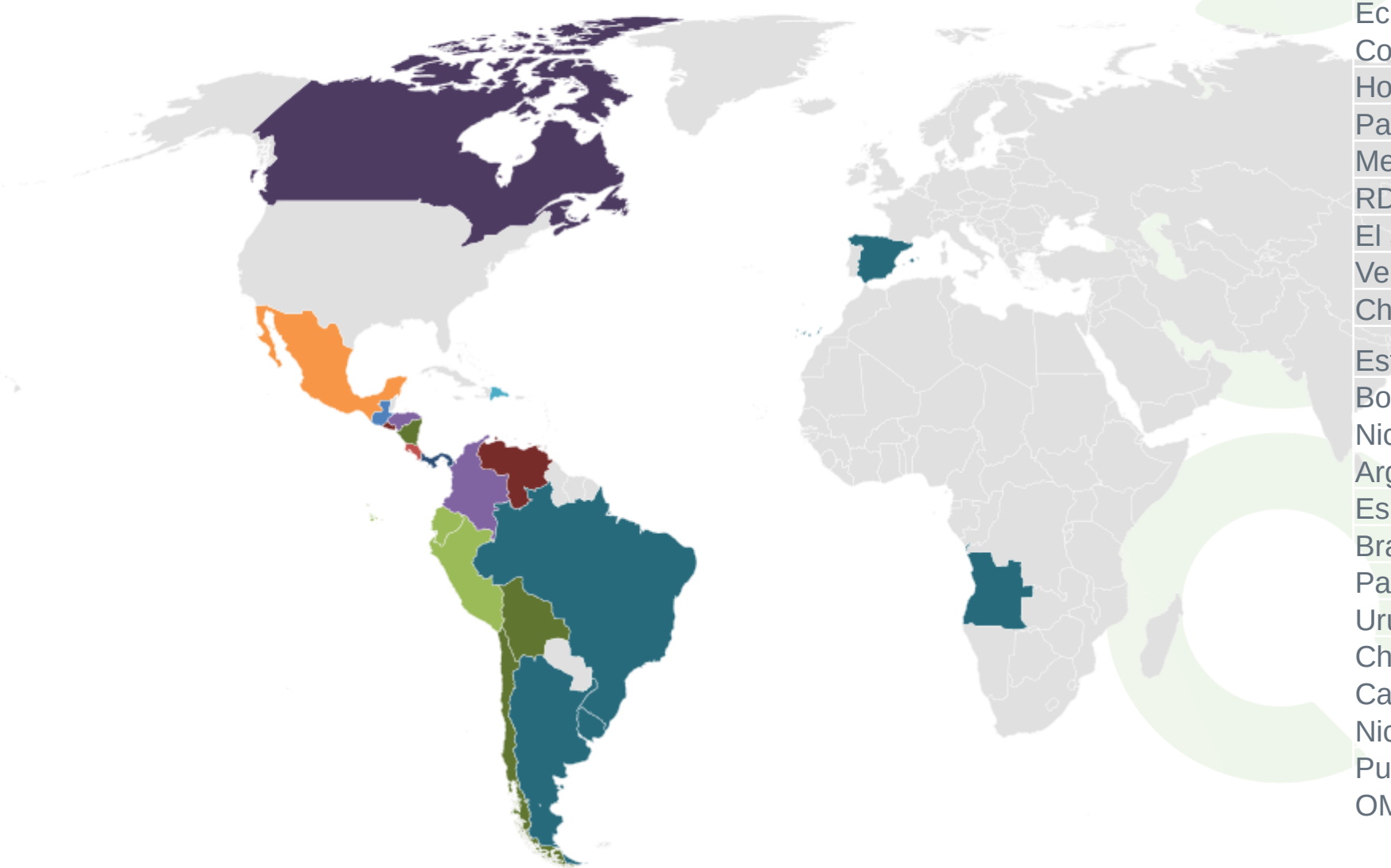
PRESENTACION DEL
I REPORTE
El estado de la Seguridad Latinoamérica

Tecnología, Seguridad, Riesgo y Auditoría

INCIBE GT
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ISACA DAY
Guatemala 2020
ONLINE

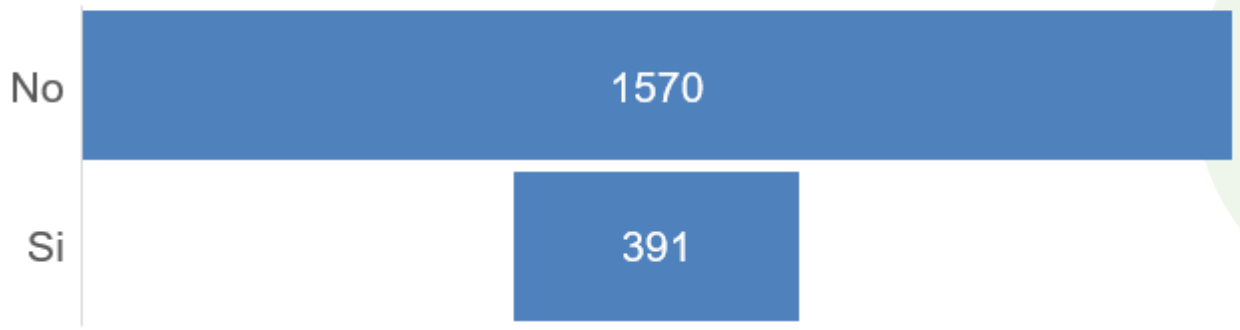
Participación 1961 PERSONAS



Guatemala	1069
Perú	140
Costa Rica	136
Ecuador	129
Colombia	101
Honduras	86
Panama	62
Mexico	56
RD	34
El Salvador	33
Venezuela	28
Chile	20
Estados Unidos	10
Bolivia	9
Nicaragua	8
Argentina	7
España	5
Brasil	5
Paraguay	4
Uruguay	3
Chile	3
Canada	3
Nicaragua	2
Puerto Rico	2
OMAN	1

ISACA*DAY*
Guatemala 2020
ONLINE

Miembros vs No Miembros

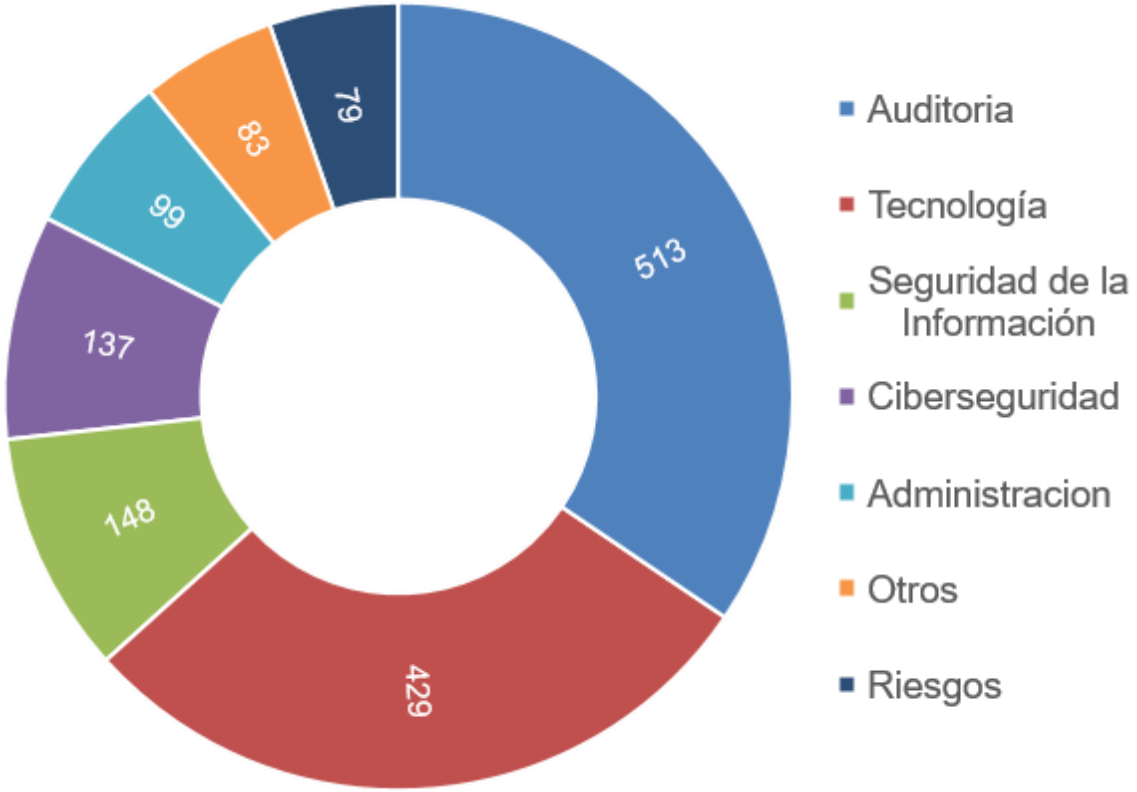


ISACA actualiza continuamente y ayuda a los profesionales y líderes empresariales de TI a cumplir con sus responsabilidades de gobierno y gestión, particularmente en las áreas de aseguramiento, seguridad, riesgo y control, para agregar valor al negocio. Capítulos de ISACA tiene la oportunidad de compartir con profesionales que necesitan especializarse en estos temas es por ello que las estrategias o campañas para incentivar en toda la región a participar de Charlas Mensuales, Asistencia a eventos, Descuentos en membresías (Profesionales, Recién Graduados y Estudiantes) entre otros son un pilar fundamental para toda la comunidad.

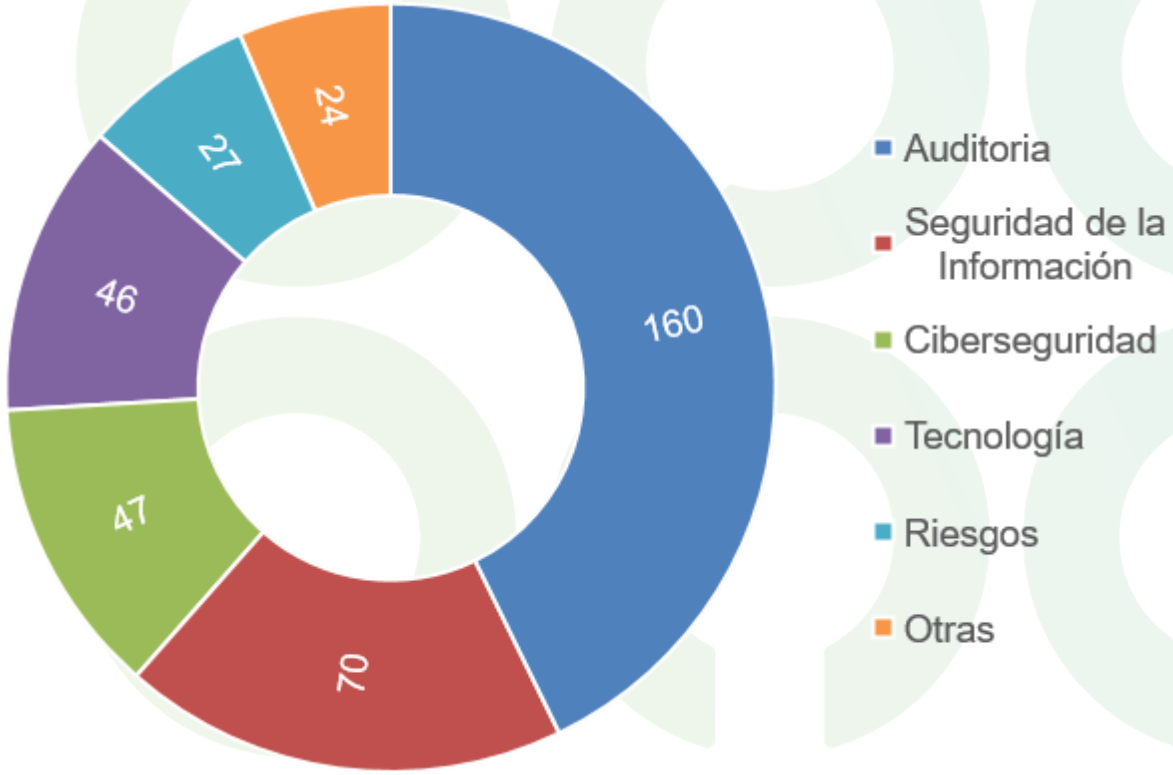
ISACADAY
Guatemala 2020
ONLINE

Actividad Profesional

No Miembros



Miembros



ISACA DAY
Guatemala 2020
ONLINE

Información Procesada

Fecha de Cierre: 28-Julio-2020

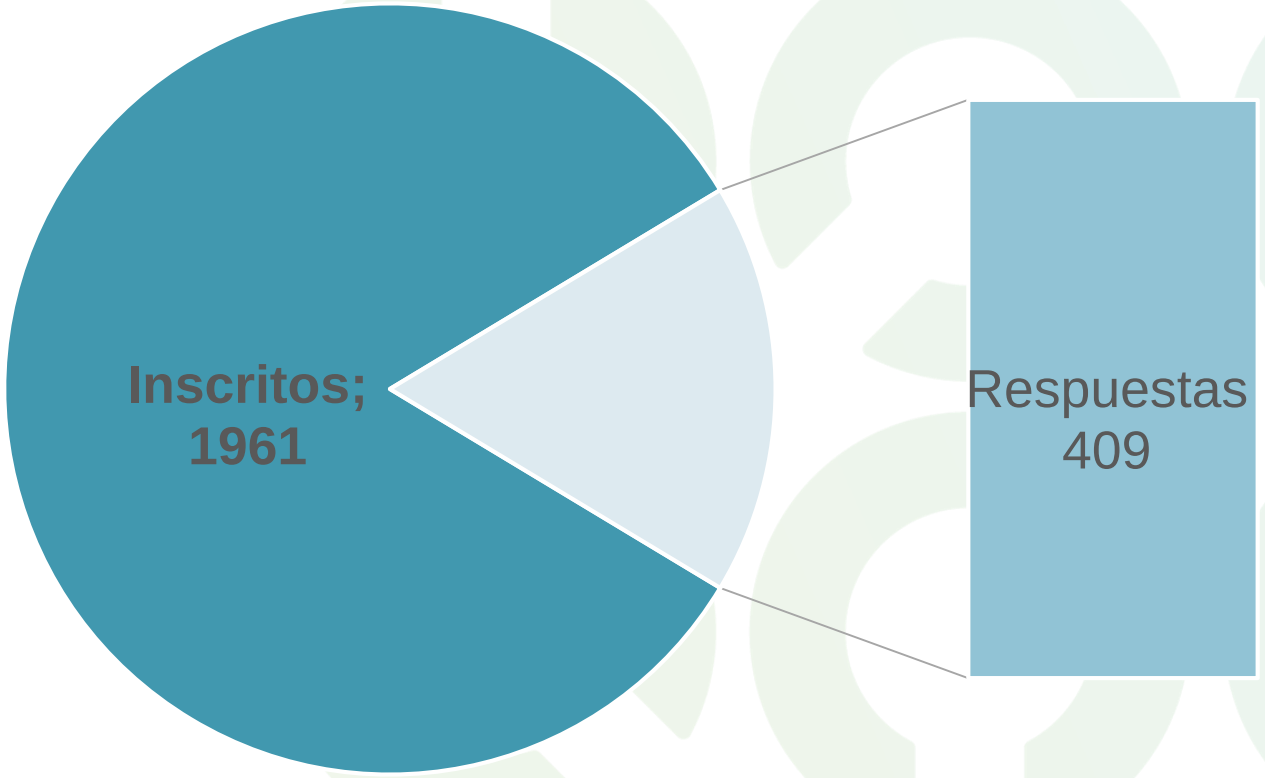
Inscritos: 1,961

Encuestas: 410

X = 20.90%

Confianza: 95%

Error: 5% (4.30%)



ISACA DAY
Guatemala 2020
ONLINE

Encuesta

- Informacion General
- Nivel de Madurez
- La gestión de la Organización
- Consideraciones Generales

CMM

Modelo de Madurez de Capacidades de Ciberseguridad

Dinámico

Existen mecanismos claros para la estrategia en función del entorno de amenazas.

Estratégico

Se han establecido los procesos clave e importantes para la organización para obtener resultados esperados.

Establecido

Algunos aspectos están establecidos y funcionando

Formativo

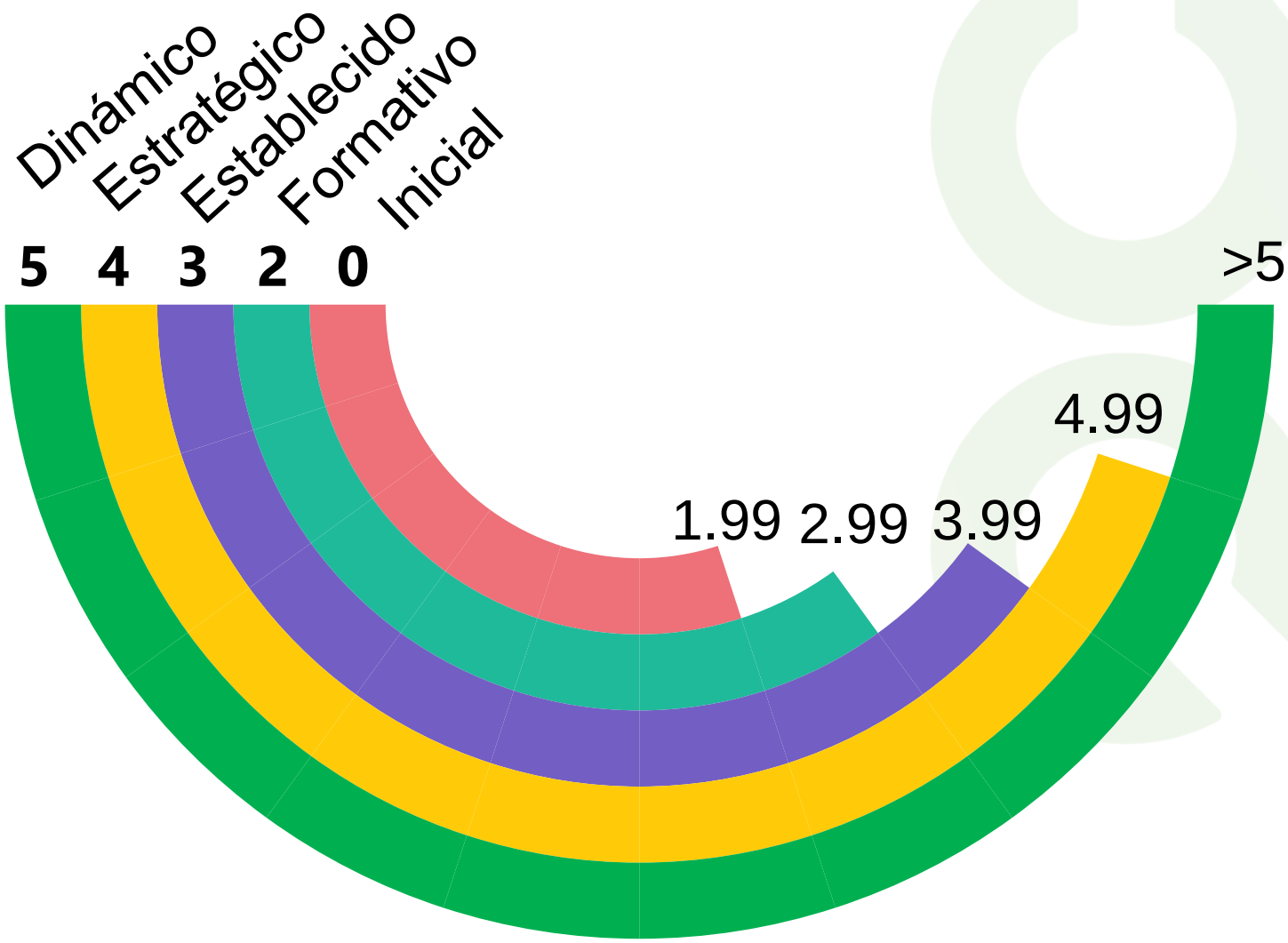
Algunas estrategias han comenzado a crecer y ser formuladas.

Inicial

En este nivel o nada existe o es de naturaleza embrionaria

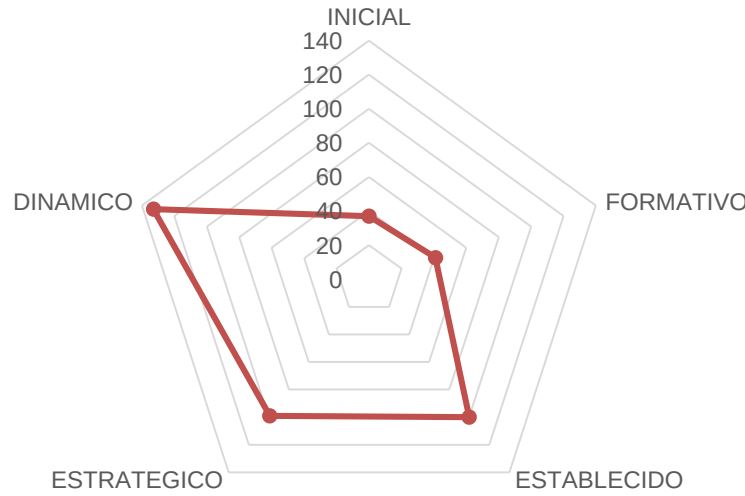
La Evaluación Continua del Riesgo Informático

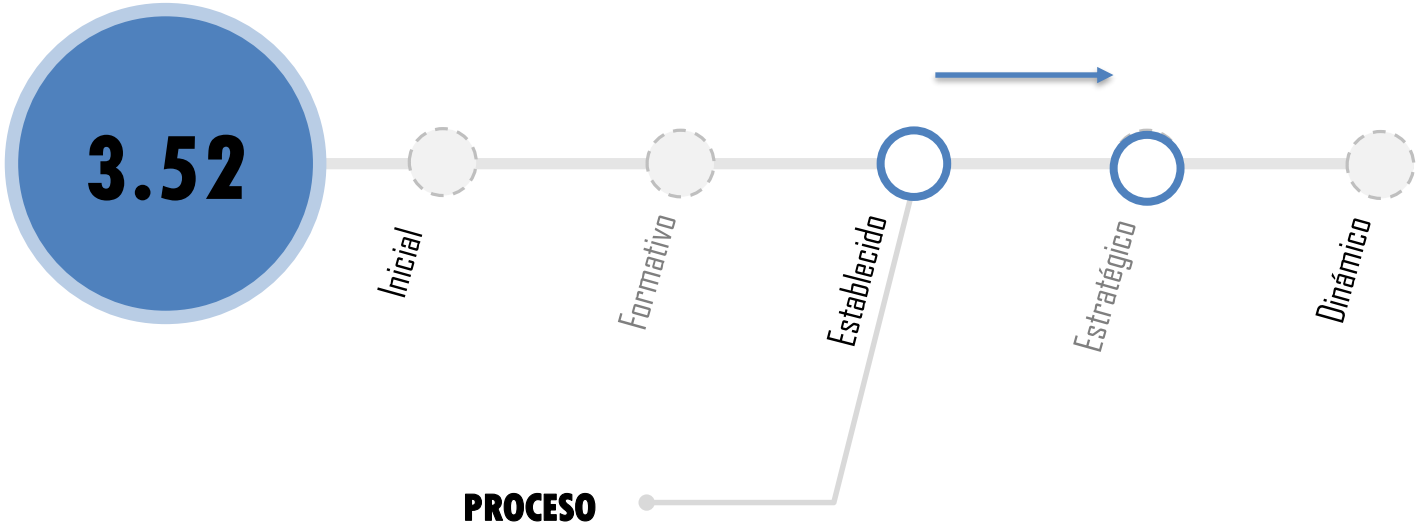
$$Ei = NM * \sum \left(\frac{X}{\Sigma Tm \int x} \right) / y$$



¿EXISTE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PUBLICADA Y ACEPTADA EN SU ORGANIZACIÓN?

Se observó que los encuestados muestran un nivel de madurez desde inicial hasta dinámico, aunque la predicción del modelo no establece aspectos de verificación, es importante anotar, que luego del análisis el nivel se encuentra en **Establecido** y madurando ya actividades hacia **Estratégico**. Concluyendo el modelo arroja un nivel de madurez de **3.52**.





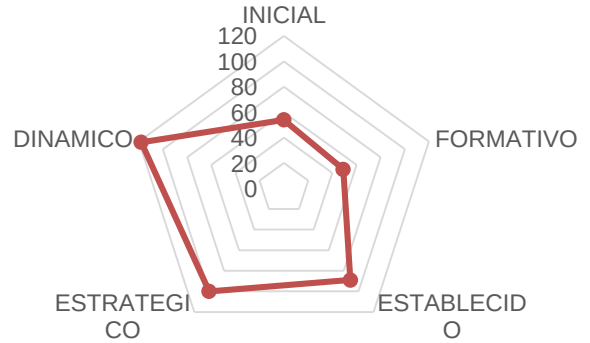
PROCESO

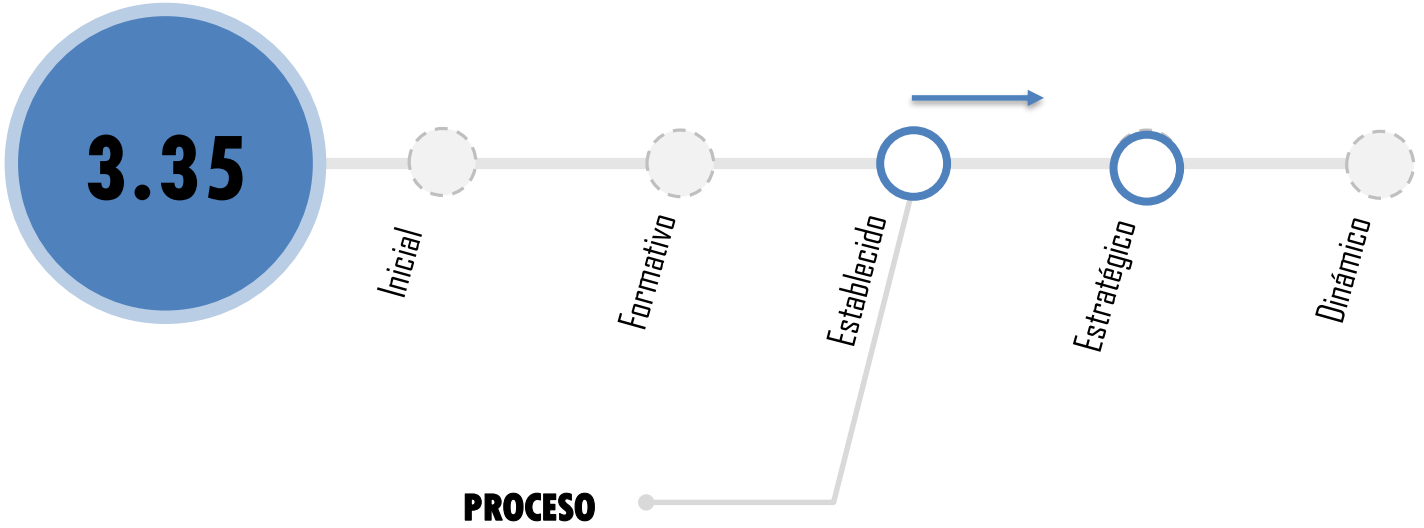
Actividades de Mejora continua, verificación de aplicabilidad, actualización periódica, partes interesadas, entre otros.

MOVEONSEC
model your cybersecurity

¿EXISTE UN CUERPO NORMATIVO DE SEGURIDAD DE LA INFORMACIÓN DENTRO DE SU ORGANIZACIÓN?

Se observa que los encuestados tienen una tendencia a indicar que existe un cuerpo normativo dentro de la organización que esta en nivel de madurez **establecido** a **estratégico** (3.35) es importante analizar mas a detalle la existencia, actividades , importancia y por fin los alcances del mismo.



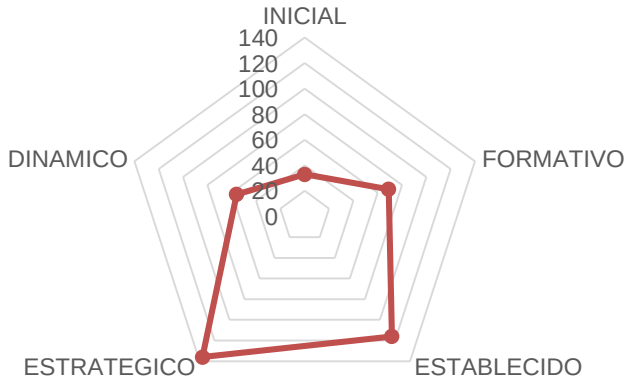


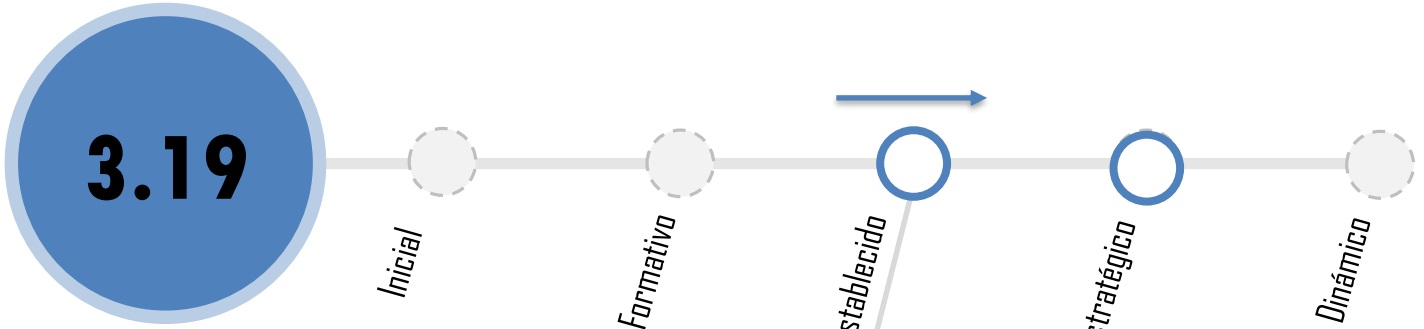
Análisis de actividades y alcance del cuerpo normativo y sus funciones.

MOVEONSEC
model your cybersecurity

¿A SU CONSIDERACIÓN, CUAL ES EL GRADO DE MADUREZ DE SU ORGANIZACIÓN RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN?

Se observa que a consideración de los entrevistados el nivel de madurez dentro de su organización, puede estar de **Formativo** a **Establecido** (**3.19**) , aunque es necesario establecer que actividades son las que se realizan actualmente para elevar su grado de gestión con respecto a la información.





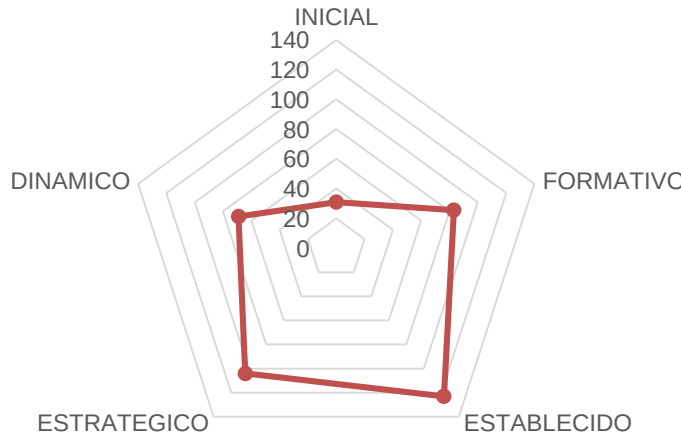
PROCESO

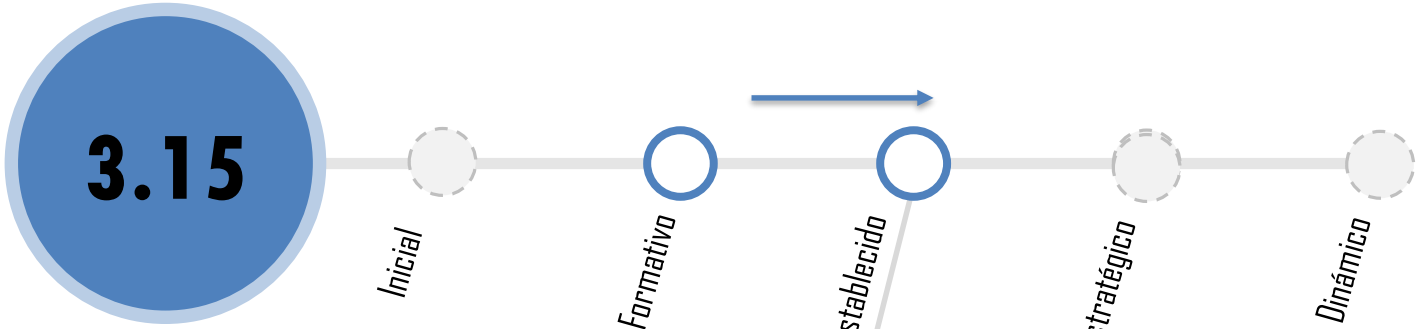
Analizar detenidamente el ~~ecosistema~~ entorno tecnológico para determinar las actividades y gestión de aseguramiento de la información.

MOVEONSEC
model your cybersecurity

¿CUAL ES EL GRADO DE CONCIENTIZACIÓN RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN EN LOS COLABORADORES DENTRO DE SU ORGANIZACIÓN?

Según los entrevistados existe un nivel entre **Formativo** y **Establecido** (**3.15**), esto a pesar de catalogarse como el eslabón más débil, parte de la concientización es inducir a los colaboradores a una utilización responsable de los servicios.





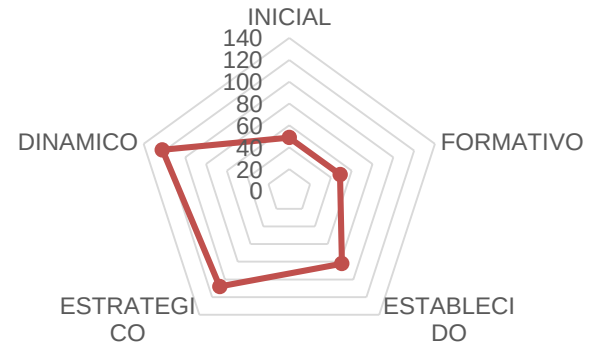
PROCESO

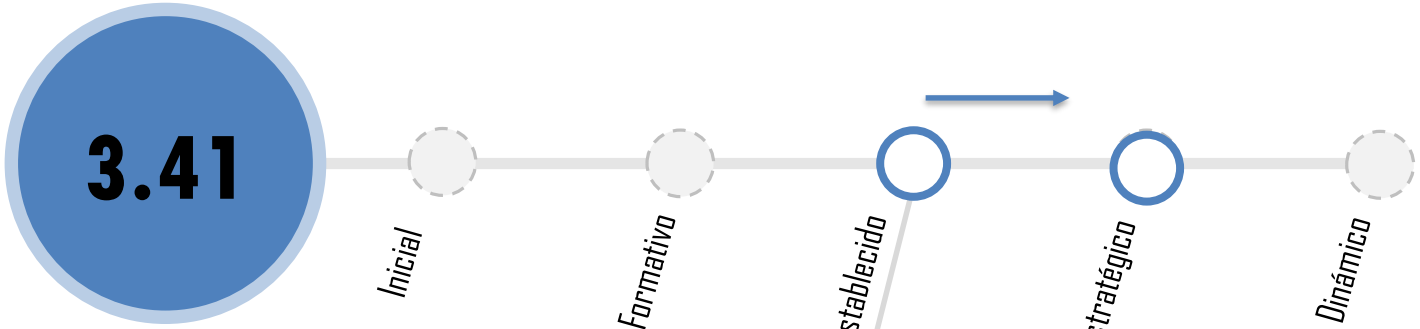
Parte del aseguramiento de los Servicios es la capacitación constante de los colaboradores, el termino "eslabón mas débil" es por la falta de madurez de los responsable de los sistemas al no realizar un configuración ideal para minimizar riesgos.

MOVEONSEC
model your cybersecurity

¿EXISTEN ESTRATEGIAS DEFINIDAS PARA LAS AUDITORIAS INTERNAS Y DE CUMPLIMIENTO?

Según los encuestados existe un nivel entre **Establecido** y **Dinámico** (**3.41**) aunque es importante determinar los alcances y procesos para realizar las auditorias





PROCESO

Analsiis de aspectos a evaluar y el valor que expone ralizar una actividad como mejora continua.

MOVEONSEC
model your cybersecurity

CIBERSEGURIDAD

RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE

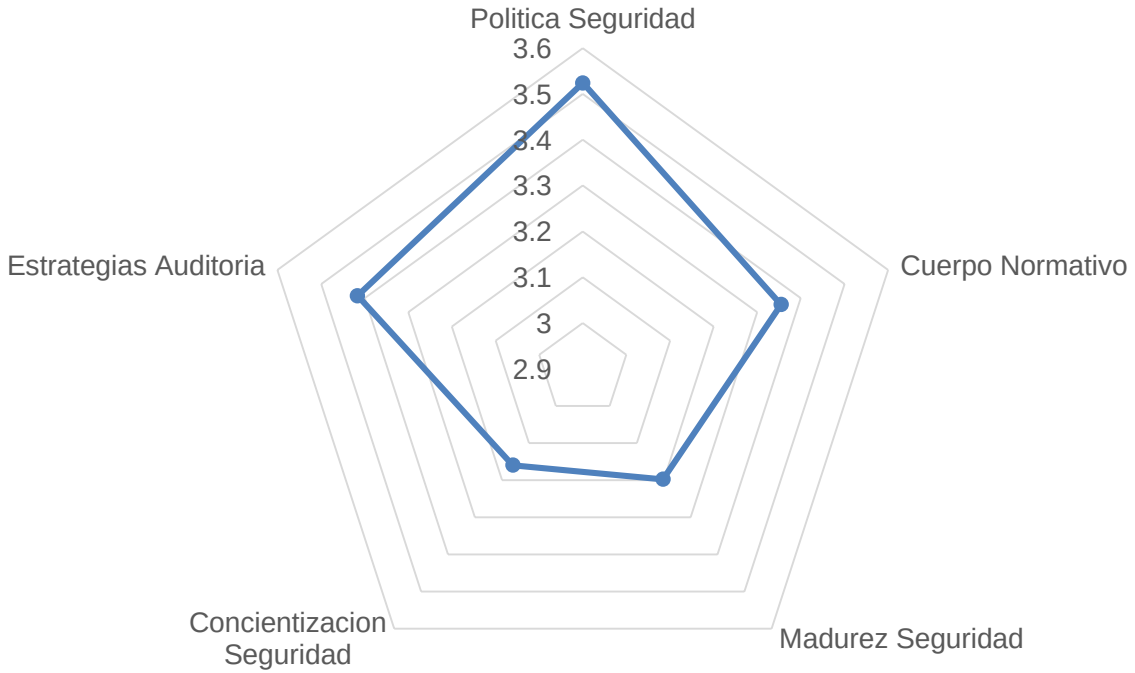
BID Mejorando vidas

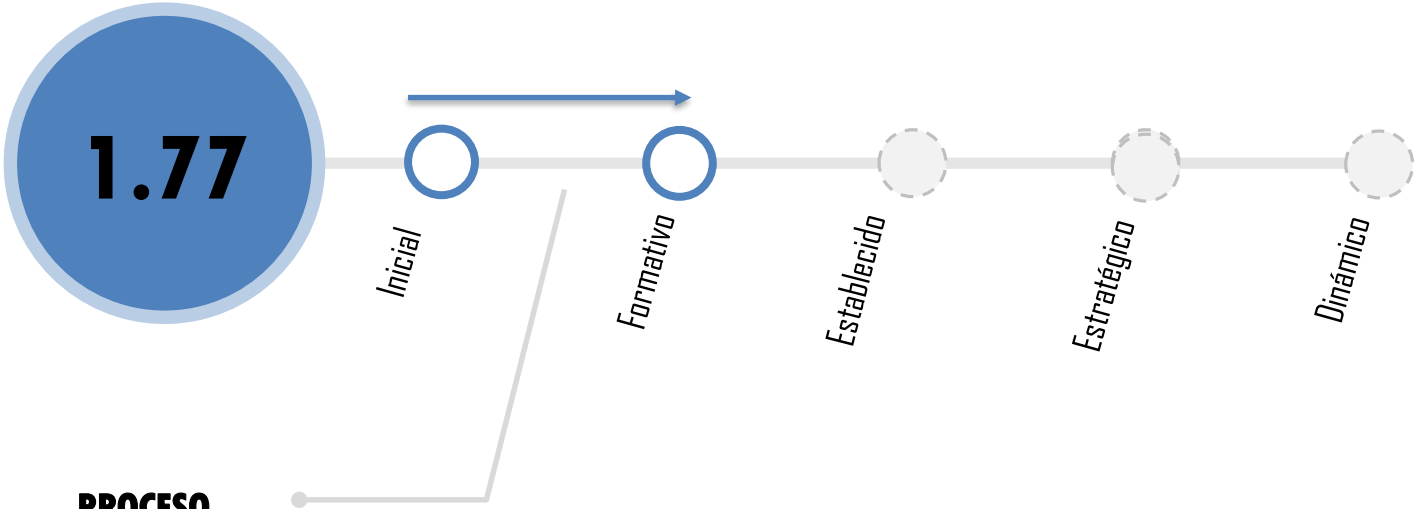
OEA Más derechos para más gente

ANALISIS FINAL NIVEL DE MADUREZ

Procesada la información los encuestados asumen que dentro de sus empresas el **grado de importancia** para cada uno de los aspectos consultados son:

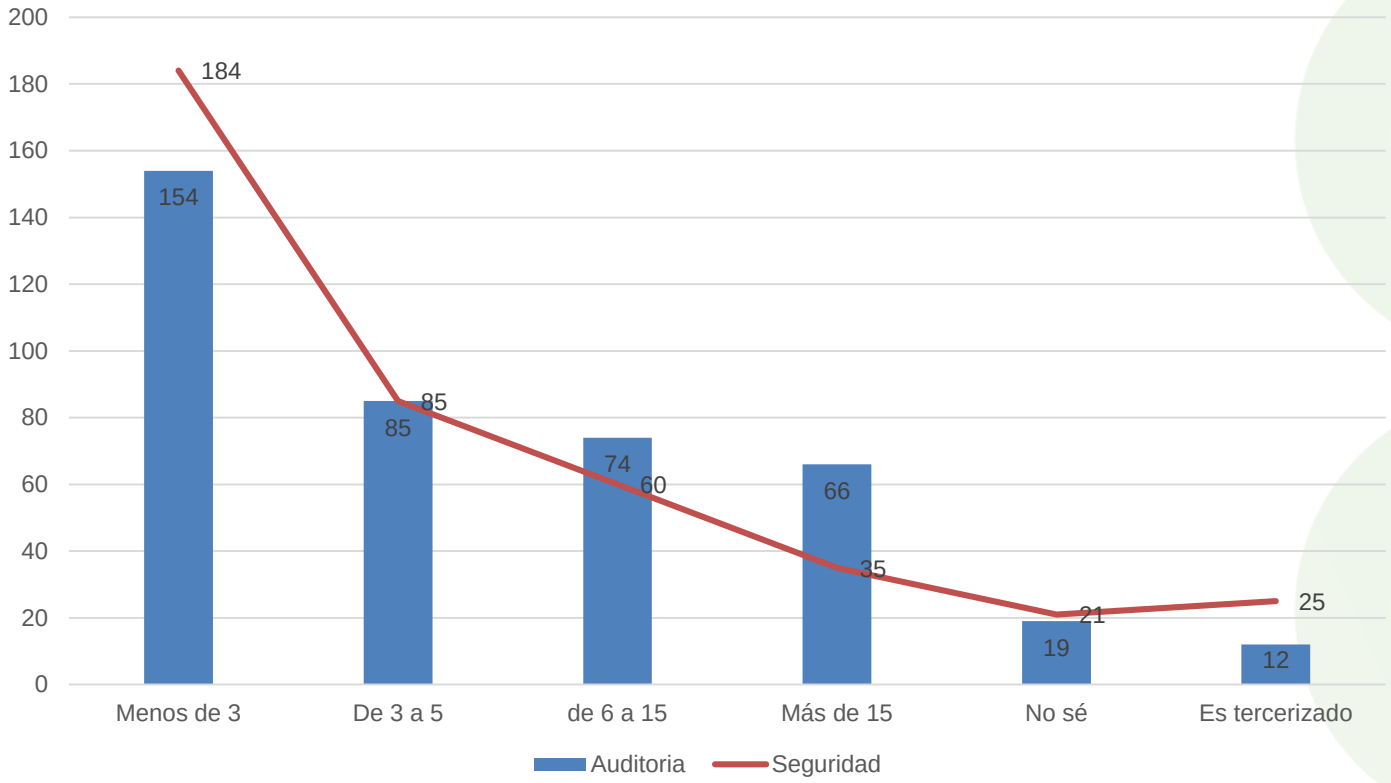
1. Políticas de Seguridad
2. Estrategias de Auditoria
3. Cuerpo Normativo
4. Madurez en Seguridad
5. Concientización a Usuarios

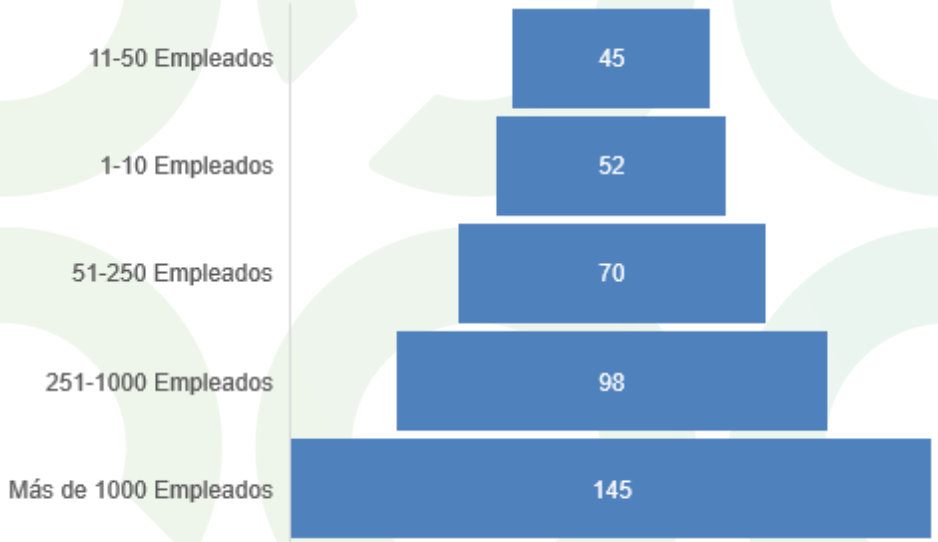




MOVEONSEC
model your cybersecurity

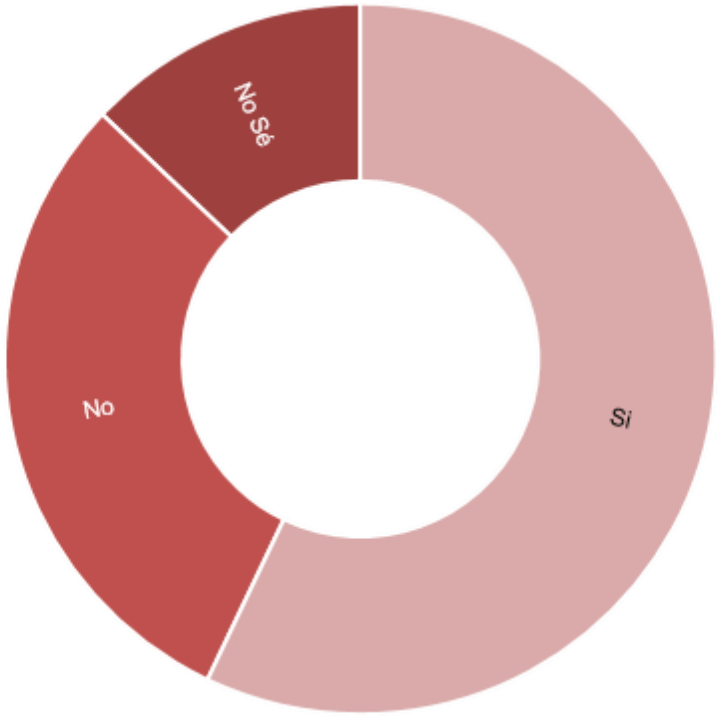
¿Dentro de su organización cuantas personas se encargan de la **Auditoria de los Sistemas** y de **Seguridad de la Información**?



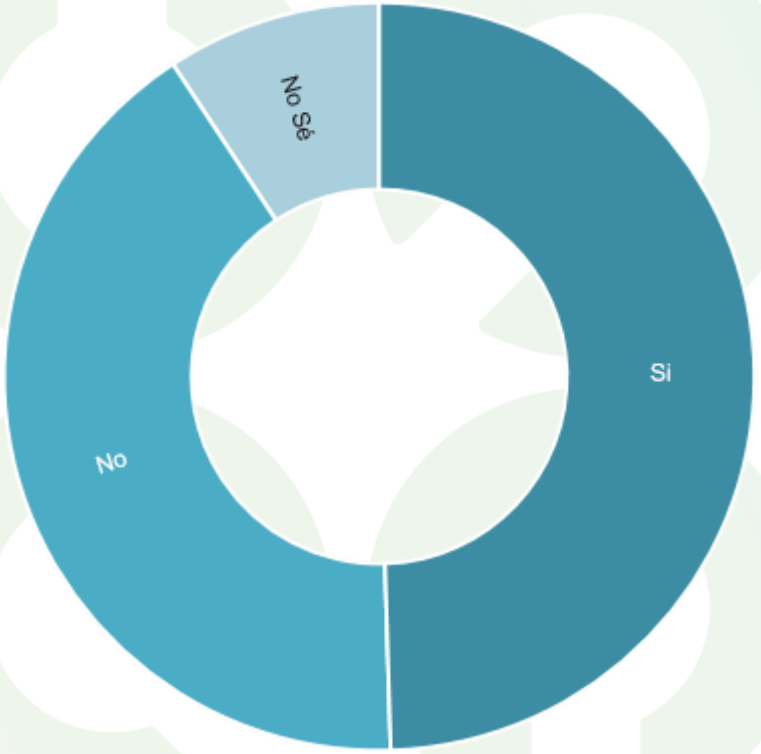


ISACA DAY
Guatemala 2020
ONLINE

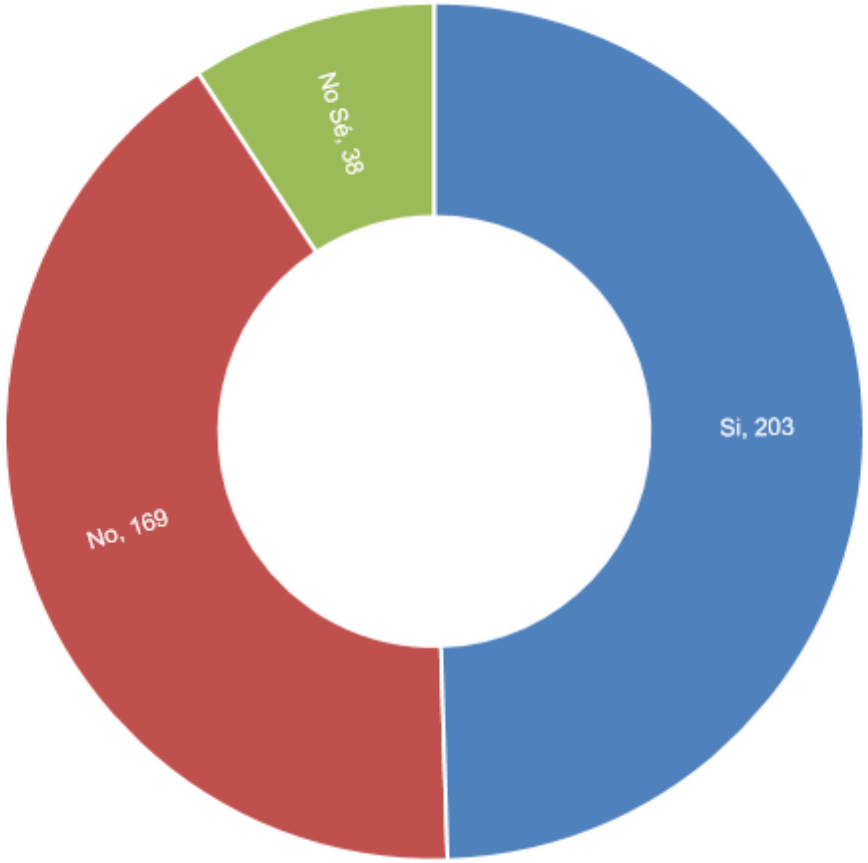
¿Sabe si existe una estrategia de Gobierno de TI dentro de su organización ?



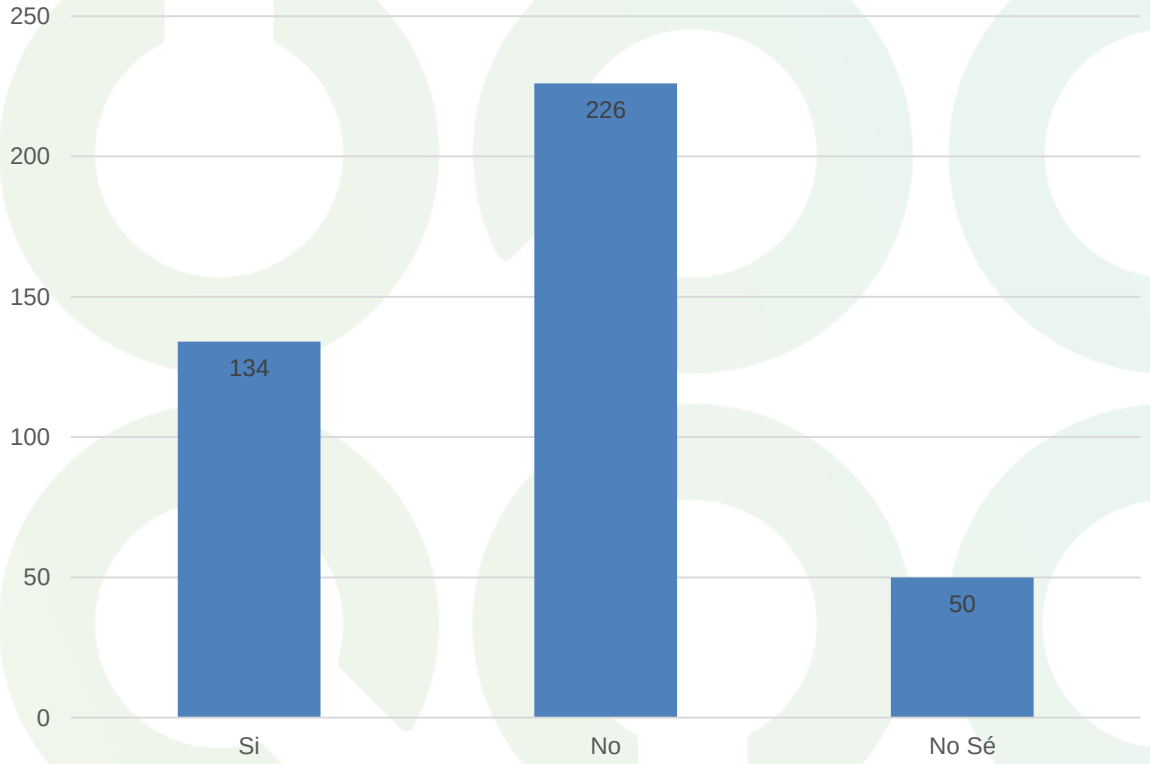
¿Existe formalmente un Director / Responsable de Auditoria de Sistemas dentro de su organización ?



¿Existe formalmente un Director / Responsable de Seguridad de la Información (CISO) dentro de su organización ?

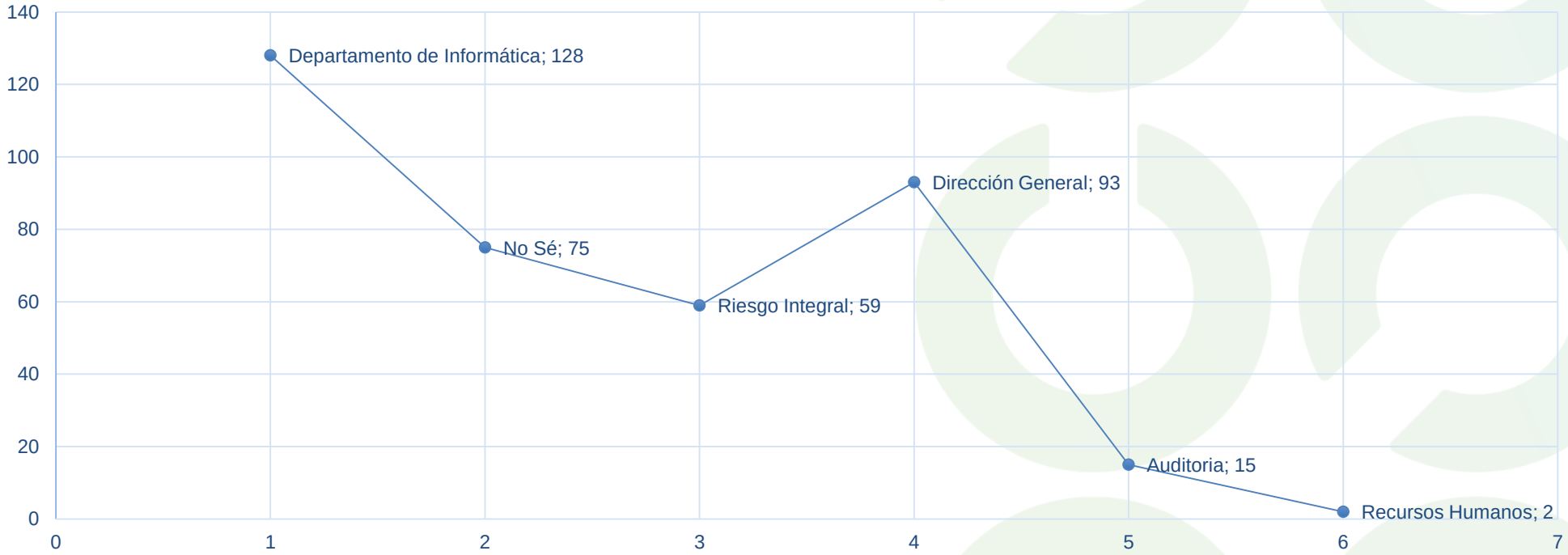


¿Existe formalmente un Director / Responsable de Ciber Seguridad(CCSO) dentro de su organización ?

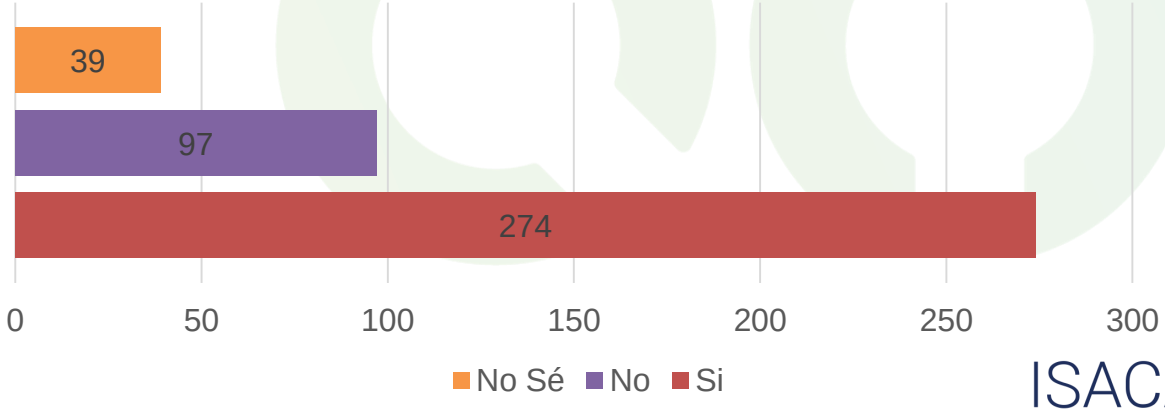


ISACA DAY
Guatemala 2020
ONLINE

¿De quién depende el CISO dentro de su organización?



¿Se realizan análisis de riesgos de la Seguridad de la Información dentro de su organización?

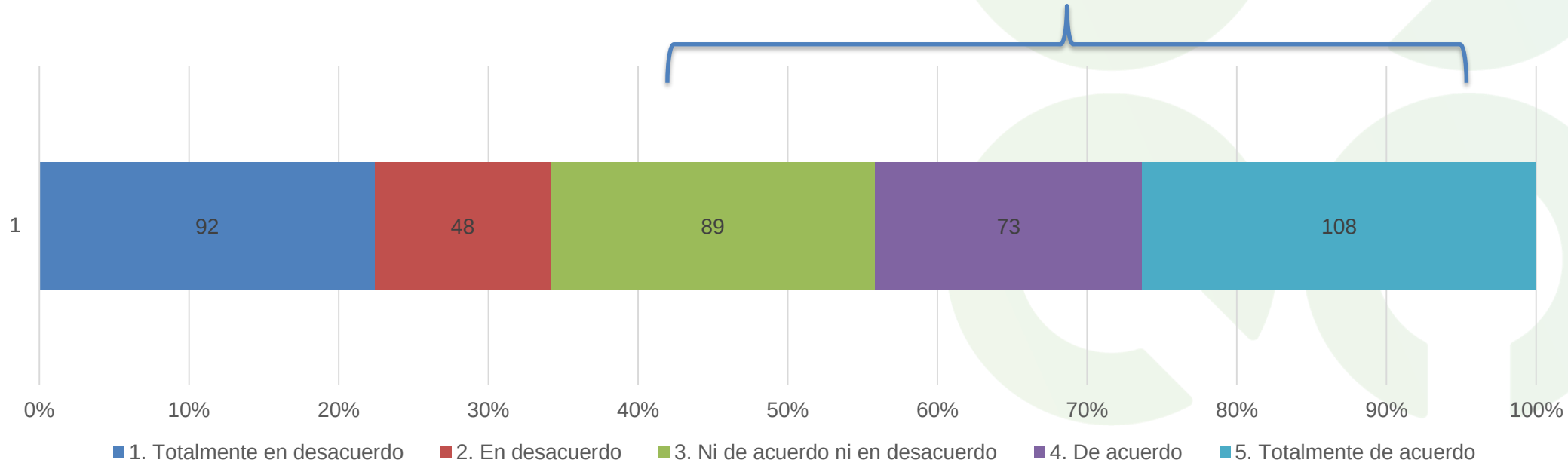


ISACA DAY
Guatemala 2020
ONLINE

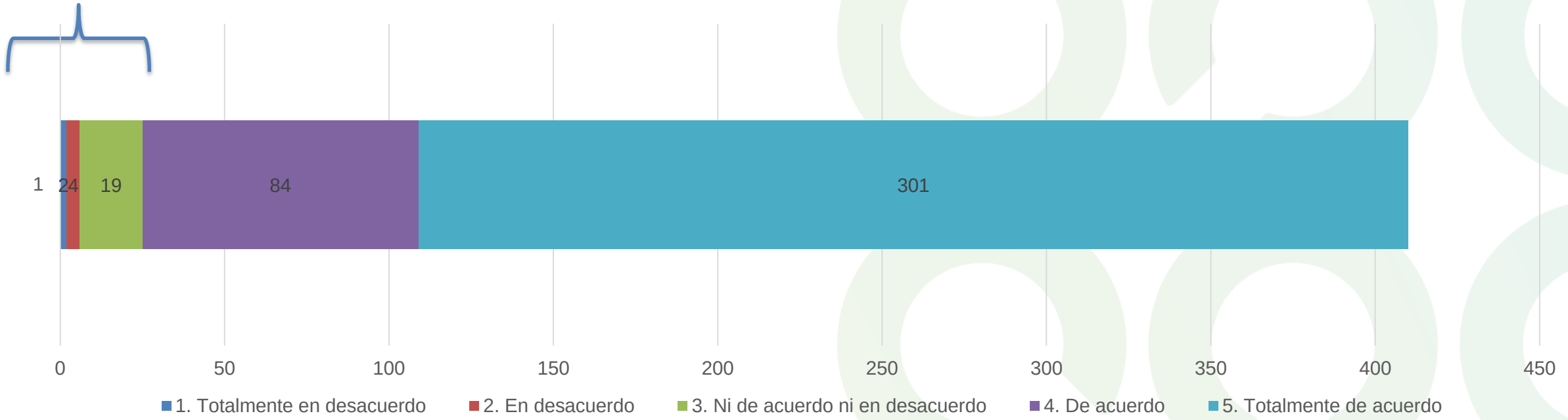
Evaluación Likert

1. Totalmente en desacuerdo
2. En desacuerdo
3. Ni de acuerdo ni en desacuerdo
4. De acuerdo
5. Totalmente de acuerdo

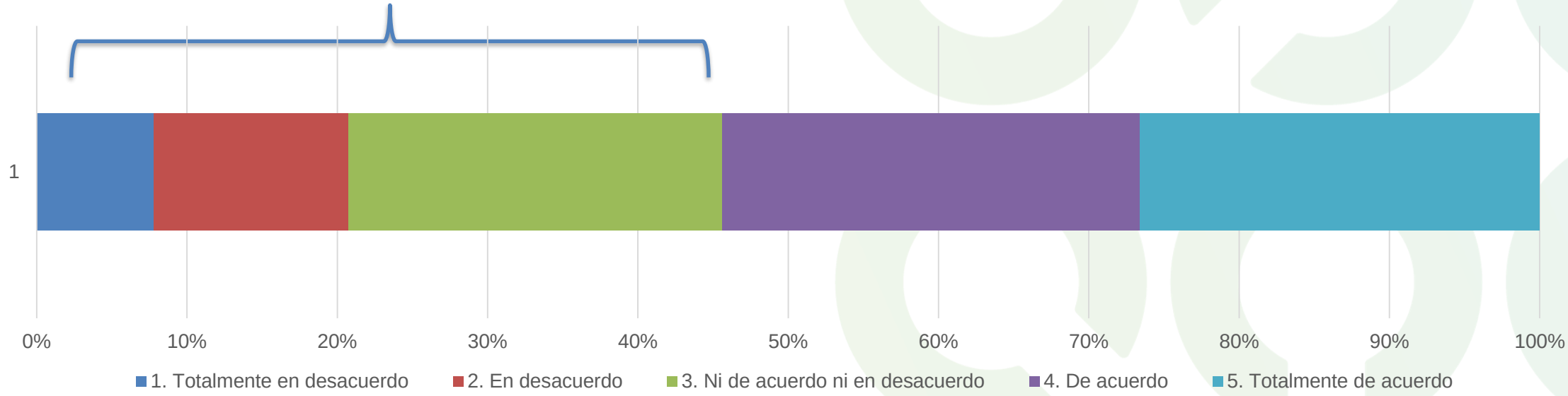
¿Considera que la ciberseguridad es un problema principalmente de TI/tecnología?



¿Considera que se necesitan actualizaciones periódicas sobre la gestión de la Seguridad de la información por parte de la organización?

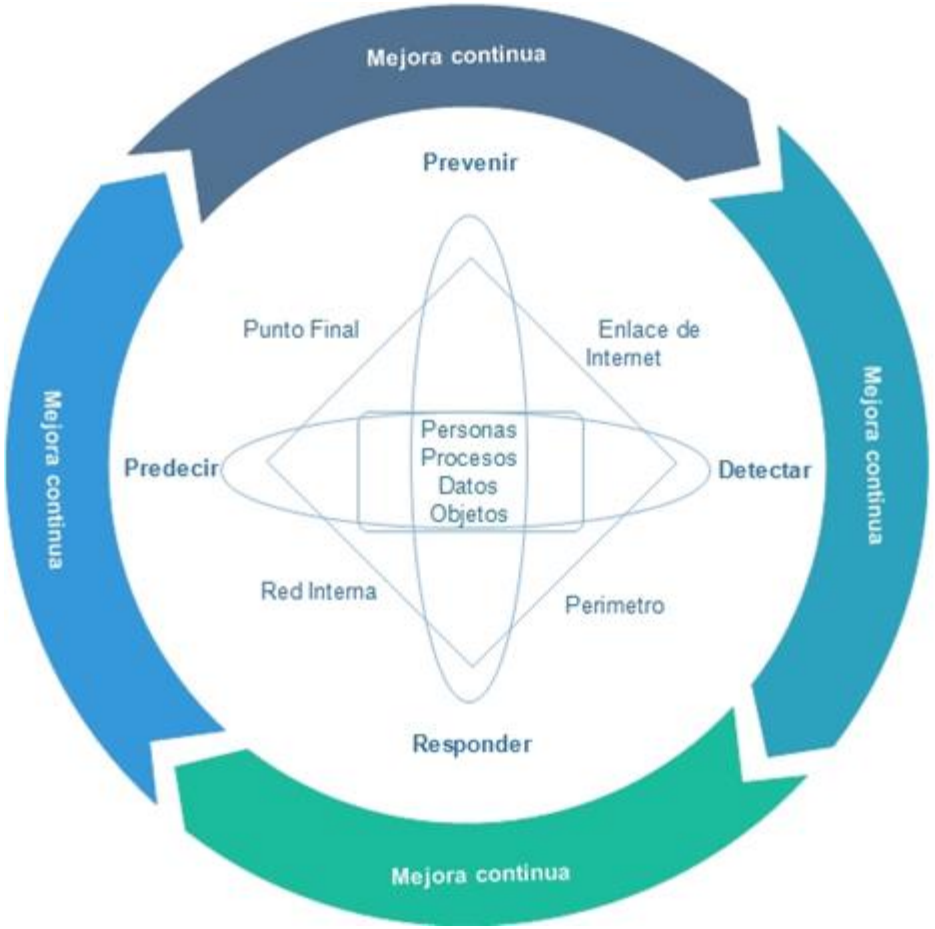


¿Brinda su Organización un marco operativo y de gestión en temas de auditoria, ciberseguridad y cumplimiento?



Esta pandemia ha traído nuevos retos para la gestión de las tecnologías,

A su criterio que más le preocupa en este tipo de actividades?



Conclusiones

- Concientización a Colaboradores en uso responsable de plataformas tecnológicas
- Alineación a la estrategia tomando en cuenta a seguridad de la información, ciberseguridad, auditoria para control del riesgo.
- Informes de Restructuras internas para aseguramiento de la información.
- Mejora continua del Marco de riesgos utilizando dentro de la organización.
- Elevar el nivel de madurez para una cultura de riesgos

ISACA DAY

Guatemala 2020

ONLINE

Prof. Armando Monzón Escobar
Director Membresías

ISACA
Guatemala City Chapter