REFERENCIA: RH/476/2024
FECHA: 24 de octubre de 2024
ASUNTO: Atención a solicitud 330003624000323.

A: Patricia Guadalupe Cardona Rosales
Titular de la Unidad de Transparencia del CETI

De: Marcela Araceli Medel Esparza
Departamento de Recursos Humanos

En atención a la solicitud de acceso a datos personales 330003624000323, en la cual se solicita lo siguiente:

> *"¿Qué sistemas de gestión de recursos humanos y/o capital humano utiliza la dependencia? Dicho sistema o sistemas cuantos años tiene operando en dicha institución. El sistema es Web o es local. El sistema puede ser operado mediante un dispositivo móvil. El sistema fue desarrollado internamente o fue construido o es prestado por algún proveedor. En caso de ser un GRP o ERP que módulos lo conforman. El sistema posee procesos de gestión de nómina: calculo de percepciones, deducciones y aportaciones. El sistema posee procesos de administración del capital humano como es: capacitación, desarrollo de personal, seguridad y salud en el trabajo. El sistema tiene incorporado algún modulo de control de puntualidad y asistencia. Se conoce en que lenguaje esta programado y en que base de datos opera."*

Al respecto, y con fundamento en los artículos 129 de la Ley General de Transparencia y Acceso a la Información Pública y 130 de la Ley Federal de Transparencia y Acceso a la Información Pública, me permito hacer de su conocimiento que esta Institución no cuenta con un sistema de gestión de recursos humanos que concentre en una sola instancia los expedientes, historial, proceso de pagos y recibos y control de personal toda vez que estas operaciones las realizan diversos subsistemas con distintos tipos de interfaces, algunos de ellos de desarrollo propio y otros por terceros, pero no conforman un sistema GRP como tal; el sistema más antiguo tiene más de 30 años en operación y el más nuevo seis años, esto según la información proporcionada por el área de Tecnologías de Información de esta Institución. En ese mismo sentido, las diferentes operaciones que se manejan con aplicaciones separadas son:

- Control de datos personales, académicos y constancias (desarrollo propio)
- Control de asistencia (desarrollo propio)
- Proceso y generación de pagos y retenciones (desarrollo propio)
- Reportes para instituciones externas y seguridad social (desarrollo propio)
- Timbrado de comprobantes fiscales digitales (proveedor)
- Control y distribución de recibos de pago (desarrollo propio)
- Control presupuestal y dispersión de pagos (proveedor)

Ahora bien, la información relativa al hospedaje, lenguaje y base de datos para las aplicaciones institucionales prioritarias, es información considerada reservada, toda vez que pueden provocar una vulnerabilidad en la seguridad de la infraestructura del Centro de Enseñanza Técnica Industrial, que pudieran ser explotadas por terceros u otras entidades maliciosas provocando un daño a esta Entidad.

Acorde a lo establecido en los artículos 113 fracción I, V, VII, 114 de la Ley General de Transparencia y Acceso a la Información Pública; 110 fracción I, V, VII de la Ley Federal de Transparencia y Accesos a la Información Pública; en el Lineamiento Décimo Séptimo fracción VIII de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, se estima que la normatividad permite clasificar como reservada información cuya difusión posibilite la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario, así como la indispensable para la provisión de bienes o servicios públicos de agua potable, de emergencia, vías generales de comunicación o de cualquier tipo de infraestructura que represente tal importancia para el Estado que su destrucción o incapacidad tenga un impacto debilitador en la segundad nacional,- toda vez que al otorgar esta información, se podría acceder a las características de los mismos en la página del fabricante, generando un riesgo para la infraestructura del CETI, debido a que la revelación detallada pudiera propiciar la explotación de alguna vulnerabilidad de segundad de hardware por parte de algún ciber-atacante, con la intención de robar datos y credenciales, provocar algún daño, suplantar la identidad, cometer algún delito, obstruir las labores institucionales e incluso intentar localizar a los servidores públicos mediante algún tipo de geolocalización, poniendo en riesgo la salud de los servidores públicos y sus familias, tal y como se encuentra considerado en la fracción V del artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública.

En esa tesitura, se estima que el daño que puede generarse por la divulgación de la información en comento es mayor que el interés público de conocerla. Por último, de ser favorable la reserva de la información solicitada, con fundamento en el artículo 99 de la Ley Federal de Transparencia y Acceso a la Información Pública, podrá permanecer con carácter de reservada por un periodo de hasta cinco años.

Es por ello, que el develar la información que requiere el solicitante implica un riesgo latente para las labores de esta institución, en específico, podría otorgar a algún atacante acceso ilícito a los equipos de cómputo e infraestructura tecnológica. Lo anterior, puesto que la divulgación de hospedaje, lenguaje y base de datos, pueden ser utilizados para vulnerar los sistemas mediante técnicas diversas de hackeo, entendiéndose estas conductas como un delito y tipificadas como tal.

PRUEBA DE DAÑO

Para dar debido cumplimiento a lo dispuesto en los artículos 103 y 104 de la Ley General de Transparencia y Acceso a la Información Pública y 102 y 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, se procede a realizar la prueba de daño:

Daño real: Con la divulgación de la información relativa a hospedaje, lenguaje y base de datos de los equipos de esta Entidad, rebelaría detalles exactos de los mismos lo que pondría en peligro la operación y funcionamiento de la infraestructura tecnológica, de igual potencializaría que dicha infraestructura sea utiliza para acceder a los sistemas de esta institución de manera remota y con esto acceder a información contenida en ellos con la intención hurtar y/o provocar la pérdida de la misma. De la misma forma al otorgarla podría provocar que algún ciber-atacante genere alguna técnica para sabotearlos y con ello alterar las labores de la Entidad.

Daño demostrable: Con la revelación de estos datos existe el riesgo y la susceptibilidad de que sean utilizados para atentar contra la infraestructura del CETI, poniendo en riesgo las labores conferidas a esta institución, así mismo, está vulnerabilidad puede provocar que los sistemas, equipos de cómputos, servidores/informáticos sean comprometidos para ser utilizados como infraestructura maliciosa por los ciber-atacantes.

Daño identificable: El divulgar la información requerida por el solicitante, estaría potencializando y generando una facilidad para lo establecido y dispuesto en el Código Penal Federal que a la letra dice:

Artículo 211 bis 1 .• - Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2 .. - Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Es importante recalcar que, al dar a conocer esta información, se podrían establecer mecanismos o técnicas de seguimiento a los activos informáticos, es decir un ciber-atacante puede establecer un monitoreo a un equipo informático especifico mediante los adaptadores de red e identificar el momento justo en que el usuario se conecta a Internet y con ello realizar una triangulación del origen de conexión, ip, MAC address, para así identificar la localización geográfica con exactitud, esto pone en riesgo la vida, segundad o salud de los servidores públicos y sus familias.

Conocer los detalles de la infraestructura informática de esta institución aprovechar a vulnerabilidad existente para violentar los protocolos de seguridad informática establecidos; pudiendo con ello, facilitar desde ataques cibernéticos, robo o perdida de información, daños o fallas a los sistemas, intervención de las comunicaciones de red, suplantación de identidad con la intención de robar información obstruyendo las labores institucionales e incluso intentar localizar a los servidores públicos mediante alguna técnica de tipo de geolocalización basada en las IPS, poniendo en riesgo la estabilidad de los equipos y la seguridad de los servidores públicos que integran esta Entidad.

Asimismo, con la información referida podrían ingresar a los dispositivos electrónicos que usan los servidores públicos de esta Entidad, con lo cual se podría propiciar el robo de identidad, geolocalización en tiempo real, robo de información y otras conductas que podrían generar atentados contra la seguridad y la vida de los servidores públicos.

El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda, pues la publicación de la información podría vulnerar o contrarrestar las acciones que tiene implementado esta Entidad en materia de seguridad informática y que permiten proteger el funcionamiento institucional. Esto es, permitiría conocer la infraestructura informática y daría cuenta de posibles vulnerabilidades que potencializarían la inhabilitación, sabotaje, robo de información o cualquier ataque a ésta, afectando las funciones constitucionales y legales.

La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, pues la difusión de la información solicitada rebasa el interés público de conocerla, ya que se podría afectar el debido funcionamiento de las actividades de esta Entidad, mismas que podrían verse obstaculizadas o paralizadas ante un ataque cibernético; ello, impediría la utilización de los sistemas, pilares de las actividades sustantivas de la Entidad. En este orden de ideas resulta preciso señalar que; el daño que puede producirse con su publicidad es mayor que el interés público de conocerla y que su divulgación lesiona el interés que protege.

A efecto de procurar que el periodo de reserva sea el estrictamente necesario, esta área considera que esta parte de la información requerida, debe permanecer con este carácter por el periodo de cinco años.

Con fundamento en los artículos 44, fracción II, 113 fracción I, V, VII, de la Ley General de Transparencia y Acceso a la Información Pública, y 65, fracción II, 110 fracción I, V, VII; de la Ley Federal de Transparencia y Acceso a la Información Pública; y del Sexagésimo segundo de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, se solicita someter a consideración del Comité de Transparencia, la presente, la presente petición de reserva.
Sin más por momento, quedo a sus órdenes.

Atentamente;

CENTRO DE ENSEÑANZA TECNICA INDUSTRIAL • RECURSOS HUMANOS

MARCELA ARACELI MEDEL ESPARZA
JEFA DEL DEPARTAMENTO DE RECURSOS HUMANOS