YARELI MIRANDA LOZADA
COORDINADORA GENERAL OPERATIVA
P R E S E N T E . –

PREGUNTAS

APARTADO 1

1. Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;

   Si, participa la Coordinación Administrativa y el área informática.

2. Señalar sí se cuenta con lo siguiente: a) un marco de mejores prácticas aplicables a la gestión de las TIC en los diferentes procesos de contratación para la adquisición, el arrendamiento de bienes o la prestación de servicios en materia de TIC y de seguridad de la información; Informar sí se cuenta con una Inventario Institucional de bienes y servicios de TIC; c) un plan de continuidad de operaciones, y señalar la fecha de implementación; d) Informar sí se ha desarrollado e implementado el plan de recuperación ante desastres, señalar la fecha de desarrollo e implementación; e) desarrollado e implementado un programa de gestión de vulnerabilidades; f) Marco de Gestión de Seguridad de la Información (MGSI) o Sistema de Gestión de Seguridad de la Información (SGSI); g) Informar sí se cuenta con una política general de seguridad de la información y en su caso, quienes intervienen y desde cuándo se implementó; h) informar sí se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución; i) Informar sí se cuenta con un Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC) o Equipo de respuesta a Incidentes Cibernéticos o en su caso SOC.

   Si se cuenta con mejoras practicas aplicables a la gestión de las TICs, a nivel estatal encabezado por la Agencia Digital de Baja California, también se cuenta con inventario de bienes y servicios de TICs, además se está trabajando en los planes de continuidad y recuperación ante desastres de la mano de la ADBC.

3. Informar sí es que se cuenta con una estrategia de ciberseguridad dentro de la institución, en caso de respuesta afirmativa, informar lo siguiente (i) referir la fecha de creación; (ii) la fecha de implementación, (iii) sí es que se ha actualizado o modificado y en cuántas ocasiones; (iv) cuáles áreas participaron en la creación de dicha estrategia ;

   Si se cuenta con una estrategia de ciberseguridad para la institución, esta se creó e implemento a partir del año 2022, solo ha sufrido 2 actualizaciones a la fecha y se creó de la mano de la FGE y la Agencia Digital de Baja California.

4. Informar sí se emplea la firma electrónica avanzada en la institución;

   No se emplea.

5. Informar sí se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos;

Actualmente se está trabajando en la elaboración del plan de recuperación.

6. Señalar si se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros;

   La entidad no realiza desarrollos propios.

7. Informar sí los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;

   Los servicios del centro de datos son propios.

8. Informar sí para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas;

   No se cuenta con lineamientos para videollamadas, toda vez que se usa el servicio de un tercero para realizarlas.

9. Informar sí se cuenta con un correo electrónico institucional; e Informar si el correo electrónico que se emplea en la institución cuenta con lo siguiente: a) inserción de leyenda de confidencialidad de la información o en su caso de transparencia y acceso a la información; c) control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios; d) Soluciones de filtrado para correo no deseado o correo no solicitado, así como programas informáticos que protejan del envío y recepción de correos electrónicos con software malicioso; e) cuenta con cifrado en el envío de información.

   No se cuenta con correo institucional con dominio propio, sin embargo a los colaboradores se les brinda uno con dominio Gmail, del cual se cuenta con control institucional por parte del área informática.

10. Informar sí se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos;}

    Se les brinda un acuerdo de confidencialidad y no divulgación al inicio de su contrato.

11. Informar sí la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes;

    La página web si cuenta con aviso de privacidad y certificados digitales vigentes.

12. Informar sí el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;

    No se ha capacitado en dicho protocolo.

13. Informar si se cuentan con: a) Los mecanismos de supervisión y evaluación que permitan medir la efectividad de los controles de seguridad de la información; b) Indicadores que permitan medir el madurez institucional en la gestión de seguridad de la información;

    No se cuenta con dichos mecanismos.

14. Informar sí dentro de la institución se cuenta con un Programa de formación en la cultura de la seguridad de la información o de ciberseguridad; y en caso afirmativo señalar: cuándo se implementó.

    No se cuenta con dicho programa.

15. Informar sí de conformidad con la Ley General de Protección de Datos Personales en Posesión de Sujetos obligados se cuenta con un sistema de gestión de protección de datos personales, en caso de ser afirmativa esta pregunta, ¿desde cuándo se adoptó y cuáles áreas participaron en su desarrollo e implementación?;

    Si se cuenta, se adoptó desde inicios de la presente administración y las áreas que participaron en el desarrollo fueron la coordinación administrativa, la coordinación operativa y recursos humanos.

16. Informar sí se cuenta con un modelo o sistema de comunicación, para informar a la sociedad en general sobre los eventos o incidentes de seguridad de la institución, y en caso de ser afirmativo, ¿cuáles áreas de la institución que participan? e informar desde cuándo se implementó;

    No se cuenta con un sistema de comunicación para informar a la sociedad en general sobre incidentes de seguridad.

17. Informar sobre sí se cuenta con un modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad de esta información, y señalar cuáles áreas de la organización participan en su implementación y desde cuándo se implementó;

    No se cuenta con dicho sistema.

18. Informar sí se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;

    Si se cuenta con lineamientos para el traslado y manejo de activos físicos.

19. Informar sí las personas encargadas de sistemas de información, donde se brinde información pública, cuentan con conocimientos comprobables en las siguientes materias (i) transparencia; (ii) protección de datos personales; (iii) archivos públicos; o, (iv) seguridad de la información.

    Si se cuenta con experiencia comprobable en materias de transparencia, protección de datos personales y seguridad de la información.

20. Informar sí han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas;

No se han tenido brechas hasta la fecha de la presente solicitud.

21. Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;

    No sé a requerido hasta la fecha la adopción de esquemas nuevos.

22. Informar sí algún sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que se emplee implica el tratamiento intensivo y/o relevante de datos personales, de conformidad de la Ley en la materia; en caso afirmativo señalar sí se han llevado a cabo evaluaciones de impacto en materia de protección de datos personales; señalar cuáles han sido las recomendaciones vertidas por el del INAI, en su caso;
    Actualmente se cuenta con un sistema integral, el cual también se encarga de la gestión de la información y no se cuenta con recomendaciones por parte del INAI.
23. Informas sí se cuenta con documento de seguridad en materia de protección de datos personales;

    Si se cuenta con documentos de seguridad para asegurar la protección de los datos personales

24. Informar sí se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información;
    Si se cuenta, se adoptó desde inicios 2022
25. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;
    Anualmente
26. Informar sí se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;

    Se llevan a cabo por parte de la Agencia Digital de Baja California de manera anual.

27. Señalar si se cuenta con un help desk que recoja las incidencias reportadas por los servidores públicos, y en su caso señalar si es interno o externo.

    No se cuenta con help desk

28. Señalar sí las páginas web de los buscadores de versiones públicas de sentencias del Tribunal, tienen certificados digitales vigentes.

    La institución no cuenta con esta información toda vez que esta le compete al PJBC.

APARTADO 2

Solicito la siguiente información.

29. Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;

    Si, participa la Coordinación Administrativa y el área informática.

30. Informar sí es que se cuenta con una estrategia de ciberseguridad dentro de la institución, en caso de respuesta afirmativa, informar lo siguiente (i) referir la fecha de creación; (ii) la fecha de implementación, (iii) sí es que se ha actualizado o modificado y en cuántas ocasiones; (iv) cuáles áreas participaron en la creación de dicha estrategia ;

    Si se cuenta con una estrategia de ciberseguridad para la institución, esta se creó e implemento a partir del año 2022, solo ha sufrido 2 actualizaciones a la fecha y se creó de la mano de la FGE y la Agencia Digital de Baja California.

31. Informar sí se cuenta con un sistema de gestión de seguridad de la información dentro de la institución;

    Actualmente se cuenta con un sistema integral, el cual también se encarga de la gestión de la información.

32. Informar sí de conformidad con la Ley General de Protección de Datos Personales en Posesión de Particulares se cuenta con lo siguiente Un sistema de gestión de protección de datos personales, en caso de ser afirmativa esta pregunta, ¿desde cuándo se adoptó y cuáles áreas participaron en su desarrollo e implementación?;

    Si se cuenta, se adoptó desde inicios de la presente administración y las áreas que participaron en el desarrollo fueron la coordinación administrativa, la coordinación operativa y recursos humanos.

33. Informar sí es que se cuenta con un plan de continuidad del negocio, para el caso de algún evento o incidente de seguridad cibernética o física e informar desde cuándo se implementó;

    No se cuenta con un plan de continuidad

34. Informar sí se cuenta con un modelo o sistema de comunicación, para informar a la sociedad en general sobre los eventos o incidentes de seguridad de la institución, y en caso de ser afirmativo, ¿cuáles áreas de la institución que participan? e informar desde cuándo se implementó;

    No se cuenta con un sistema de comunicación para informar a la sociedad en general sobre incidentes de seguridad.

35. Informar sobre sí se cuenta con un modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad de esta información, y señalar cuáles áreas de la organización participan en su implementación y desde cuándo se implementó;

    Si se cuenta, se adoptó desde inicios de la presente administración (2021) y las áreas que participaron en el desarrollo fueron la coordinación administrativa, la coordinación operativa y recursos humanos.

36. Informar sí se realiza capacitación continua a los servidores públicos en materia de ciberseguridad y cada cuándo se lleva a cabo, así como los temas que se abordan;

    Se recibe capacitación por parte de la Agencia Digital de baja California en materia de ciberseguridad abordando los siguientes temas gobierno seguro, campaña de ciberseguridad, amenazas avanzadas, superficie de ataque MITRE.

37. Informar sí se cuenta con un procedimiento en caso de detección de alguna amenaza o vulneración de seguridad y cuál es el área encargada de atender los reportes;

    Si se cuenta con un proceso, el área encargada es el área informática.

38. Informar sí se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;

    Si se cuenta con lineamientos para el traslado y manejo de activos físicos.

39. Informar sí las personas encargadas de sistemas de información, donde se brinde información pública, cuentan con conocimientos comprobables en las siguientes materias (i) transparencia; (ii) protección de datos personales; (iii) archivos públicos; o, (iv) seguridad de la información.

    Si se cuenta con experiencia comprobable en materias de transparencia, protección de datos personales y seguridad de la información.

40. Informar sí han tenido brechas de ciberseguridad desde el año 2014 a la fecha de la presente solicitud y señalar cuántas;

    No se han tenido brechas hasta la fecha de la presente solicitud.

41. Informar sí se cuenta con un modelo de madurez de seguridad de la información o ciberseguridad dentro de la institución, en caso afirmativo informar desde cuándo se implementa;

    No se cuenta con uno.

42. Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;

    No sé a requerido hasta la fecha la adopción de esquemas nuevos.

43. Informar sí algún sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que se emplee implica el tratamiento intensivo y/o relevante de datos personales, de conformidad de la ey en la materia; en caso afirmativo señalar sí se han llevado a cabo evaluaciones de impacto en materia de protección de datos personales; señalar cuáles han sido las recomendaciones vertidas por el del INAI, en su caso;

    Actualmente se cuenta con un sistema integral, el cual también se encarga de la gestión de la información y no se cuenta con recomendaciones por parte del INAI.

44. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;

    Anualmente

45. Informar sí se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;

Se llevan a cabo por parte de la Agencia Digital de Baja California de manera anual.

46. Señalar si se cuenta con un sistema de gestión de incidentes y cuáles áreas de la institución participan en este;

    No se cuenta con un sistema de gestión de incidentes.

47. Señalar si se cuenta con un help desk que recoja las incidencias reportadas por los servidores públicos, y en su caso señalar si es interno o externo.

    No se cuenta con help desk.

48. Señalar si se cuenta con un equipo de respuesta a incidentes cibernéticos, especificar si es interno o externo.

    Si se cuenta y este es interno de la institución.

APARTADO 3

49.Indicar si cuenta con alguna solución tecnológica para juicios en línea, tribunal virtual, e-justice, justicia electrónica, ciberjusticia, ciberseguridad o inteligencia artificial.

La institución no cuenta con esta información toda vez que esta le compete al PJBC.

50.En caso de contar con alguna solución para el propósito antes señalado, indicar el nombre de la solución tecnológica, dirección de internet donde es accesible, año de inicio de operaciones, materia legal del juicio de la materia de su competencia.
51.En caso de que no cuente con una solución tecnológica para este propósito y tiene conocimiento de alguno en su entidad , favor de indicar el sujeto obligado que pudiera contener dicha información.

La institución no cuenta con esta información toda vez que esta le compete al PJBC.

Me gustaría saber de qué manera aplican medios, instrumentos o aplicaciones que hagan uso de inteligencia artificial dentro del funcionamiento interno de su institución o al momento de brindar servicios a la ciudadanía. En caso de que no, saber si se tienen proyectos para aplicar dicho tipo de tecnología. A su vez se pide conocer lo siguiente:
52.Qué programas, algoritmos, sistemas de inteligencia artificial, sistemas de decisiones judiciales asistidas, algoritmos o programas de selección aleatoria de casos a jueces, tiene y opera.

La institución no cuenta con esta información toda vez que esta le compete al PJBC.

53.El número de registros existentes de lo solicitado en el punto anterior.

a. *Las fechas de operación.*
b. *El funcionamiento y operación de cada sistema o algoritmo con el que cuenta.*
c. *Los contratos de su uso o adquisición.*

La institución no cuenta con esta información toda vez que esta le compete al PJBC.

54.¿Cómo procede y opera la selección y asignación aleatoria de casos a los jueces y juzgados en todas las materias? ¿Cómo se garantiza la independencia judicial a través de estos sistemas se selección y asignación aleatoria de casos?

La institución no cuenta con esta información toda vez que esta le compete al PJBC.

55.¿Qué datos se utilizan para la selección y asignación aleatoria de casos? (sic)

La institución no cuenta con esta información toda vez que esta le compete al PJBC.

JOSÉ LUIS NORIEGA ESTRADA
ENCARGADODE INFORMÁTICA