UT/SIP/185/2024

SOLICITUD DE INFORMACIÓN PÚBLICA CON LOS SIGUIENTES DATOS:

FOLIO DE PNT: 280527624000186 **FECHA DE RECEPCIÓN: 22/10/2024**

INFORMACIÓN SOLICITADA:

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;
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.
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 ;
4. INFORMAR SÍ SE EMPLEA LA FIRMA ELECTRÓNICA AVANZADA EN LA INSTITUCIÓN;
5. INFORMAR SÍ SE REALIZAN SIMULACROS SOBRE EL PLAN DE RECUPERACIÓN DE DESASTRES O EN CASO DE INCIDENTES CIBERNÉTICOS;
6. SEÑALAR SI SE CUENTAN CON LINEAMIENTOS DE PROGRAMACIÓN Y DESARROLLO DE SISTEMAS INFORMÁTICOS SEGUROS;
7. INFORMAR SÍ LOS SERVICIOS DE CENTROS DE DATOS SON PROPIOS, DE OTRA INSTITUCIÓN GUBERNAMENTAL O DE UN TERCERO;

8. INFORMAR SÍ PARA EL TRABAJO REMOTO SE CUENTAN CON LINEAMIENTOS DE SEGURIDAD PARA LAS VIDEOLLAMADAS;
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.
10. INFORMAR SÍ SE CUENTAN CON MECANISMOS PARA EVITAR LA DIVULGACIÓN NO AUTORIZADA DE DATOS O INFORMACIÓN INSTITUCIONAL POR PARTE DE LOS SERVIDORES PÚBLICOS;
11. INFORMAR SÍ LA PÁGINA WEB DE LA INSTITUCIÓN CUENTA CON: A) AVISO DE PRIVACIDAD; B) 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;
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;
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.