Anexo 1
Descripción de la herramienta de autoevaluación para el sector salud provista por el BID

El objetivo de la herramienta de autoevaluación para el sector salud es permitir que los responsables de las organizaciones evalúen su situación de ciberseguridad basándose en las mejores prácticas de la industria.

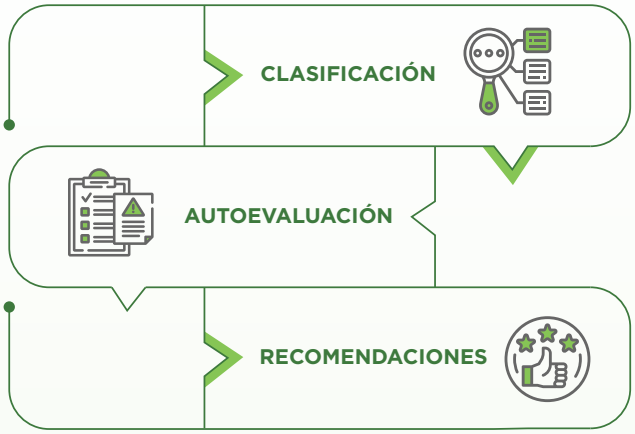
La figura 1 muestra la lógica implementada por la herramienta de autoevaluación, que consta de tres etapas: **clasificación, autoevaluación y recomendaciones**.

La etapa de clasificación tiene como objetivo definir un nivel de ciberseguridad que la organización debe cumplir. La herramienta recomienda tres posibles niveles organizacionales (BÁSICO, MEDIO y AVANZADO) en función de los cuales se establecen los requerimientos de seguridad de la información requeridos y, por ende, qué preguntas son incluidas en la autoevaluación.

Dada la heterogeneidad de las empresas y organizaciones del sector salud que van a utilizar la autoevaluación, lo primero que se debe realizar es comprender el tipo de organización que se está evaluando. **Los tipos de organizaciones contemplados en la versión v0.7.2 son:**

- Hospital
- Farmacia
- Laboratorio
- Ministerio o ente regulador
- Prestador o agrupación de prestadores u otros

FIGURA 1 • Lógica implementada



Para cada tipo de organización se definió un conjunto de preguntas con el objetivo de medir el tamaño de la organización según las distintas variables de negocio. Dichas preguntas se construyeron tomando como referencia los factores organizacionales que utiliza HITRUST para definir los niveles de implementación.

La tabla 1 muestra las preguntas de clasificación utilizadas en la versión v0.7.2 de la herramienta de autoevaluación, detallando la fuente utilizada en su construcción o sin fuente, en caso de que la elaboración estuviera basada en la experiencia del equipo.

TABLA 1 • Preguntas de clasificación utilizadas en la versión 0.7.2

Pregunta y Respuesta	Fuente
¿Cuántas camas tiene la organización? • BÁSICO: Menor a 200 • MEDIO: Entre 200 y 750 • AVANZADO: Mayor a 750	HITRUST
¿Qué cantidad de pacientes admiten hospitalariamente por año? • BÁSICO: Menor a 7.500 • MEDIO: Entre 7.500 y 20.000 • AVANZADO: Mayor a 20.000	HITRUST
¿Cuántas personas tienen derecho a recibir atención en la organización (afiliados/socios/otros)? • BÁSICO: Menor a 1.000.000 • MEDIO: Entre 1.000.000 y 7.500.000 • AVANZADO: Mayor a 7.500.000	HITRUST
¿Qué cantidad de consultas médicas ofrecen anualmente? • BÁSICO: Menor a 1.000.000 • MEDIO: Entre 1.000.000 y 6.000.000 • AVANZADO: Mayor a 6.000.000	HITRUST
¿Qué cantidad de proveedores de servicios médicos (laboratorios/ imagenología/otros) disponen? • BÁSICO: Menor a 10 • MEDIO: Entre 10 y 30 • AVANZADO: Mayor a 30	(sin fuente)
¿Qué cantidad de estudios realizan anualmente? • BÁSICO: Menor a 25.000 • MEDIO: Entre 25.000 y 100.000 • AVANZADO: Mayor a 100.000	(sin fuente)

En función del tipo de organización se presentan las preguntas correspondientes de clasificación y se sugiere ejecutar el formulario en el nivel máximo de respuesta para alguna de las preguntas de clasificación. Por ejemplo, si un hospital responde que tiene más de 750 camas (AVANZADO) y admite hospitalariamente por año entre 7.500 y 20.000 personas (MEDIO), la herramienta va a sugerir responder la autoevaluación en nivel AVANZADO. Dicha clasificación es una sugerencia y se permite al usuario cambiarla. Esto se debe a que puede haber otro tipo de factores no contemplados en la herramienta (por ejemplo, regulatorios) que sitúen la organización en otro nivel.

El siguiente paso es evaluar por medio de un conjunto de preguntas el nivel actual de la organización en aspectos de ciberseguridad tomando como base lo propuesto por el NIST-CSF. Con tal cometido se definieron preguntas y se profundizan por nivel organizacional (BÁSICO, MEDIO y AVANZADO).

La tabla 2 muestra la cantidad de preguntas agrupadas por función del NIST-CSF y del nivel organizacional en el que se está ejecutando la herramienta de autoevaluación.

Con este modelo se logró un número acotado de preguntas que se incrementa por cada nivel. El total de preguntas para una evaluación en nivel básico es 25, en nivel medio es 44 (25 + 19) y en nivel avanzado 66 (25 + 19 + 22).

Para mayor detalle sobre las preguntas de evaluación de la herramienta y la lógica de dependencias entre las mismas recomendamos leer el Anexo "Preguntas de autoevaluación para el sector salud provista por el BID".

Una vez ejecutada la autoevaluación se pasa a la siguiente etapa que es la de recomendaciones. En esta etapa se calcula un puntaje respecto de cada función y categoría del NIST-CSF. El puntaje o *scoring* se calcula realizando un promedio de los resultados por función y por categoría; cada opción de cada pregunta tiene un valor fijo asignado.

La figura 2 muestra la representación gráfica en forma de radar del puntaje por cada función del NIST-CSF (en la versión v0.7.2 de la herramienta, con un ejemplo ficticio).

Las recomendaciones constan de una descripción general y de acciones concretas a ejecutar para mejorar el nivel de madurez de la organización en cada categoría del NIST-CSF. La herramienta selecciona qué recomendaciones debe mostrar dependiendo del puntaje obtenido en cada categoría y un umbral de aceptación predefinido a juicio experto.

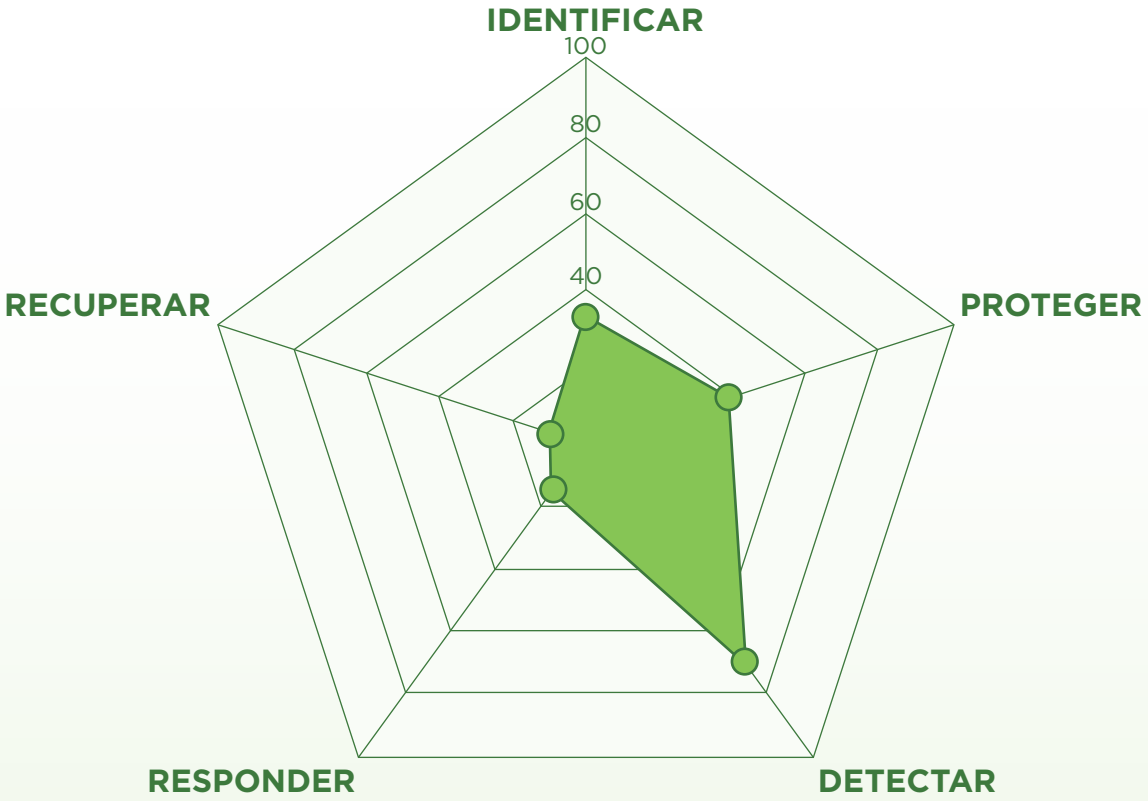
Para validar que la herramienta cumple con los objetivos planteados se ejecutaron dos actividades. La primera fue un *focus group* con referentes de diferentes universidades de la región. La segunda fue una prueba de concepto de la herramienta en organizaciones de salud de ALC con el fin de validar su comportamiento en campo. **De ambas actividades se extrajeron lecciones aprendidas y recomendaciones, algunas de las cuales fueron incorporadas a la versión actual, y se generó una lista de mejoras a evaluar en un futuro, como, por ejemplo:**

- puntajes (*scoring*) ponderados,
- mejoras en las reglas para sugerir recomendaciones o incluir/excluir acciones concretas en las recomendaciones,
- agregar material en las preguntas que permita apoyar en la generación de habilidades o comprensión de las preguntas,
- mejorar el perfilado de la persona que ejecuta la autoevaluación para personalizar las preguntas.

TABLA 2 • Preguntas agrupadas por función del NIST-CSF

	Básico	Medio	Avanzado
GENERAL	5	0	0
IDENTIFICAR	3	8	9
PROTEGER	11	5	5
DETECTAR	3	2	4
RESPONDER	2	2	2
RECUPERAR	1	2	2
TOTAL	**25**	**19**	**22**

FIGURA 2 • Resultado de la autoevaluación de nivel MEDIO



Anexo 2
Preguntas de autoevaluación para el sector salud provista por el BID

Este anexo describe las preguntas utilizadas por la herramienta de autoevaluación para el sector salud descrita en el anexo anterior.

Se construyeron preguntas vinculadas a cada subcategoría del NIST-CSF. Esto no quiere decir que exista un mapeo uno a uno entre las subcategorías y las preguntas. Algunas preguntas aportan información para evaluar más de una subcategoría. Lo que sí se aseguró es que toda categoría del NIST-CSF tiene al menos una pregunta asociada, lo que es sumamente importante pues, como se mencionó anteriormente, las recomendaciones se generaron asociadas a dichas categorías.

La tabla 3 muestra las preguntas incluidas en la versión v0.7.2 de la herramienta de autoevaluación.

TABLA 3 • Preguntas incluidas en la versión v0.7.2 de la herramienta de autoevaluación

Identificador	Función	Categoría	Pregunta
GR-SC1	General	-	¿Tiene un equipo dedicado a la seguridad de la información? Opciones: • NO. • SÍ.
GR-SC2	General	-	¿Cuál es el tamaño actual del equipo de seguridad de la información en relación con la cantidad de personas que trabajan en la organización? Opciones: • 1 de cada 1.000. • 1 de cada 100. • 1 de cada 10. • 1 de cada 5.

TABLA 3 • Preguntas incluidas en la versión v0.7.2 de la herramienta de autoevaluación (*cont.*)

Identificador	Función	Categoría	Pregunta
GR-SC3	General	-	¿Destina presupuesto para ciberseguridad? Opciones: • NO. • SÍ.
GR-SC4	General	-	¿Qué porcentaje del presupuesto de TI dedica a ciberseguridad? (umbrales) En caso de tener presupuestos independientes, se debe responder con la relación porcentual entre los mismos. Opciones: • Menor al 1%. • Entre 1% y 3%. • Entre 3% y 6%. • Mayor al 6%.
GR-SC5	General	-	¿Cuál es el tamaño actual del equipo de TI en relación con la cantidad de personas que trabajan en la organización? Opciones: • 1 de cada 1.000. • 1 de cada 100. • 1 de cada 10. • 1 de cada 5.
ID-B1	Identificar	ID.AM	¿Tiene un inventario actualizado para alguno de los siguientes activos? • Dispositivos físicos (PCs, dispositivos móviles, *routers*, servidores, *storage*, etc.).

TABLA 3 • Preguntas incluidas en la versión v0.7.2 de la herramienta de autoevaluación (*cont.*)

Identificador	Función	Categoría	Pregunta
ID-B1	Identificar	ID.AM	• Aplicaciones, sistemas y plataformas de *software*. • Redes. Opciones: • Ninguno • SÍ, tengo inventariados algunos de los activos de la organización, pero no está actualizada la información de detalle de cada uno. • SÍ, tengo inventariados todos los activos de la organización, pero no está actualizada la información de detalle de cada uno. • SÍ, tengo inventariados todos los activos de mi organización y está actualizada la información de detalle de cada uno.
ID-B2	Identificar	ID.AM	En su organización, ¿quién maneja los temas relacionados con la seguridad de la información o la ciberseguridad? Opciones: • Nadie. • El equipo de TI. • El personal dedicado a seguridad dentro de TI. • El equipo especializado de seguridad e independiente de TI.

TABLA 3 • Preguntas incluidas en la versión v0.7.2 de la herramienta de autoevaluación (*cont.*)

Identificador	Función	Categoría	Pregunta
ID-B3	Identificar	ID-B3	¿Debe cumplir alguna normativa específica del sector como, por ejemplo, la Ley de protección de datos personales o la Ley de Historia Clínica? Opciones: • NO. • SÍ.
ID-M1	Identificar	ID.AM	¿Tiene clasificada la información de los activos en concordancia con leyes, políticas, estándares y guías? Un posible ejemplo de clasificación es dividir la información en pública, de uso interno, confidencial y secreta. Opciones: • NO. • Parcialmente. • SÍ.
ID-M2	Identificar	ID.AM	¿Cuenta su organización con procedimientos que garanticen la protección del flujo de información interna y con el exterior? Opciones: • NO. • Parcialmente. • SÍ.

TABLA 3 • Preguntas incluidas en la versión v0.7.2 de la herramienta de autoevaluación (*cont.*)

Identificador	Función	Categoría	Pregunta
ID-M3	Identificar	ID.AM	¿Tiene asignados los siguientes roles? • Responsable de seguridad de la información (CISO). • Equipo de respuesta a incidentes de seguridad. • Responsable de gestión de riesgos de seguridad. • Responsable de gestión de vulnerabilidades. Opciones: • Ninguno. • CISO. • Todos.
ID-M4	Identificar	ID.GV	¿Cuál de los siguientes elementos son utilizados en su organización? • Políticas asociadas a Seguridad de la Información. • Procesos asociados a Seguridad de la Información. • Procedimientos asociados a Seguridad de la Información. Opciones: • Ninguno. • Solamente procedimientos. • Solamente procesos y procedimientos. • Todos.

TABLA 3 • Preguntas incluidas en la versión v0.7.2 de la herramienta de autoevaluación (*cont.*)

Identificador	Función	Categoría	Pregunta
ID-M5	Identificar	ID.GV	¿Tiene apoyo de un equipo multidisciplinario (abogados y técnicos) para el análisis de los requerimientos para cumplir con las normativas aplicables? Opciones: • NO. • SÍ.
ID-M6	Identificar	ID.RA	¿Se identifican y analizan las vulnerabilidades de los activos? Opciones: • NO. • NO, pero si me notifican se toman acciones correctivas. • SÍ, en los activos críticos. • SÍ y existe un proceso de gestión de vulnerabilidades asociado.
ID-M7	Identificar	ID.RA	¿En función de las amenazas y las vulnerabilidades, se determinan los riesgos y su impacto? Opciones: • NO. • SÍ. • SÍ y en función de esto se definen controles para llevar el riesgo a un nivel aceptable para la organización.

TABLA 3 • Preguntas incluidas en la versión v0.7.2 de la herramienta de autoevaluación (*cont.*)

Identificador	Función	Categoría	Pregunta
ID-M8	Identificar	ID.SC	¿Tiene definidos acuerdos de niveles de servicio (SLA) con los proveedores de servicios críticos? Opciones: • NO. • SÍ.
ID-A1	Identificar	ID.AM	¿Tiene definidas políticas y procedimientos que pautan el inventariado de activos? Opciones: • NO. • SÍ.
ID-A2	Identificar	ID.AM	¿Tiene herramientas automatizadas para la gestión del inventario de activos? Opciones: • NO. • Parcialmente. • SÍ.
ID-A3	Identificar	ID.AM	¿Actualiza el inventario en el momento que cambia? Opciones: • NO. • SÍ.
ID-A4	Identificar	ID.BE	¿Tiene identificados los proveedores, sistemas y recursos en general (internos y externos) necesarios para brindar los servicios críticos de su organización? Opciones: • NO. • Parcialmente. • SÍ.

TABLA 3 • Preguntas incluidas en la versión v0.7.2 de la herramienta de autoevaluación (*cont.*)

Identificador	Función	Categoría	Pregunta
ID-A5	Identificar	ID.GV	¿Tiene implementado un SGSI con procedimientos de mejora continua? Opciones: • NO. • En proceso de implementación. • SÍ.
ID-A6	Identificar	ID.GV	¿Tiene conformado un comité de seguridad de la información? Opciones: • NO. • SÍ.
ID-A7	Identificar	ID.GV	¿El comité de seguridad de la información tiene asesoría legal para velar por el cumplimiento de la normativa vigente? Opciones: • NO. • SÍ.
ID-A8	Identificar	ID.RM	Formalmente, ¿tiene un plan de tratamiento de riesgos? Opciones: • NO. • SÍ.
ID-A9	Identificar	ID.SC	¿Sus proveedores y socios externos realizan una evaluación de riesgos de la cadena de suministros? Opciones: • NO. • SÍ.

TABLA 3 • Preguntas incluidas en la versión v0.7.2 de la herramienta de autoevaluación (*cont.*)

Identificador	Función	Categoría	Pregunta
PR-B1	Proteger	PR.AC	¿Tiene un equipo encargado de la gestión de usuarios (identidades y credenciales)? Opciones: • No tengo identificados a los usuarios. • SÍ y se hace a mejor esfuerzo. • SÍ y está sistematizado con un proceso formal. • SÍ, está sistematizado con un proceso formal y el mismo se audita en forma periódica.
PR-B2	Proteger	PR.AC	¿Tiene un equipo encargado de la gestión de autoriza-ción para dispositivos? Opciones: • No tengo identificados los dispositivos. • SÍ y se hace a mejor esfuerzo. • SÍ y está sistematizado con un proceso formal. • SÍ, está sistematizado con un proceso formal y el mismo se audita en forma periódica.
PR-B3	Proteger	PR.AC	¿Implementa controles para acceso físico? Opciones: • NO. • Solamente en los servidores. • Los servidores y el resto de los equipos están bajo llave o con videovigilancia.

TABLA 3 • Preguntas incluidas en la versión v0.7.2 de la herramienta de autoevaluación (*cont.*)

Identificador	Función	Categoría	Pregunta
PR-B4	Proteger	PR.AC	¿Su organización tiene accesos remotos? Opciones: • NO. • SÍ.
PR-B5	Proteger	PR.AC	¿Implementa controles para acceso remoto? Opciones: • NO. • Con múltiples herramientas, sin gestión centralizada (por ejemplo RDP, VNC, etc.) y sin medidas extra de seguridad. • Con gestión centralizada, utilizando herramientas como VPN + RDP, VPN + VNC, entre otras. • Con gestión centralizada e implementada adecuadamente mediante procesos.
PR-B6	Proteger	PR.DS	¿Se protegen los datos en su almacenamiento (papel, discos, cintas, respaldos, entre otros) agregando controles como, por ejemplo, control de acceso físico, control de acceso lógico, cifrado, etc.? Opciones: • NO. • Solamente en algunos casos. • SÍ. • SÍ y se valida que las medidas de cifrado sean adecuadas para la confidencialidad de la información.

TABLA 3 • Preguntas incluidas en la versión v0.7.2 de la herramienta de autoevaluación (*cont.*)

Identificador	Función	Categoría	Pregunta
PR-B7	Proteger	PR.DS	¿Se protegen los datos en tránsito utilizando tecnologías como, por ejemplo, SSL, HTTPs, VPNs, etc.? Opciones: • NO. • Tránsito hacia el exterior de la organización. • Tránsito incluyendo interior y exterior de la organización. • SÍ, en ambas direcciones, y se valida que las medidas de cifrado sean adecuadas para la confidencialidad de la información.
PR-B8	Proteger	PR.DS	En el caso de que sus empleados o proveedores manejen información confidencial, ¿tiene firmados acuerdos de confidencialidad? Opciones: • NO. • Solamente con los proveedores, pero no con los empleados. • Con empleados y con algunos proveedores. • Con los empleados y con todos los proveedores.
PR-B9	Proteger	PR.IP	¿Se realizan respaldos de la información? Opciones: • NO. • SÍ, locales. • SÍ, en un sitio remoto.

TABLA 3 • Preguntas incluidas en la versión v0.7.2 de la herramienta de autoevaluación (*cont.*)

Identificador	Función	Categoría	Pregunta
PR-B10	Proteger	PR.IP	¿Se testean respaldos de la información? Opciones: • NO. • SÍ. • SÍ, de forma periódica.
PR-B11	Proteger	PR.PT	¿Se cuenta con registros de *log* de los activos (aplicaciones, sistemas operativos, equipamiento de red, etc.)? Opciones: • NO. • SÍ, pero no se cuenta con políticas de retención. • SÍ y se cuenta con políticas de retención. • SÍ, se cuenta con políticas de retención y se revisan periódicamente.
PR-M1	Proteger	PR.AC	¿Tiene separación de ambientes y cada persona accede solamente a la información que le corresponde? Opciones: • NO. • Tengo separación de ambientes, pero todos los usuarios/roles pueden acceder a cualquiera de ellos. • SÍ.

TABLA 3 • Preguntas incluidas en la versión v0.7.2 de la herramienta de autoevaluación (*cont.*)

Identificador	Función	Categoría	Pregunta
PR-M2	Proteger	PR.AC	¿Tiene la red segmentada según la sensibilidad de los activos y la exposición? Opciones: • NO. • SÍ, tengo la red segmentada pero no se cuenta con criterios claros para la segmentación (riesgos, sensibilidad de la información, etc). • SÍ.
PR-M3	Proteger	PR.AT	¿Tiene un programa de concientización y formación en seguridad de la información? Opciones: • NO. • De manera esporádica se imparten charlas sobre la temática. • Periódicamente el personal recibe charlas sobre la temática. • SÍ.
PR-M4	Proteger	PR.DS	¿Hace un cálculo de la proyección de crecimiento de los sistemas que dan soporte a los servicios? Opciones: • NO. • Al momento de realizar las compras, se hace una proyección de crecimiento durante la vida útil del equipamiento. • SÍ.

TABLA 3 • Preguntas incluidas en la versión v0.7.2 de la herramienta de autoevaluación (*cont.*)

Identificador	Función	Categoría	Pregunta
PR-M5	Proteger	PR.IP	¿Tiene definida una línea base de la configuración de los sistemas de información? Opciones: • NO. • SÍ, pero no se revisa a menos que haya cambios el sistema. • SÍ y se revisa periódicamente. • SÍ, se revisa periódicamente y se siguen procesos de gestión de configuración.
PR-A1	Proteger	PR.AT	¿Tiene un programa de concientización y formación en seguridad de la información especializado para los usuarios privilegiados? Opciones: • NO. • De manera esporádica se imparten charlas sobre buenas prácticas. • Periódicamente el personal recibe charlas sobre buenas prácticas. • SÍ y se sigue un plan de capacitaciones en seguridad de la información o ciberseguridad.
PR-A2	Proteger	PR.IP	¿Implementa el ciclo de vida de desarrollo de sistemas? Opciones: • NO. • SÍ. • SÍ y se documenta formalmente.

TABLA 3 • Preguntas incluidas en la versión v0.7.2 de la herramienta de autoevaluación (*cont.*)

Identificador	Función	Categoría	Pregunta
PR-A3	Proteger	PR.IP	¿Su ciclo de vida de desarrollo de sistemas tiene tareas de seguridad embebidas (S-SLDC)? Opciones: • NO. • SÍ, se incorporan algunas actividades pero no de forma sistematizada. • SÍ, se incluyen las actividades y se trabajan en forma de mejora continua.
PR-A4	Proteger	PR.MA	¿Planifica el mantenimiento y reparación de sus activos? Opciones: • NO. • SÍ, pero no tengo registro de las reparaciones. • SÍ y se registran los mismos. • SÍ y tengo un proceso de aprobación de las reparaciones.
PR-A5	Proteger	PR.PT	¿Tiene los registros de *log* de los activos estandarizados y centralizados? Opciones: • NO. • SÍ, están centralizados. • SÍ, están centralizados y estandarizados para su explotación.

TABLA 3 • Preguntas incluidas en la versión v0.7.2 de la herramienta de autoevaluación (*cont.*)

Identificador	Función	Categoría	Pregunta
DE-B1	Detectar	DE.CM	¿Tiene una solución de antivirus? Opciones: • NO. • En algunos equipos. • En todos los equipos.
DE-B2	Detectar	DE.CM	¿La solución de antivirus se encuentra actualizada? Opciones: • NO. • SÍ.
DE-B3	Detectar	DE.CM	¿Se revisan las alertas de su solución de antivirus? Opciones: • NO. • SÍ, de forma esporádica. • SÍ, se tiene un proceso asociado.
DE-M1	Detectar	DE.CM	¿Se monitorea la red para detectar potenciales eventos de ciberseguridad? Opciones: • NO. • SÍ, tengo eventos configurados en los activos existentes en la organización (por ejemplo, *firewalls*). • SÍ, tengo reglas específicas implementadas en los sistemas de monitoreo de seguridad de la organización.

TABLA 3 • Preguntas incluidas en la versión v0.7.2 de la herramienta de autoevaluación (*cont.*)

Identificador	Función	Categoría	Pregunta
DE-M2	Detectar	DE.CM	¿Con qué periodicidad se realizan escaneos de vulnerabilidades? Opciones: • NO se realizan. • SÍ, de forma aislada a los sistemas principales. • SÍ, de forma aislada a todos los activos de la organización con acceso a información sensible. • SÍ, de manera periódica y se hace una gestión de las vulnerabilidades.
DE-A1	Detectar	DE.AE	¿Tienen conocimiento del comportamiento normal de sus sistemas y flujos de datos esperados? Por ejemplo, la cantidad de usuarios que utilizan normalmente un sistema, el flujo normal de datos de red, la cantidad de registros de *log* que escribe un sistema o la cantidad de correos enviados por día en la organización, entre otros. Opciones: • NO. • SÍ, para los sistemas principales. • SÍ, con umbrales definidos y análisis de causa/impacto cuando se exceden los mismos.

TABLA 3 • Preguntas incluidas en la versión v0.7.2 de la herramienta de autoevaluación (*cont.*)

Identificador	Función	Categoría	Pregunta
DE-A2	Detectar	DE.AE	¿Los datos de los eventos se agrupan y correlacionan desde múltiples fuentes y sensores? Opciones: • NO. • SÍ, de forma *ad-hoc*. • SÍ, utilizando un sistema de gestión de seguridad de la información y eventos (SIEM). • SÍ y se analizan con un equipo de operaciones de seguridad (SOC).
DE-A3	Detectar	DE.CM	¿Se controla la actividad de los proveedores de servicios externos para detectar posibles eventos de ciberseguridad? Opciones: • NO. • SÍ, se controlan intentos de actividad no permitida en los mecanismos de acceso definidos como, por ejemplo, actividad no prevista en las VPNs.

TABLA 3 • Preguntas incluidas en la versión v0.7.2 de la herramienta de autoevaluación (*cont.*)

Identificador	Función	Categoría	Pregunta
DE-A4	Detectar	DE.DP	¿Cuentan con procesos y procedimientos de detección de eventos de seguridad? Un evento de seguridad es una ocurrencia identificada en el estado de un sistema, servicio o red que puede ser relevante para la seguridad del mismo. Opciones: • NO. • SÍ. • SÍ, y se incorpora lo aprendido en los incidentes como mejora de los mismos.
RS-B1	Responder	RS.RP	¿Tiene definida la forma de atención de un incidente de seguridad de la información? Opciones: • NO. • SÍ, sin responsabilidades definidas y sin documentar. • SÍ, con responsabilidades definidas y sin documentar. • SÍ, con responsabilidades definidas y documentado.

TABLA 3 • Preguntas incluidas en la versión v0.7.2 de la herramienta de autoevaluación (*cont.*)

Identificador	Función	Categoría	Pregunta
RS-B2	Responder	RS.CO	¿Los incidentes se comunican y coordinan con las partes interesadas internas y externas, según corresponda? Opciones: • NO. • SÍ, con el equipo interno. • SÍ, con partes internas y externas en los casos que corresponda.
RS-M1	Responder	RS.MI	¿Qué tipo de acciones toma ante un incidente de seguridad de la información? Opciones: • Ninguna. • Se contiene el mismo, por ejemplo, aislando los activos afectados. • Se contiene el mismo y se toman medidas para reducir su impacto.
RS-M2	Responder	RS.AN	En caso de un incidente, ¿se analizan las causas y se recolecta la información como evidencia? Opciones: • NO. • SÍ, se analizan las causas y el impacto de los incidentes. • SÍ, se analizan las causas y el impacto de los incidentes haciendo un análisis forense en los casos que corresponde.

TABLA 3 • Preguntas incluidas en la versión v0.7.2 de la herramienta de autoevaluación (*cont.*)

Identificador	Función	Categoría	Pregunta
RS-A1	Responder	RS.IM	Las lecciones aprendidas durante el análisis de los incidentes, ¿son incorporadas para las futuras actividades de respuesta? Opciones: • NO. • Solamente en algunos casos. • SÍ, en todos los casos.
RS-A2	Responder	RS.CO	En caso de un incidente, ¿se notifica a los involucrados de la afectación en la seguridad de sus datos? Opciones: • NO. • Solamente en algunas ocasiones, aunque esto puede implicar incumplimientos normativos. • SÍ, siempre que tengo obligación normativa. • SÍ, en todos los casos.

TABLA 3 • Preguntas incluidas en la versión v0.7.2 de la herramienta de autoevaluación (*cont.*)

Identificador	Función	Categoría	Pregunta
RC-B1	Recuperar	RC.RP	Los procesos y procedimientos de recuperación, ¿son ejecutados y mantenidos para asegurar la restauración oportuna de los sistemas o activos afectados? Opciones: • NO tengo planes de recuperación para mis sistemas críticos. • SÍ, tengo planes de recuperación para algunos sistemas críticos. • SÍ, tengo planes de recuperación para todos mis sistemas críticos pero no los pruebo periódicamente. • SÍ, tengo planes de recuperación para todos mis sistemas críticos y los pruebo periódicamente.
RC-M1	Recuperar	RC.RP	Los procesos y procedimientos de recuperación, ¿están documentados y comunicados? Opciones: • NO. • SÍ, están documentados pero no comunicados. • SÍ, están documentados y comunicados.

TABLA 3 • Preguntas incluidas en la versión v0.7.2 de la herramienta de autoevaluación (*cont.*)

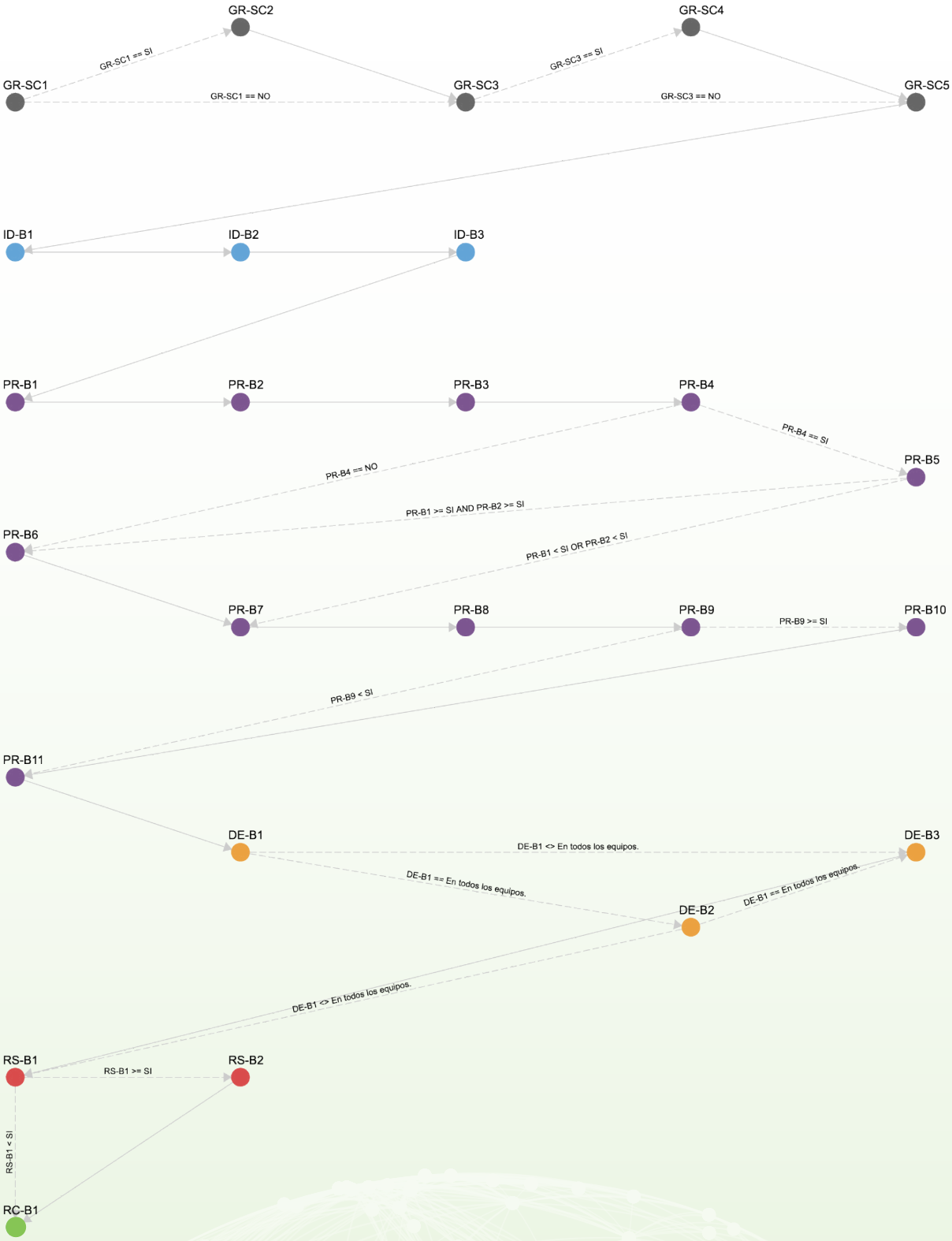
Identificador	Función	Categoría	Pregunta
RC-M2	Recuperar	RC.IM	Las lecciones aprendidas durante la recuperación, ¿son incorporadas para las futuras actividades? Opciones: • NO. • Solamente en algunos casos. • SÍ, en todos los casos.
RC-A1	Recuperar	RC.RP	¿Realiza simulacros que validen los procesos y procedimientos de recuperación? Opciones: • NO. • SÍ.
RC-A2	Recuperar	RC.CO	¿Son gestionadas las comunicaciones con los interesados (internos y externos) y las relaciones públicas? Opciones: • NO. • SÍ. • SÍ y se tiene un plan para dicha gestión.

Las preguntas pueden tener dependencias entre sí, por lo cual se definió un lenguaje de reglas en la herramienta que permite determinar en qué casos debe hacerse o no una determinada pregunta. Dicha funcionalidad mejora la usabilidad, pues es normal tener preguntas que profundizan o se relacionan con preguntas anteriores. Por ejemplo, si alguien responde que no tiene accesos remotos en su organización (pregunta **PR-B4**), no aplica preguntar qué controles implementa sobre dichos accesos remotos (pregunta **PR-B5**).

Con el objetivo de lograr una representación gráfica de las dependencias, se generó un grafo de dependencias. Las preguntas se muestran como un círculo, sobre el mismo se muestra el identificador de la pregunta y las aristas son las transiciones entre las mismas. El color del círculo es el mismo al utilizado por la función del NIST asociada a la pregunta.

La figura 3 muestra el grado de dependencias entre preguntas de nivel organizacional BÁSICO implementado en la versión v0.7.2 de la herramienta de autoevaluación.

FIGURA 3 • Grado de dependencias entre preguntas de nivel organizacional BÁSICO implementado en la versión v0.7.2 de la herramienta de autoevaluación.



Las condiciones en las aristas del grafo tienen operadores lógicos AND y OR, mientras que las expresiones utilizan operadores de comparación.

Con el fin de facilitar la lectura del grafo, los operadores de comparación se deben leer de una forma laxa que explicaremos a continuación con ejemplos.

Consideremos la pregunta DE-B1 que dice "¿Tiene una solución de antivirus?" y sus opciones son:

1. NO.
2. En algunos equipos.
3. En todos los equipos.

Las opciones son una lista ordenada. Entonces, cuando decimos PR-B9 = "En todos los equipos", se traduce como que el índice de la respuesta de PR-B9 es igual a 3. En este caso es una condición que dice si se tiene antivirus en todos los equipos o no.

Si quisiéramos escribir la condición que represente que se tiene antivirus sin importar en cuantos equipos, se podría escribir de cualquiera de las siguientes maneras:

- PR-B9 <> "NO".
- PR-B9 >= "En algunos equipos".

Recordemos que comparamos los índices de las opciones y por esto ambas expresiones son equivalentes.
Para simplificar el grafo, adicionalmente se muestra SÍ en lugar del texto completo cuando el texto de la opción comienza con SÍ.

En la herramienta de autoevaluación, durante el proceso de respuesta del cuestionario, se puede solicitar ver dicho grafo. En este caso, se muestra el grafo filtrado por nivel organizacional en el que se está trabajando (BÁSICO, MEDIO y AVANZADO) y marcando las preguntas efectivamente respondidas representando el nodo como un diamante. Desde el grafo de preguntas, al hacer foco en el nodo que representa la pregunta, se puede ver un *popup* con los datos de dicha pregunta, como se muestra en la figura 4.

FIGURA 4 • *Popup* con los datos de dicha pregunta

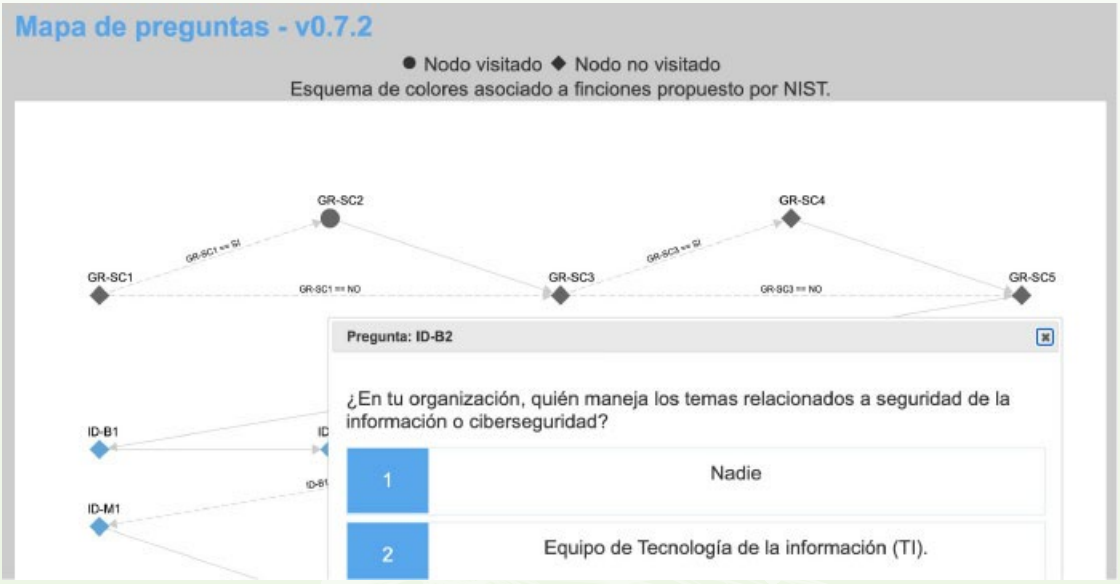


TABLA 4 • Dependencias de las preguntas

Identificador	Dependencia
GR-SC2	IndiceRespuesta(‘GR-SC1’) == 4
GR-SC4	IndiceRespuesta(‘GR-SC3’) == 4
ID-M1	IndiceRespuesta(‘ID-B1’) > 1
ID-M3	IndiceRespuesta(‘ID-B2’) > 1
ID-M5	IndiceRespuesta(‘ID-B3’) == 4
ID-M6	IndiceRespuesta(‘ID-B1’) > 1
ID-A1	IndiceRespuesta(‘ID-B1’) > 1
ID-A2	IndiceRespuesta(‘ID-B1’) > 1
ID-A3	IndiceRespuesta(‘ID-B1’) > 1
ID-A4	IndiceRespuesta(‘ID-B1’) > 1
ID-A5	IndiceRespuesta(‘ID-M4’) == 4
ID-A6	IndiceRespuesta(‘ID-M3’) > 2
ID-A7	IndiceRespuesta(‘ID-A5’) == 4
ID-A8	IndiceRespuesta(‘ID-M7’) == 4
ID-A9	IndiceRespuesta(‘ID-M8’) == 4
PR-B5	IndiceRespuesta(‘PR-B4’) == 4
PR-B6	(IndiceRespuesta(‘PR-B1’) > 1) && (IndiceRespuesta(‘PR-B2’) > 1)
PR-B10	IndiceRespuesta(‘PR-B9’) > 2
PR-A1	IndiceRespuesta(‘PR-M3’) > 2
PR-A3	IndiceRespuesta(‘PR-A2’) > 2
PR-A5	IndiceRespuesta(‘PR-B11’) > 1
DE-B2	IndiceRespuesta(‘DE-B1’) == 4
DE-B3	IndiceRespuesta(‘DE-B1’) == 4
DE-A2	IndiceRespuesta(‘DE-M1’) > 2
DE-A3	IndiceRespuesta(‘DE-M1’) > 2
DE-A4	(IndiceRespuesta(‘DE-A1’) > 2) && (IndiceRespuesta(‘DE-A2’) > 1)
RS-B2	IndiceRespuesta(‘RS-B1’) > 1
RS-M1	IndiceRespuesta(‘RS-B1’) > 1
RS-M2	IndiceRespuesta(‘RS-B1’) > 1
RS-A1	((IndiceRespuesta(‘RS-B1’) > 2) && (IndiceRespuesta(‘RS-M2’) > 2))
RS-A2	((IndiceRespuesta(‘RS-B1’) > 1) && (IndiceRespuesta(‘RS-B2’) > 1))
RC-M1	IndiceRespuesta(‘RC-B1’) > 1
RC-M2	IndiceRespuesta(‘RC-B1’) > 1
RC-A1	IndiceRespuesta(‘RC-B1’) == 4
RC-A2	IndiceRespuesta(‘RC-B1’) == 4

AUTORES: Pablo Alzuri, Florencia Cabral, Santiago Paz, Ariel Nowersztern y Pablo Libedinsky.
DISEÑO: www.souvenirme.com

BID