

**Información relacionada proporcionada por el Área generadora de la información solicitada.**

**Solicitud de información de Ref. BANDESAL-2021-0017.**

## **REQUERIMIENTOS:**

### **I. RESPECTO DE LA NORMATIVA TÉCNICA Y LEGAL VIGENTE INTERNA Y EXTERNA**

En términos generales respecto de lo solicitado en el numeral uno, es preciso hacer mención que la Ley de Acceso a la Información Pública (LAIP), establece en su Art. 10 la información oficiosa que debe ponerse a disposición del público, dentro de la cual se contempla en el numeral 1 el marco normativo aplicable a cada ente obligado, en ese sentido debe hacerse saber al interesado que el marco legal aplicable al Banco de Desarrollo de la República de El Salvador (BANDESAL), se encuentra publicado en el Portal de Transparencia y que puede ser consultado en los siguientes enlaces:

- <https://www.transparencia.gob.sv/institutions/bandesal/documents/otros-documentos-normativos>;
- <https://www.transparencia.gob.sv/institutions/bandesal/documents/ley-principal-que-rige-a-la-institucion>; y
- <https://www.transparencia.gob.sv/institutions/bandesal/documents/manuales-basicos-de-organizacion>.

### **II. RESPECTO DE LA NORMATIVA TÉCNICA INTERNA RELACIONADA A LA GERENCIA DE TECNOLOGÍA, DESCRIPCIÓN DE HARDWARE, SOFTWARE E INFRAESTRUCTURA DEL CENTRO DE COMPUTO DE LA GERENCIA DE TECNOLOGÍA**

La normativa interna específica de la Gerencia de Tecnología y los requerimientos relacionados a la descripción del hardware, software e infraestructura del centro de cómputo de la Gerencia de Tecnología, es importante citar lo establecido en las Normas Técnicas para la Gestión de la Seguridad de la Información (NRP- 23), emitidas por el Comité de Normas del Banco Central de Reserva de El Salvador, que establecen en su Art. 3 los siguientes términos "(. . .) k) **Ciberseguridad**: desarrollo de capacidades técnicas para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar la confidencialidad,

integridad y disponibilidad de la información en el ciberespacio y que es esencial para la operación de la entidad; ( . . ) w) **Infraestructura o plataforma tecnológica:** componentes de hardware y software en los cuales se recopila, procesa, transmite y almacena la información relacionada con productos y servicios financieros que ofrece la entidad( . . )"

Asimismo, el Art. 4 de dichas Normas dispone que: "Las entidades deberán contar con una estructura organizacional acorde a sus productos, servicios, operaciones, tamaño, perfil de riesgos y modelo de negocio, de tal forma que delimite claramente las funciones, roles, responsabilidades y facultades asociadas a la seguridad de la información y la ciberseguridad, así como los niveles de dependencia e interrelación que corresponde con cada una de las demás áreas de la entidad. Asimismo, las entidades deberán asegurarse de **que todo su personal reconozca a la seguridad de la información y ciberseguridad como una de sus responsabilidades, aplicando las medidas de confidencialidad** que fueran necesarias. La información cuya seguridad deberá preservarse, será la que **de acuerdo a la clasificación de los activos de información que realice la entidad, requiera un tratamiento de aseguramiento o protección.**"

Adicionalmente, el Art. 11 de la norma antes citada que se refiere a la **Seguridad lógica**, contempla que para gestión de la seguridad lógica de la información que se administre, las entidades deben considerar, dentro de otros, los controles sobre accesos remotos y dispositivos móviles que interactúen con **la infraestructura de tecnología de la entidad y lo controles sobre configuración segura de hardware, software, equipo de comunicación, dispositivos móviles; limitando servicios, protocolos, puertos v usuarios.**

En igual forma, el Art. 28 de las NRP-23 regula que "Las entidades deben adoptar medidas que aseguren la protección y **confidencialidad de la información bajo su responsabilidad**, como datos personales, e información que reciben de sus clientes, usuarios de servicios, proveedores, **entre otros**; sin perjuicio de lo establecido en el marco legal vigente".

Por lo anterior, en atención a la normativa antes citada, se confirma la obligación de BANDESAL de realizar una efectiva gestión del riesgo de ciberseguridad, por lo que debe hacerse del conocimiento del interesado que la información solicitada relacionada a normativa técnica legal interna relacionada a la Gerencia de Tecnología, descripción de hardware, software y esquema de infraestructura actual del Centro de Computo de la Gerencia de Tecnología es **CONFIDENCIAL** de conformidad a lo establecido en el literal d) del Art. 24 de la Ley de Acceso a la Información Pública en atención a lo establecido en las NRP-23 que regula lo referente a la protección de la infraestructura tecnológica y organizacional que garantiza la custodia de la información digital de todos los usuarios del sistema financiero, esto incluye pero no se limita a la plataforma digital institucional al hardware y software, ya que de hacerlo la institución vulneraría su obligación de resguardo

y confidencialidad omitiendo lo controles de ciberseguridad, a que se refiere de forma vinculante y obligatoria la normativa emitida por el Banco Central de Reserva.

### **III. RESPECTO DE LA DESCRIPCIÓN DEL RECURSO HUMANO DE LA GERENCIA DE TECNOLOGÍA**

En relación al recurso humano de la Gerencia de Tecnología, debe informarse al interesado que la Gerencia de Tecnología está compuesta por dos unidades, la primera, Unidad de Sistemas, con 9 técnicos y un jefe de Área; y, la segunda, Unidad de Soporte Técnico, con 10 colaboradores más un jefe. Ambas unidades lideradas por un Gerente de Tecnología.