

TRABAJO DE GRADO
Opción Seminario-Diplomado.

1

Análisis de Amenazas y Propuesta de un Plan de Concientización para Prevenir Ataques de
Ingeniería Social en el Datacenter de la Empresa PanamProject

Corporación Universitaria Remington.

Facultad de Ingenierías

Ingeniería de Sistemas / Tecnología desarrollo de software

Mariana Acevedo González

Sara Noemí Parra Bernal

Ana Sofía Giraldo Quintero

Docente: Ing. Esp. Alfonso Valencia MSc.

Seminario Ciberseguridad y Ciberdefensa

2026

Dedicatoria

Dedicamos este trabajo, en primer lugar, a nuestras familias, por su amor, apoyo y comprensión durante todo nuestro proceso de formación profesional. A quienes estuvieron presentes en los momentos de esfuerzo y dificultad, brindándonos motivación para continuar y alcanzar esta meta.

También dedicamos este logro a nosotras mismas, por la perseverancia, el compromiso y el trabajo en equipo que nos permitieron superar los diferentes desafíos que surgieron durante el desarrollo de este proyecto.

Agradecimientos

Agradecemos a Dios por permitirnos culminar esta etapa de nuestra formación académica, por brindarnos fortaleza y perseverancia durante el desarrollo de este trabajo.

A nuestras familias, por su apoyo incondicional, su acompañamiento fue fundamental para alcanzar esta meta.

A nuestra universidad y a los docentes que hicieron parte de nuestra formación, por compartir sus conocimientos y experiencias, nutriendo nuestro crecimiento académico y profesional.

De manera especial, queremos agradecer a nosotras mismas, porque sin conocernos al inicio de este proyecto logramos construir un equipo basado en el respeto, la confianza, el compromiso y el apoyo mutuo. Cada una aportó lo mejor de sí para sacar adelante este trabajo y juntas demostramos que con dedicación y trabajo en equipo, podemos alcanzar grandes resultados.

Finalmente, agradecemos a todas las personas que de una u otra manera, contribuyeron a la realización de este trabajo y que nos brindaron su apoyo para alcanzar satisfactoriamente este logro.

Tabla de Contenidos

Resumen.....	7
Objetivo General.....	9
Objetivos Específicos.....	10
Marco Contextual.....	11
Marco Conceptual.....	15
Seguridad Informática.....	15
Características de la Información.....	16
Amenazas, Riesgos y Vulnerabilidades.....	16
Ingeniería Social.....	17
Métodos y Tipos de Ingeniería Social.....	18
Rasgos de los Ataques de Ingeniería Social.....	18
Prevención y Concientización.....	19
Respuesta Ante Ataques.....	20
Desarrollo e Implementación del Aprendizaje.....	21
Descripción del Ejercicio.....	21
Tabla 1.....	22
Identificación de Procesos y Activos Relevantes.....	27
Identificación de Amenazas de Ingeniería Social.....	29
Identificación de Vulnerabilidades.....	31
Propuestas de Medidas de Concientización.....	33
Plan de Concientización.....	35
Conclusiones.....	43
Referencias.....	44
Anexos.....	45

Tabla de Figuras

Figura 1	23
Figura 2	24
Figura 3	25
Figura 4	26
Figura 5	40
Figura 6	41

Tabla de Anexos

Anexo 1	45
Anexo 2	47
Anexo 3	56

Resumen

El presente trabajo tiene como objetivo identificar y analizar las amenazas que pueden generar un riesgo relacionado con la ingeniería social en las operaciones de Datacenter de la empresa PanamProject,¹ esta es una empresa colombiana que ofrece soluciones tecnológicas, cuentan con operaciones en Bogotá, Medellín, Ciudad de México y Miami. Debido a la variedad de servicios que maneja y al contacto constante de sus empleados con clientes y usuarios, es importante conocer los riesgos que pueden surgir por errores humanos y por técnicas de manipulación utilizadas por los ciberdelincuentes. El Datacenter se enfoca especialmente en las actividades que tienen relación con el área de atención al cliente, por lo cual, se busca reconocer las principales labores que realizan los operadores, determinando cuáles pueden estar expuestas a situaciones como phishing, vishing, smishing, pretexting, suplantación de identidad o accesos no autorizados. Este análisis es importante porque la seguridad no depende únicamente de herramientas tecnológicas, también depende del comportamiento y conocimiento de las personas que manejan la información y los activos. Por esta razón, la prevención requiere capacitación, verificación de mensajes y solicitudes, políticas de seguridad y controles de acceso. Finalmente, se plantea un plan de concientización para fortalecer el proceso de validación de autorizaciones estableciendo los canales de comunicación oficiales, responsables y mecanismos de escalamiento. Con esto se busca

¹ Autorización transmitida vía correo electrónico por Daissy Cárdenas líder CPD de la empresa PanamProject, el 8 de septiembre de 2026. Copia de este documento se adjunta en el anexo 1.

fortalecer la cultura de seguridad de los empleados, concientizándolos de las amenazas existentes derivadas de los ataques de ingeniería social.

Palabras clave: Ingeniería social, Tabnabbing, Scareware, Hackeo de correo electrónico, Correos spam, Phishing y manipulación del usuario.

Objetivo General

Identificar las amenazas derivadas de la ingeniería social en el proceso de operaciones del Datacenter de la empresa PanamProject, así como diseñar una propuesta de concientización para que los empleados reconozcan y prevengan este tipo de amenazas.

Objetivos Específicos

- Identificar las principales amenazas asociadas a la ingeniería social que podrían afectar las operaciones del Datacenter de la empresa PanamProject.
- Diseñar una propuesta de concientización dirigida a los empleados del Datacenter, con el fin de fortalecer el reconocimiento y la prevención frente a las amenazas de ingeniería social.
- Establecer el conducto regular para el reporte de posibles amenazas o incidentes de ingeniería social, definiendo los roles y funciones de las personas involucradas en su atención.
- Formular recomendaciones para una posible implementación y validación posterior de las medidas propuestas.

Marco Contextual

PanamProject es una empresa colombiana dedicada a brindar soluciones de tecnología en diferentes sectores, esta empresa opera en dos ciudades en Colombia que son Bogotá y Medellín y fuera de ella están en Ciudad de México (México) y Miami (USA), cuenta con 110 personas como motor de fuerza laboral que permiten brindar soluciones a diferentes problemáticas tecnológicas (Panamproject, s.f.), esta empresa cuenta con áreas de servicio al cliente, mantenimiento, Operación Datacenter, monitoreo continuo, soporte 7x24 y administración de redes, los cuales se encargan de recibir y gestionar los requerimientos de los clientes en cuanto a funcionamiento de sus servicios y también de contactar a personas de interés a fin de ofrecer sus soluciones, debido a esto resulta importante analizar las amenazas de ingeniería social que se pueden presentar en el diario de estas labores, por lo cual el proyecto analizará estas amenazas en las actividades del área de Operación Datacenter de esta empresa, a fin de realizar un correcto análisis se partirá de las principales labores que se hacen a diario en este departamento, lo cual permitirá identificar que actividades son de especial interés que puedan derivar en posibles escenarios de riesgo.

Para este análisis, se tomará en cuenta los procedimientos que ya están establecidos en la empresa con respecto a la ciberseguridad, a fin de identificar cuales se están cumpliendo en su plenitud, cuáles de manera parcial y cuáles no se están cumpliendo.

La finalidad de este análisis es diseñar una propuesta de concientización dirigida a los empleados, con el fin de fortalecer el reconocimiento y la prevención frente a estas

amenazas, así como también establecer el conducto regular para el reporte de estas situaciones en la que se dé a conocer los roles y funciones de las personas involucradas en la atención de los mismos y por último, formular recomendaciones para una posible implementación y validación de las medidas de prevención propuestas.

Dentro de este contexto, es importante resaltar algunas situaciones relacionadas con la ingeniería social que se presentaron recientemente en la empresa PanamProject. Estas situaciones permiten tener una visión más amplia de los riesgos a los que están expuestos los empleados durante el desarrollo de las actividades y de la importancia de reconocer este tipo de amenazas dentro de las operaciones del Datacenter.

A continuación, se describen algunas de las situaciones identificadas en la empresa, estas serán utilizadas como referencia para el desarrollo del análisis y la propuesta planteada en este trabajo.

Situaciones Relacionadas con la Ingeniería Social Identificadas en la Compañía

Durante el desarrollo de las labores en la empresa se han presentado situaciones en las que los empleados ha recibido solicitudes que pueden estar relacionadas con técnicas de ingeniería social. Entre las situaciones identificadas se encuentran las siguientes:

- **Situación 1.** Retiro de un activo de la empresa sin la debida autorización.

En el mes de agosto del presente año se presenta el cliente solicitando el retiro de un servidor, para lo cual se tiene un procedimiento establecido, en el cual se deben cumplir los siguientes pasos:

- Validar permisos de la persona que ingresa

- Se debe contar con una tarea o solicitud activa, en la cual se describa lo que se va a realizar durante la actividad.
- Validación de la parte o servidor a retirar.
- Verificar Autorización escrita para el retiro del equipo
- Acompañamiento técnico del personal correspondiente

El operador se saltó 3 de los 4 pasos mencionados, dado que solo valido que la persona tuviera permisos. La persona presento la factura del equipo, y solo con este documento dio salida al activo. Debido a esto en el momento se encuentra activo un proceso de investigación sobre el evento y el operador fue retirado de su cargo.

- **Situación 2.** Acceso a área crítica sin la correcta validación.

En el mes de agosto del presente año se presentó una falla critica con un servidor al interior de un rack, por lo cual el cliente se presentó en el Datacenter solicitando acceso para realizar un cambio de equipo, indicando que estaba fallando y podía llegar a generar un daño más grande en el rack en general y llegaría a afectar a otros clientes. Para los cambios de equipos se tiene un procedimiento establecido en el cual se deben cumplir los siguientes pasos:

- Validar permisos de la persona que ingresa
- Se debe contar con una tarea o solicitud activa, en la cual se describa lo que se va a realizar durante la actividad.
- Validación de la parte o servidor a ingresar
- Verificar autorización escrita para el ingreso del equipo
- Acompañamiento técnico del personal correspondiente

- Factibilidad para instalación o cambio del equipo
- Dado que era un caso de emergencia se debe notificar al jefe inmediato, al responsable del datacenter y al jefe del área encargada de controlar flujo eléctrico.

El operador omitió gran parte del proceso, permitió el acceso del personal y el equipo nuevo, sin el debido acompañamiento ni autorización realizaron el cambio del equipo, su ubicación y lo conectaron en una toma que no estaba permitido para este tipo de activos, el operador no realizó la debida notificación, porque se dejó presionar por la urgencia del momento y del cliente. El equipo dañado no lo pudieron retirar dado que el hecho ocurrió un domingo y no se permite el retiro de equipos los domingos. Debido a esto en el momento se encuentra activo un proceso de investigación sobre el evento, así como el equipo dañado está retenido y en custodia hasta que se aclare lo ocurrido y el operador está enfrentando un proceso de descargos.

Por último, estas situaciones muestran que el factor humano puede representar un elemento importante dentro de la seguridad de las operaciones, especialmente cuando tienen acceso a información, áreas o activos utilizados en el Datacenter.

Posterior a los eventos y con el fin de concientizar al personal sobre las situaciones ocurridas, se realizaron 2 reuniones con los operadores, la primera reunión se realizó con los operadores en turno, dando las indicaciones pertinentes de forma muy general de la situación ocurrida. La segunda reunión se realizó con todo el equipo, en la cual se dieron instrucciones sobre la situación, así como también se aclararon dudas para quienes aún tenían alguna inquietud o vacíos en los procesos realizados. Así mismo se

dieron instrucciones claras del proceso a seguir en futuras situaciones de ingreso, instalación o retiro de equipos.

Marco Conceptual

Seguridad Informática

La seguridad informática es un aspecto importante para proteger la información que manejan las organizaciones, se pueden definir como el conjunto de políticas, controles y procedimientos orientados a preservar la confidencialidad, integridad y disponibilidad de la información frente a diversas amenazas. Además, cuando una amenaza llega a afectar la información, es crucial buscar su recuperación lo más pronto posible debido a que se debe dar continuidad al negocio. Desde esta perspectiva, la seguridad informática trasciende la implementación de barreras técnicas; abarca la identificación sistemática de amenazas, la mitigación de riesgos y el establecimiento de mecanismos eficaces de recuperación operacional (ISO/IEC 27001, 2022).

Por otra parte, en el mundo cibernético existen amenazas y las personas por la curiosidad son más propensas a caer en diversas trampas, esto evidencia que la seguridad no depende exclusivamente de herramientas o infraestructura tecnológica, sino de manera prioritaria de las personas que interactúan con los sistemas y gestionan la información. En consecuencia, el factor humano y la responsabilidad compartida continúan posicionándose como elementos determinantes en la postura de ciberseguridad organizacional, siendo el eslabón clave para la prevención o materialización de brechas de seguridad (Verizon, 2025).

Características de la Información

Para que la información tenga un verdadero valor dentro de una organización, es necesario que conserve ciertas características fundamentales, entre ellas se encuentran la confidencialidad, que garantiza que únicamente las personas autorizadas puedan acceder a la información; la integridad, que busca mantener los datos completos, exactos y confiables durante su procesamiento; y la disponibilidad, que permite que los usuarios autorizados puedan acceder a la información y a los recursos relacionados cuando los necesiten (ISO & IEC, 2022).

Estas características son especialmente importantes para el desarrollo del presente proyecto, ya que un ataque de ingeniería social puede afectar directamente la seguridad de la información, facilitar accesos no autorizados y generar modificaciones, pérdida o exposición de datos, afectando tanto su confidencialidad como su integridad; además, dependiendo de su alcance, puede comprometer la disponibilidad de los servicios del centro de datos (Datacenter), ocasionando interrupciones en las operaciones de la organización; a esto se le suman posibles consecuencias legales y afectaciones a la reputación de la compañía, especialmente cuando la información comprometida pertenece a clientes, empleados o terceros.

Amenazas, Riesgos y Vulnerabilidades

La gestión de la seguridad de la información está relacionada con la identificación y el tratamiento de las amenazas, los riesgos y las vulnerabilidades que pueden afectar a una organización. Estos riesgos pueden tener diferentes causas y no necesariamente presentan la misma probabilidad de ocurrencia ni generan las mismas consecuencias, por

esto es importante identificarlos y analizarlos de manera sistemática, con el fin de establecer controles que respondan de forma adecuada al nivel de riesgo y permitan prevenir o reducir sus posibles efectos (ISO & IEC, 2022).

El análisis de riesgos permite entender el origen de las amenazas, identificar las vulnerabilidades presentes tanto en la infraestructura como en los procesos de la organización y determinar las posibles consecuencias operacionales, financieras y de reputación que podrían producirse si un riesgo llega a hacerse realidad; desde esta perspectiva, una adecuada gestión del ciberriesgo requiere evaluar de manera continua las vulnerabilidades existentes, prestando atención a aquellas relacionadas con el factor humano y los procedimientos internos, para saber si es necesario implementar medidas preventivas y de respuesta que contribuyan a reducir la probabilidad de ocurrencia de los incidentes y a limitar sus posibles impactos (NIST, 2025).

Ingeniería Social

La ingeniería social es una de las principales amenazas relacionadas con los humanos. Se describe como una “táctica de ataque que busca manipular a las personas para que compartan información, descarguen programas, ingresen a determinados sitios, envíen dinero o realicen acciones que puedan comprometer su seguridad” (IBM, s. f). Una de sus principales características es que aprovecha el error humano, la curiosidad o la manipulación psicológica en lugar de depender únicamente de vulnerabilidades técnicas. Un ejemplo de esta amenaza se evidenció durante la pandemia del COVID-19, se difundieron campañas masivas por WhatsApp en las que mencionaban que la aerolínea Avianca estaba regalando vuelos, o que Estados Unidos iba a transferir ayudas

económicas humanitarias y que solo con ingresar a un link y registrar ciertos datos personales ya se quedaba inscrito para acceder a estos beneficios, estas situaciones claramente estaban enfocadas en engañar a las personas a fin de conseguir información personal.

Métodos y Tipos de Ingeniería Social

La ingeniería social puede presentarse mediante diferentes métodos, cómo se explica en el sitio web de Kaspersky (s. f.) entre los más conocidos se encuentra el phishing, mediante el cual el atacante se hace pasar por una persona o institución de confianza para conseguir información, también se encuentra el spear phishing que utiliza información más específica para dirigirse a determinadas personas, siguiendo la misma línea, el whaling se dirige a objetivos considerados de alto valor, otro tipo es el vishing, que utiliza llamadas de voz indicando que se devuelva la llamada porque hay un mensaje importante que necesitan compartir, entre otras modalidades, el smishing utiliza mensajería de texto y en el pretexting el atacante utiliza una identidad o situación falsa para ganarse la confianza de la víctima, existen también los ataques de cebo, el acceso físico, el tailgating, los ataques de reciprocidad, el scareware y los ataques del abrevadero (watering hole attack). Cómo se puede leer estos tipos son los más relevantes, pero obviamente existen muchos más tipos y cada día puede que sigan surgiendo más amenazas.

Rasgos de los Ataques de Ingeniería Social

Una característica importante de estos ataques es que buscan influir en las emociones de las personas. En el sitio web de IBM se señala que estas técnicas se apoyan

en la motivación humana y utilizan diferentes situaciones para conseguir que la víctima actúe de una determinada manera. Entre ellas se encuentran la suplantación de marcas o autoridades y la generación de miedo o urgencia IBM (s. f.).

En el sitio web de Kaspersky se concientiza a las personas de estos ataques, por lo cual ellos dan unas recomendaciones para identificar un posible ataque, entre estas se encuentran, si se siente demasiado miedo, curiosidad o entusiasmo, es probable que la persona actúe sin analizar suficientemente la situación. Por esta razón, una de las recomendaciones es detenerse y verificar la información antes de responder a un mensaje, abrir un enlace o permitir el acceso solicitado Kaspersky (s. f.).

Prevención y Concientización

Debido a que la ingeniería social se relaciona directamente con el comportamiento de las personas, la prevención no depende únicamente de herramientas tecnológicas. En el sitio web de Kaspersky (s. f.) se señala que la protección frente a este tipo de ataques comienza con la educación y el conocimiento de las amenazas. También recomienda verificar los mensajes, enlaces y la identidad de las personas antes de proporcionar información o permitir algún tipo de acceso.

Por otro lado, IBM (s. f.) también plantea diferentes medidas para reducir estos riesgos, entre ellas la concientización de los usuarios, las políticas de seguridad y los controles relacionados con el acceso. Estas medidas buscan disminuir la posibilidad de que una persona sea engañada y entregue información o realice una acción que pueda comprometer a la organización.

Respuesta Ante Ataques

Cuando una amenaza logra aprovechar una vulnerabilidad y afecta la infraestructura o alguno de los activos de la organización, pueden generarse consecuencias directas tanto en la operación como en la seguridad de los sistemas, por esta razón, la gestión de la seguridad de la información no debe enfocarse únicamente en prevenir y reducir los riesgos, sino también en contar con planes de respuesta que permitan actuar de manera organizada frente a un incidente; estos planes deben contemplar acciones de retención, recuperación de la información y continuidad de las operaciones (NIST, 2025).

De igual manera, contar con procedimientos de respuesta claros y con personal preparado para actuar ante este tipo de situaciones puede ayudar a reducir el tiempo durante el cual los servicios permanecen afectados y al mismo tiempo, disminuir los costos financieros y las posibles afectaciones a la reputación de la organización derivados de una brecha de seguridad (IBM, 2025). Por esto, es importante establecer medidas preventivas, correctivas y de recuperación que permitan a la organización responder de manera oportuna cuando una amenaza llega a materializarse.

Desarrollo e Implementación del Aprendizaje

Descripción del Ejercicio

El desarrollo del ejercicio permitió aplicar los conocimientos adquiridos durante el seminario de ciberseguridad y ciberdefensa, relacionando temas como la identificación, análisis y respuesta ante riesgos de ciberseguridad. A fin de realizar la propuesta a la empresa PanamProject, se inició con solicitar permiso mediante correo electrónico a la líder CPD en el cual se dio la autorización para desarrollar el proyecto, siempre y cuándo se cumplieran los acuerdos de confidencialidad. Seguido a esto se preparó una entrevista dirigida a la líder CPD la cual permitió conocer las principales actividades que se realizan en la empresa y que permiten garantizar la continuidad, disponibilidad y seguridad de la infraestructura tecnológica, así mismo esta entrevista permitió conocer las amenazas de ingeniería social que pueden afectar las operaciones de la empresa. Teniendo en cuenta que los operadores Datacenter son quienes están a diario en contacto con el personal y técnicos que ingresan a los Datacenter, se preparó una encuesta dirigida a los operadores,² con el fin de conocer que tan preparados se sienten para afrontar diferentes situaciones. Después de realizar la entrevista a la Líder CPD y de aplicar la encuesta a los operadores Datacenter, se realizó el análisis de amenazas basado en los datos obtenidos de estos ejercicios, dicho análisis permitió conocer cuáles son los eventos que de ocurrir en la compañía generan el mayor impacto en la ejecución de las labores diarias de la

² El detalle de la entrevista de puede ver en el anexo 3.

empresa. Los resultados obtenidos en la encuesta aplicada a los operadores, así como su análisis se presentan a continuación:

Tabla 1

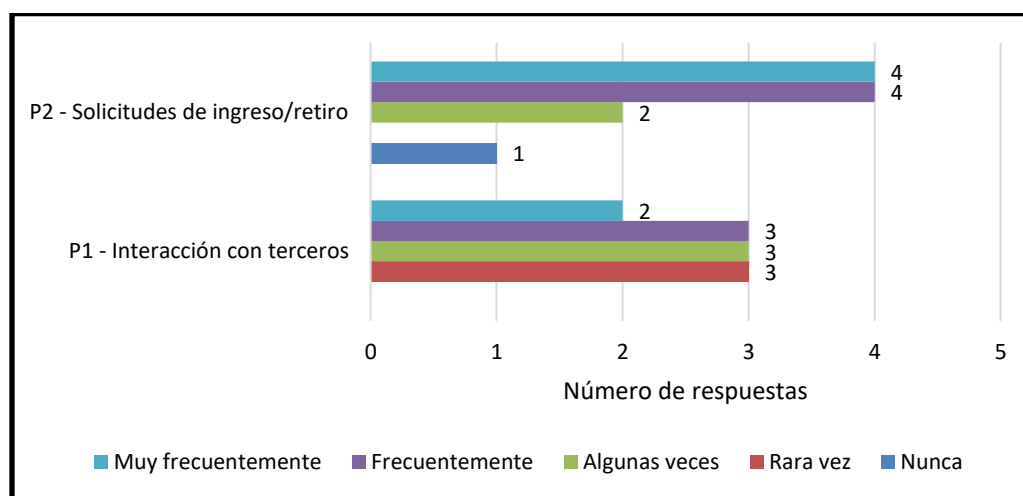
Tabla de caracterización de la encuesta

Elemento	Descripción
Población objetivo	Operadores de Datacenter
Número de participantes	11 operadores
Número de preguntas	16
Tipo de instrumento	Encuesta anónima
Escala de valoración	De 1 a 5
Preguntas de frecuencia	Preguntas 1 y 2
Pregunta abierta	Pregunta 16
Temas abordados	Interacción con terceros, procedimientos, ingeniería social, reporte de incidentes y capacitación
Finalidad	Complementar la información obtenida mediante la entrevista a la Líder CPD

Nota. Elaboración propia a partir de los resultados de la encuesta aplicada a los operadores del Datacenter.

Figura 1

Diagrama de barras horizontales que muestra la frecuencia de interacción con personal y recepción de solicitudes de ingreso

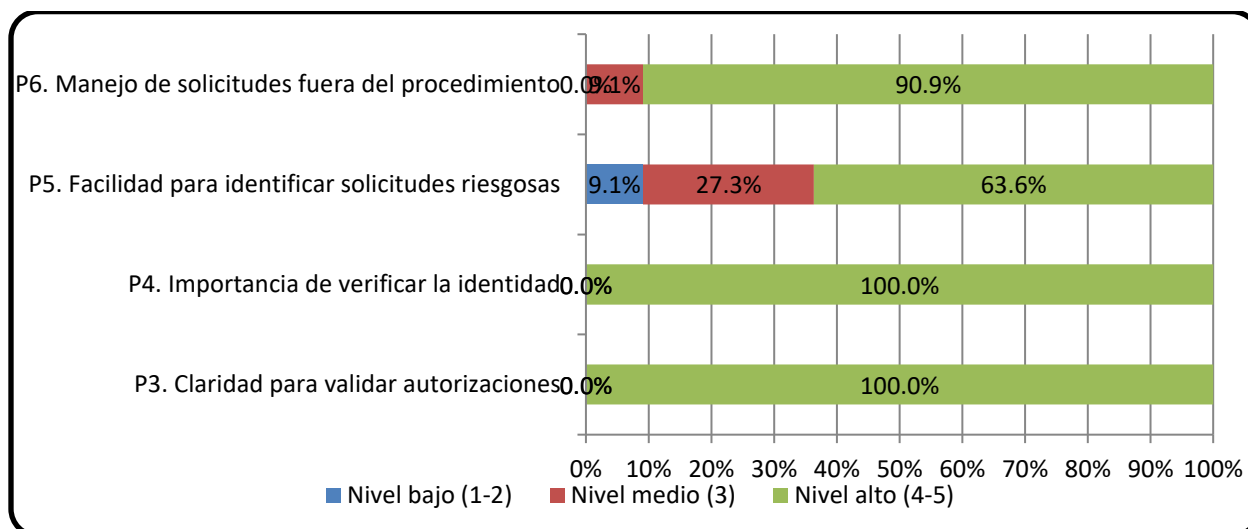


Nota. Elaboración propia a partir de los resultados de la encuesta aplicada a los operadores del Datacenter.

Los resultados muestran que los operadores mantienen contacto con terceros con diferentes niveles de frecuencia. Asimismo, las solicitudes relacionadas con el ingreso de personas, equipos, elementos o medios se presentan principalmente de manera frecuente o muy frecuente. Esta interacción constituye un aspecto relevante para el análisis de amenazas de ingeniería social, debido a que puede generar escenarios en los que se solicite validar identidades, autorizaciones o permisos.

Figura 2

Diagrama de barras horizontales apiladas al 100% que muestra la validación y cumplimiento de procedimientos

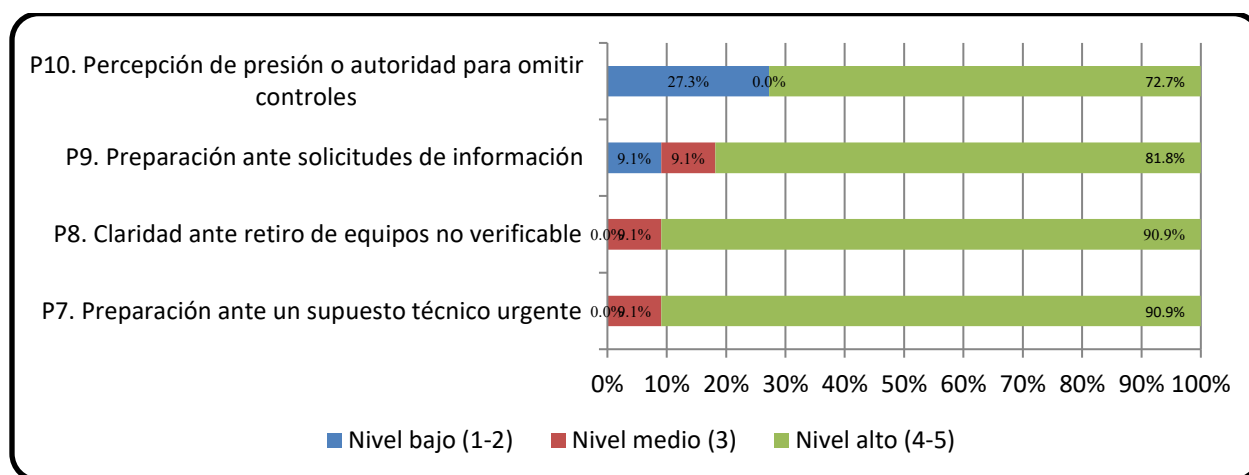


Nota. Elaboración propia a partir de los resultados de la encuesta aplicada a los operadores del Datacenter.

Se observa una percepción alta respecto a la claridad del procedimiento para validar autorizaciones y la importancia de verificar la identidad de terceros. Sin embargo, en la identificación de solicitudes que pueden representar un riesgo se presenta una mayor dispersión de las respuestas. El 9,1% de los participantes se ubica en el nivel bajo y el 27,3% en el nivel medio, lo que en conjunto representa el 36,4% de las respuestas. Con este resultado se evidencia una oportunidad de fortalecimiento mediante la socialización de criterios de alerta y ejemplos de situaciones sospechosas.

Figura 3

Diagrama de barras horizontales apiladas al 100% que muestran las situaciones de ingeniería social



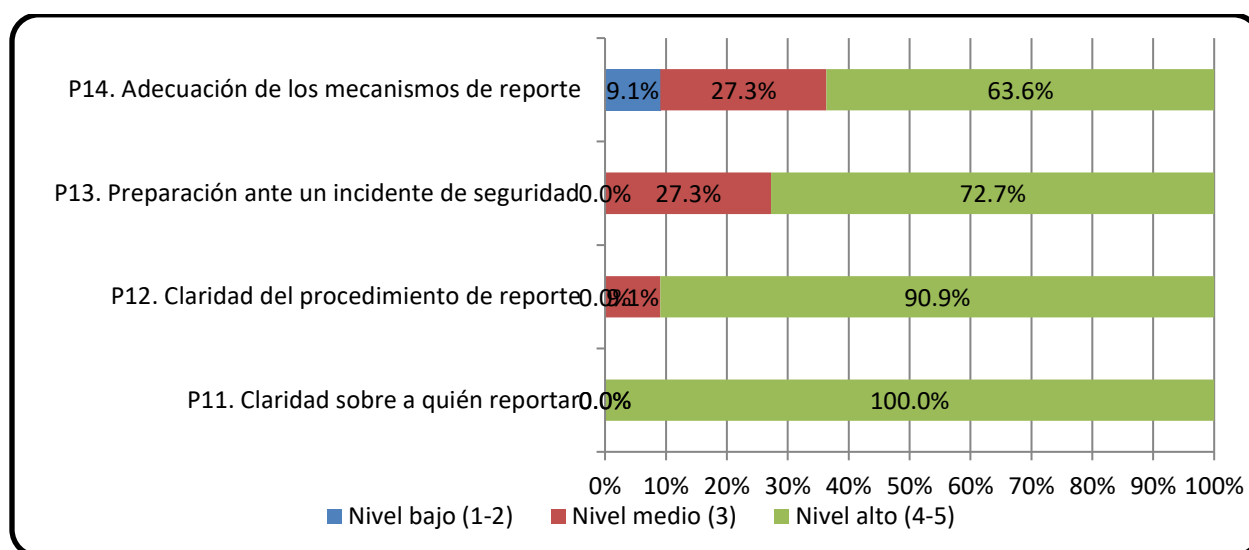
Nota. Elaboración propia a partir de los resultados de la encuesta aplicada a los operadores del Datacenter.

La mayoría de los participantes manifestó niveles altos de preparación o claridad frente a los escenarios hipotéticos relacionados con la suplantación de técnicos, el retiro de equipos y la solicitud de información operativa. No obstante, un 27,3% de los participantes calificó en niveles bajo o medio su percepción sobre la posibilidad de identificar o gestionar situaciones relacionadas con solicitudes de información. Adicionalmente, el 72,7% percibe que podrían presentarse intentos de utilizar la presión, la urgencia o la autoridad para lograr la omisión de procedimientos. Estos resultados justifican la inclusión de controles de validación, escalamiento y capacitación dentro de la propuesta de concientización. Se debe tener en cuenta que en la pregunta 10, el 72,7% no significa que el control sea adecuado; significa que esa proporción percibe con

puntuación alta la posibilidad de que se utilice presión o autoridad para omitir procedimientos.

Figura 4

Diagrama de barras horizontales apiladas al 100% que muestra el reporte y respuesta ante incidentes



Nota. Elaboración propia a partir de los resultados de la encuesta aplicada a los operadores del Datacenter.

Los resultados reflejan una percepción alta respecto al conocimiento de los responsables y de los procedimientos de reporte, sin embargo, se identifican mayores niveles de respuesta media o baja en la preparación ante un posible incidente y en la percepción sobre la adecuación de los mecanismos de reporte. Estos aspectos deben considerarse en la propuesta de concientización, especialmente en lo relacionado con las acciones que deben ejecutarse, los responsables y los canales de escalamiento.

El 90,9% de los participantes en la encuesta realizada a los operadores calificó con niveles altos la necesidad de fortalecer la capacitación en identificación de ingeniería social y respuesta ante situaciones sospechosas. Este resultado respalda la inclusión de actividades de sensibilización, capacitación periódica, ejercicios prácticos y simulaciones de escenarios de amenaza como medidas de concientización.

Seguido a este análisis se empezó a definir el plan de concientización ante incidentes que será entregado a la empresa a fin de que puedan ser analizadas y de ser aceptadas puedan ayudar a disminuir el impacto de los eventos. Este procedimiento resulta importante ya que la gestión de la seguridad de la información va más allá de adquirir licencias e implementar herramientas tecnológicas, también se requiere establecer procedimientos que indiquen como actuar cuando se presenta un incidente. La gestión del ciberriesgo debe ser estructurada mediante un proceso sistemático dividido en diferentes fases claramente definidas, las cuales van a permitir abordar de una manera más integra los riesgos operacionales y humanos en la infraestructura tecnológica como se menciona en NIST, 2025. Así mismo el adoptar controles continuos de formación y respuesta responde a los lineamientos normativos de gestión de riesgos.

Identificación de Procesos y Activos Relevantes

En la entrevista aplicada a la líder CPD³ de la empresa PanamProject se identificaron las principales actividades que se realizan en una jornada laboral a fin de

³ El detalle de la entrevista de puede ver en el anexo 2.

garantizar la continuidad, disponibilidad y seguridad de la infraestructura tecnológica, las cuales se describen a continuación:

- Monitoreo de las instalaciones y de los sistemas críticos.
- Control y gestión de accesos, atención y acompañamiento de personal autorizado.
- Recepción y entrega de equipos o elementos.
- Gestión de solicitudes de ingreso.
- Verificación de trabajos programados, acompañamiento a técnicos y contratistas.
- Revisión de condiciones de las áreas técnicas y registro de novedades e incidentes.

De estas actividades mencionadas aquellas que requieren mayor atención o estricto cumplimiento de procedimientos son las que están relacionadas con el control de acceso, ingreso de personal externo, ingreso o retiro de equipos, reporte de incidentes y manos remotas. Estas actividades requieren especial rigurosidad porque una validación incorrecta o el incumplimiento de un procedimiento puede afectar la seguridad física, la disponibilidad de los servicios, la integridad de la infraestructura o la confidencialidad de la información.

Por otra parte, también se realizó la identificación de los activos relevantes que tiene la empresa y que pueden resultar afectados si ocurre un incidente de ciberseguridad, considerando como los más relevantes los activos intangibles que son:

- La reputación de la empresa.
- La propiedad intelectual.
- Datos recolectados de los clientes, empleados y socios.

- Medios de pago.
- Documentación legal de la empresa.
- Software como bases de datos.
- Aplicativos para la realización diaria de las actividades.

Entre los activos tangibles se cuentan con:

- Equipos de cómputo para la realización de las actividades del datacenter.

Finalmente, esta actividad permitió conocer más a la empresa identificando sus actividades diarias y los activos que tienen a fin de que mediante este trabajo se puedan dar pautas para disminuir las amenazas de ingeniería social que se pueden presentar en la ejecución de las labores.

Identificación de Amenazas de Ingeniería Social

Actualmente, la sociedad se encuentra ciberconectada, ya sea mediante las redes sociales, dispositivos tecnológicos que hay en los hogares de tipo IoT, los dispositivos móviles en los que se ven noticias a diario y otros medios que hacen parte de la vida cotidiana, diariamente las personas se relacionan entre sí, aun cuando muchas de ellas ni se conocen, teniendo esto en cuenta no hay manera de estar 100% protegidos de la ingeniería social, pero si es posible tener educación y aprender técnicas de seguridad que pueden disminuir las diferentes amenazas que se presentan continuamente como el robo de información, y esto mismo ocurre en una empresa. El aprendizaje constante es fundamental, ya que el factor humano sigue siendo uno de los más explotados en los incidentes de ciberseguridad a nivel global, donde el éxito de los ataques depende en su mayoría de la manipulación de la confianza y el incumplimiento de los procedimientos,

como lo menciona (Verizon, 2025; ENISA, 2025). Por esto mismo es clave y crucial el fortalecer la cultura organizacional enfocado en la concientización y el cumplimiento de los controles de seguridad para reducir el riesgo operacional mencionado en ISO/IEC 27001, 2022

Basados en la entrevista anteriormente mencionada que se realizó a la líder CPD se identificaron algunas amenazas relacionadas con la interacción que existe entre los operadores del Datacenter y el personal interno de la empresa que puede ser de otras áreas, proveedores y clientes, otras amenazas identificadas son cuando se producen actividades urgentes como fallas, indisponibilidad de servicios o alarmas, esto hace que haya personal fuera del horario habitual y que por la emergencia del momento no se realice el debido control de ingreso y salida de personas o activos. Se encontró otra amenaza y es cuando el operador está nuevo en la labor, dado que es más vulnerable y se le puede presionar para suministrar información o ingreso de personas desconocidas y por la falta del conocimiento sobre quien tiene la autoridad para aprobar una actividad existe la posibilidad de caer en errores, otra amenaza identificada es el exceso de confianza dado que se le puede permitir el ingreso a compañeros de otras áreas y no realizar el debido control de ingreso y salida, también y unido a esta misma amenaza está el suministro de información que no está clasificada para esa persona que pertenece a un área diferente.

A partir de esta información, se puede identificar el phishing como una de las técnicas utilizadas dentro de la ingeniería social; este tipo de ataque busca engañar a las personas mediante mensajes que aparentan ser de fuentes confiables, con el objetivo de

lograr que interactúen con enlaces, archivos o sitios web maliciosos y en algunos casos, entreguen información sensible. La efectividad de estos ataques también está relacionada con factores humanos, como el conocimiento que tienen los usuarios sobre seguridad y su capacidad para identificar señales de phishing (Canham, 2024); ligado a este ataque está el Spear-phishing aquí se aprovechan de la ignorancia de la persona para hacerse pasar por una fuente legítima y hacer que revele información confidencial Kaspersky (s. f.), otro ejemplo de ataque por ingeniería social que se puede presentar en la empresa es el Tailgating, cómo explica Fortinet (2026), es cuando alguien intenta ingresar a un lugar al cuál no está autorizado y se valen de la cortesía de las personas situándose por detrás de alguien que tenga acceso y así ingresar sin tener que validar su identidad, este ataque se puede presentar en la empresa cuando ingresan proveedores y personal externo a la empresa

Identificación de Vulnerabilidades

A partir de la entrevista realizada a la Líder CPD, se identifican varias vulnerabilidades relacionadas principalmente con el factor humano y con la posibilidad de que terceros intenten aprovecharse de situaciones de presión, urgencia o falta de información para evadir los controles establecidos, aquí se presentan las vulnerabilidades:

- **Suplantación de Identidad:** Una de las principales vulnerabilidades es la suplantación de identidad, ya que los operadores tienen contacto frecuente con técnicos, contratistas, proveedores y personal externo, existe la posibilidad de que una persona se presente como alguien autorizado y solicite acceso a las instalaciones o la realización de

una actividad, esto aumenta cuando la autorización se comunica verbalmente, por teléfono o mediante un correo que no puede ser validado fácilmente.

- **Presión para Actuar Rápidamente:** Otra vulnerabilidad importante es la presión para actuar rápidamente, situaciones como fallas críticas, alarmas o supuestas emergencias pueden hacer que el operador tome decisiones apresuradas y omitir alguna de las validaciones requeridas, aunque la operación del Datacenter exige responder rápidamente ante incidentes, una urgencia no debe ser una razón para eliminar los controles de seguridad.
- **Dificultad para Validar Algunas Autorizaciones:** También se identifica como vulnerabilidad la dificultad para validar algunas autorizaciones, especialmente cuando provienen de personas desconocidas, cuando no existe evidencia documental o cuando no está claro quién tiene la autoridad para aprobar una actividad; esto puede generar dudas en el operador y aumentar la posibilidad de que se permita una acción sin contar con la confirmación correspondiente.
- **Retiro de Equipos, Herramientas o Elementos:** El retiro de equipos, herramientas o elementos es otra vulnerabilidad, ya que una persona podría intentar retirar un activo indicando que cuenta con autorización sin que esta pueda ser comprobada. Una situación de este tipo podría afectar la seguridad física, la continuidad de la operación o incluso generar pérdida de información.
- **Entrega de Información Técnica u Operativa:** Finalmente, hay una vulnerabilidad relacionada con la entrega de información técnica u operativa. Un operador puede recibir solicitudes de información sobre equipos, ubicación de

infraestructura, configuraciones, diagramas o demás datos que no hacen parte de sus funciones, y si no existen criterios claros sobre qué información puede o no suministrarse, una persona podría obtener información útil para realizar posteriormente otro tipo de ataque.

Propuestas de Medidas de Concientización

Para reducir los riesgos identificados, se propone fortalecer los controles existentes y especialmente, preparar a los operadores para responder correctamente ante situaciones de ingeniería social.

Principalmente se recomienda realizar capacitaciones periódicas sobre ingeniería social, explicando situaciones que realmente puedan presentarse durante la operación del Datacenter, incluyendo ejemplos y simulaciones de suplantación, llamadas de personas que se hacen pasar por superiores, solicitudes urgentes, intentos de retiro de equipos y solicitudes de información, ya que permiten evaluar cómo reaccionan los operadores ante una situación de presión. Estos ejercicios pueden ayudar a identificar posibles fallas en los procedimientos y reforzar la capacidad del personal para detener una actividad cuando la autorización no pueda ser comprobada.

Se debe fortalecer el proceso de validación de autorizaciones, procurando que las solicitudes de acceso, trabajos, retiros de equipos y actividades especiales puedan ser verificadas mediante canales definidos, teniendo muy presente también que se debe establecer de manera clara quiénes son los responsables de autorizar cada tipo de actividad y quiénes pueden actuar como reemplazo, para cuando el responsable principal

no esté disponible; así se evitaría que el operador tenga que tomar decisiones por cuenta propia ante una situación que no pueda validar.

También seguir manteniendo la trazabilidad de los movimientos de personas y activos, registrando los ingresos, salidas, equipos, herramientas y demás elementos que ingresen o sean retirados del Datacenter, pues estos registros pueden ser de gran utilidad tanto para prevenir incidentes como para realizar una investigación posterior si llegara a ocurrir algo.

Por último, es importante promover una cultura en la que el operador tenga la autoridad y el respaldo para decir "no" cuando una solicitud no pueda ser validada, ya que el operador debe ser consciente de cuando detener temporalmente una actividad por motivos de seguridad, y no sienta que es una falla en el servicio, sino una medida preventiva necesaria.

Plan de Concientización

Etapas Previas: Capacitación y Entrenamiento Práctico

Antes de aplicar las fases establecidas en este plan, los operadores deberán recibir actividades de concientización orientadas al reconocimiento y prevención de situaciones de ingeniería social, estas deberán desarrollarse de manera práctica, utilizando ejemplos relacionados con las actividades que realizan los operadores durante su jornada laboral, de forma que los conocimientos adquiridos puedan relacionarse directamente con las situaciones que podrían presentarse durante la operación del Datacenter, la concientización deberá abordar los siguientes temas:

Conceptos Básicos de Ingeniería Social

Inicialmente se deberán explicar los conceptos fundamentales de ingeniería social, incluyendo la manera en que un atacante puede utilizar factores humanos para obtener acceso a información, instalaciones o activos. También se deberán presentar las principales técnicas utilizadas para este tipo de ataques, como phishing, vishing, smishing y pretexting, entre otras.

Ingeniería Social Aplicada a la Operación del Datacenter

A partir de los conceptos anteriores, los operadores deberán analizar situaciones que puedan presentarse específicamente durante la operación del Datacenter, para esto se podrán plantear escenarios relacionados con el retiro de equipos sin la autorización correspondiente, solicitudes de ingreso a áreas restringidas, supuestas emergencias o solicitudes realizadas por personas que manifiesten representar a un cliente o a un responsable de la empresa. El objetivo será que los operadores identifiquen cómo podrían

presentarse estas situaciones dentro de sus actividades habituales y relacionen cada escenario con los controles y procedimientos establecidos en este plan.

Reconocimiento de Señales de Alerta

Durante las actividades de concientización se deberán identificar las principales señales que pueden indicar un intento de manipulación, entre ellas la presión para actuar rápidamente, solicitudes que pretendan omitir procedimientos, inconsistencias en la información suministrada, personas que no puedan demostrar su identidad o autorización y solicitudes realizadas mediante canales no establecidos.

Aplicación Práctica y Evaluación

De manera periódica, la empresa podrá realizar ejercicios controlados con algunos operadores, mediante situaciones ficticias similares a las que podrían presentarse durante la operación, estos ejercicios podrán incluir solicitudes urgentes, intentos de ingreso a áreas restringidas, retiro de equipos o solicitudes de información sin la autorización correspondiente; con el propósito de verificar si el operador reconoce las señales de alerta y aplica adecuadamente los procedimientos establecidos, sin afectar la operación normal del Datacenter.

Los resultados de las actividades de concientización y de los ejercicios controlados deberán ser utilizados para identificar dificultades y controles que requieran fortalecimiento; cuando se identifiquen oportunidades de mejora, se deberán establecer las acciones correspondientes y, cuando sea necesario, actualizar los contenidos de capacitación, procedimientos o controles.

Fase 1. Identificación

Ante una solicitud que presente características inusuales, presión, urgencia o inconsistencias, el operador debe mantener la calma y detener o no iniciar la actividad solicitada hasta completar las validaciones correspondientes. En esta etapa, el operador debe: Identificar qué actividad está siendo solicitada, para determinar quién realiza la solicitud y el nombre de la empresa o área, después evitar actuar únicamente con base en la urgencia que dice tener la persona, y, por último, no permitir el acceso, retiro de activos o ejecución de actividades hasta confirmar la autorización correspondiente. Se espera que la actividad queda controlada mientras se valida la solicitud.

Fase 2. Validación de Identidad y Autorización

La validación dependerá del tipo de solicitud.

Para el ingreso de personas, se debe comprobar

Identificación de la persona, empresa a la que pertenece, motivo de la visita, persona o área que autoriza el ingreso.

Para el retiro o traslado de equipos o activos, comprobar

Identificación del activo, información registrada del equipo, persona responsable del retiro, empresa a la que pertenece, autorización correspondiente, y coincidencia entre la solicitud y los registros disponibles. El efecto deseado es que la identidad, el motivo de la actividad y la autorización quede confirmada antes de continuar.

Fase 3. Manejo de Supuestas Emergencias

Cuando la persona indique que se trata de una emergencia o solicite actuar de manera inmediata, el operador debe mantener la calma y realizar la validación por los

canales establecidos, esta debe ser confirmada con el responsable correspondiente, por ejemplo: responsable de turno, líder de Operaciones de Datacenter, responsable técnico del servicio o área involucrada. Se espera es que la situación sea confirmada por un responsable autorizado antes de ejecutar acciones que impliquen acceso, intervención o entrega de información.

Fase 4. Protección de la Información

Si durante la interacción se solicita información técnica, operativa, de infraestructura o cualquier otro dato que no se encuentre dentro de las funciones autorizadas del operador, dicha información no debe ser suministrada; la solicitud debe ser remitida al área o responsable autorizado para su validación y atención. El resultado previsto es que se evita la divulgación de información a personas cuya identidad, autorización o necesidad de acceso no haya sido validada.

Fase 5. Escalamiento y Registro

Si la situación presenta características sospechosas, existen inconsistencias o no es posible validar la solicitud, el operador debe escalar inmediatamente el caso al responsable correspondiente y después de esto se debe dejar registro, como mínimo de: Fecha y hora del evento, persona involucrada, empresa o entidad, motivo de la solicitud, actividad que pretendía realizar, responsable o autorizador indicado, validaciones que se hicieron por el operador, resultado de esas validaciones, que acciones se tomaron y el responsable al que se realizó el escalamiento; y cuando aplique, se deben conservar las evidencias disponibles, tales como registros de acceso, tickets, correos electrónicos, comunicaciones, registros de cámaras y cualquier otra evidencia relacionada con la

situación. El resultado que se espera es que el incidente quede documentado y se conserve la información necesaria para su análisis posterior.

Fase 6. Análisis y Cierre

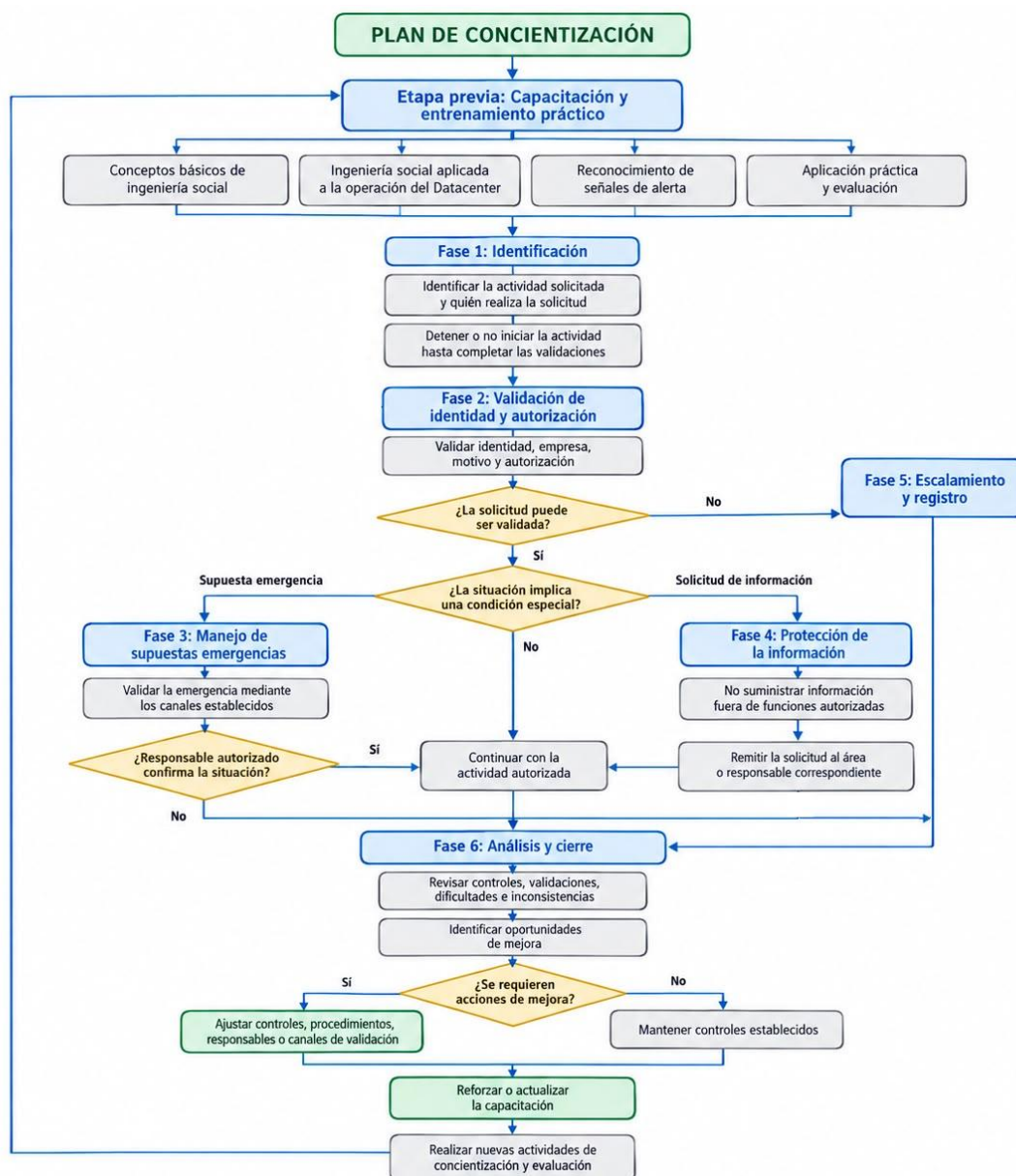
Una vez atendida la situación, el caso debe ser revisado para determinar qué ocurrió y establecer las acciones de seguimiento correspondientes. La revisión debe considerar:

- ¿Qué controles permitieron detectar o contener la situación?
- ¿Qué validaciones fueron efectivas?
- ¿Qué dificultades se presentaron durante la atención?
- ¿Existieron inconsistencias o vacíos en el procedimiento?
- ¿Qué controles podrían fortalecerse?
- ¿Es necesario actualizar procedimientos, responsables o canales de validación?
- ¿Se requiere reforzar la capacitación de los operadores a partir de lo ocurrido?

Esto para determinar si se trató de un intento de ingeniería social, una solicitud real que no pudo ser validada en el momento o una situación que requiere acciones adicionales. El resultado esperado es que se generen oportunidades de mejora y, cuando corresponda, acciones correctivas, preventivas o de capacitación.

Figura 5

Workflow - Diagrama de flujo del plan de concientización sobre ingeniería social en el Datacenter

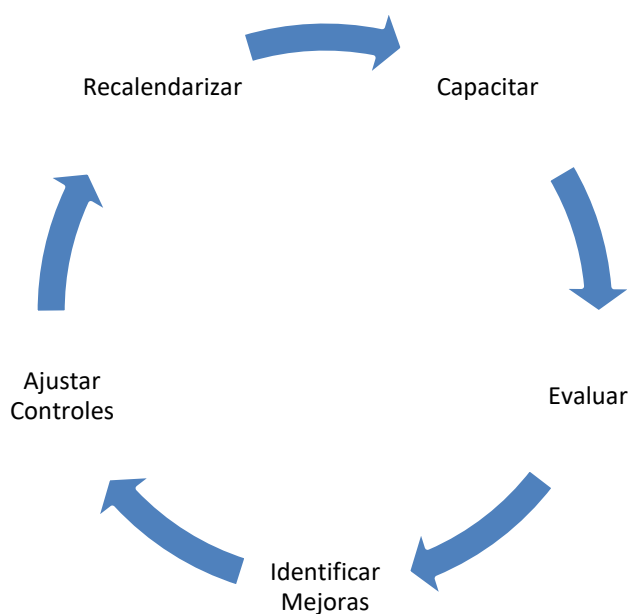


Nota. Elaboración propia.

Ciclo de mejora continua

Figura 6

Diagrama circular que muestra las 5 fases interconectadas de mejora continua



Nota. Elaboración propia.

1. **Capacitación Iniciales:** Este paso se realiza en las medidas de mitigación y corresponde a ejecutar los programas de formación y sensibilización dirigidos a los empleados del Datacenter.
2. **Evaluar:** Mediante simulacros de ataques de ingeniería social, cuestionarios y otros se comprobará el nivel de retención de los empleados ante las medidas de mitigación.
3. **Identificación de Oportunidades de Mejora:** A partir de los resultados de evaluación, se deben de analizar las debilidades detectadas y a partir de ellas determinar qué aspectos del plan requieren ajustes.

4. **Ajuste y Actualización de Controles:** Se mejoran los procedimientos de acuerdo a las oportunidades de mejora del punto anterior.
5. **Reiteración del Ciclo:** Se mejoran los procedimientos y materiales de acuerdo con las oportunidades del punto 3 para garantizar un aprendizaje organizaciones continuo.

Conclusiones

Se logró identificar que las operaciones del Datacenter están expuestas a diferentes amenazas de ingeniería social, especialmente en actividades relacionadas con el ingreso de personas, retiro de equipos, solicitudes de información y situaciones de emergencia, estas amenazas pueden aumentar cuando existe presión, urgencia o dificultad para validar una autorización.

El análisis permitió evidenciar que el factor humano tiene un papel importante en la seguridad de las operaciones, porque aunque los operadores conocen los procedimientos establecidos, todavía se puede fortalecer más la identificación de situaciones sospechosas y la respuesta ante posibles incidentes; se concluye esto ya que la encuesta mostró la necesidad de fortalecer la capacitación sobre ingeniería social, pues el 90,9% de los participantes consideró importante reforzar la formación para identificar y responder ante situaciones sospechosas.

Finalmente, se propuso un plan de concientización y respuesta ante incidentes que establece acciones de identificación, validación, protección de la información, escalamiento, registro y análisis; el plan busca fortalecer los controles existentes y promover una cultura en la que los operadores puedan detener una actividad cuando no sea posible comprobar su autorización.

Referencias

- Canham, M., Dawkins, S., & Jacobs, J. (2024). Not all victims are created equal: Investigating differential phishing susceptibility. National Institute of Standards and Technology.
<https://doi.org/10.6028/NIST.GCR.24-029>
- European Union Agency for Cybersecurity. (2025). ENISA threat landscape 2025.
<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>
- Fortinet. (2026). Ataque de cola: Ejemplos y prevención.
<https://www.fortinet.com/lat/resources/cyberglossary/tailgating-attack>
- IBM. (s. f.). ¿Qué es la ingeniería social? <https://www.ibm.com/mx-es/think/topics/social-engineering>
- IBM. (2025). Cost of a Data Breach Report 2025. <https://www.ibm.com/reports/data-breach>
- International Organization for Standardization, & International Electrotechnical Commission. (2022). ISO/IEC 27001:2022 information security, cybersecurity and privacy protection. Information security management systems. Requirements. International Organization for Standardization.
- Kaspersky. (s. f.). ¿Qué es la ingeniería social? <https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering>
- NIST Computer Security Resource Center. (2025, 20 de noviembre). Incident response.
<https://csrc.nist.gov/projects/incident-response>
- Panam Project. (s. f.). Quiénes somos. <https://panamproject.com/quienes-somos/>
- Verizon. (2025). 2025 Data breach investigations report. Verizon Business.
<https://www.verizon.com/business/resources/reports/dbir/>

Anexos

Anexo 1

Respuesta al correo solicitando autorización para realizar el proyecto en la empresa PanamProject.

RE: Solicitud de autorización para proyecto académico en ciberseguridad

Fecha: 2026-09-08 13:04

Estimada Sara,

En atención a la propuesta presentada para el desarrollo de la primera fase del proyecto del *Seminario de Ciberseguridad y Ciberdefensa*, nos permitimos comunicar la viabilidad de la iniciativa bajo el estricto cumplimiento de los acuerdos de confidencialidad, políticas de seguridad corporativa y nuestro rol como contratistas de la organización.

Con el fin de salvaguardar la infraestructura tecnológica, la operación del Datacenter y los activos de información de la compañía, la participación en este ejercicio académico estará sujeta a los siguientes lineamientos operativos:

- **Inexistencia de acceso directos o privilegios:** No se otorgará acceso a bases de datos, sistemas de producción, consolas de administración ni archivos con información sensible o confidencial.
- **Prohibición de modificación y publicación:** Queda estrictamente restringida la modificación de configuraciones o procedimientos operativos, así como la publicación de datos operativos reales o nombres comerciales.
- **Mecanismo de recopilación de información:** El diagnóstico se

limitará exclusivamente al levantamiento de información de alto nivel mediante entrevistas cualitativas, formularios estructurados no sensibles o revisión de procesos generalizados (sin incluir datos identificables).

- **Anonimización estricta de entregables:** Todos los datos e informes resultantes deberán ser completamente anonimizados y presentarse en términos conceptuales y cuantitativos generales, garantizando que no se exponga la topología, vulnerabilidades específicas ni datos de clientes o personal.

Bajo estas condiciones, autorizamos el inicio de la **Fase 1 (Diagnóstico y Planeación)** enfocada en el equipo de Operadores de Datacenter, orientando el alcance hacia un análisis cualitativo sobre riesgos de ingeniería social.

Quedamos a disposición para coordinar las sesiones de levantamiento de información bajo el esquema acordado.

Anexo 2

Guía de preguntas de la entrevista realizada a la Líder CPD de la empresa PanamProject.

Caracterización del proceso

1. ¿Cuáles son las principales actividades que realiza un operador de Datacenter durante una jornada normal?

RTA: Durante una jornada normal, el operador de Datacenter realiza actividades orientadas a garantizar la continuidad, disponibilidad y seguridad de la infraestructura tecnológica. Entre ellas se encuentran el monitoreo de las instalaciones y de los sistemas críticos, control y gestión de accesos, atención y acompañamiento de personal autorizado, recepción y entrega de equipos o elementos, gestión de solicitudes de ingreso, verificación de trabajos programados, acompañamiento a técnicos y contratistas, revisión de condiciones de las áreas técnicas y registro de novedades e incidentes.

2. ¿Cuáles de estas actividades requieren mayor atención o estricto cumplimiento de procedimientos?

RTA: Principalmente las relacionadas con control de acceso, ingreso de personal externo, retiro de equipos, reporte de incidentes y manos remotas.

Estas actividades requieren especial rigurosidad porque una validación incorrecta o el incumplimiento de un procedimiento puede afectar la seguridad física, la disponibilidad de los servicios, la integridad de la infraestructura o la confidencialidad de la información.

3. ¿Con qué tipos de personas interactúan habitualmente los operadores?

RTA: Los operadores interactúan habitualmente con:

- Personal interno de la organización.
- Personal de otras áreas.
- Técnicos especializados.
- Proveedores.
- Contratistas.
- Personal de clientes, cuando aplique.
- Personal de empresas de telecomunicaciones, energía, mantenimiento u

otros servicios relacionados con la infraestructura.

4. ¿Qué actividades requieren validar la identidad, autorización o permisos de una persona antes de realizar una determinada acción?

RTA: Toda actividad dentro del área blanca que implique el ingreso al Datacenter o a áreas restringidas. La validación debe realizarse antes de permitir la actividad, no después de iniciarla.

5. ¿Qué actividades requieren registrar o controlar el ingreso y salida de personas, equipos, elementos o medios?

RTA: El ingreso y salida de personal, técnicos, contratistas y proveedores debe quedar sujeto a los mecanismos de control establecidos. Igualmente, debe existir trazabilidad sobre el ingreso, traslado o retiro de equipos, herramientas, materiales, repuestos, dispositivos y demás elementos que puedan afectar la operación o la seguridad del Datacenter.

Situaciones de riesgo

6. ¿Qué situaciones podrían generar un riesgo para la operación cuando una persona solicita acceso, información o la realización de alguna actividad?

RTA: El principal riesgo se presenta cuando la persona no puede demostrar de manera verificable que está autorizada, cuando proporciona información inconsistente, cuando la solicitud no corresponde con una actividad programada o cuando pretende obtener acceso o información que excede el alcance de su trabajo. También representan un riesgo las solicitudes realizadas por teléfono, correo o verbalmente sin una validación suficiente, especialmente cuando buscan generar confianza o presión sobre el operador.

7. ¿Se han presentado o podrían presentarse situaciones en las que una persona solicite realizar una actividad de manera urgente o fuera del procedimiento habitual?

RTA: Sí. En una operación de infraestructura crítica pueden presentarse situaciones urgentes relacionadas con fallas, indisponibilidad de servicios, alarmas, mantenimiento no programado o requerimientos de clientes. La urgencia no debería eliminar los controles. En estos casos se debe aplicar el mecanismo establecido para validar la emergencia y obtener las autorizaciones correspondientes, dejando la respectiva trazabilidad.

8. ¿Qué circunstancias podrían llevar a un operador a omitir, flexibilizar o realizar de manera incorrecta un procedimiento establecido?

RTA: Entre las principales circunstancias se encuentran la presión por atender una emergencia, solicitudes insistentes de terceros, falta de claridad sobre quién tiene la

autoridad para aprobar una actividad, exceso de confianza, desconocimiento del procedimiento, falta de capacitación o situaciones en las que el operador considere que retrasar una actividad podría afectar el servicio. Por esta razón es importante que los procedimientos sean claros y que el operador tenga definido a quién escalar una situación cuando no pueda validarla por sus propios medios.

9. ¿Qué tipo de solicitudes podrían resultar difíciles de validar para un operador antes de autorizar o ejecutar una actividad?

RTA: Las solicitudes más complejas son aquellas que involucran una supuesta emergencia, solicitudes realizadas por personas que el operador no conoce, autorizaciones comunicadas verbalmente, solicitudes provenientes de otras áreas sin evidencia documental, retiro de equipos o elementos con autorizaciones que no pueden ser verificadas y solicitudes de acceso a información técnica u operativa.

10. ¿Qué situaciones podrían generar presión sobre el operador para actuar rápidamente o tomar una decisión sin realizar todas las validaciones?

RTA: Una falla crítica, una alarma, una interrupción de servicio, la presencia de un supuesto técnico que manifiesta una emergencia, llamadas insistentes de superiores o clientes, amenazas de afectación del servicio o solicitudes relacionadas con trabajos que supuestamente deben realizarse inmediatamente. En estos escenarios es fundamental que el operador entienda que la presión o urgencia no reemplaza la autorización.

Ingeniería social

11. ¿Qué tan frecuente considera que los operadores interactúan con personal externo o terceros?

RTA: La interacción con personal externo es frecuente, especialmente con técnicos, contratistas, proveedores, empresas de mantenimiento y personal relacionado con servicios de telecomunicaciones, energía, aires, seguridad y otros sistemas asociados a la infraestructura. Por esta razón, el factor humano constituye un elemento importante dentro de la seguridad operacional.

12. ¿Qué mecanismos o procedimientos se utilizan actualmente para verificar que una persona está autorizada para realizar una actividad?

RTA: La validación debe realizarse mediante los mecanismos definidos por la organización, tales como identificación personal, verificación de la solicitud o autorización y confirmación con las áreas responsables cuando sea necesario. Cuando alguno de estos mecanismos no permita confirmar la autorización, el operador debe detener la actividad y escalar la situación.

13. ¿Cómo debería actuar un operador si un supuesto técnico manifiesta tener una situación de emergencia y solicita acceso inmediato?

RTA: Debe mantener la calma y evitar tomar decisiones basadas únicamente en la urgencia manifestada por la persona. Debe solicitar su identificación, verificar la empresa a la que pertenece, validar la existencia de la emergencia y confirmar la autorización con el responsable correspondiente. Si la autorización no puede ser confirmada, no debe permitir el acceso únicamente por la presión o urgencia alegada y debe escalar la situación al responsable de turno o al área correspondiente.

14. ¿Cómo debería actuar un operador si alguien solicita retirar un equipo o elemento indicando que cuenta con autorización, pero esta no puede ser verificada?

RTA: No debe autorizar el retiro hasta confirmar formalmente la autorización.

Debe validar la identidad de la persona, el equipo o elemento que pretende retirar, la autorización correspondiente y el responsable que aprobó la actividad. Si existe alguna inconsistencia, debe suspender el retiro y reportar la situación.

15. ¿Cómo debería actuar un operador si una persona solicita información técnica u operativa que no está autorizado a proporcionar?

RTA: Debe abstenerse de entregar la información y explicar que, por políticas de seguridad y alcance de su función, no está autorizado para suministrarla. La solicitud debe ser direccionada al área o responsable competente. Esto aplica especialmente para información relacionada con infraestructura, configuraciones, ubicación de equipos, credenciales, diagramas, direccionamiento, capacidades, vulnerabilidades o cualquier información que pueda comprometer la seguridad.

Controles y preparación

16. ¿Qué controles o medidas considera que actualmente ayudan a prevenir situaciones de ingeniería social dentro del proceso de Operaciones de Datacenter?

RTA: Los principales controles son el control de acceso físico, la identificación y validación del personal, el registro de ingresos y salidas, la autorización previa de trabajos, el acompañamiento o supervisión de terceros cuando corresponde, la trazabilidad de equipos y elementos, los registros operativos y la posibilidad de escalar situaciones que no puedan ser validadas.

Estos controles permiten establecer una barrera antes de que una persona pueda acceder físicamente a infraestructura o información crítica.

17. ¿Considera que los operadores cuentan con la capacitación o lineamientos necesarios para identificar y manejar situaciones relacionadas con ingeniería social?

RTA: Los operadores cuentan con lineamientos operativos y de seguridad que permiten gestionar las actividades habituales. Sin embargo, considero conveniente fortalecer continuamente la capacitación específica en ingeniería social, suplantación de identidad, manejo de situaciones de presión, identificación de comportamientos sospechosos y protocolos de escalamiento. La capacitación debe ser periódica y acompañarse de casos prácticos o simulaciones.

18. ¿Qué aspectos considera que podrían fortalecerse para reducir el riesgo de este tipo de situaciones?

RTA: Consideraría importante fortalecer:

- Capacitación periódica en ingeniería social.
- Simulaciones de escenarios reales.
- Claridad en los responsables de autorización.
- Procedimientos específicos para emergencias.
- Mecanismos de validación de autorizaciones.
- Trazabilidad de ingreso y retiro de equipos.
- Revisión periódica de permisos y accesos.
- Canales de escalamiento claramente definidos.
- Cultura de seguridad que permita al operador decir “no” o detener una

actividad cuando no pueda validar una autorización, sin temor a represalias por retrasar una solicitud.

Incidentes y respuesta

19. ¿Qué considera que debería hacerse inmediatamente ante la identificación de una situación sospechosa?

RTA: El operador debe mantener el control de la situación, no permitir que la actividad continúe hasta realizar las validaciones correspondientes, evitar entregar información adicional y comunicar inmediatamente la situación al responsable definido. Debe preservar los registros y evidencias disponibles y evitar confrontaciones innecesarias con la persona involucrada.

20. ¿A quién o a qué área debería reportarse una situación de este tipo?

RTA: Inicialmente debe reportarse al responsable o líder de Operaciones de Datacenter y nuestro líder técnico de parte de nuestro cliente.

21. ¿Existe actualmente un procedimiento general para reportar y atender incidentes relacionados con situaciones de seguridad?

RTA: Existen mecanismos y procedimientos de gestión y escalamiento de novedades e incidentes. No obstante, considero importante que estos procedimientos sean conocidos por todos los operadores y que exista claridad sobre el canal específico que debe utilizarse frente a una situación de posible ingeniería social.

22. ¿Qué dificultades podrían presentarse al momento de reportar o atender un incidente?

RTA: Las principales dificultades podrían estar relacionadas con la falta de información inicial, incertidumbre sobre la legitimidad de la solicitud, presión por resolver rápidamente una situación, falta de disponibilidad inmediata del responsable que

debe autorizar una actividad o desconocimiento del canal correcto de escalamiento. Por ello es importante contar con responsables alternos y mecanismos de escalamiento claramente definidos.

23. ¿Qué información considera importante registrar cuando ocurre una situación sospechosa o un incidente?

RTA: Se debe registrar, como mínimo:

- Fecha y hora del evento.
- Identificación de la persona involucrada.
- Empresa a la que manifiesta pertenecer.
- Motivo de la solicitud.
- Actividad que pretendía realizar.
- Equipo, activo o infraestructura involucrada.
- Persona o área que supuestamente autorizó la actividad.
- Medio por el cual se recibió la solicitud.
- Validaciones realizadas.
- Respuesta o actuación del operador.
- Personas o áreas a las que se escaló.
- Evidencias disponibles, como registros de acceso, tickets, correos,

comunicaciones o registros de cámaras, cuando corresponda.

- Resultado final de la situación.

Anexo 3

Cuestionario de la encuesta aplicada a los operadores del Datacenter.

Encuesta académica – Seminario de Ciberseguridad y Ciberdefensa**Interacción y exposición**

Preguntas relacionadas con la interacción habitual con personal interno, terceros y otras personas durante las actividades de operación.

1. ¿Con qué frecuencia interactúa con personal externo o terceros durante sus actividades?

- Nunca
- Rara vez
- Algunas veces
- Frecuentemente
- Muy frecuentemente

2. ¿Con qué frecuencia recibe solicitudes relacionadas con el ingreso de personas, equipos, elementos o medios?

- Nunca
- Rara vez
- Algunas veces
- Frecuentemente
- Muy frecuentemente

Validación y cumplimiento de procedimientos

Preguntas orientadas a conocer la percepción sobre la claridad y cumplimiento de los procedimientos establecidos.

En una escala de 1 a 5 evalúe las siguientes situaciones

3. ¿Qué tan claro tiene el procedimiento que debe seguir para validar la autorización de una persona antes de permitirle realizar una actividad?

1 - 2 - 3 - 4 - 5

4. ¿Qué tan importante considera verificar la identidad y autorización de terceros antes de permitirles realizar una actividad?

1 - 2 - 3 - 4 - 5

5. ¿Qué tan fácil considera que es identificar cuándo una solicitud puede representar un riesgo de seguridad?

1 - 2 - 3 - 4 - 5

6. ¿Considera que los procedimientos actuales permiten manejar adecuadamente solicitudes que se presentan fuera del procedimiento habitual?

1 - 2 - 3 - 4 - 5

Situaciones de ingeniería social

Situaciones hipotéticas relacionadas con engaño, suplantación, presión o solicitudes no habituales.

En una escala de 1 a 5 evalúe las siguientes situaciones

7. Si una persona que usted no reconoce manifiesta ser un técnico autorizado y solicita ingresar con carácter urgente, ¿Qué tan preparado se siente para actuar correctamente?

1 - 2 - 3 - 4 - 5

8. Si una persona solicita retirar un equipo o elemento indicando que tiene autorización, pero esta no puede ser verificada, ¿Qué tan claro tiene el procedimiento que debe seguir?

1 - 2 - 3 - 4 - 5

9. Si una persona solicita información técnica u operativa que usted considera que no debería proporcionar, ¿Qué tan preparado se siente para manejar la situación?

1 - 2 - 3 - 4 - 5

10. ¿Qué tan frecuente considera que una persona podría intentar utilizar la urgencia, presión o autoridad para lograr que un operador omita un procedimiento?

1 - 2 - 3 - 4 - 5

Reporte y respuesta a incidentes

Preguntas relacionadas con la identificación, reporte y actuación ante situaciones sospechosas o posibles incidentes de seguridad.

En una escala de 1 a 5 evalúe las siguientes situaciones

11. ¿Qué tan claro tiene a quién debe informar una situación sospechosa relacionada con seguridad?

1 - 2 - 3 - 4 - 5

12. ¿Qué tan claro tiene el procedimiento que debe seguir cuando identifica una situación sospechosa?

1 - 2 - 3 - 4 - 5

13. ¿Qué tan preparado considera que está para actuar ante un posible incidente de seguridad?

1 - 2 - 3 - 4 - 5

14. ¿Considera que actualmente existen mecanismos adecuados para reportar oportunamente una situación sospechosa o incidente?

1 - 2 - 3 - 4 - 5

Capacitación y mejora

Preguntas orientadas a identificar necesidades de capacitación y oportunidades de mejora.

En una escala de 1 a 5 evalúe las siguientes situaciones

15. ¿Considera necesario fortalecer la capacitación de los operadores en identificación de ingeniería social y respuesta ante situaciones sospechosas?

1 - 2 - 3 - 4 - 5

16. Desde su experiencia, ¿Qué aspecto considera que podría mejorarse para prevenir o atender situaciones de ingeniería social o seguridad dentro del proceso?

Respuesta abierta