Oficina del Comisionado de Seguros de Puerto Rico

Guía de Implementación de Controles de Ciberseguridad para la Industria de Seguros

v. 1.0

Redactada en apoyo para la adopción de la Regla Núm. 108, "*Reglamento de Ciberseguridad para la Industria de Seguros*"

Tabla de Contenido

Objetivos y Alcance

Este documento tiene el propósito de orientar a toda persona que ostente una licencia o autorización para contratar negocio de seguros, emitida por la Oficina del Comisionado de Seguros de Puerto Rico (OCS), sobre las mejores prácticas en la implementación efectiva de controles de ciberseguridad. Este documento se publica con el fin de apoyar a los regulados en el cumplimiento con la Regla Núm. 108, "*Reglamento de Ciberseguridad para la Industria de Seguros*".

La seguridad de los datos de seguros es un aspecto clave en el desarrollo de una industria de excelencia, competitividad, solvencia y solidez mundial, centrada en proteger el interés público y promover el bienestar económico de Puerto Rico. Este es el objetivo principal de la Regla Núm. 108, cuya base es la Ley Modelo de Seguridad de Datos de Seguros de NAIC.

Aunque la Regla Núm. 108 incluye excepciones en cuanto a aplicabilidad, esta guía sirve como referencia para orientar a cualquier asegurador, organización de servicios de salud, agente, agente general, corredor, ajustador, organismo tarifador y organismo asesor de servicios. Los siguientes controles se incluyen para que cada entidad evalúe, comprenda e identifique la implementación adecuada de políticas, procesos y salvaguardas para proteger los datos que almacena, procesa, controla y transfiere, según la complejidad de su operación. El resultado final será una mitigación efectiva de riesgo cibernético y una aceptación consciente y controlada del mismo en su organización.

Esta guía se adhiere al marco de ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) para cumplir con los siguientes objetivos principales:

(1) Proteger y asegurar la confidencialidad, integridad y disponibilidad de los datos en la industria de Seguros;

(2) Proteger los datos contra acceso o uso no autorizado para evitar daños al consumidor;

(3) Definir y periódicamente reevaluar el período de retención de los datos según son necesarios para la operación.

Marco de Ciberseguridad del NIST

El NIST ofrece un marco de ciberseguridad (CSF, por sus siglas en inglés) de las mejores prácticas para para mitigar el riesgo cibernético de su operación y determinar qué controles de ciberseguridad debe implementar. El marco de ciberseguridad NIST CSF 2.0 que se publica en el 2024 está compuesto por seis funciones: gobernar, identificar, proteger, detectar, responder y recuperar.

Función	Categoría	Identificador de Categoría
Gobernar (GV)	Contexto organizativo	GV.OC
	Estrategia de gestión de riesgos	GV.RM
	Funciones, responsabilidades y autoridades	GV.RR
	Política	GV.PO
	Supervisión	GV.OV
	Gestión de riesgos de la cadena de suministro en materia de seguridad cibernética	GV.SC
Identificar (ID)	Gestión de activos	ID.AM
	Evaluación de riesgos	ID.RA
	Mejora	ID.IM
Proteger (PR)	Gestión de identidades, autenticación y control de acceso	PR.AA
	Concienciación y capacitación	PR.AT
	Seguridad de datos	PR.DS
	Seguridad de plataformas	PR.PS
	Resistencia de la infraestructura tecnológica	PR.IR
Detectar (DE)	Monitoreo continuo	DE.CM
	Análisis de eventos adversos	DE.AE
Responder (RS)	Gestión de incidentes	RS.MA
	Análisis de incidentes	RS.AN
	Notificación y comunicación de la respuesta al incidente	RS.CO
	Mitigación de incidentes	RS.MI
Recuperar (RC)	Ejecución del Plan de Recuperación de Incidentes	RC.RP
	Comunicación de la recuperación del incidente	RC.CO

1. **Gobernanza**: Describe el contexto organizacional, la estrategia de manejo de riesgos, roles, responsabilidades, autoridad, políticas, procesos y supervisión.

2. **Identificación**: Busca describir las categorías dentro de cada función para manejar el riesgo cibernético según la operación lo requiere. Incluye identificación de activos, evaluación de riesgos, impacto y mejoras.

3. **Proteger:** Cubre los controles y procesos para garantizar la disponibilidad, integridad y el acceso autorizado a infraestructura y servicios críticos.

4. **Detectar:** Se enfoca en actividades para descubrir eventos de ciberseguridad, ya sea de forma proactiva o a través de alertas y monitoreo.

5. **Responder:** Define las acciones que se tomarán durante un incidente de ciberseguridad, desde análisis forense hasta comunicaciones y mitigación.

6. **Recuperar:** Busca restablecer los sistemas o activos afectados por un incidente cibernético para reanudar los procesos ordinarios de la organización.

Relación entre Ciberseguridad y Privacidad

Si bien la ciberseguridad y la privacidad son disciplinas independientes, sus objetivos se solapan en varias circunstancias comunes. Un programa integral de seguridad cibernética mitigará aquellos riesgos de privacidad relacionados con la pérdida de confidencialidad, integridad y disponibilidad de los datos.

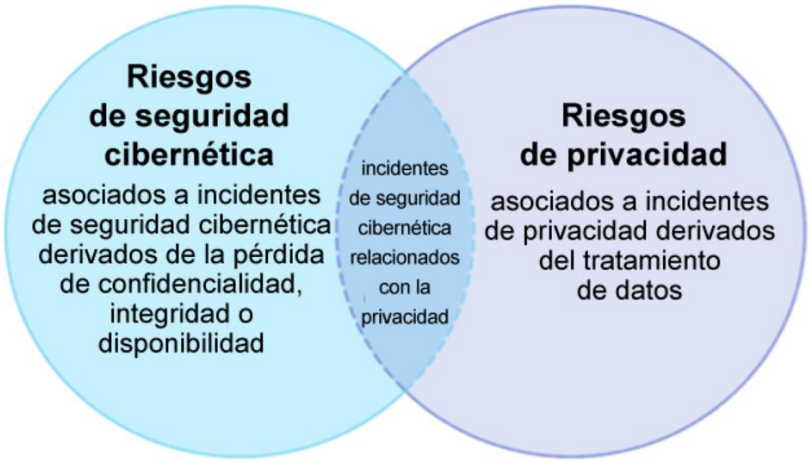

Fig. 6. Relación entre los riesgos de seguridad cibernética y privacidad

FUENTE: Marco de Seguridad Cibernética (CSF) 2.0 del NIST

Controles de GOBERNANZA

Función NIST CSF
GOBERNAR

Los controles de gobernanza son **administrativos**. Buscan que la estrategia y las políticas de ciberseguridad de la organización se establezcan, se comuniquen y se supervisen.

Funciones de **gobernanza** para todo tipo de entidad:

1. ENTENDER

- Todas las partes comprenden y toman en consideración las necesidades y expectativas de la empresa sobre ciberseguridad. (GV.OC-02)

- Se comprenden y gestionan los requisitos legales, regulatorios y contractuales de ciberseguridad, incluyendo las obligaciones de privacidad y derechos civiles. (GV.OC-03)

El Artículo 8.E de la Regla Núm. 108 requiere ***Supervisión por la Junta de Directores*** *para asegurar que en los más altos niveles empresariales se discuta el programa de ciberseguridad y sus actualizaciones periódicas.*

Ejemplo:
Establecer un proceso para dar visibilidad y seguimiento internamente a sus requisitos de cumplimiento con la OCS y otras entidades regulatorias, así como sus obligaciones contractuales de ciberseguridad con proveedores, socios y clientes. Si su operación es compleja, se beneficiará en la medida que estos procesos se documenten formalmente.

Regla Núm. 108, Art. 8.C:
"El Regulado realizará una evaluación de riesgos en la cual:
(1) ***Designará a uno o más empleados, afiliados, suplidor externo o Contratista de Servicios designado para actuar a nombre del Regulado para que sea responsable del Programa de Ciberseguridad"***

- Se establecen, comunican, comprenden y aplican las funciones, responsabilidades y autoridades relacionadas con el manejo de riesgo cibernético. (GV.RR-02)

Ejemplos:
Documentar quiénes son responsables de las actividades de ciberseguridad y cómo se debe consultar e informar a esos equipos e individuos.

Incluir en la descripción de funciones de cada puesto sus responsabilidades de ciberseguridad y los requisitos de desempeño.

Existen distintos marcos y metodologías para evaluar el riesgo cibernético. Visite el Portal de Ciberseguridad de la OCS para más información: https://ciberseguridad.ocs.pr.gov

2. EVALUAR

- Se comprenden y se comunican efectivamente los objetivos, las capacidades y los servicios críticos que ofrece o que se esperan de la organización. (GV.OC-04)

  Ejemplos:
  Determinar los activos y operaciones vitales para lograr los objetivos de negocio. Establecer y comunicar objetivos de resiliencia (ej., objetivos de tiempo de recuperación) para la prestación de servicios críticos bajo distintas condiciones (bajo ataque, durante la recuperación, funcionamiento normal, etc.).

Según el Art. 8.C de la Regla Núm. 108, la evaluación de riesgos además:

- ***Identificará amenazas internas o externas que sean razonablemente previsibles…***

- ***Evaluará la posibilidad y daño potencial de estas amenazas, tomando en consideración la sensibilidad de la Información No-Pública;***

- ***Diseñará y evaluará la suficiencia de las políticas, procesos y salvaguardas, incluyendo:***
  (a) El adiestramiento y la administración de los empleados;
  (b) Los sistemas de información: el diseño de la red, los programas, la clasificación de datos, la gobernanza, el procesamiento, el almacenaje electrónico, la transmisión y la disposición; y,
  (c) Detectar, prevenir y responder a los ataques, intrusiones u otros fallos de los sistemas.

- ***Implementará salvaguardas de la información para manejar las amenazas identificadas en la evaluación continua, y al menos una vez al año evaluará la eficacia de los controles claves, los sistemas y los procedimientos…***

Según las mejores prácticas…

Analice el riesgo que presenta su operación
Repase las actividades y tareas de cada división, evaluando el riesgo cibernético que podría representar cada una para identificar posibles amenazas y daños.

Realice escaneos de vulnerabilidades regulares
Para identificar vulnerabilidades presentes en sus sistemas de información, es recomendable hacer escaneos de vulnerabilidades al menos cada tres meses. CISA ofrece estos servicios libre de costo.

Comprender su riesgo de ciberseguridad le ayudará a crear controles administrativos:
Implemente políticas y procesos a ser adoptados por su personal para proteger su equipo, la red, sus cuentas de usuario y los datos de su empresa. Algunos ejemplos de políticas claves incluyen:

- *Política de Ciberseguridad*
- *Política para el Uso de Tecnología*
- *Política para el Manejo de Datos*
- *Política para el Manejo de Activos*
- *Política para el Adiestramiento de Empleados sobre Ciberseguridad*
- *Política para el Manejo de Acceso*
- *Política para la Respuesta a Incidentes*

Una vez creados los controles administrativos (políticas, estándares y procesos), implemente los controles técnicos correspondientemente.
Las políticas son una aceptación consciente del riesgo identificado, y una declaración sobre las medidas de protección que usará la empresa. Cada herramienta técnica debe configurarse de acuerdo a estas políticas.

- Se lleva a cabo la planificación y debida diligencia para reducir riesgos antes de contratar con contratistas de servicio y terceros. (GV.SC-06)

  Ejemplo:
  Evaluar a posibles proveedores y terceros de forma exhaustiva, que sea proporcional al nivel de riesgo, criticidad y complejidad de la relación con cada proveedor o tercero, y que se integre de una manera coherente al proceso de adquisiciones.

Regla Núm. 108, Art.8.D.2.d:
"(d) Mantener un programa de supervisión a proveedores de servicios con acceso a Información No-Pública, que incluya acuerdos de servicio y requiera controles de seguridad cibernética."

Vea las guías del NIST sobre cómo evaluar el riesgo cibernético de un posible proveedor: https://nist.gov/itl/smallbusinesscyber/guidance-topic/choosing-vendorservice-provider

Regla Núm. 108, Art. D.3:
"Incluir los riegos de ciberseguridad en el proceso de manejo de riesgos empresariales del Regulado y en los informes requeridos en los Artículos 32.040, y 53.070 del Código de Seguros de Puerto Rico y la Regla 104 sobre Gobernanza Corporativa."

3. PRIORIZAR

- Las actividades y los resultados del análisis de riesgo de ciberseguridad se incluyen en los procesos de gestión de riesgo empresarial. (GV.RM-03)

  Ejemplos:
  Incluir el tema de ciberseguridad cuando se discutan y se planifique el manejo de riesgos de cumplimiento, financiero, operacional, regulatorio, reputacional, etc.
  Incluir un gerente de ciberseguridad en las actividades y discusiones de planificación de riesgo empresarial.

4. COMUNICAR

- La alta gerencia se hace responsable de comunicar los riesgos de ciberseguridad y fomenta una cultura consciente de los riesgos, ética y de mejora continua. (GV.RR-01)

  Ejemplo:
  Compartir las expectativas de los líderes con respecto a una cultura segura y ética, sobretodo cuando surjan oportunidades para resaltar ejemplos positivos o negativos de manejo de riesgos de ciberseguridad.

- La política de ciberseguridad se establece dentro del contexto organizacional, la estrategia de ciberseguridad y las prioridades, y es comunicada y aplicada efectivamente. (GV.PO-01)

  Ejemplos:
  Comunicar la política de ciberseguridad a todo el personal de la organización, así como los estándares y procesos de apoyo.
  Requerir que el personal acuse recibo de la política de ciberseguridad al ser contratados, anualmente, y siempre que la misma sea actualizada.

Controles de IDENTIFICACIÓN

Función NIST CSF
IDENTIFICAR

Para poder proteger los activos de una organización, estos se deben identificar primero. Con este ejercicio se puede determinar el nivel de protección adecuado para cada activo en función de su sensibilidad y criticidad para su misión empresarial.

Funciones de **identificación** para todo tipo de entidad:

1. ENTENDER

- Se mantienen inventarios del hardware gestionado por la organización. (ID.AM-01)
- Se mantienen inventarios de software, servicios y sistemas gestionados por la organización. (ID.AM-02)
- Se mantienen inventarios de los servicios prestados por los proveedores. (ID.AM-04)

  Ejemplo:
  Llevar inventario de las computadoras, servidores, tabletas y celulares de la organización, así como **las plataformas y servicios en línea de terceros** que utilizan en sus procesos.

Regla Núm. 108, Art.8.D.2.e:
"Identificar y administrar la informacion, el personal, los dispositivos, los sistemas, e instalaciones que permitan que el Regulado logre sus propositos empresariales conforme a su importancia relativa a los objetivos empresariales y la estrategia de manejo de riesgos de la organizacion."

Regla Núm. 108, Art.8.D.2.j:
"Regularmente probar y monitorear los sistemas y procedimientos para detectar los ataques efectuados e intentados, o intrusiones en el Sistema de Informacion, así como en la red, ast como documentar el resultado de estas pruebas."

Art.8.D.5:
"Realizar pruebas de vulnerabilidad regularmente en sus Sistemas de Información, con herramientas que identifiquen claramente las vulnerabilidades, segun lo indique esta Oficina."

2. EVALUAR

- Se evalúa la efectividad del programa de ciberseguridad y se identifican mejoras en los procesos, procedimientos y actividades a partir de estas evaluaciones. (ID.IM-01)

  Ejemplo:
  Evaluar sus servicios críticos, tomando en consideración amenazas actuales.

- Se identifican, se validan y se registran las vulnerabilidades en todos los activos de información. (ID.RA-01)

3. PRIORIZAR

- Se mantiene un inventario actualizado de datos, que incluya sus categorías, metadatos y clasificaciones correspondientes. (ID.AM-07)

  Ejemplo:
  Hacer una lista de información no-pública para poder identificar fácilmente dónde y cómo se almacena, se procesa y se usa.

- La organización comprende el riesgo de seguridad cibernética para la organización, los activos y los individuos. (ID.RA)

Regla Núm. 108, Art.8.D.2.e:
"Identificar y administrar la información, el personal, los dispositivos, los sistemas, e instalaciones que permitan que el Regulado logre sus propósitos empresariales conforme a su importancia relativa a los objetivos empresariales y la estrategia de manejo de riesgos de la organización."

4. COMUNICAR

- Se establecen, comunican, mantienen y mejoran las políticas y los planes relacionados con ciberseguridad a todo el personal y terceros relevantes. (ID.IM-04)

  Ejemplo:
  Crear y adoptar un plan de respuesta a incidentes, un plan continuidad del negocio, y un plan de recuperación ante desastres para responder y recuperarse de eventos adversos que puedan interrumpir la operación, exponer información confidencial, o poner en peligro la misión y viabilidad de la organización.

- Se comunica al personal la importancia de identificar mejoras en los procesos, procedimientos y actividades de ciberseguridad. (ID.IM)

Controles de **PROTECCIÓN**

Función NIST CSF
PROTEGER

La función de proteger abarca la implementación de controles de seguridad para prevenir o reducir el riesgo cibernético.

Funciones de **protección** para todo tipo de entidad:

1. ENTENDER

- Los privilegios de acceso, los derechos y las autorizaciones se definen en una política, se gestionan, se aplican y se revisan, e incorporan los principios de privilegio mínimo (PoLP) y la separación de funciones. (PR.AA-05)

  Ejemplos:
  Crear y adoptar una política para **limitar el acceso y los privilegios al mínimo necesario** para que cada empleado desempeñe sus funciones.

2. EVALUAR

- Se le brinda al personal talleres de concienciación y capacitación en seguridad cibernética para que puedan realizar sus tareas relacionadas con ciberseguridad. (PR.AT)
  - Se adiestra al personal para que tenga el conocimiento necesario para realizar tareas generales teniendo en cuenta los riesgos de ciberseguridad. (PR.AT-01)
  - Se adiestra a las personas con funciones especializadas para que cuenten con los conocimientos y aptitudes necesarias para realizar sus tareas teniendo en cuenta los riesgos de ciberseguridad. (PR.AT-02)

3. PRIORIZAR

- Los usuarios, servicios y hardware están autenticados, usando un administrador de contraseñas para ayudar al personal a generar y proteger contraseñas seguras. (PR.AA-03)

- Siempre se cambian los credenciales del manufacturero y se administran adecuadamente todos los credenciales del personal, así como la identidad de los usuarios, servicios y equipos. (PR.AA-01)

  Ejemplos:
  Tramitar solicitudes al área de IT para cualquier nuevo acceso o acceso adicional que se le asigne a un empleado, contratista o tercero, según sea necesario. Utilizar **credenciales distintos y únicos**, no compartir cuentas ni contraseñas entre empleados.

Regla Núm. 108, Art.8.D.2:
"Implementar las siguientes medidas de seguridad, segun lo amerite su infraestructura, plantilla, operación y sistemas de información:
a) Mantener un programa formal de entrenamientos sobre las modalidades de riesgo cibernético para su personal, y llevar récord del desempeño del empleado en el programa.
b) Adiestrar y asignarle responsabilidades del Programa de Ciberseguridad a los empleados;
c) Establecer controles de acceso efectivos en los Sistemas de Información, incluidos los controles para autenticar (tales como la autenticación multifactorial) y permitir acceso solamente a personas autorizadas, para proteger contra la adquisición, alteración, divulgación o destrucción no autorizada de la Información No-Pública"

- En el hardware, el software (ej., *firmware*, sistemas operativos, aplicaciones) y los servicios de las plataformas físicas y virtuales, se actualizan regularmente y se implementan los parchos según estén disponibles, usando automatización y recordatorios siempre que sea posible. (PR.PS-02)

Puede mantenerse al tanto de nuevas vulnerabilidades que han sido explotadas y verificadas en: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

- Se hacen respaldos de sus datos y se prueban periódicamente. (PR.DS-11)

- Se encripta el disco completo de sus tabletas y otros dispositivos móviles para proteger los datos almacenados en los mismos. (PR.DS-01)

4. COMUNICAR

- Se comunica al personal cómo reconocer ataques comunes, informar de ataques o actividades sospechosas y realizar tareas básicas de higiene cibernética. (PR.AT-01/02)

  Ejemplos:
  Explicar el posible impacto y las consecuencias de violar las políticas de ciberseguridad, tanto para los usuarios individualmente como para la organización en su conjunto.
  Evaluar periódicamente al personal sobre su comprensión de las prácticas básicas de ciberseguridad.

Controles de **DETECCIÓN**

Función NIST CSF
DETECTAR

La función de detectar se enfoca en encontrar y analizar posibles ataques y situaciones comprometedoras en materia de ciberseguridad.

Regla Núm. 108, Art.8.D.2:

f) Restringir el acceso fiisico a las áreas donde se encuentre la Informacion No-Pública, para que sea únicamente accesible a las personas autorizadas; […]

j) Regularmente probar y monitorear los sistemas y procedimientos para detectar los ataques efectuados e intentados, o intrusiones en el Sistema de Información, así como en la red, así como documentar el resultado de estas pruebas;

k) Incluir procesos de respaldo, resguardo y gestión de registros ("Audit logs") dentro del Programa de Ciberseguridad diseñados para detectar y responder a los Incidentes de Ciberseguridad y para reconstruir las transacciones financieras significativas de manera que se provea un apoyo adecuado a las operaciones normales y obligaciones del Regulado

Funciones de **detección** para todo tipo de entidad:

1.ENTENDER

- Se comprende cómo identificar los indicadores más comunes de un incidente de ciberseguridad. (DE.CM)

2.EVALUAR

- Se evalúan regularmente los sistemas de información y servicios externos para detectar desviaciones del comportamiento esperado o típico. (DE.CM-06/09)

- Se evalúa regularmente la seguridad física para identificar señales de manipulación u otra actividad sospechosa. (DE.CM-02)

3.PRIORIZAR

- Actualizar el antivirus / antimalware en los dispositivos empresariales: ej. servidores, computadoras y *smartphones*. (DE.CM-09)
- Contratar a un proveedor de servicio para monitorear la actividad sospechosa en computadoras y redes, si la entidad no tiene la capacidad de hacerlo internamente. (DE.CM)

4. COMUNICAR

- Comunicarse con un respondedor de incidentes certificado sobre los detalles relevantes del incidente para ayudarlos a analizarlo y mitigarlo. (DE. AE-06/07)

Controles de **RESPUESTA**

Función NIST CSF
RESPONDER

La función de responder aumenta su habilidad de tomar decisiones con respecto a un incidente de ciberseguridad detectado.

Funciones de **respuesta** para todo tipo de entidad:

1. ENTENDER

- Comprender su plan de respuesta a incidentes y quién tiene la autoridad y la responsabilidad de implementar los distintos aspectos del plan. (RS. MA-01)

2. EVALUAR

- Evaluar su capacidad para responder a un incidente de ciberseguridad. (RS. MA-01)
- Evaluar el incidente para determinar su gravedad, lo que sucedió y el vector de ataque. (RS. AN-03, RS. MA-03)

3. PRIORIZAR

- Priorizar las decisiones para contener y erradicar el incidente, evitando daños mayores. (RS.MI)

Vea la guía del NIST para responder a un incidente cibernético (SP 800-61 Rev. 2): https://csrc.nist.gov/pubs/sp/800/61/r2/final

Regla Núm. 108, Art.10:
"El Regulado notificará al Comisionado un Incidente de Ciberseguridad tan pronto sea posible, dentro de las 72 horas despues del momento en que se haya determinado que ocurrió un Incidente de Ciberseguridad."
[Lea más sobre cómo y a quién debe notificarle un incidente de ciberseguridad]

4. COMUNICAR

- Comunicar un incidente de ciberseguridad confirmado a todas las partes interesadas internas y externas (por ejemplo, clientes, socios comerciales, agencias de aplicación de la ley, organismos reguladores) según lo exijan las leyes, reglamentos, contratos o políticas.
(RS. CO-02/03)

Regla Núm. 108, Art.8.H.2:
"El plan de respuesta a los incidentes deberá atender lo siguiente:
(a) El proceso interno de respuesta a un Incidente de Ciberseguridad;
(b) Los objetivos del plan de respuesta a incidentes;
(c) La defimicion clara de los roles, responsabilidades y niveles de autoridad para tomar decisiones, incluyendo nombres de empleados y proveedores de respuesta a incidentes; (d) Comunicaciones extemas e intemas y la manera en que se comparte la información."

Controles de **RECUPERACIÓN**

Función NIST CSF
RESPONDER

La función de recuperar conlleva restaurar activos y operaciones que se vieron afectados por un incidente de ciberseguridad.

Funciones de **recuperación** para todo tipo de entidad:

1. ENTENDER

- Comprender quiénes (dentro y fuera de su empresa) tiene responsabilidades de recuperación. (RC. RP-01)

2. EVALUAR

- Repasar lo sucedido preparando un informe posterior a la acción, por su cuenta o en colaboración con un proveedor, que documente el incidente, las acciones de respuesta y recuperación tomadas, y las lecciones aprendidas. (RC. RP-06)
- Evaluar la integridad de sus datos y activos respaldados antes de utilizarlos para la restauración. (RC. RP-03)

3. PRIORIZAR

- Priorizar sus acciones de recuperación en función de las necesidades, los recursos y los activos de la organización afectados. (RC. RP-02)

Regla Núm. 108, Art.8.H.2:

"El plan de respuesta a los incidentes deberá atender lo siguiente: […]

e) Identificación de requisitos para la remediación de toda debilidad identificada en los Sistemas de Información y controles asociados;

f) Documentación y preparación de informes relacionados con los Incidentes de Ciberseguridad y las actividades correspondientes de respuesta; y

g) La evaluación y revisión del plan de respuesta a incidentes, según fuera necesario después de un Incidente de Ciberseguridad."

4. COMUNICAR

- Comunicarse de forma regular y segura con las partes interesadas internas y externas. (RC.CO)
- Comunicar y documentar el incidente y su remediación, ante de reanudar las actividades normales. (RC. RP-06)

Para crear planes de recuperación, puede dejarse llevar por los recursos disponibles en: https://www.ready.gov/business/emergency-plans/recovery-plan

Historial de Revisiones

Versión	Fecha	Revisiones	Aprobada por

Guía de Implementación de Controles de Ciberseguridad para la Industria de Seguros
Versión: 1.0
Publicada: 25 de septiembre de 2024
Aprobada por: Lcdo. Alexander S. Adams Vega, Comisionado de Seguros
Contacto: ciberseguridad@ocs.pr.gov