10	**Incidente de seguridad de la información:** Evento no deseado que tiene una probabilidad significativa de comprometer la confidencialidad, integridad y disponibilidad de la información y las operaciones involucradas a ella.
4.2.11	**Incidente de Seguridad Digital:** Evento o serie de eventos que pueden comprometer la confianza, los datos personales, la información, entre otros activos de información del Programa, a través de tecnologías digitales.
4.2.12	**Integridad:** Característica/propiedad por la cual la información conserva su exactitud y se encuentra completa.
4.2.13	**Mesa de Ayuda:** Aplicación institucional en donde se registran todos los incidentes de seguridad de la información y servicios de tecnología.
4.2.14	**Oficial de Datos Personales:** Es el rol designado al/a la Jefe/a de la Unidad de Asesoría Jurídica del Programa, quién será responsable de velar por el cumplimiento de las normas en materia de protección de datos personales del Programa, informar o asesorar a la entidad sobre las disposiciones de protección de datos personales, promover la cultura de protección de datos personales, asegurar la atención de las solicitudes para el ejercicio de los derechos

[1] Conforme al Decreto de Urgencia N° 007-2020

	a la protección de datos personales y reportar a la Autoridad Nacional de Protección de Datos Personales los incidentes de seguridad que impliquen la vulneración de datos personales. En el Programa se designa mediante Resolución de Dirección Ejecutiva.
4.2.15	**Oficial de Seguridad de la información y Confianza Digital:** Es el rol designado a un servidor de la Unidad de Tecnologías de la Información, que conforma a su vez el Comité de Gobierno Digital del Programa Nacional de Asistencia Solidaria "Pensión 65"; quién será responsable de coordinar la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información (SGSI) en la entidad, atendiendo políticas y normas en materia de seguridad digital, confianza y gobierno digitales, entre otras funciones indicadas en las normativas gubernamentales vigentes. En el Programa se designa mediante Resolución de Dirección Ejecutiva.
4.2.16	**Plan de contingencias informático:** Documento que contiene las actividades para que el Programa pueda recuperarse de un desastre informático y restablecer sus operaciones.
4.2.17	**Propietario de activo de información:** Una persona o grupo de trabajo designado por el Programa, quien tiene la responsabilidad de implementar los controles y/o disposiciones para el cuidado de los activos de información, bajo responsabilidad. Es el responsable de la información y de los procesos que la manipulan sean estos manuales o electrónicos.
4.2.18	**Respuestas a incidentes de seguridad digital:** Procesos y tecnologías de una organización para detectar y responder a ciber amenazas, brechas de seguridad o ciberataques. El objetivo de la respuesta a incidentes es evitar ciberataques antes de que se produzcan y minimizar el coste y la disrupción de las operaciones asociados a los ciberataques que lleguen a producirse.
4.2.19	**Seguridad de la Información:** Es la parte del Sistema de Gestión Integral, basado en un enfoque del riesgo del negocio para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.
5.	**DESARROLLO DEL PROCEDIMIENTO**
5.1	**Responsabilidades**
5.1.1	**Personal del Programa:** a) Los/as colaboradores/as son responsables de reportar inmediatamente cualquier situación anormal, no común, que hayan podido detectar en el transcurso de sus labores, servicios u operaciones, a través de la Mesa de Ayuda de la Unidad de Tecnologías de la Información. b) Los/as colaboradores/as son responsables de reportar cualquier debilidad observada o detecta, así como reportar actividades que transgredan la seguridad de la información, a través de la Mesa de Ayuda de la Unidad de Tecnologías de la Información.
5.1.2	**El/La Oficial de Seguridad de la Información y Confianza Digital** a) Es responsable de velar por el cumplimiento del presente procedimiento, y registrar el incidente de seguridad de la Información que ha sido reportado en el Anexo N° 03 "Formato de Registro de Incidentes de Seguridad de la Información (Físico y lógico), así como analizar el incidente recibido y coordinar con los responsables del tratamiento del incidente de seguridad de la información. b) El/La Oficial de Seguridad de la Información y Confianza Digital, y el/la propietario/a del activo determinan si es que los/las colaboradores/as pueden solucionar el incidente o recomendar que se solicite apoyo externo para poder dar una solución al mismo. c) El/La Oficial de Seguridad de la Información y Confianza Digital coordina con el/la Oficial de Datos Personales, en caso se presuma y/o se haya confirmado la existencia de datos personales comprometidos en el incidente, a fin de que el/la Oficial de Datos Personales, evalúe el impacto y/o acciones que correspondan en el ámbito jurídico. d) El/La Oficial de Seguridad de la Información y Confianza Digital mantiene actualizado

	la lista de contactos para la comunicación ante Incidentes de Seguridad de la Información (Anexo N°01), y lo socializa a las Unidades de Organización del Programa.
5.1.3	**El/la Jefe/a de la Unidad de Organización** El/la Jefe/a de la Unidad de Organización que ha sido afectado por el incidente y el/la propietario/a del activo, realizan el seguimiento al incidente de seguridad de la información hasta su solución.
5.1.4	**Equipo de Respuesta de Seguridad de la Información (ERSI)** El Equipo de respuesta de Seguridad de la Información (ERSI), es el equipo responsable de participar en el proceso de atención de incidentes física y lógica de seguridad de la información cuyo nivel de criticidad es alto o medio, y que puede comprometer la confidencialidad, integridad y disponibilidad de la información en el Programa.
5.1.5	**Equipo de Respuesta ante Incidentes de Seguridad Digital (CSIRT[2])** Cuando un incidente corresponda a la seguridad digital, el Equipo de Respuesta ante Incidentes de Seguridad Digital (CSIRT), el responsable de tomar acción necesaria para dar solución al incidente reportado.
5.1.6	**El/la Jefe/a de la Unidad de Tecnologías de la Información** Es responsable de coordinar con su personal, para mantener controles de seguridad digital, equipos actualizados, así como monitorear la red interna, con el fin de prevenir incidentes de seguridad. Debe brindar las facilidades con el personal a su cargo cuando le sea solicitado para participar de la solución del incidente de seguridad de la información.
5.1.7	**De la Comunicación del Incidente de Seguridad de la Información** En caso de que existan datos personales sensibles o confidenciales que se encuentren comprometidos el/la Oficial de Seguridad y Confianza Digital - UTI, comunica el alcance del incidente a la Dirección Ejecutiva, Oficial de Datos Personales y Unidades correspondientes, para que puedan determinar tanto la comunicación a nivel interno y/o a nivel externo, según lo consideren necesario.
5.2	**Consideraciones**
5.2.1	Para el seguimiento y control de los incidentes de seguridad de la información, el/la Oficial de Seguridad y Confianza Digital utiliza el Anexo N°03 "Formato de Registro de Incidentes de Seguridad de la Información (Físico y lógico)".
5.2.2	La documentación registrada en el Anexo N° 03, de la solución de los incidentes deberá servir para retroalimentar y fortalecer el proceso de gestión de incidentes de seguridad de la información.
5.3	**Requisito de entradas para iniciar el procedimiento**

	Fuente	**Descripción**
5.3.1	Colaboradores - Unidad de Organización	Reportar el incidente de seguridad de la información en el aplicativo de Mesa de Ayuda o mediante llamada telefónica a los contactos para la comunicación ante Incidentes de Seguridad de la Información.
5.3.2	Política de Seguridad de la Información – Pensión 65	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.

[2] Por sus siglas en inglés

5.3.3	Protección de datos personales	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.
5.4	**Descripción de las actividades**	
5.4.1	**Identificación del incidente**	
5.4.1.1	Colaboradores – Unidad de Organización	Reportar incidentes de seguridad de la información a través de la Mesa de Ayuda. **¿Se encuentra disponible la mesa de ayuda?** Sí: Continuar en el numeral 5.4.1.4. No: Va a la actividad siguiente.
5.4.1.2	Colaboradores – Unidad de Organización	Contactar vía telefónica inmediatamente a los contactos del Anexo N° 01. Continuar en el numeral 5.4.1.3.
5.4.1.3	Contactos de comunicación ante incidentes de Seguridad de la Información (Anexo N° 01)	Atender el reporte del/de la colaborador/a y proceder a informar al/a la Oficial de Seguridad y Confianza Digital respecto al incidente. Continuar en el numeral 5.4.1.4
5.4.1.4	Oficial de Seguridad y Confianza Digital	Identificar si es un incidente de seguridad de la información de acuerdo a lo indicando en el Anexo N° 02 "Incidente de seguridad de la información". **¿Es un incidente de seguridad de la información?** Sí: Continuar en la actividad 5.4.1.6. No: Continuar en la siguiente actividad.
5.4.1.5	Analista en Infraestructura – UTI	Iniciar el Procedimiento de **"Atención de incidencias"** vigente, relacionado a tecnologías de la información.
5.4.1.6	Oficial de Seguridad y Confianza Digital	Identificar el tipo de incidente de acuerdo con lo establecido el Anexo 2 "Incidentes de Seguridad de la Información". - Si es un incidente de seguridad digital: Iniciar el "**Instructivo de respuestas ante incidentes de seguridad digital"** vigente; y finalizar actividad. - Si es un incidente que afecta al Centro de Datos: Iniciar el "**Plan de Contingencias Informático"** vigente, en los procesos de Ejecución y Recuperación; y continuar en el numeral 5.4.2.1. - Si es un incidente que afecta a los activos de información física o lógica: Continuar en el numeral 5.4.2.1.
5.4.2	**Evaluación de la criticidad del incidente**	
5.4.2.1	Oficial de Seguridad y Confianza Digital	Analizar que activos de información se encuentran involucrados en conjunto con los propietarios.

5.4.2.2	Oficial de Seguridad y Confianza Digital	Evaluar la criticidad del incidente de seguridad, de acuerdo con el Anexo N° 04 "Nivel de Criticidad del incidente". Continuar en el numeral 5.4.3.1.
5.4.3	**Coordinación y comunicación del incidente**	
5.4.3.1	Oficial de Seguridad y Confianza Digital	Comunicar, vía correo electrónico y telefónica (de ser necesario), el incidente, a los/las propietarios/as de los activos de información de las Unidades de Organización que hayan sido afectadas y/o a los demás a los/as colaboradores/as que considere necesarios. **¿Se encuentran comprometidos datos personales sensibles?** - Sí: Comunicar al/ a la Oficial de Datos Personales, Dirección Ejecutiva, y Unidades que considere necesario, a través de los medios de comunicación disponible. Continuar en la actividad 5.4.3.4. - No: Continúa en el numeral 5.4.4.1
5.4.3.4	Oficial de Seguridad y Confianza Digital	Si se requiere la participación de algún especialista informático, solicitar al/a la Jefe(a) de la UTI para que disponga la participación del especialista de la Unidad u externo de ser necesario. Continuar en la actividad 5.4.4.1.
5.4.4	**Acciones ante el incidente - derivación**	
5.4.4.1	Equipo de respuesta a incidentes de Seguridad de la Información (ERSI)	Tomar las acciones inmediatas de acuerdo con el nivel de criticidad del incidente (Anexo N° 04 "Nivel de criticidad del incidente").
5.4.4.2	Equipo de respuesta a incidentes de Seguridad de la Información (ERSI)	Establecer una cadena de custodia y no eliminar ninguna evidencia hasta que el incidente se haya cerrado y posterior a ello.
5.4.4.3	Equipo de respuesta a incidentes de Seguridad de la Información (ERSI)	¿Se resuelve el incidente de seguridad? Sí: Ir al numeral 5.4.5.1. No: realizar el nivel de escalamiento interno o externo. Continuar en el numeral 5.4.4.1.
5.4.5	**Post – incidente**	
5.4.5.1	Equipo de respuesta al incidente	Verificar que los activos de información afectados vuelvan a su condición operativa.
5.4.6	**Cierre del incidente**	
5.4.6.1	Oficial de Seguridad y Confianza Digital	Registrar el detalle del incidente de acuerdo con los apartados indicados en el Anexo 03 "Formato de Registro de Incidentes de Seguridad de la Información (Físico y lógico)".
5.4.6.2	Oficial de Seguridad y Confianza Digital	Comunicar, los resultados de las acciones tomadas para hacer frente al incidente, a la Dirección Ejecutiva, a los colaboradores que reportaron el incidente (de corresponder) y a los afectados por el mismo.
5.4.6.3	Oficial de Seguridad y Confianza Digital	Remitir el informe del incidente de seguridad de la Información a las Unidades de Organización que correspondan.
5.4.6.4	Oficial de Seguridad y Confianza Digital	Coordinar con las Unidades de Organización afectadas, medidas preventivas de acuerdo con el incidente solucionado.

5.5	**DOCUMENTOS O REGISTROS QUE SE GENERAN (SALIDAS)**	
	Destino	Salida o Producto
5.5.1	UTI, DE	ANEXO N° 03 Formato de Registro de Incidentes de Seguridad de la Información (Físico y lógico).
6.	**PROCESO RELACIONADO**	
	A03 Gestión de Sistemas y Tecnologías de la Información	
7.	**ANEXO**	
7.1	Anexo N°01 “Contactos para la comunicación ante Incidentes de Seguridad de la Información”.	
7.2	Anexo N° 02 “Incidentes de Seguridad de la Información”.	
7.3	Anexo N° 03 “Formato de Registro de Incidentes de Seguridad de la Información (Físico y lógico)”.	
7.4	Anexo N° 04 “Nivel de criticidad del incidente”.	
7.5	Anexo N° 05 Flujograma	

ANEXO N° 01

Contactos para la comunicación ante Incidentes de Seguridad de la Información

CONTACTOS PARA LA COMUNICACIÓN ANTE INCIDENTES DE SEGURIDAD	
1° Contacto	**Soporte Tecnológico**
	https://mesadeayuda.pension65.gob.pe/
2° Contacto	**Oficial de Seguridad de la Información y Confianza Digital** Oficialsi@pension65.gob.pe
3° Contacto	**Jefe(a) de la UTI**

La UTI mantendrá actualizados los datos personales de los contactos y los remitirá a todas las Unidades de Organización mediante documento Interno, a través del Sistema de Gestión Documental.

ANEXO N° 02
Incidentes de Seguridad de la Información

a) Incidentes que afecten al Centro de Datos

ID	Definición
INSC01	Evento: Incendio, Sismo e inundaciones que afecten al Centro de Datos
INSC02	Evento: Interrupción de energía eléctrica y Falla de UPS y/o grupo electrógeno (Centro de Datos)
INSC03	Falla física de servidores críticos
INSC04	Falla en Motor de Base de Datos
INSC05	Falla del Sistema Operativo de los servidores
INSC06	Caída o interrupción del servicio de internet del Centro de Datos
INSC07	Ausencia imprevista del personal técnico critico de la UTI
INSC08	Otros incidentes no incluidos anteriormente.

b) Incidentes que afecten a los activos de información física o lógica

ID	Definición
INS01	**Acceso no autorizado a información en papel**: Esto ocurre cuando personas no autorizadas obtienen acceso físico a documentos confidenciales, sensibles. Puede incluir robo de documentos, archivos que se dejan desatendidos o accesibles en una oficina, o copias no autorizadas de información impresa.
INS02	**Pérdida o Robo de documentos físicos confidenciales:** El robo de archivos, carpetas o documentos impresos que contienen información sensible.
INS03	**Desechos inadecuados de información confidencial**: La eliminación inapropiada de documentos físicos sensibles sin destrucción adecuada, lo que permite que otros tengan acceso a ellos.
INS04	**Pérdida o robo de dispositivos físicos**: La pérdida o el robo de dispositivos como computadoras portátiles, teléfonos móviles o unidades USB que contienen datos confidenciales. Esto puede exponer la información almacenada en esos dispositivos.
INS05	**Desechos inadecuados de documentos**: No eliminar adecuadamente documentos o registros sensibles antes de desecharlos. Los documentos en papel que no se destruyen correctamente pueden ser recuperados por personas no autorizadas.
INS06	**Ruptura de la cadena de custodia**: Esto se refiere a situaciones en las que la integridad y la custodia de evidencia o documentos son comprometidas. Por ejemplo, si un documento clave en una investigación se manipula o se destruye antes de que pueda ser examinado.
INS07	**Errores humanos**: Acciones involuntarias o accidentales que conducen a la pérdida o divulgación de información física sensible. Esto puede incluir la eliminación accidental de datos, enviar información incorrecta o no seguir procedimientos de seguridad adecuados.
INS08	**Acceso no autorizado a oficinas o instalaciones físicas (restringidas):** Intrusos que ingresan a edificios o instalaciones empresariales sin autorización y pueden robar información o causar daños.
INS09	**Problemas de gestión de políticas de seguridad**: Falta de cumplimiento de políticas de seguridad de la información en una organización, como no seguir políticas de clasificación de datos, no realizar capacitación adecuada o no implementar medidas de seguridad física.
INS10	**Robo de identidad:** El uso no autorizado de la identidad de una persona para cometer fraude en ámbito físico, como cuando alguien obtiene una tarjeta de acceso a un ambiente de acceso restringido.
INS11	**Sabotaje interno**: Acciones intencionadas por parte de personal interno que dañan

ID	Definición
	deliberadamente documentos con información crítica, sensible de la organización.
INS12	**Destrucción no autorizada de documentos físicos:** La eliminación intencionada de documentos sin permiso o antes de lo programado.
INS13	**Incidentes de seguridad en la cadena de suministro**: Problemas relacionados con la seguridad de los proveedores o terceros que tienen acceso a la información de una organización.
INS14	**Fuga de información en llamadas telefónicas**: La divulgación de información sensible durante llamadas telefónicas no seguras o la grabación no autorizada de conversaciones.
INS15	Otros incidentes no incluidos anteriormente.

c) Incidentes de seguridad digital

ID	Amenaza	Descripción	Tipo
INSD01	Código malicioso (malware o ransomware)	Software cuyo objetivo es infiltrarse o dañar PC, servidor u otro dispositivo de red, sin el conocimiento del usuario y con finalidades muy diversas.	• Virus. • Gusanos. • Troyanos. • Spyware. • Rootkit. • Ransomware (secuestro). • Herramienta para Acceso Remoto (RAT).
INSD02	Afectación de disponibilidad	Ataques dirigidos a poner fuera de servicio los sistemas, al objeto de causar daños en la productividad y/o la imagen corporativa.	• Denegación [Distribuida] del Servicio DoS/DDoS. • Fallo (Hardware/Software).
INSD03	Obtención de información	Ataques dirigidos a recabar información fundamental que permita avanzar en ataques más sofisticados, a través de ingeniería social o de identificación de vulnerabilidades.	• Sabotaje. • Divulgación no autorizada de información. • Identificación de activos y vulnerabilidades (escaneo). • Sniffing. • Ingenieria social. • Phishing.
INSD04	Intrusiones	Ataques dirigidos a la explotación de vulnerabilidades de diseño, de operación o de configuración de diferentes tecnologías, con el objeto de introducirse de forma fraudulenta en los sistemas de la organización.	• Compromiso de cuenta de usuario. • Defacement (desfiguración). • Falsificación de petición entre sitios cruzados. • Inyección SQL. • Phishing. • Pharming. • Ataque de fuerza bruta • Inyección de Ficheros Remota. • Explotación de vulnerabilidad software / hardware. • Acceso no autorizado a red.

INSD05	Compromiso de la información	Incidentes relacionados con el acceso y fuga (Confidencialidad), modificación o borrado (Integridad) de información no pública.	• Acceso no autorizado a la información. • Modificación y borrado no autorizada de información. • Publicación no autorizada de información. • Ex filtración de información.
INSD06	Contenido abusivo	Ataques dirigidos a dañar la imagen de la organización o a utilizar sus medios electrónicos para otros usos ilícitos (tales como la publicidad, la extorsión o, en general la ciberdelincuencia).	• Spam (Correo Basura). • Acoso / extorsión / mensajes ofensivos. • Pederastia/ racismo/ apología de la violencia/delito.
INSD07	Violación a Políticas institucionales	Incidentes relacionados por violaciones de usuarios de las políticas de seguridad aprobadas por la organización.	• Abuso de privilegios por usuarios. • Acceso a servicios no autorizados. • Sistema desactualizado • Otros.
INSD08	Otros	Otros incidentes no incluidos anteriormente.	

ANEXO N° 03
Formato de Registro de Incidentes de Seguridad de la Información (Físico y lógico)

Código:			
1. Comunicación			
1.1. Notificación			
Fecha		**Hora**	
Tipo de Comunicación			
Mesa de Ayuda			
Correo Electrónico			
Teléfono Móvil			
Otros:			
1.2. Datos del que comunica			
Colaborador		**Proveedor de servicio**	
Nombres y Apellidos			
DNI			
Cargo		**Unidad de Organización**	
2. Registro			
Tipo de Incidente			
3. Descripción del Incidente			
(Descripción) (¿Cómo se detectó el incidente?) (Equipos o dispositivos involucrados)			
4. Nivel de Criticidad			

5. Especialistas (de ser necesario)

N°	Nombres y Apellidos	Cargo	Unidad Orgánica

6. Personal comunicado

N°	Nombres y Apellidos	Cargo	Unidad Orgánica

7. Acciones Inmediatas

N°	Descripción Acción Tomada	Fecha

8. Investigación del Incidente
Causas del incidente

Firmado digitalmente por TORRES MARQUINA Juan Daniel FAU 20547960051 soft
Motivo: Soy el autor del documento
Fecha: 28.05.2024 16:07:46 -05:00

9. Evidencias del Incidente				
Evidencias recolectadas				
10. Escalamiento del Incidente				
Escalamientos realizados				
Fecha / Hora				
Responsable				
Comentarios				
11. Alternativas de Solución al Incidente				
Solución propuesta				
12. Cierre del incidente				
Fecha y hora				
Solución implementada				
¿Se aplicó medidas disciplinarias?	SI		NO	
Lecciones aprendidas				
Responsable de la Solución				
DNI				
Unidad de organización				

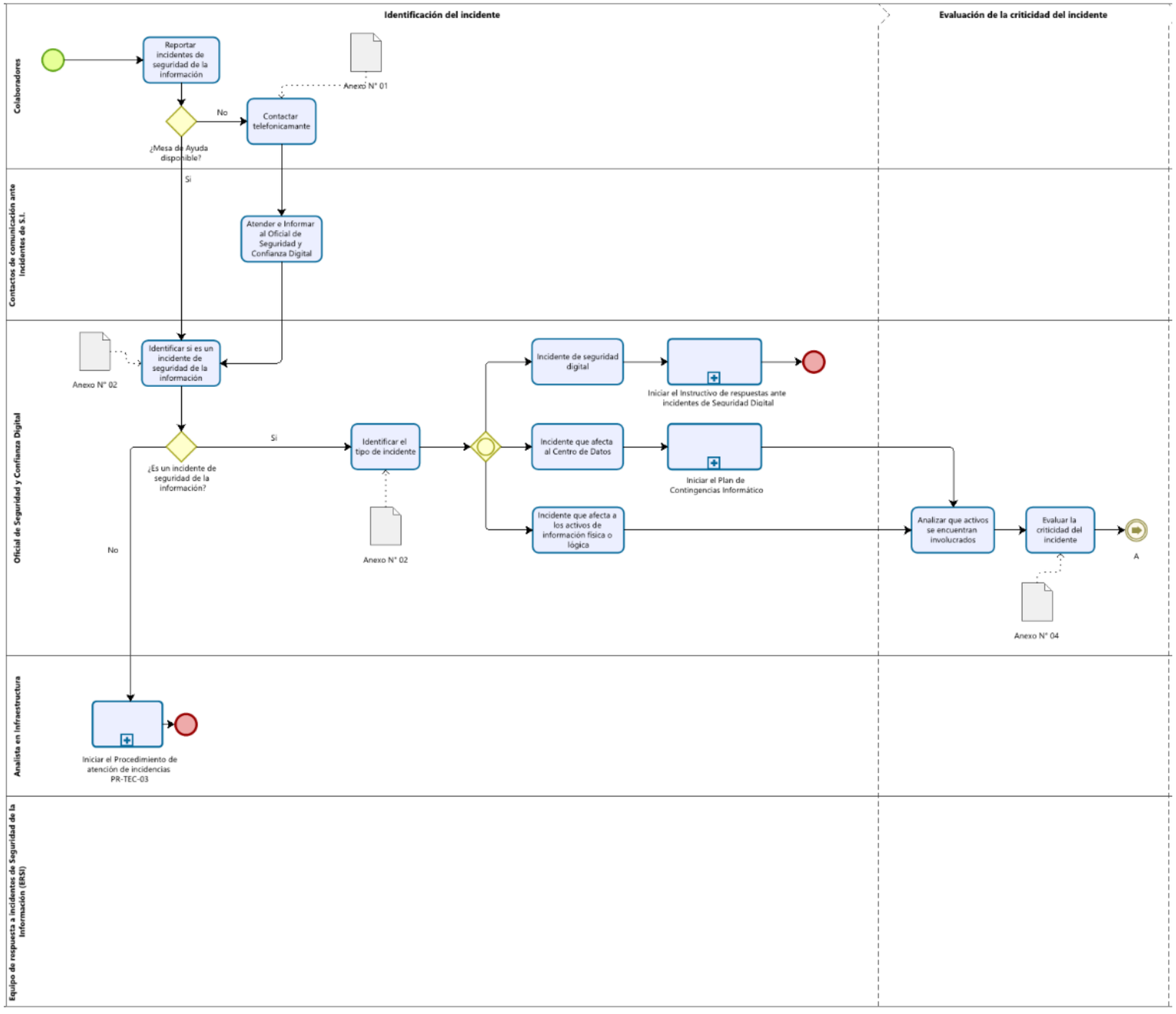
Firma del Oficial de Seguridad y Confianza Digital

Firmado digitalmente por TORRES MARQUINA Juan Daniel FAU 20547960051 soft
Motivo: Soy el autor del documento
Fecha: 28.05.2024 16:08:01 -05:00

ANEXO N° 04
Nivel de Criticidad del incidente

Nivel	Descripción	Impacto Potencial	Medidas Inmediatas	Revisión y Prevención
Alto	Incidentes con un impacto potencial que pueden causar daños graves a la organización	Pérdida financiera. Impacto en la reputación. Impacto legal. Posible daño a personas.	Se podrán tomar algunas de las siguientes acciones de ser necesarias: Evacuar el área o instalaciones. Documentar la escena inicial sin alterarla. Llamar a las autoridades pertinentes (policía, bomberos, etc.) Activar alarmas y/o sistemas de emergencia. Bloquear y asegurar áreas comprometidas. Comunicar a todo el personal la situación y las acciones a seguir. Desconectar o aislar sistemas comprometidos o en riesgo. Revisar y activar de ser posible planes de continuidad y/o de recuperación ante desastres. Resguardar información crítica y backups de información física o lógica. Verificar el estado de infraestructura critica. Registrar y monitorear las entradas y salidas de la organización de todos los usuarios. Reforzar medidas de seguridad en áreas afectadas. Evaluar posibles consecuencias o impactos derivados. Revisar grabaciones o registros relacionados. Resguardar evidencia o elementos comprometidos. Solicitar apoyo externo si es necesario. Revisar y adaptar protocolos de acceso más rígidos. Establecer monitoreo intensivo en áreas vulnerables. Otros...	Capacitaciones frecuentes. Revisiones de protocolos. Inspecciones regulares. Evaluaciones de riesgo.
Medio	Incidentes con impacto moderado.	Pérdida financiera menor Impacto reputacional menor Violaciones menores de protocolo	Evaluación de seguridad. Revisiones de protocolos. Otros…	Feedback y ajustes. Revisiones anuales.
Bajo	Incidentes con bajo impacto.	Violaciones menores sin pérdida real Incidentes que no afectan operación o reputación	Registro y monitoreo.	Monitoreo constante. Capacitaciones al personal del Programa.

ANEXO N° 05 FLUJOGRAMA



ANEXO N° 05 FLUJOGRAMA (continuación del anterior flujo)