Consulta Pública – Estrategia Nacional de Ciberseguridad

Sugerencias y Recomendaciones:

1. **Enfoque en la Experiencia del Usuario**:
    - **Simplificación de Procedimientos**: Implementar mecanismos de autenticación robustos pero fáciles de usar, como la autenticación multifactor basada en biometría, que ofrezca seguridad sin complicar la experiencia del usuario.
2. **Capacitación Continua y Personalizada**:
    - **Programas de Educación Modular**: Crear programas de educación continua en ciberseguridad con módulos adaptados a diferentes niveles de conocimiento y roles **dentro de las organizaciones y empresas**.
    - **Campañas de Concientización Masivas**: Desarrollar campañas de concientización sobre ciberseguridad que incluyan temas relevantes como la protección contra phishing, ransomware y la importancia de la privacidad de datos, dirigidas a diversos grupos etarios y sectores.
3. **Promoción de Buenas Prácticas de Ciberseguridad**:
    - **Incentivar la Seguridad por Diseño**: Promover la implementación de principios de seguridad desde la fase de diseño en todo desarrollo tecnológico, asegurando que la ciberseguridad sea un componente integral y no un añadido posterior.
    - **Normas y Certificaciones**: Establecer un sistema de certificaciones de ciberseguridad para empresas, que incentive a las organizaciones a adoptar buenas prácticas a cambio de beneficios fiscales o de reconocimiento público.
4. **Colaboración Público-Privada**:
    - **Establecer Alianzas Estratégicas**: Fomentar alianzas entre el sector público y privado para compartir información sobre amenazas y desarrollar soluciones innovadoras en ciberseguridad.
    - **Laboratorios de Innovación en Ciberseguridad**: Crear laboratorios de innovación conjuntos entre universidades, el gobierno y empresas para investigar y desarrollar nuevas tecnologías de ciberseguridad.
5. **Fortalecimiento de Infraestructuras Críticas**:
    - **Evaluaciones Regulares de Seguridad**: Implementar auditorías regulares de seguridad en infraestructuras críticas, utilizando estándares internacionales, para identificar vulnerabilidades y asegurar su protección.
    - **Redundancia y Resiliencia**: Desarrollar planes de contingencia que incluyan infraestructuras redundantes y mecanismos de recuperación rápida ante incidentes cibernéticos.
6. **Monitoreo y Respuesta a Incidentes**:
    - **Plataformas de Respuesta Rápida**: Implementar plataformas automatizadas de monitoreo y respuesta a incidentes que utilicen inteligencia artificial para detectar y neutralizar amenazas en tiempo real.

- **Equipos Especializados**: Fortalecer los equipos de respuesta a incidentes cibernéticos con formación continua y recursos avanzados para la gestión de crisis.

7. **Promoción de la Conciencia en la Gestión de Contraseñas:**

- **Educación sobre Contraseñas Fuertes**: Incluir en las campañas educativas consejos prácticos sobre cómo crear contraseñas seguras, como el uso de frases largas y mezclas de caracteres especiales, en lugar de simplemente exigir contraseñas complejas sin explicación.
- **Uso de Gestores de Contraseñas**: Promover el uso de gestores de contraseñas entre los ciudadanos y en las organizaciones para facilitar la gestión segura de credenciales sin necesidad de memorizar múltiples contraseñas complejas

8. Autenticación Multifactor Simple y Accesible:

- **SMS y Aplicaciones de Autenticación**: Para usuarios que no están familiarizados con la tecnología avanzada, fomentar el uso de SMS o aplicaciones de autenticación como una forma de segunda capa de seguridad sobre todo en los puntos de sensibilidad crítica. Esto balancea seguridad con facilidad de uso.
- **Autenticación Biométrica**: Implementar y promover la autenticación biométrica (huellas dactilares, reconocimiento facial) en servicios gubernamentales y críticos, lo que mejora la seguridad sin añadir pasos adicionales complicados para el usuario.

9. Implementación de "Zero Trust" sin Complicaciones:

- **Políticas de Seguridad Graduales**: Introducir políticas de seguridad basadas en "Zero Trust" de manera gradual para que las organizaciones y usuarios se adapten sin interrumpir significativamente las operaciones.
- **Acceso Condicional Inteligente**: Usar sistemas de acceso condicional que permitan acceso solo a dispositivos seguros y desde ubicaciones confiables, minimizando los riesgos de comprometer la red sin que los usuarios lo perciban como un obstáculo.

10. Uso Seguro de la Nube y Herramientas de Colaboración:

- **Seguridad en la Nube Simplificada**: Fomentar la adopción de soluciones en la nube con configuraciones de seguridad predefinidas que los usuarios finales no necesiten modificar. Esto puede incluir el uso de plataformas seguras para los correos electrónicos y mensajería de las empresas con controles de acceso basados en roles.
- **Colaboración Segura**: Incluir recomendaciones para el uso seguro de herramientas de colaboración online (como Zoom, Teams) con guías simples para activar características de seguridad, como salas de espera y contraseñas para reuniones.

11. Conciencia y Prevención de Phishing:

- **Alertas Simples y Claras**: Crear campañas que enseñen a los usuarios cómo identificar correos electrónicos sospechosos y mensajes de phishing, utilizando ejemplos visuales fáciles de entender, principalmente dentro de las empresas a todo el personal que usa dispositivos conectados a Internet
- **Mantener y monitorear las actualizaciones periódicas de sistemas operativos páginas webs y aplicaciones que pueden representar vulnerabilidades**

12. Ciberseguridad en la Educación:

- **Integración en el Currículo Escolar**: Incluir módulos de ciberseguridad básicos en el currículo escolar desde niveles primarios, enseñando a los niños sobre la seguridad online de manera lúdica y educativa.

- **Talleres para Padres y Maestros**: Ofrecer talleres gratuitos para padres y maestros sobre cómo proteger a los niños en línea, asegurando que también ellos estén preparados para guiar a los más jóvenes.

13. Incentivos para la Implementación de Buenas Prácticas:

- **Premios y Reconocimientos**: Crear un programa de premios para empresas y organizaciones que implementen con éxito medidas de ciberseguridad innovadoras y efectivas, fomentando la competencia sana y el progreso continuo.
- **Beneficios Fiscales**: Proponer incentivos fiscales o descuentos en servicios de seguridad para pequeñas y medianas empresas (MiPymes) que cumplan con ciertos estándares de ciberseguridad, promoviendo una adopción más amplia.

14. Pruebas de Resiliencia y evaluaciones periódicas:

- **Evaluación de la Resiliencia Organizacional**: Evaluar y mejorar continuamente la resiliencia de las organizaciones mediante planes de contingencia y recuperación ante incidentes cibernéticos.

15. Acceso a Recursos y Soporte:

- **Portal de Asistencia en Línea**: Crear un portal de fácil acceso donde los ciudadanos y empresas puedan obtener información, guías, y soporte en tiempo real sobre ciberseguridad, con recursos adaptados a diferentes niveles de conocimiento.

Estas recomendaciones y sugerencias están basadas en varios años de experiencia de trabajo vinculado a servicios de Internet en entornos informáticos a empresas y buscan mejorar la seguridad cibernética en Uruguay sin complicar innecesariamente los procedimientos para los usuarios finales, asegurando que la ciberseguridad se integre de manera fluida en la vida cotidiana y en las operaciones de las organizaciones

Marcelo Sorondo

SORONDO.IT
Internet - Media – Comunicación
Treinta y Tres Orientales 937 #1002
Paysandú - Uruguay