

Notas explicativas del cuestionario de la Evaluación Nacional de Riesgos Cibernéticos

ENRC XXX

*Estas notas explicativas deben ser editadas para adaptarlas al propósito del usuario que realiza una ENRC*

## Contexto

La organización <nombre de la organización que comisiona> ha comisionado una Evaluación Nacional de Riesgos Cibernéticos (**ENRC**)con el objetivo de ayudar a planificar una mayor inversión en ciberseguridad y en resiliencia. Las razones para realizar esta Evaluación Nacional de Riesgos a la Ciberseguridad son:

o El desarrollo económico y social de <nombre del país> dependerá de la existencia de niveles significativos de conectividad a través del ciberespacio. Como en muchas naciones donde la digitalización se está introduciendo a una escala importante, la economía, la administración del gobierno y la provisión de servicios esenciales dependerán cada vez más de la integridad del ciberespacio; de la infraestructura, y de los sistemas y datos que los sustentan. Esto traerá consigo oportunidades para la innovación, el crecimiento y la eficiencia, pero es probable que acarree también riesgos de perturbación social y económica.

o En ocasiones, al introducir hardware y software para facilitar el entorno digital interconectado, se ha priorizado tanto la eficiencia, como el costo y la conveniencia del usuario, pero no siempre se ha considerado la seguridad desde un principio. Los actores maliciosos (estados hostiles, organizaciones e individuos criminales o terroristas) pueden aprovechar tales deficiencias. El gobierno requiere garantías de que los sistemas adquiridos en el mercado comercial proporcionarán niveles adecuados de continuidad productiva mediante seguridad y resiliencia cibernética.

El gobierno puede utilizar sus propios recursos para hacer frente a las amenazas cibernéticas. Sin embargo, la escala y la naturaleza dinámica de tales amenazas implican que ningún gobierno puede, por sí mismo, abordar todos los aspectos de la ciberseguridad y ciber resiliencia. Al contrario, se necesita un enfoque en el que la industria, los proveedores de infraestructura y otros socios en el desarrollo del país colaboren entre sí y con el gobierno para proteger las redes, los servicios y los datos. Por lo tanto, el propósito de esta ENRC es:

* Proporcionar al Gobierno una base racional para priorizar su propia inversión en ciberseguridad nacional
* Ayudar a comunicar los riesgos identificados a las partes interesadas clave para crear una cultura de gestión de ciber-riesgos, seguridad y resiliencia.

## Método

La ENRC comenzará con una Encuesta de sistemas cibernéticos significativos en uso por parte de organizaciones y empresas que utilizan estos sistemas para brindar servicios que son esenciales para la economía, el gobierno y el bienestar de la población. Estos servicios de infraestructura nacional son:

*“Estructuras, sistemas, sitios, información, personas, redes y procesos necesarios para el funcionamiento del país y de los cuales depende la vida diaria. Por lo general, estos incluyen energía, alimentos, agua, salud, transporte, suministro de dinero, comunicaciones, servicios de emergencia y aspectos del ejercicio del gobierno, incluida la defensa. También comprenden algunas funciones, sitios y organizaciones que no son fundamentales para el mantenimiento de los servicios esenciales, pero que necesitan protección debido al peligro potencial que representan para el público (por ejemplo, instalaciones químicas)”.*

La ENRC utiliza un método simplificado de evaluación cualitativa de riesgos para identificar aquellos sistemas que corren un riesgo mayor de interrupción de servicios esenciales para la economía o la sociedad. Esta 'evaluación de riesgo', completamente basada en la información proporcionada voluntariamente por los participantes en la Encuesta (usted) en respuesta a este Cuestionario confidencial, podría dar pie a más discusiones confidenciales a fin de permitir que el Gobierno evalúe riesgos mayores.

## El Cuestionario

* Las respuestas al cuestionario serán confidenciales. El cuestionario se alojará en [un sitio web Seguro del gobierno]. [Se tomarán otras medidas para proteger la información]. [El detalle de las respuestas no será compartido con otros participantes].
* Las organizaciones participantes podrán contactar a [los organizadores] para clarificar preguntas; y se les podrá solicitar que se reúnan con [los organizadores] para clarificar algunas de sus respuestas. Se entregará retroalimentación uno a uno a [todos] los participantes en la encuesta después de la fase de evaluación inicial o final de la ENRC.
* Se debe responder un cuestionario por cada servicio ciberdependiente significativo que la organización participante identifique como de interés para la Encuesta.
* El cuestionario no está diseñado como una auditoría de seguridad cibernética sino para realizar una evaluación cualitativa (no cuantitativa) de riesgos a nivel nacional.
* El cuestionario utiliza opciones de respuesta múltiples (respuestas de puntuación), para las preguntas clave, pero permite que se den respuestas escritas breves en otros casos; mantenga las respuestas breves y no incluya descripciones detalladas ni datos técnicos.

El Cuestionario le pedirá que describa la naturaleza del riesgo cibernético en su organización, en cinco secciones:

* Información sobre su organización y los sistemas cibernéticos críticos en uso
* Para cada sistema cibernético crítico, usted identificará:
* Características críticas del sistema de cada activo cibernético crítico
* Identificación del peor de los escenarios razonables que ilustre las amenazas y los peligros con mayor probabilidad de afectar el sistema
* Los impactos de un ataque exitoso o de la interrupción de sus sistemas cibernéticos críticos
* Su estimación respecto de las cualidades de ciberseguridad/resiliencia de sus sistemas cibernéticos críticos

## Cómo se calculan los riesgos a la ciberseguridad

Las respuestas se utilizarán para estimar el riesgo a la ciberseguridad del país de acuerdo con la siguiente fórmula:

## Cuestionario. sección 1: información sobre su organización

**Esta sección servirá para registrar información sobre la organización; a qué sector de infraestructura nacional pertenece y qué servicios proporciona utilizando sistemas cibernéticos críticos. Por razones de confidencialidad, el nombre de la organización y los sistemas cibernéticos identificados se codificarán antes de que la información de las Secciones 2 a 5 se analice y se compare con la información proporcionada por otros participantes, de modo que la evaluación colectiva del riesgo permanezca anónima.**

**Para efectos de esta encuesta,** los sistemas cibernéticos son sistemas y redes de información (hardware, software e infraestructura asociada), incluidos los datos alojados en ellos y los servicios que brindan. **La ciberseguridad** alude a la protección de los sistemas cibernéticos contra el acceso no autorizado, daño o uso indebido**.** Esto incluye daños causados intencionalmente por un operador del sistema (la "amenaza interna"), o accidentalmente al no seguir los procedimientos de seguridad. La **"ciber resiliencia"** hace referencia a la capacidad de prepararse para, detectar, responder y recuperarse rápidamente de ataques o incidentes cibernéticos y, por lo tanto, limitar su impacto.

1.1 Nombre de la organización – auto-explicativo.

1.2 Enumere los servicios que brinda su organización: - describa la gama de servicios que proporciona su organización y que dependen de los sistemas cibernéticos a los que usted alude en su respuesta al Cuestionario (NB, la versión Word de la Encuesta requiere una respuesta completa al Cuestionario para cada sistema cibernético significativo).

1.3 ¿A qué Sector de la infraestructura nacional pertenece su organización? – el cuestionario enumera los sectores de infraestructura nacional más específicos entre los cuales elegir.

1.4 Enumere los sistemas cibernéticos críticos: enumere solo los sistemas cibernéticos que utiliza su organización para proporcionar/apoyar la prestación de servicios que son críticos para el "bien público" (bienestar público, economía, servicios esenciales). Pueden ser varios sistemas vinculados con características similares, en cuyo caso enumérelos como uno solo. Usted deberá responder un cuestionario completo por cada sistema que enumere– Vea Pregunta 2.1.

1.5 Ciberseguridad dentro de la organización: esta pregunta alude a la medida en que se reconocen los riesgos a la ciberseguridad a nivel directivo (en lugar de a niveles más bajos, los cuales están cubiertos por la Sección 5) dentro de la organización; y si existe (o no) una Cultura Corporativa de gestión del riesgo cibernético.

**Cuestionario, sección 2: características del sistema crítico**

**Esta sección se concentra en uno de sus sistemas críticos y aborda las características y funciones del sistema.**

2.1. ¿A cuál de los sistemas cibernéticos en 1.4 se refiere este cuestionario? ¿Qué departamento, organización o empresa es responsable de este sistema? Cada respuesta al cuestionario solo debe describir un sistema cibernético. Si su organización ha identificado más de uno en respuesta a la Sección 1, debe identificar a qué sistema alude este cuestionario y qué departamento o parte de su organización es responsable de él.

2.2 Breve descripción del sistema: describa brevemente el sistema y sus funciones. No se requiere detalles técnicos.

2.3 Indique brevemente por qué este sistema ha sido identificado por usted como un sistema importante que presta o apoya la prestación de servicios que son esenciales para el funcionamiento del país.

2.4 Conectividad del sistema: un elemento significativo del riesgo que presentan los sistemas cibernéticos es la medida en que están aislados de otros sistemas o redes, y la medida en que los "cortafuegos" que los aíslan pueden erosionarse con el tiempo. Considere si su sistema es verdaderamente independiente o se ha vinculado parcialmente a otras redes en uso dentro o fuera de la organización. Considere también hasta qué punto el sistema controla los resultados físicos (como lo hacen, por ejemplo, los sistemas SCADA, el "Internet de las cosas") que afectan la vida diaria.

2.5 Alojamiento del sistema: se explica por sí mismo

2.6 y 2.7. Responsabilidad por la seguridad cibernética: si el sistema no está alojado en TI que es propiedad de su organización y está administrado por ella (consulte 2.3), entonces la responsabilidad por la seguridad puede dividirse entre su organización y un proveedor externo. En ese caso, marque 'No' y explique en 2.7.

2.8 Criticidad interna del negocio: las respuestas a esta pregunta deben tener en cuenta la medida en que existe una copia de seguridad/redundancia efectiva en su sistema, lo que permite mitigar los efectos de una interrupción; si existe alguna duda sobre la eficacia de los sistemas de respaldo (p. ej., porque pueden estar expuestos al mismo riesgo que el sistema principal), la calificación debe reflejarlo.

2.9 Criticidad externa del negocio: esta pregunta solamente considera cuántas personas y organizaciones dependen del servicio que está brindando, utilizando el sistema cibernético identificado en 2.1, para su bienestar, sustento o actividades.

2.11 Dependencias externas: esta pregunta se refiere específicamente a las dependencias cibernéticas: dependencia directa de los sistemas cibernéticos (por ejemplo, Internet) que son operados por otras organizaciones. No incluya la dependencia de servicios no cibernéticos proporcionados por otros (p. ej., suministro de electricidad), incluso si cree que es probable que dependan del ciberespacio.

2.12 Dependencias internas: esta pregunta indaga si otros sistemas operados por otras organizaciones dependen directamente del sistema cibernético cubierto por este cuestionario.

## Cuestionario, sección 3: riesgos cibernéticos

**Esta sección busca identificar el riesgo cibernético y determinar cuál sería el "peor escenario razonable" para ilustrar los riesgos para su sistema. El riesgo cibernético es un evento que afecta objetos de valor (propiedad, continuidad del negocio, rentabilidad, etc.) para sus organizaciones. Esta Encuesta le invita a construir un escenario que represente lo peor que razonablemente le podría ocurrir a su sistema dada su función; los tipos de 'actores de amenazas' que se sabe que están motivados para atacar dichos sistemas, y los métodos (‘vectores de amenazas') con que ellos cuentan para hacerlo. Consulte el Anexo A para obtener extractos de la Estrategia Nacional de Seguridad Cibernética del Reino Unido que describen los diferentes tipos de actores de amenazas y vectores de ataque (metodología) y proporciona ejemplos que pueden ayudarle a responder las preguntas de esta sección.**

3.1 Los tres aspectos de la seguridad de la información. Esta pregunta busca averiguar cuál de los siguientes aspectos es el más importante para el sistema que ha descrito en esta respuesta al cuestionario. La definición de los tres aspectos es la siguiente:

|  |  |
| --- | --- |
| Disponibilidad | El usuario puede acceder a la información cuando la necesita. |
| Integridad | la información no ha sido modificada accidental o deliberadamente, y es precisa y completa |
| Confidencialidad | la información solo está disponible para aquellos que tienen derecho a conocerla |

Las definiciones de las puntuaciones utilizadas para evaluar la importancia de los aspectos del árbol de la seguridad de la información para su organización son las siguientes:

|  |  |
| --- | --- |
| Bajo | Este aspecto de la seguridad de la información no es significativo para la prestación de servicios esenciales y cualquier interrupción del funcionamiento del sistema, pérdida de integridad o violación de información confidencial tendrá poco impacto en la prestación de servicios o la reputación de la organización. |
| Mediano | Este aspecto de la seguridad de la información es importante para la prestación exitosa de algunos servicios, y cualquier interrupción en la operación del sistema, pérdida de integridad o violación de información confidencial tendrá un impacto limitado y manejable en algunos servicios clave y en la reputación de la organización. |
| Alto  | Este aspecto de la seguridad de la información es muy importante para la prestación exitosa de servicios esenciales y cualquier interrupción en el funcionamiento del sistema, pérdida de integridad o violación de información confidencial tendrá un impacto severo en algunos servicios clave y en la reputación de la organización. |
| Muy alto | Este aspecto de la seguridad de la información es fundamental para la prestación satisfactoria de servicios esenciales, y cualquier interrupción del funcionamiento del sistema, pérdida de integridad o violación de la información confidencial tendrá un impacto grave, generalizado y de largo plazo en los servicios clave y en la reputación de la organización. |

3.2 Importancia de la inteligencia respecto de amenazas cibernéticas: las organizaciones cuyos sistemas cibernéticos están expuestos a la amenaza de un ataque confían en la obtención de información actualizada sobre los actores de amenazas y las metodologías de amenazas para garantizar que sus sistemas permanezcan seguros y para desencadenar una respuesta efectiva a incidentes. Estas preguntas buscan identificar qué tan rápido puede usted obtener información actualizada sobre amenazas cibernéticas y qué tan importante cree usted que es dicha información para la seguridad del sistema que está evaluando. La definición de las puntuaciones utilizadas para evaluar la importancia de la inteligencia sobre amenazas para su organización es la siguiente:

|  |  |
| --- | --- |
| 1 | No se utiliza la inteligencia sobre amenazas como parte del enfoque de la organización para abordar la seguridad cibernética. |
| 2 | La inteligencia sobre amenazas está disponible ocasionalmente, pero no es un aspecto importante en el enfoque para abordar la seguridad cibernética. |
| 3 | A veces se busca y se utiliza de manera ad hoc la inteligencia sobre amenazas para optimizar la seguridad cibernética. |
| 4 | La inteligencia sobre amenazas es una parte importante del abordaje de la seguridad cibernética y existe un proceso para garantizar que se tomen las medidas adecuadas para responder a amenazas nuevas o cambiantes. |
| 5 | La inteligencia sobre amenazas es una parte esencial del enfoque de la seguridad cibernética y se utiliza para brindar una respuesta oportuna a los cambios en el entorno de amenazas a la seguridad cibernética. |

3.4 La capacidad de su organización para acceder a la inteligencia sobre amenazas se evalúa de la siguiente manera:

|  |  |
| --- | --- |
| 1 | La inteligencia sobre amenazas no está disponible |
| 2 | La inteligencia sobre amenazas está ocasionalmente disponible de forma ad-hoc |
| 3 | Se accede periódicamente (por ejemplo, mensualmente) a al menos una fuente relevante de inteligencia sobre amenazas. |
| 4 | Varias fuentes de inteligencia sobre amenazas de alta calidad son consultadas y la información es analizada activa y frecuentemente (por ejemplo, diariamente) |
| 5 | Múltiples fuentes (todas las fuentes) de inteligencia de alta calidad sobre amenazas son consultadas y la información es analizada activamente para obtener una visión personalizada casi en tiempo real del entorno de amenazas a la seguridad cibernética. |

3.5 – 3.6 ¿Qué **actores de amenazas** cibernéticas le preocupan más? ¿Qué vectores de **ciberataque** le preocupan más? Esta pregunta alude solo al sistema cibernético que se está evaluando: teniendo en cuenta la importancia relativa de (consulte la Pregunta 3.1) la disponibilidad, integridad y confidencialidad de los datos en su sistema, qué tipo de actor de amenazas (criminal, estatal, patrocinado por el estado, hacktivistas, terroristas) es más probable que esté motivado y sea capaz de atacar el sistema con éxito, y qué metodología de ataque le preocupa a usted más. Para algunas organizaciones/sistemas, la interrupción accidental es una preocupación tan grande como cualquier actor de amenazas malicioso.

| **Actor de amenazas** | **Vectores de amenazas comúnmente asociados** |
| --- | --- |
| Cibercriminales | Crímenes cibernético-**dependientes** (por ejemplo, los que implican desarrollar y propagar malware para obtener ganancias financieras, piratear para robar, dañar, distorsionar o destruir datos, redes. Incluye ransomware y amenazas de denegación de servicio distribuido (DDoS) para extorsión |
| Delitos **facilitados** por la cibernética: delitos tradicionales aumentados en escala por el uso de computadoras, redes u otras formas de TIC (p. ej., fraude cibernético y robo de datos) |
| Amenazas de un Estado o patrocinadas por un Estado (generalmente encubierto) | Interrupciones vergonzosas de las comunicaciones, TI y servicios en red, etc. |
| Espionaje |
| Capacidades cibernéticas ofensivas, incluidas las capacidades destructivas que amenazan la seguridad de Infraestructura Nacional Crítica, (CNI en inglés) los sistemas de control industrial, el "Internet de las cosas", etc. |
| Terroristas | Capacidad técnica, hasta ahora baja, incluidas desfiguraciones, 'doxing' (donde los datos personales pirateados se 'filtran' en línea) diseñados para atraer la atención de los medios de comunicación e intimidar a las víctimas |
| La amenaza futura puede aumentar a medida que una generación cada vez más alfabetizada en informática explote las posibilidades de desfiguración o actividad DDoS contra los Estados. |
| Hacktivistas, internos y otros | Actividad disruptiva (desfiguración del sitio web; DDoS) y algunos daños más duraderos por parte de personas con una reivindicación |
| Amenaza interna: robo de datos confidenciales y propiedad intelectual; posible ataque de denegación de servicio distribuido (DDoS) |
| Accidental | Daños accidentales por infección involuntaria de los sistemas en red por parte de los empleados |

3.7 Escenario del peor de los casos razonables: se le pide que use sus respuestas "principales", a 3.1, 3.5 y 3.6 para construir un escenario de la siguiente manera:

“El peor de los casos razonables para este sistema es un ataque exitoso de [respuesta principal a 3.5] usando [respuesta principal a 3.6] que resulte en una violación significativa de [respuesta principal a 3.1]”

**Cuestionario, sección 4: impactos**

**Esta Sección le pide que calcule la escala del impacto en caso de un ataque según el peor escenario razonable. Para el propósito de esta Encuesta, suponga que el ataque es exitoso, incluso si considera que es poco probable (la probabilidad de un ataque exitoso será parte de la evaluación luego de completar la Sección 5). Puede que le resulte útil considerar el historial de casos adjunto a esta nota que brinda ejemplos de organizaciones en todo el mundo que han sido atacadas con éxito.**

**Los impactos se miden teniendo en cuenta qué tan generalizados, intensos y duraderos es probable que sean. Se tiene en cuenta el impacto global. Si el impacto en un área es insignificante, utilice la columna "sin impacto".**

4.1 Impacto en las personas que usan sus servicios: la medida aquí es cuántas personas que confían en sus servicios se verían afectadas por un ataque exitoso.

4.2 Impacto en otros servicios esenciales: esta pregunta apunta a averiguar cuántos **otros** servicios esenciales se verían afectados por una interrupción en su sistema cibernético. Si la respuesta es que no hay consecuencias colaterales para otras organizaciones en los sectores de infraestructura nacional, marque "sin impacto" en cada una.

* Un ‘impacto bajo’ es aquel en el que es probable que cualquier impacto sea limitado, localizado en un área y de corta duración (minutos en lugar de horas).
* Un ‘impacto medio’ sería más intenso, no localizado, pero no a nivel nacional, y de mayor duración (horas).
* Un 'impacto alto' implicaría una interrupción muy significativa y generalizada del servicio, durante un período sostenido (días).

El estudio de caso 3 (el ataque a la red eléctrica de 2013 en Ucrania) brinda un ejemplo de un ataque cibernético que no solo afecta a los clientes directos de una organización que es atacada, sino que también tiene efectos colaterales indirectos sobre una base de clientes más amplia a través de los dueños de otra infraestructura nacional.

4.3 Estime el impacto en la industria y la economía. Como se puede ver en los estudios de caso en el Anexo A, el daño financiero puede llegar fácilmente a los $100 millones. En consecuencia, la escala utilizada para esta ENRC es

|  |  |  |
| --- | --- | --- |
| Escala | % del GDP | $ equivalente [ajuste al tamaño de la economía] o adopte las siguientes cifras |
| Bajo | Menos de 0.01% | Menos de $10 millones |
| Mediano | 0.01-0.1% | $10-100 millones |
| Alto | 0.1-1% | $100-1,000 millones |
| Muy alto | Más de 1% | Más de $1 mil millones |

4.4 Estime el impacto en los "objetos de valor" no materiales para [país X]. Los juicios aquí serán subjetivos, pero lo invitamos a considerar tres dimensiones para cada tipo de impacto:

• Intensidad: ¿el impacto es muy intenso o menos intenso en una escala del 1 al 3?

• Alcance: es el impacto localizado o generalizado (en todo el país), en una escala del 1 al 3

• Duración: es el impacto de corta duración (días) o de larga duración (meses), en una escala de 1 a 3

La combinación de las puntuaciones le dará una puntuación de impacto general de bajo (3-4), medio (5-6) o alto (7-9)

[4.6 Reservado para el uso de la ENRC para medir el riesgo cibernético en eventos internacionales organizados por el país x]

**Cuestionario, sección 5: vulnerabilidades del sistema**

Le invitamos a evaluar usted mismo la vulnerabilidad de sus sistemas cibernéticos

<Opción 1> [utilizando un enfoque simplificado basado en los '10 pasos para la seguridad cibernética', documento original del Centro Nacional de Seguridad Cibernética del Reino Unido que recomienda un régimen basado en los 10 pasos que se enumeran a continuación:

**Centro Nacional de Seguridad Cibernética del Reino Unido: 10 pasos para la seguridad cibernética**

1. **Régimen de Gestión de Riesgos.** Incorporar un régimen adecuado de gestión de riesgos en toda la organización. Éste debe estar respaldado por una estructura de gobierno empoderada que cuente con el respaldo activo de la junta directiva y de los gerentes senior. Comunique claramente su enfoque sobre la gestión de riesgos con el desarrollo de políticas y prácticas aplicables. Éstas deben tener como objetivo garantizar que todos los empleados, contratistas y proveedores conozcan el enfoque y sepan cómo se toman las decisiones y cuáles son los límites de riesgo aplicables.
2. **Configuración Segura.** Tener un enfoque para identificar construcciones y procesos de tecnología de referencia para garantizar la gestión de la configuración puede mejorar en gran medida la seguridad de los sistemas. Usted debe desarrollar una estrategia para eliminar o deshabilitar la funcionalidad innecesaria de los sistemas y corregir rápidamente las vulnerabilidades conocidas, generalmente mediante la aplicación de parches. De lo contrario, es probable que aumente el riesgo de compromiso de los sistemas y la información.
3. **Seguridad de la red.** Las conexiones de sus redes a Internet y otras redes asociadas exponen sus sistemas y tecnologías a ataques. Al crear e implementar algunas políticas simples y respuestas arquitectónicas y técnicas apropiadas, usted puede reducir las posibilidades de que estos ataques tengan éxito (o causen daños a su organización). Es casi seguro que las redes de su organización abarcan muchos sitios, y el uso del trabajo móvil o remoto y los servicios en la nube dificultan la definición de un límite de red fijo. En lugar de centrarse únicamente en las conexiones físicas, piense en dónde se almacenan y procesan sus datos, y dónde un atacante tendría la oportunidad de interferirlos.
4. **Administrar los privilegios de los usuarios.** Si a los usuarios se les proporcionan privilegios de sistema o derechos de acceso a datos que no necesita, el impacto del uso indebido o el compromiso de la cuenta de ese usuario será más grave de lo necesario. Todos los usuarios deben contar con un nivel razonable (pero mínimo) de privilegios y derechos sobre el sistema según necesiten para su función. La concesión de privilegios de sistema muy elevados debe controlarse y administrarse cuidadosamente. Este principio, a veces, se denomina "privilegio mínimo".
5. **Educación y sensibilización del usuario.** Los usuarios tienen un papel fundamental que desempeñar en la seguridad de su organización. Por ello es importante que las reglas de seguridad y la tecnología proporcionada les permitan hacer su trabajo y ayudar a mantener la seguridad de la organización. Esto puede ser respaldado por una entrega sistemática de programas de sensibilización y capacitación que brinden experiencia en seguridad y ayuden a establecer una cultura consciente de la seguridad.
6. **Gestión de incidentes.** Todas las organizaciones experimentarán incidentes de seguridad en algún momento. Invertir para establecer políticas y procesos efectivos de gestión de incidentes ayudará a optimizar la resiliencia; respaldar la continuidad del negocio, aumentar la confianza de los clientes y las partes interesadas y, potencialmente, reducir cualquier impacto. Usted debe identificar fuentes reconocidas (internas o externas) con experiencia especializada en gestión de incidentes.
7. **Prevención de malware.** El software malicioso o malware es un término genérico que cubre cualquier código o contenido que pueda tener un impacto malicioso e indeseable en los sistemas. Cualquier intercambio de información conlleva cierto grado de riesgo de que se intercambie malware, lo que podría afectar gravemente a sus sistemas y servicios. El riesgo puede reducirse desarrollando e implementando políticas antimalware apropiadas como parte de un enfoque general de "defensa en profundidad".
8. **Monitoreo.** El monitoreo del sistema proporciona una capacidad que tiene como objetivo detectar ataques reales o intentos de ataque a sistemas y servicios comerciales. Un buen monitoreo es esencial para responder a ataques de manera efectiva. Además, el monitoreo le permite asegurarse de que los sistemas se utilicen adecuadamente de acuerdo con las políticas de la organización. El monitoreo es a menudo una capacidad clave necesaria para cumplir con los requisitos legales o reglamentarios.
9. **Control de medios extraíbles.** Los medios extraíbles proporcionan una ruta común para la introducción de malware y la exportación accidental o deliberada de datos confidenciales. Debe tener clara la necesidad comercial de usar medios extraíbles y aplicar los controles de seguridad apropiados para su uso.
10. **Trabajo en casa y móvil.** El trabajo móvil y el acceso remoto a los sistemas ofrece grandes beneficios, pero deja al descubierto nuevos riesgos que deben gestionarse. Usted debe establecer políticas y procedimientos basados en el riesgo que admitan el trabajo móvil o el acceso remoto a los sistemas que sean aplicables a los usuarios, así como a los proveedores de servicios. Capacite a los usuarios sobre el uso seguro de sus dispositivos móviles en los entornos en los que es probable que trabajen].

<Opción 2> [utiliza un enfoque simplificado basado en los últimos '10 pasos para la ciberseguridad' del Centro Nacional de Seguridad Cibernética del Reino Unido, que recomienda un régimen basado en los 10 pasos que se enumeran a continuación:

1. **Arquitectura y configuración.** El panorama de la tecnología y la ciberseguridad está en constante evolución. Para abordar esto, las organizaciones deben asegurarse de que sus sistemas y servicios cuenten con una buena seguridad cibernética desde el principio, y que esos sistemas y servicios puedan mantenerse y actualizarse para adaptarse de manera efectiva a las amenazas y riesgos emergentes.
2. **Gestión de activos.** La gestión de activos abarca la forma en que usted puede establecer y mantener el conocimiento necesario de sus activos. Con el tiempo, los sistemas generalmente crecen orgánicamente y puede ser difícil mantener una comprensión de todos los activos en su entorno. Los incidentes pueden ocurrir como resultado de no comprender completamente un entorno, ya sea un servicio sin parches, una cuenta de almacenamiento expuesta en la nube o un documento mal clasificado. Asegurarse de conocer todos estos activos es un precursor fundamental para poder comprender y abordar los riesgos resultantes. Comprender cuándo sus sistemas ya no serán compatibles puede ayudarle a planificar mejor las actualizaciones y los reemplazos y así contribuir a evitar el empleo de sistemas heredados vulnerables.
3. **Seguridad de los datos.** Los datos deben ser protegidos contra el acceso, la modificación o la eliminación no autorizados. Esto implica garantizar que los datos estén protegidos en tránsito, en reposo y al final de su vida útil (es decir, desinfectar o destruir de manera efectiva los medios de almacenamiento después de su uso). En muchos casos, los datos estarán fuera de su control directo, por lo que es importante considerar las protecciones que puede aplicar, así como las garantías que puede necesitar de terceros. Con el aumento de los ataques de ransomware cada vez más personalizados que impiden que las organizaciones accedan a sus sistemas y a los datos almacenados en ellos, se debe tomar otras medidas de seguridad relevantes incluido el mantenimiento de copias de seguridad actualizadas, aisladas y sin conexión de todos los datos importantes.
4. **Compromiso y formación.** Las personas deben estar en el centro de cualquier estrategia de ciberseguridad. Una buena seguridad considera la forma en que las personas trabajan en la práctica y no se interpone en el modo en que las personas realizan su trabajo. Las personas también pueden ser uno de sus recursos más efectivos para prevenir incidentes (o detectar cuándo ha ocurrido uno) siempre que participen adecuadamente y exista una cultura de seguridad cibernética positiva que los aliente a hablar. Ayudar a su personal a adquirir las habilidades y los conocimientos necesarios para trabajar de forma segura es algo que se logra a menudo a través de la concienciación o la formación. Esto no solo ayuda a proteger su organización, sino que también demuestra que valora a su personal y reconoce su importancia para el negocio.
5. **Gestión de acceso e identidad.** Es necesario proteger el acceso a los datos, sistemas y servicios. Comprender quién o qué necesita acceso y en qué condiciones es tan importante como saber quién debe permanecer fuera. Usted debe elegir los métodos apropiados para establecer y probar la identidad de los usuarios, dispositivos o sistemas, con la confianza suficiente para tomar decisiones de control de acceso. Un buen enfoque para la administración de identidades y accesos hará que sea difícil para los atacantes fingir que son legítimos, al mismo tiempo que mantendrá el acceso de los usuarios legítimos a lo que necesitan de un modo lo más simple posible.
6. **Gestión de incidentes.** Los incidentes pueden tener un gran impacto en una organización en términos de costos, productividad y reputación. Por lo tanto, contar con una buena gestión de incidentes reducirá el impacto de éstos cuando sucedan. Ser capaz de detectar y responder rápidamente a los incidentes ayudará a prevenir daños mayores, y reducirá el impacto financiero y operativo. Gestionar el incidente mientras está en el centro de atención de los medios reducirá el impacto reputacional. Finalmente, aplicar lo aprendido de un incidente después de éste posibilitará que usted esté mejor preparado para futuras ocurrencias.
7. **Registro y seguimiento.** La recopilación de registros es esencial para comprender cómo se utilizan sus sistemas y es la base del monitoreo de seguridad (o protección). En caso de que surja una inquietud o un posible incidente de seguridad, las buenas prácticas de registro le permitirán apreciar retrospectivamente lo que sucedió y comprender el impacto del incidente. El monitoreo de seguridad va más allá e implica el análisis activo de la información de registro para buscar signos de ataques conocidos o comportamiento inusual del sistema lo que permite a las organizaciones detectar eventos que podrían considerarse un incidente de seguridad y responder en consecuencia para minimizar su impacto.
8. **Gestión de riesgos.** Asumir riesgos es una parte natural de hacer negocios. La gestión de riesgos entrega información para la toma de decisiones de manera que se pueda lograr el equilibrio correcto entre amenazas y oportunidades para cumplir mejor sus objetivos comerciales. La gestión de riesgos en el dominio de la seguridad cibernética ayuda a garantizar que la tecnología, los sistemas y la información de su organización estén protegidos de la manera más adecuada y que los recursos se concentren en las cosas que más importan para su negocio. Un buen enfoque de gestión de riesgos estará integrado en toda su organización y complementará la forma en que gestiona otros riesgos comerciales.
9. **Seguridad de la cadena de suministro.** La mayoría de las organizaciones confían en proveedores para entregar productos, sistemas y servicios. Un ataque a sus proveedores puede ser tan perjudicial para usted como uno dirigido directamente a su propia organización. Las cadenas de suministro a menudo son grandes y complejas, y asegurar la cadena de suministro de manera efectiva puede ser difícil porque las vulnerabilidades pueden ser inherentes, introducidas o explotadas en cualquier punto dentro de ella. El primer paso es comprender su cadena de suministro, incluidos los proveedores de productos básicos, como los proveedores de servicios en la nube y aquellos proveedores con los que usted tiene un contrato personalizado. Ejercer influencia donde usted pueda y alentar la mejora continua ayudará a optimizar la seguridad en toda su cadena de suministro.
10. **Gestión de vulnerabilidades.** La mayoría de los incidentes de ciberseguridad son el resultado de la acción de atacantes que explotan vulnerabilidades divulgadas públicamente para obtener acceso a sistemas y redes. Los atacantes, a menudo indiscriminadamente, buscarán explotar las vulnerabilidades tan pronto como se hayan revelado. Por lo tanto, es importante (y esencial para cualquier sistema que se pueda explotar desde Internet) instalar actualizaciones de seguridad lo antes posible para proteger su organización. Algunas vulnerabilidades pueden ser más difíciles de solucionar, y un buen proceso de gestión de vulnerabilidades le ayudará a comprender cuáles son las más graves y cuáles deben abordarse primero.]

<Opción 3> Emplea un enfoque simplificado basado en los controles V8 del Centro para la Seguridad de Internet que recomienda un régimen basado en las 18 áreas de control enumeradas a continuación:

1. **Inventario y control de los activos de la empresa.** Todos los activos de hardware se identifican y su ubicación y los usuarios que necesitan acceder a ellos se registran y actualizan a medida que cambian. Los activos se enumeran en una base de datos segura, que solo los usuarios privilegiados actualizan periódicamente. Se realiza una copia de seguridad de una lista maestra y se mantiene segura lejos de la versión en la que se trabaja. Las listas de activos empresariales se gestionan de forma activa mediante el mantenimiento de un inventario; del seguimiento de la ubicación de los activos en la red y geográficamente, y comprobando periódicamente su precisión. Estas listas incluyen todos los activos empresariales en este sistema. Esta lista permitirá un conocimiento preciso de la totalidad de los activos de la empresa que necesitan monitoreo y protección.
2. **Inventario y control de activos de software.** Se identifican todos los activos de software, se inventarían sus usuarios y ubicaciones; se actualizan a medida que cambian y se verifica la precisión, incluidos los detalles de la aplicación y el estado del soporte del proveedor. Solo se permite la ejecución de software autorizado y éste se incluye en una base de datos segura actualizada regularmente solo por usuarios privilegiados. Se realiza una copia de seguridad de una lista maestra y se mantiene de forma segura lejos de la versión en que se trabaja. Esta lista permitirá un conocimiento preciso de la totalidad de los activos que deben monitorearse y protegerse en toda la empresa. Esto también admitirá la identificación de versiones o activos de software y firmware no autorizados y no administrados que deben eliminarse o remediarse.
3. **Protección de los datos** Un proceso de gestión de datos maduro aborda, como mínimo, la identificación de los datos, la confidencialidad, quién es el propietario de los datos y quién está autorizado para acceder a los datos según sea necesario. Para hacer esto, los datos deben clasificarse por sensibilidad o criticidad, y se debe establecer límites de retención de datos y establecer una política probada de eliminación de datos. Las políticas de datos se revisan y los controles de datos se actualizan al menos una vez al año o cuando se produzcan cambios importantes en la empresa que podrían afectar estas medidas de seguridad.
4. **Configuración segura de los activos y el software de la empresa.** Se establecen y mantienen procesos de configuración seguros para los activos empresariales (dispositivos de usuario final, incluidos dispositivos portátiles y móviles, no informáticos/IoT y servidores) y software (sistemas operativos y aplicaciones). Estos activos y su configuración se revisan periódicamente; la documentación de control de configuración se actualiza anualmente o cuando se producen cambios importantes en la empresa que podrían afectar estos controles.
5. **Gestión de cuentas.** El acceso a los datos se controla cuidadosamente mediante una gestión de cuentas controlada por inventario en toda la empresa. Los sistemas deben estar protegidos contra el acceso no autorizado y las bases de datos deben cifrarse a un nivel adecuadamente alto tanto en reposo en sistemas de archivos y bases de datos como en tránsito dentro de este sistema y hacia servicios externos. La autenticación de múltiples factores está implementada para controlar el acceso de los usuarios con contraseñas únicas configuradas según estrictas políticas de control de administración de cuentas.
6. **Gestión del control de acceso.** Un sistema bien gestionado garantizará que la administración de cuentas asegure de manera proactiva que solo los usuarios autorizados puedan usar este sistema y que el rol de cualquier usuario privilegiado se reduzca a lo esencial según un enfoque de "privilegio mínimo". Esto reducirá la superficie de ataque potencial de una cuenta comprometida ya que son los usuarios privilegiados los que pueden causar el mayor daño en un sistema. Este sistema utilizará procesos y herramientas para asignar y administrar la autorización de las credenciales de las cuentas de usuario, incluidas las cuentas de administrador así como las cuentas de servicio, los activos y el software de la empresa.
7. **Gestión continua de vulnerabilidades.** La gestión de vulnerabilidades es una tarea constante para garantizar que la identificación lo más temprana posible de vulnerabilidades. Las vulnerabilidades existen en casi todos los sistemas y pueden afectar los activos de software, firmware o hardware. Un sistema de gestión de vulnerabilidades maduro permitirá a los mantenedores del sistema asegurarse de que los atacantes no puedan usar las vulnerabilidades existentes o recientes para comprometer este sistema. Un sistema maduro también desarrollará un plan para evaluar y rastrear continuamente las vulnerabilidades en todos los activos dentro de la infraestructura de este sistema. Además, monitoreará las fuentes públicas y privadas de la industria para obtener nueva información sobre vulnerabilidades y sobre cualquier cambio en las tácticas o herramientas de los actores de amenazas.
8. **Gestión de registros de auditoría.** Un sistema maduro recopilará todos los eventos. Estos registros van desde actividades de rutina, como la actividad de inicio de sesión del usuario, hasta eventos especiales como apagados del sistema o cambios importantes en el sistema. Un sistema maduro puede recopilar, alertar sobre, revisar y conservar registros de eventos y proporcionar herramientas de auditoría que podrían ayudar a detectar la presencia de actores de amenazas en este sistema, comprender sus acciones hasta el momento o recuperar el sistema de un ataque.
9. **Protecciones de correo electrónico y de navegador web.** Un sistema bien administrado admitirá la comunicación segura a través del correo electrónico y la navegación web para reducir la probabilidad de que ingrese malware dañino a este sistema. Un sistema bien protegido garantiza que el tráfico web y de correo electrónico hacia y desde el sistema está protegido mediante navegadores aprobados que imponen el uso de HTTPS, y solo a las URL aprobadas. Los dispositivos orientados a Internet están protegidos mediante cortafuegos y puertas de enlace de seguridad para limitar el malware que ingresa a este sistema. La protección DNS reduce la probabilidad de un ataque DoS o DDoS. Los sistemas de correo electrónico escanean el tráfico entrante en busca de malware y el tráfico saliente en busca de datos confidenciales o anomalías. Con una protección y detección de amenazas continuamente mejoradas que cubren el correo electrónico y los vectores web, los usuarios entienden plenamente que los atacantes buscan manipular el comportamiento humano a través del compromiso directo, como es el caso del phishing.
10. **Defensas contra el malware.** Los diseños y configuraciones seguros previenen y controlan la instalación, el movimiento y la ejecución de código malicioso. Esto debería aplicarse a todos los vectores y superficies de ataque. Incluso si el malware ingresara al sistema, un atacante no podría obtener privilegios elevados ni moverse lateralmente a través de la red sin ser detectado. Un sistema completamente seguro contrarresta la amenaza a través de una defensa en profundidad que cubre la educación del usuario, el bloqueo a nivel de dispositivo y el monitoreo continuo. Un sistema seguro detecta el malware, lo contiene y se recupera de él.
11. **Recuperación de datos.** Un sistema seguro implementa, prueba y mantiene un proceso de recuperación de datos. Este se revisa y actualiza anualmente o cuando se producen cambios empresariales significativos en este sistema. Se realiza una copia de seguridad periódica del sistema seguro mediante un proceso automatizado lo que garantiza que los datos de la copia de seguridad estén segregados y cifrados. Estas copias de seguridad de datos se prueban periódicamente.
12. **Gestión de infraestructura de red.** Un sistema maduro posee una infraestructura de red actualizada que incluye el uso de las últimas versiones de software y se revisa mensualmente. Un sistema maduro cuenta con una arquitectura segura que aborda la segmentación de la red con principios de privilegios mínimos e implementa la Infraestructura como Código (IaC), respaldada por protocolos de comunicación y redes seguras en este sistema como SSH, HTTPS y 802.1X, incluida la configuración segura de los sistemas inalámbricos. Los planes de arquitectura del sistema se mantienen actualizados y almacenados de forma segura.
13. **Monitoreo y defensa de la red.** Un sistema maduro posee un Sistema de Gestión de Incidentes y Eventos de Seguridad (SIEM en inglés) efectivo y probado. El propietario del sistema comprende y controla los límites de la red de este sistema, incluidos los externos a la organización. Se implementa un Sistema de Detección de Intrusos basado en host (HIDS en inglés) junto con un Sistema de Detección de Intrusos en la red (NIDS, en inglés) en todo este sistema, incluso fuera de las instalaciones. Las aplicaciones antimalware actualizadas se instalan y supervisan de acuerdo con el diseño de configuración segura. Se aplica control de acceso al acceso remoto y se supervisa todo el tráfico de la red incluyendo capacidad de filtrado de tráfico.
14. **Sensibilización sobre seguridad y capacitación en habilidades.** Un sistema maduro y de alto rendimiento contará con usuarios capacitados en seguridad para que identifiquen las últimas amenazas y vulnerabilidades. Un sistema maduro mantendrá un programa de sensibilización sobre seguridad. Éste influirá en el comportamiento del personal para que sea consciente de la seguridad y se mantenga debidamente capacitado todo lo cual reducirá los riesgos en ciberseguridad. El personal estará sensibilizado sobre el uso la Autenticación Multifactor (MFA en inglés), y todos los empleados que utilicen el sistema conocerán los procedimientos para realizar informes sobre incidentes y ataques de phishing.
15. **Gestión de proveedores de servicios.** Un sistema seguro y bien gestionado que depende de los proveedores para entregar productos, sistemas y servicios, es aquel en el que el proveedor entiende a cabalidad lo que le provee la cadena de suministro, incluyendo las obligaciones contractuales, y tiene una política de gestión de proveedores que se actualiza periódicamente. Los proveedores de servicios se clasifican según el conocimiento de los datos del sistema incluyendo la sensibilidad de los datos, el volumen, los requisitos de disponibilidad y el cumplimiento normativo. Y el riesgo se evalúa contra el servicio que brindan a este sistema.
16. **Seguridad del software de aplicación.** Un sistema seguro garantizará que el ciclo de vida de la seguridad del software ya sea desarrollado internamente, alojado o adquirido se gestione y comprenda bien desde una perspectiva de riesgo de seguridad cibernética. Esto ayudará a prevenir, detectar y remediar las debilidades de seguridad antes de que puedan afectar a los sistemas de la empresa en general.
17. **Gestión de respuesta a incidentes.** Un sistema seguro y bien administrado tendrá una capacidad de respuesta a incidentes comprobada y documentada (p. ej., políticas, planes, procedimientos, roles definidos, capacitación y comunicaciones) para prepararse, detectar y responder rápidamente a un ataque. Se llevan a cabo ejercicios de respuesta a incidentes de rutina, y este sistema se mejora a partir de las lecciones aprendidas cada vez. Se imparte formación para garantizar que todo el personal sepa identificar, informar sobre y responder a los eventos e incidentes e identifique las diferencias entre ellos. Los roles clave de respuesta se asignan y se actualizan periódicamente.
18. **Pruebas de penetración.** Un sistema maduro estará regularmente involucrado en pruebas de eficacia y resiliencia de los activos de la empresa. Esto se llevará a cabo identificando y explotando las debilidades en los controles (personas, procesos y tecnología) y simulando los objetivos y acciones de un atacante. Esto se realizará mediante Pruebas de Penetración (Penetration Testing) y Red Teaming en que se simula un ataque para descubrir debilidades en la seguridad del sistema. Luego se desarrolla un Plan de Acción de Remediación (RAP en inglés) para garantizar que todas las debilidades, vulnerabilidades y brechas identificadas se solucionarán dentro de un plazo acordado.]

<Opción 4> [utiliza un enfoque simplificado basado en los controles cibernéticos NIST 800-53, que recomienda un régimen basado en las 20 áreas de control enumeradas a continuación:

1. **Control de Acceso (AC en inglés).** La familia de controles AC consta de requisitos de seguridad que detallan el registro del sistema. Esto incluye quién tiene acceso a qué activos y capacidades de generación de informes como administración de cuentas, privilegios del sistema y registro de acceso remoto para determinar cuándo los usuarios tienen acceso al sistema y su nivel de acceso.
2. **Sensibilización y entrenamiento (AT en inglés).** Los conjuntos de control de la familia de controles AT son específicos para su capacitación y procedimientos de seguridad, incluidos los registros de capacitación de seguridad.
3. **Auditoría y rendición de cuentas (AU en inglés).** La familia de controles AU consta de controles de seguridad relacionados con las capacidades de auditoría de una organización. Esta incluye políticas y procedimientos de auditoría, registro de auditoría, generación de informes de auditoría y protección de la información de auditoría.
4. **Evaluación, autorización y seguimiento (CA en inglés).** La familia de controles CA incluye controles que complementan la ejecución de evaluaciones de seguridad, autorizaciones, monitoreo continuo, plan de acciones e hitos e interconexiones de sistemas.
5. **Gestión de la configuración (CM en inglés).** Los controles de CM son específicos de las políticas de gestión de la configuración de una organización. Esto incluye una configuración básica para operar como base para futuras construcciones o cambios en los sistemas de información. Adicionalmente, esto incluye inventarios de componentes del sistema de información y un control de análisis de impacto en seguridad.
6. **Planificación de contingencia (CP en inglés).** La familia de controles CP incluye controles específicos para el plan de contingencia de una organización en caso de que ocurra un evento de ciberseguridad. Esto incluye controles como pruebas del plan de contingencia, actualizaciones, capacitación, copias de seguridad y restauración del sistema.
7. **Identificación y autenticación (IA en inglés).** Los controles de IA son específicos para las políticas de identificación y autenticación de una organización. Esto incluye la identificación y autenticación de usuarios organizacionales y no organizacionales y cómo la gestión de esos sistemas.
8. **Respuesta a incidentes (IR en inglés).** Los controles de IR son específicos para las políticas y procedimientos de respuesta a incidentes de una organización. Esto incluye capacitación en respuesta a incidentes, pruebas, monitoreo, informes y plan de respuesta.
9. **Mantenimiento (MA en inglés).** Los controles MA en NIST 800-53 rev 5 detallan los requisitos de mantenimiento de los sistemas organizacionales y las herramientas utilizadas.
10. **Protección de medios (MP en inglés).** La familia de controles MP incluye controles específicos para el acceso, marcado, almacenamiento, políticas de transporte, desinfección y uso de medios organizacionales definidos.
11. **Protección física y ambiental (PE en inglés).** La familia de controles PE se implementa para proteger contra amenazas física a los sistemas, los edificios y la infraestructura de soporte relacionada. Estos controles incluyen autorizaciones de acceso físico, monitoreo, registros de visitantes, cierre de emergencia, energía, iluminación, protección contra incendios y protección contra daños por agua.
12. **Planificación (PL en inglés)** Los controles de PL en NIST 800-53 son específicos para las políticas de planificación de seguridad de una organización y deben abordar el propósito, el alcance, las funciones, las responsabilidades, el compromiso de gestión, la coordinación entre entidades y el cumplimiento de la organización.
13. **Gestión del programa (PM en inglés).** La familia de controles de PM es específica para quién administra su programa de ciberseguridad y cómo éste funciona. Incluye, entre otros, un plan de infraestructura crítica, un plan de programa de seguridad de la información, hitos y procesos del plan de acción, estrategia de gestión de riesgos y arquitectura empresarial.
14. **Seguridad del personal (PS en inglés).** Los controles de PS se relacionan con la forma en que una organización protege a sus funcionarioa a través del riesgo de posición, selección de personal, cese de empleo, transferencias, sanciones y acuerdos de acceso.
15. **Procesamiento y transparencia de la información de identificación personal (PT en inglés).** La familia de controles PT cubre procesos para administrar información de identificación personal, garantizar el consentimiento, avisos de privacidad, sistemas de registros y categorías específicas de información de identificación personal.
16. **Evaluación de riesgos (RA en inglés).** La familia de controles RA se relaciona con las políticas de evaluación de riesgos y las capacidades de exploración de vulnerabilidades de una organización. El uso de una solución integrada de gestión de riesgos como CyberStrong puede ayudarle a optimizar y automatizar sus esfuerzos en el cumplimiento de NIST 800 53.
17. **Adquisición de sistemas y servicios (SA en inglés).** La familia de controles SA se correlaciona con los controles que protegen los recursos asignados y el desarrollo del ciclo de vida del sistema de una organización. Esto incluye controles de documentación del sistema de información, controles de gestión de desarrollo de configuración y controles de evaluación y pruebas de seguridad del desarrollador.
18. **Protección de sistemas y comunicaciones (SC en inglés).** La familia de controles SC es responsable de los procedimientos de protección de sistemas y comunicaciones. Esto incluye protección de límites, protección de información en reposo, dispositivos informáticos colaborativos, protección criptográfica, protección contra denegación de servicio y muchos otros.
19. **Integridad del sistema y de la información (SI en inglés).** La familia de controles SI se correlaciona con los controles que protegen el sistema y la integridad de la información. Esta familia de controles incluye NIST SI 7, que comprende reparación de fallas, protección contra código malicioso, monitoreo del sistema de información, alertas de seguridad, integridad de software y firmware y protección contra correo no deseado.
20. **Gestión de riesgos de la cadena de suministro.** La familia de controles SR se concentra en garantizar que los controles y procesos de la cadena de suministro estén habilitados, que haya procedencia en la cadena de suministro, que los componentes estén autenticados y que se implementen las estrategias de adquisición adecuadas.]

## Anexo A

**AMENAZAS Y PELIGROS A LA CIBERSEGURIDAD**

**(Extracto de la Estrategia Nacional de Ciberseguridad del Reino Unido, Capítulo 3)**

**Cibercriminales**

Esta estrategia aborda el delito cibernético en el contexto de dos formas interrelacionadas de actividad delictiva:

**•** Delitos ciberdependientes: delitos que solo se pueden cometer mediante el uso de dispositivos de tecnología de la información y las comunicaciones (TIC), en los que los dispositivos son tanto la herramienta para cometer el delito como el objetivo de este (por ejemplo, desarrollar y propagar malware con fines financieros). obtener, piratear para robar, dañar, distorsionar o destruir datos y/o redes o actividades); y fi

**•** Ciberdelitos: delitos tradicionales que pueden aumentar en escala o alcance mediante el uso de computadoras, redes informáticas u otras formas de TIC (como el fraude cibernético y el robo de datos).

Gran parte de los ciberdelitos más graves (principalmente fraude, robo y extorsión) contra el Reino Unido sigue siendo perpetrado predominantemente por grupos delictivos organizados (OCG, en inglés) de habla rusa con motivaciones financieras situados en Europa del Este con muchos de los servicios del mercado criminal alojados en esos países. Sin embargo, la amenaza también emana de otros países y regiones y del interior del Reino Unido con amenazas emergentes en el sur de Asia y en África occidental las cuales son cada vez más preocupantes.

Incluso cuando se identifica a los individuos clave responsables de las actividades delictivas cibernéticas más dañinas contra el Reino Unido, es a menudo difícil para las agencias policiales internacionales y del Reino Unido procesarlos pues se encuentran en jurisdicciones con acuerdos de extradición limitados o inexistentes.

Estos OCG son los principales responsables de desarrollar e implementar el malware cada vez más avanzado que infecta las computadoras y las redes de los ciudadanos del Reino Unido, su industria y su gobierno. Impacta a todo el Reino Unido y el efecto acumulativo es significativo. Estos ataques se están volviendo cada vez más agresivos y conflictivos, como lo ilustra el uso creciente de ransomware y amenazas de denegación de servicio distribuido (DDoS) para la extorsión.

Si bien los OCG pueden representar una amenaza significativa para nuestra prosperidad y seguridad conjunta, igualmente preocupante es la amenaza continua que representan ciberdelitos menos sofisticados pero generalizados llevados a cabo contra individuos u organizaciones más pequeñas.

**Estados y amenazas patrocinadas por estados**

Nos encontramos regularmente con intentos por parte de estados y de grupos patrocinados por estados de penetrar las redes del Reino Unido para obtener ventajas políticas, diplomáticas, tecnológicas, comerciales y estratégicas. Tales ataques se concentran principalmente en los sectores de gobierno, defensa, finanzas, energía y telecomunicaciones.

La capacidad y el impacto de estos ciber-programas estatales varía. Las naciones más avanzadas continúan mejorando sus capacidades; integrando servicios de encriptación y anonimización en sus herramientas para permanecer encubiertos. Si bien tienen la capacidad técnica para implementar ataques sofisticados, a menudo pueden lograr sus objetivos utilizando herramientas y técnicas básicas contra objetivos vulnerables porque las defensas de sus víctimas son deficientes.

Solo un puñado de estados tiene la capacidad técnica para representar una amenaza grave para la seguridad y la prosperidad general del Reino Unido. Pero muchos otros estados están desarrollando sofisticados programas cibernéticos que podrían representar una amenaza para los intereses del Reino Unido en un futuro próximo. Muchos estados que buscan desarrollar su capacidad de espionaje cibernético pueden comprar herramientas de explotación de redes informáticas "listas para usar" y reutilizarlas para realizar espionaje.

Más allá de la amenaza de espionaje, un pequeño número de actores de amenazas extranjeros hostiles han desarrollado y desplegado capacidades cibernéticas ofensivas, incluidas las destructivas. Estas capacidades amenazan la seguridad de la infraestructura nacional crítica y los sistemas de control industrial del Reino Unido. Algunos estados pueden usar estas capacidades en contravención al derecho internacional en la creencia de que pueden hacerlo con relativa impunidad alentando a otros a hacer lo mismo. Si bien los ataques destructivos en todo el mundo siguen siendo raros, están aumentando en número e impacto.

**Terroristas**

Los grupos terroristas continúan aspirando a llevar a cabo actividades cibernéticas dañinas contra el Reino Unido y sus intereses. La capacidad técnica actual de los terroristas se considera baja. No obstante, el impacto de actividades de baja capacidad contra el Reino Unido hasta la fecha ha sido desproporcionadamente alto. Simples desfiguraciones y actividades de doxing (donde datos personales pirateados se "filtran" en línea) permiten a los grupos terroristas y a sus partidarios atraer la atención de los medios e intimidar a sus víctimas.

La evaluación actual es que los ataques terroristas físicos, en lugar de los ocurridos en el ciber espacio, seguirán siendo la prioridad de los grupos terroristas en el futuro inmediato. A medida que una generación cada vez más alfabetizada en informática se involucra en el extremismo con el potencial de intercambiar habilidades técnicas mejoradas, prevemos un mayor volumen de actividad disruptiva de baja sofisticación (desfiguración o DDoS) contra el Reino Unido. También aumentará la posibilidad de que surja una cantidad de actores solitarios extremistas calificados, y, de igual manera, crecerá el riesgo de que una organización terrorista intente reclutar a un infiltrado establecido.

Es probable que los terroristas utilicen cualquier capacidad cibernética para lograr el máximo efecto posible. Por lo tanto, incluso un aumento moderado de la capacidad terrorista puede constituir una amenaza importante para el Reino Unido y sus intereses.

**Hacktivistas**

Los grupos hacktivistas están descentralizados y actúan orientados a problemas. Forman y seleccionan sus objetivos en respuesta a agravios percibidos introduciendo un carácter de “justiciero” a muchos de sus actos. Si bien la mayor parte de la actividad cibernética de los hacktivistas es de naturaleza disruptiva (desfiguración de sitios web o DDoS), los hacktivistas más hábiles han logrado infligir daños mayores y duraderos a sus víctimas.

**AMENAZA INTERNA**

La amenaza interna sigue representando un riesgo cibernético para las organizaciones en el Reino Unido. Los infiltrados maliciosos que son empleados de confianza de una organización y tienen acceso a sistemas y datos críticos representan la mayor amenaza. Éstos pueden causar daños financieros y de reputación mediante el robo de datos confidenciales y de propiedad intelectual. También pueden representar una ciberamenaza destructiva si utilizan su conocimiento o acceso privilegiado para facilitar o lanzar un ataque con el objetivo de interrumpir o degradar servicios críticos en la red de sus organizaciones o de borrar datos de la red.

Igualmente representan una preocupación aquellos empleados que causan daños a la ciberseguridad accidentalmente al hacer clic inadvertidamente en un correo electrónico de phishing; al conectar un USB infectado a una computadora o al ignorar los procedimientos de seguridad y descargar contenido no seguro de Internet. Si bien estos individuos no tienen la intención de dañar a la organización, su acceso privilegiado a los sistemas y datos implica que sus acciones pueden causar tanto daño como las de un infiltrado malicioso. Estos individuos son a menudo víctimas de la ingeniería social: sin darse cuenta, pueden proporcionar acceso a las redes de su organización o cumplir de buena fe instrucciones que benefician al estafador.

El riesgo cibernético general que representa la amenaza interna para una organización no se reduce solo al acceso no autorizado a los sistemas de información y a su contenido. Los controles de seguridad física que protegen esos sistemas del acceso inapropiado o de la eliminación de datos confidenciales o de información patentada en diferentes medios son igualmente importantes. Del mismo modo, un elemento importante en un enfoque integral de la seguridad es la vigencia de una sólida cultura de seguridad entre los miembros del personal de manera que sean conscientes de la amenaza que representan los empleados descontentos, el fraude en la fuerza laboral y el espionaje industrial y de otro tipo.

**ESTUDIO DE CASO 1: COMPROMISO DE TALKTALK**

El 21 de octubre de 2015, el proveedor de telecomunicaciones del Reino Unido, TalkTalk, informó sobre un ciberataque exitoso y una posible violación de los datos de los clientes. Una investigación posterior determinó que se había accedido a una base de datos que contenía detalles de clientes a través de servidores de Internet abiertos al público, con los registros de aproximadamente 157 000 clientes en riesgo, incluidos nombres, direcciones y detalles de cuentas bancarias. El mismo día, varios empleados de TalkTalk recibieron un correo electrónico con una demanda de pago de rescate en Bitcoins. Los atacantes entregaron información detallada de la estructura de la base de datos como prueba aparente de que se había accedido a ella. El informe de TalkTalk sobre la violación ayudó a la policía, con el apoyo de especialistas de la Agencia Nacional contra el Crimen, a arrestar a los principales sospechosos, todos con base en el Reino Unido, en octubre y noviembre de 2015.

El ataque demostró que las vulnerabilidades pueden persistir incluso dentro de las grandes ciber organizaciones. Su explotación puede tener un efecto desproporcionado en términos de daño a la reputación e interrupción operativa, y este incidente generó una gran atención de los medios. Los informes tempranos de TalkTalk sobre la infracción permitieron que las fuerzas del orden respondieran de manera oportuna y que tanto el público como el gobierno mitigaran la posible pérdida de datos confidenciales. El incidente le costó a TalkTalk un estimado de £60 millones y la pérdida de 95.000 clientes, así como una fuerte caída en el precio de sus acciones.

**ESTUDIO DE CASO 2: ATAQUE AL SISTEMA SWIFT DEL BANCO DE BANGLADESH**

 La Sociedad para las Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT) proporciona una red que permite a las instituciones financieras de todo el mundo enviar y recibir información sobre transacciones financieras de forma segura. Dado que SWIFT envía órdenes de pago que deben liquidarse mediante cuentas corresponsales que las instituciones tienen entre sí, hace tiempo que existe la preocupación de que este proceso se vea comprometido por ciberdelincuentes u otros actores maliciosos, que buscan inyectar órdenes de pago ilegítimas en el sistema o, en el peor de los casos, intentar deshabilitar o interrumpir la funcionalidad de la propia red SWIFT.

A principios de febrero de 2016, un atacante accedió al sistema de pago SWIFT del Banco de Bangladesh e instruyó al banco de la Reserva Federal de Nueva York para que transfiriera dinero de la cuenta del Banco de Bangladesh a cuentas en Filipinas. El intento de fraude fue de US$951 millones. el sistema bancario impidió 30 transacciones por un valor de US$850 millones; sin embargo, se concretaron cinco transacciones por un valor de US$101 millones. Desde entonces se han recuperado 20 millones de dólares los cuales fueron rastreados hasta Sri Lanka. Los 81 millones de dólares estadounidenses restantes transferidos a Filipinas fueron lavaron a través de casinos y algunos de los fondos se enviaron luego a Hong Kong.

La investigación forense iniciada por el Banco de Bangladesh reveló que se había instalado malware en los sistemas del banco y éste se había utilizado para recopilar información sobre los procedimientos utilizados por el banco para pagos internacionales y transferencias de fondos. Un análisis posterior realizado por BAE Systems del malware vinculado al ataque, reveló una funcionalidad sofisticada para interactuar con el software local Alliance Access de SWIFT que se ejecuta en la infraestructura del Banco de Bangladesh. BAE concluyó "que los delincuentes están realizando ataques cada vez más sofisticados contra las organizaciones de víctimas, particularmente en el área de intrusiones en la red".

**ESTUDIO DE CASO 3: ATAQUE A LA RED ELÉCTRICA DE UCRANIA**

Un ciberataque contra las empresas de distribución de electricidad de Ucrania occidental Prykarpattya Oblenergo y Kyiv Oblenergo llevado a cabo el 23 de diciembre de 2015, provocó un gran corte de energía con la interrupción de más de 50 subestaciones en las redes de distribución. Según se informó, la región experimentó un apagón durante varias horas y muchos clientes en otras áreas sufrieron interrupciones menores en sus suministros de energía lo que afectó a más de 220.000 consumidores. Algunos atribuyeron el ataque al uso del malware BlackEnergy3 después de que se identificaron muestras del mismo en la red.

Al menos seis meses antes del ataque, los atacantes habían enviado correos electrónicos de phishing a las oficinas de las empresas eléctricas en Ucrania que contenían documentos maliciosos de Microsoft Office. Sin embargo, es improbable que el malware haya logrado abrir los interruptores automáticos que provocaron la interrupción. Es más probable que el malware sirviera a los atacantes para recopilar credenciales que les permitieran obtener control remoto directo de aspectos de la red lo cual, posteriormente, les permitiría desencadenar la interrupción.

Este incidente en Ucrania es el primer caso confirmado de un ciberataque disruptivo en una red eléctrica. Instancias como esta demuestran aún más la necesidad de buenas prácticas de ciberseguridad en toda la Infraestructura Nacional Crítica (CNI).