**Plan de continuidad PAC**

Documento de continuidad de software libre en las Instituciones

**Marco de Ciberseguridad del NIST** en su negocio en estas cinco áreas: identificación protección, detección, respuesta y recuperación.

1. **Identificación**

Se identifican los activos de las instituciones públicas son:

Hardware

Software

1. **Protección**

* Controlar quiénes acceden a su red y usan sus computadoras y otros dispositivos.
* Use programas de seguridad para proteger los datos.
* Codifique los datos delicados, tanto cuando estén almacenados o en tránsito.
* Haga copias de seguridad de los datos con regularidad.
* Actualice los programas de seguridad con regularidad, en lo posible, automatice estas actualizaciones.
* Implemente políticas formales para la eliminación segura de archivos electrónicos y dispositivos en desuso.
* Capacite sobre ciberseguridad a todas las personas que usen sus computadoras, dispositivos y redes. Usted puede ayudar a los empleados a comprender su riesgo personal además de la función crucial que cumplen en el lugar de trabajo.

1. **Detección**

* Monitoree sus computadoras para controlar si detecta acceso de personal no autorizado a sus computadoras, dispositivos (soportes de almacenamiento de datos de tipo USB) y software.
* Revise su red para controlar si detecta usuarios o conexiones no autorizados.
* Investigue cualquier actividad inusual en su red o por parte de su personal.

1. **Respuesta**

• Notificar a los clientes, empleados y otros cuyos datos pudieran estar en riesgo.

• Mantener en funcionamiento las operaciones del negocio.

• Reportar el ataque a los encargados del cumplimiento de la ley y otras autoridades.

• Investigar y contener un ataque.

Se trata de analizar datos de cliente con sugerencias del sistema

• Actualizar su política y plan de ciberseguridad con las lecciones aprendidas.

• Prepararse para eventos inadvertidos (como emergencias climáticas) que puedan poner en riesgo los datos.

1. **Recuperación**

* Repare y restaure los equipos y las partes de su red que resultaron afectados.
* Mantenga informados a sus empleados y clientes de sus actividades de respuesta y recuperación.

**El Perfil**

Los perfiles son la alineación única de una organización de sus requisitos y objetivos organizacionales, la tolerancia al riesgo y los recursos con respecto a los resultados deseados del Framework Core. Los perfiles se pueden utilizar para identificar oportunidades para mejorar la postura de ciberseguridad comparando un perfil “actual” con un perfil “objetivo”. La identificación del perfil actual les permite a las organizaciones realizar una revisión objetiva (sin implicar esto una auditoría formal u otras evaluaciones técnicas) de su programa de ciberseguridad en relación con el CSF y conocer certeramente cuál es su situación actual de seguridad. Teniendo en cuenta la evaluación del riesgo organizacional, los requisitos de cumplimiento y los objetivos organizacionales, se puede crear un perfil objetivo, que, en comparación con el perfil actual, informará la estrategia de liderazgo y las prioridades para la contratación, capacitación, cambios de políticas, cambios de procedimientos y adquisición de tecnología.

**Identificar**

Ayuda a desarrollar un entendimiento organizacional para administrar el riesgo de ciberseguridad de los sistemas, las personas, los activos, los datos y las capacidades. La comprensión del contexto empresarial, los recursos que respaldan las funciones críticas y los riesgos relacionados con la ciberseguridad permiten que una organización se centre y priorice sus esfuerzos, de acuerdo con su estrategia de administración de riesgos y sus necesidades comerciales.

**Proteger**

Describe las medidas de seguridad adecuadas para garantizar la entrega de servicios de las infraestructuras críticas. Esta función contempla la capacidad de limitar o contener el impacto de un potencial evento de ciberseguridad.

**Detectar**

Define las actividades necesarias para identificar la ocurrencia de un evento de ciberseguridad., permitiendo el descubrimiento oportuno de los mismos.

**Responder**

Incluye actividades necesarias para tomar medidas con respecto a un incidente de ciberseguridad detectado, desarrollando la capacidad de contener el impacto de un potencial incidente.

**Recuperar**

Identifica las actividades necesarias para mantener los planes de resiliencia y para restaurar cualquier capacidad o servicio que se haya deteriorado debido a un incidente de ciberseguridad. Esta función es compatible con la recuperación oportuna de las operaciones normales para reducir el impacto de un incidente de ciberseguridad.