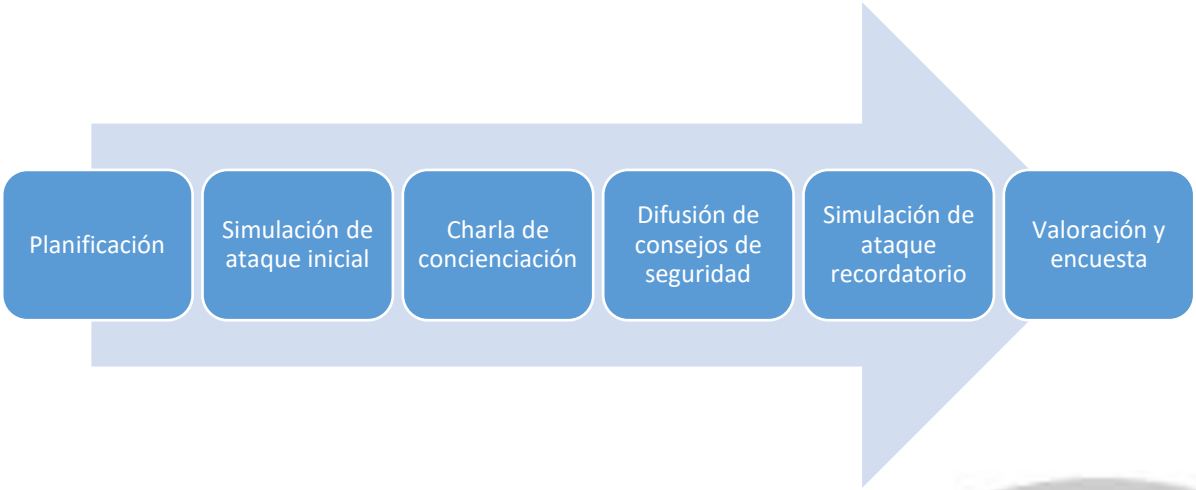
Introducción:

El objetivo de este ciberejercicio es obtener una visión general del grado de concienciación de nuestros usuarios con respecto a la seguridad de la información. Cada organización es diferente, por lo que cada ciberejercicio podrá ser personalizado, de acuerdo a las características propias de ésta.
Los ciberejercicios constan de las siguientes fases:



Fase 1: Planificación

Duración: 5 días laborales
Descripción: Evaluación inicial del nivel de concienciación en seguridad y preparación del ciberejercicio

Para la planificación del ciberejercicio, el CERT-PY requerirá la colaboración de una o más persona de la organización. Es fundamental que el ciberejercicio esté debidamente autorizado, en lo posible, por la máxima autoridad; sin embargo, es importante que la preparación de los simulacros de ataque pase desapercibida para el mayor número de empleados posible y que solo unas pocas personas, solo las estrictamente necesarias, sepan de su existencia.
Durante la planificación se establecerá el escenario de ataque y el vector de ataque, de acuerdo al nivel de madurez que se pretende evaluar. En el caso de organizaciones que cuentan con un bajo nivel de concienciación en sus usuarios, un escenario y vector básico podrá ser suficiente para una

evaluación inicial. Sin embargo, para organizaciones que cuentan con un mayor grado de concienciación, será necesario diseñar escenarios y vectores más avanzados para poner a los usuarios a prueba.
Es importante recordar que en ningún caso los ataques incluirán ningún tipo de daño a sistemas, extracción de información ni persistencia.
Los recursos tecnológicos serán, en su mayoría, proveídos por el CERT-PY. En caso de ser requeridos recursos adicionales, se coordinará con la organización participante.

Fase 2: Simulación de ataque inicial

Duración: 3-10 días laborales
Descripción: Simulación de un ataque dirigido a usuarios de la organización y evaluación del mismo

El objetivo de estos «ataques dirigidos» es exponer a los usuarios de la organización a una amenaza de ciberseguridad controlada y evaluar el actuar de los mismos.
Se plantea un ataque dirigido a través del envío de un correo electrónico que contiene un enlace que simula un *phishing*. El escenario deberá adaptarse de acuerdo a cada organización y su contexto, de modo a parecer legítimo y/o atractivo para el usuario.
Se trata de un escenario controlado, en el que la apertura del enlace no realizará ninguna acción sobre el sistema o información de la "víctima", sino la redirigirá a la página web del CERT-PY donde se le indicará qué fue lo que pasó, explicando el riesgo que supone lo que hizo y se le dará unas advertencias y consejos de seguridad.
Es fundamental que los usuarios que hayan caído en el ataque no lo comenten entre sus compañeros, de modo a poder observar las reacciones naturales y propias de cada usuario.
Al finalizar el periodo de simulación de ataque, se elaborará un reporte general de acuerdo a las acciones observadas: cuántos usuarios han abierto los correos sospechosos, cuántos han abierto los enlaces, cuántos han introducido datos, qué grupos laborales son los más afectados, etc.

Fase 3: Charla de concienciación

Duración: 1 día laboral - 2~4 horas
Descripción: Charla de concienciación de los riesgos de ciberseguridad para los usuarios

Luego de la fase de simulación de ataque y la evaluación de los resultados de la misma, el CERT-PY ofrecerá una charla de concienciación dirigida a los usuarios de la organización, en la que se expondrán los riesgos de seguridad a los que estamos expuestos a diario, así como las medidas de seguridad que podemos adoptar en el día a día para reducir esos riesgos. Las charlas estarán orientadas a usuarios regulares de la tecnología, no se tratará de una charla técnica y no requerirá ningún conocimiento técnico.

Es fundamental que todos los usuarios de la organización, o al menos la mayor cantidad posible, participe de esta charla. De acuerdo a lo que se haya planificado con la organización, se podrá dictar una o varias charlas, distribuidas en una o más jornadas. Por ejemplo, en caso de tratarse de una organización muy grande y/o que no sea posible convocar a todos los usuarios a una única charla, la misma podrá ser planificada para varios grupos, en diversos horarios.

La charla de concienciación podrá ser reforzada con cualquier material adicional de concienciación, tales como videos, folletos, trípticos, etc. El CERT-PY propondrá una serie de materiales de apoyo, en su mayoría en formato digital. Se podrá coordinar con la organización los medios adecuados de difusión.

Fase 4: Difusión de consejos de seguridad

Duración: 2 - 4 meses
Descripción: Campaña de concienciación y capacitación de usuarios en seguridad de la información

La organización, con el apoyo del CERT-PY, llevará a cabo una amplia campaña de concienciación para toda la organización, de modo a difundir y reforzar las buenas prácticas de ciberseguridad que todo usuario debe llevar a cabo. Esta campaña buscará que cada usuario sea consciente de su rol en la

seguridad de la información, sintiéndose partícipe del resguardo de la misma, así como se buscará que aprenda y adopte ciertas medidas básicas de seguridad en el uso diario de la tecnología y del Internet. Para que la campaña pueda impactar en los usuarios y que pueda ser asimilada, es necesario que la misma se prolongue una cantidad adecuada de tiempo, recomendándose un mínimo de 2 meses.
Durante la campaña, la organización podrá difundir diversos tipos de materiales de concienciación, tales como videos cortos, folletos, un consejo semanal, afiches en las oficinas, etc. El CERT-PY propondrá una serie de materiales de apoyo, en su mayoría en formato digital. La organización podrá organizar diferentes actividades y/o medios de difusión durante la fase de campaña de concienciación. Esta podrá extenderse más allá del periodo del ciberejercicio, pasando a formar parte de un plan de concienciación permanente en la organización.
Se recomienda siempre dejar un cierto espacio de tiempo entre la distribución de un material y el siguiente, de modo proporcionar tiempo suficiente para que los usuarios tengan la oportunidad de asimilar los contenidos y conceptos explicados.

Fase 5 - Simulación de ataque recordatorio

Duración: 3-10 días laborales
Descripción: Simulación de un nuevo ataque dirigido a usuarios de la organización y evaluación final luego del proceso de concienciación

Se considera oportuno, una vez pasados unos 3~6 meses de la primera simulación de ataque, repetir las pruebas de los ataques dirigidos o realizar una nueva con el fin de que sea algo nuevo para los empleados, cambiando el escenario y/o el vector de ataque.
Esta nueva simulación de ataque tiene dos objetivos. Por una parte, buscará que los usuarios recuerden los consejos de seguridad difundidos durante las campañas de concienciación. Por otra parte, permitirá evaluar el impacto de este ciberejercicio en cuanto al aumento del grado de concienciación en ciberseguridad en la organización, en comparación al nivel que se tenía antes de iniciar.

Fase 6: Valoración y encuesta de satisfacción

Duración: 10 ~ 20 minutos
Descripción: Valoración sobre el ciberejercicio

Una vez se haya finalizado el ciberejercicio, la organización completará una breve encuesta de valoración del mismo, acerca de su experiencia y opinión sobre el proceso de implantación y su utilidad en materia de concienciación de la seguridad de la información.
La encuesta deberá ser completada únicamente por las personas de la organización que estuvieron involucrados en la implantación del ciberejercicio. De forma opcional, otras personas de la organización también podrán completarla.
De esta forma el CERT-PY obtendrá una retroalimentación de información continua y una base sobre la que mejorar nuestros ciberejercicios.