Lineamientos de Ciberseguridad y Ciber resiliencia del BCRA *Autodiagnóstico*

El siguiente cuestionario se ha desarrollado con el fin de ayudar a identificar por sí mismo, el estado actual de su organización respecto de los Lineamientos de Ciberseguridad y Ciber resiliencia, basados en el trabajo del G7.

La organización que lo desee puede responder estas preguntas y obtener un autodiagnóstico sobre el grado de adopción de los principios definidos.

1. ***¿Su organización tiene en cuenta los Lineamientos de Ciberseguridad y Ciber resiliencia establecidos?***
   - 1.1. ¿Tiene su organización una estrategia de ciberseguridad adaptada a sus características particulares, perfil de riesgo y análisis de impacto en el negocio?
   - 1.2. ¿Su organización utiliza un marco de referencia para la gestión de la ciberseguridad y ciber resiliencia?
   - 1.3. ¿Cuenta la organización con estructuras organizativas, roles y funciones adecuados para poner en práctica los Lineamientos?
   - 1.4. ¿Participa ciberseguridad en todos los proyectos de la organización desde el inicio?
   - 1.5. ¿Cuenta con una metodología para la gestión del ciber riesgo integrado al riesgo corporativo que incluya todos los controles relevantes implementados?
   - 1.6. ¿Implementa un monitoreo continuo del ciber riesgo?
   - 1.7. ¿Se ha definido, implementado y probado adecuadamente un Plan de Respuesta ante Ciber incidentes que provoquen un evento disruptivo en la organización?
   - 1.8. ¿Ha debatido o evaluado en su organización las ventajas y desventajas del intercambio de información sobre ciber incidentes y ciber amenazas o modalidades de fraude? ¿Ha iniciado acciones para compartir información?

2. ***¿Su organización tiene en cuenta los criterios de ciberseguridad en la toma de decisiones?***
   - 2.1. ¿Incorpora la gestión de ciber riesgos desde el diseño, para nuevos productos y servicios?
   - 2.2. ¿Se consideran aspectos de ciberseguridad al evaluar la efectividad de las operaciones del negocio y la infraestructura existente? ¿Incluye también a las infraestructuras o servicios informáticos provistos por terceras partes?
   - 2.3. ¿La alta gerencia o a nivel estratégico supervisa el diseño, la implementación y efectividad de los programas de ciberseguridad?

2.4. ¿Recibe el Directorio o la alta gerencia reportes de amenazas o ciber incidentes graves de su industria periódicamente a fin de tomar decisiones informadas tanto a corto como a mediano plazo?
2.5. ¿Influyen los reportes de amenazas y vulnerabilidades en la definición del apetito del riesgo de la organización?

3. ¿Su organización es consciente que una disrupción[1] es altamente probable?

3.1. Teniendo en cuenta que la implementación de controles de prevención y detección por capas reducen la probabilidad de incidentes, ¿su organización implementa seguridad en capas?
3.2. En la actualidad sabemos que no se puede garantizar un entorno completamente seguro, por lo que se asume que ciertos incidentes ocurrirán, ¿quiénes toman las decisiones en su organización, entienden que la asignación de recursos se debe alinear a la estrategia de ciberseguridad?
3.3. ¿Se realizan pruebas integrales del Plan de respuesta a ciber incidentes?
3.4. ¿Se integran los planes de Respuesta a incidentes con los Planes de Continuidad del Negocio?
3.5. ¿El Plan de Continuidad del Negocio está alineado con las prioridades establecidas en el Análisis de Impacto en el Negocio?

4. ¿Su organización se adapta a las vulnerabilidades y amenazas que surgen todo el tiempo? ¿Adopta un enfoque de ciberseguridad adaptativo?

4.1. ¿Se promueven ciber ejecicios a nivel entidad, industria o entre sectores?
4.2. ¿Se prepara la organización para las crisis (situaciones inesperadas), planificando posibles escenarios y pensando en la contención y recuperación?
4.3. ¿Se promueve un enfoque de aprendizaje y mejora continua como parte de la estrategia de ciberseguridad?

5. ¿Su organización construye una cultura de ciberseguridad?

5.1. ¿Desarrolla la organización un programa continuo para que las habilidades, capacidades y conductas en ciberseguridad sean internalizadas para todos los integrantes?
5.2. ¿Se consideran la concientización de todo el personal y la ciberseguridad en los procesos al mismo nivel que las soluciones tecnológicas? ¿Se refleja en las decisiones de inversión?
5.3. ¿Los programas de capacitación y concientización en ciberseguridad son igualmente dirigidos a usuarios, empleados y alta gerencia?
5.4. Teniendo en cuenta que una ciberseguridad efectiva se basa en involucrar y educar a las personas. ¿Se realizan las campañas necesarias? ¿Se miden los avances?
5.5. ¿La estrategia de capacitación y concientización en ciberseguridad se elabora con el objetivo de transformar el paradigma conocido como: *"las personas son el eslabón más débil"* en el nuevo paradigma *"las personas son el activo más valioso"?*

[1] **Disrupción**: Evento anticipado/previsto o no, que causa una desviación negativa no planificada en la entrega de productos o servicios de acuerdo con los objetivos de la organización.